Decentralized Web
webinar series by

METROPOLITAN NEW YORK LIBRARY COUNCIL

INTERNET ARCHIVE

Web

LIBRARY FUTURES

Resource guide

session 03

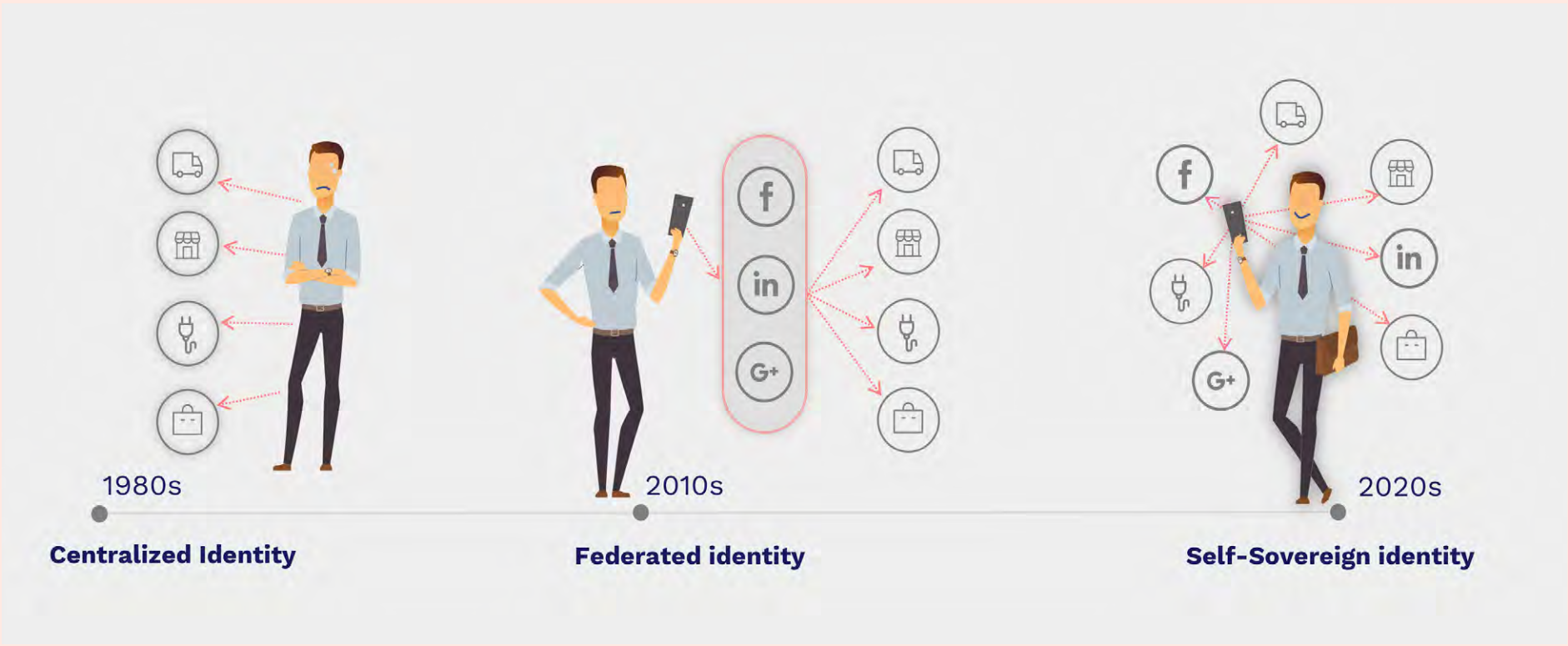
Decentralized Identity

Thursday, March 31, 2022

Identity and Trust

Digital identity can be understood as *the information we associate with ourselves, other people, and things* (Kamoosi, 2020). Or, in other words, identity is “how we keep track of people and things and, in turn, how they keep track of us” (Andrieu, 2017).

On the Internet, where our interactions are conducted remotely, we need mechanisms to establish trust, to enable users to verify who they’re interacting with at any given time. In Kim Cameron’s words “the Internet was built without an identity layer” (Cameron, 2005), a state of affairs that can be dangerous to users, as it exposes them to fraud, identity theft, *catfish*ing, and other kinds of deception. Without any mechanisms to verify each others’ identity, internet users can only choose between trusting their counterparts (and accepting the risks) and refusing to engage or interact with online users.



↑ Centralized identity, federated identity and SSI (gataca.io Blog, 2021).

Today, we typically trust *centralized* record-keepers (governments, our bank…) to manage our identities for us. These centralized authorities keep extensive records of our personal information that effectively serve as a basis of trust for users when interacting with a system. They verify our identity by accessing our passports, ID cards, and other *credentials*.

Over time, we have also moved to *federated identity*: allowing services to use accounts at platforms such as Google and Facebook for authentication. In federated systems, users are forced to place their trust in "middlemen" who may not always have their best interests at heart, or who may not take good care of their personal information.

Over the last twenty years, a movement has formed calling for *user-centric, decentralized identity*. This movement asks: who should be allowed to create and store the information associated with an individual? Can we cut out the middleman and still trust in the security of our private information and credentials? What if you could maintain control over your personal identity and share only what is needed?

One of the goals of *decentralized identity* is to give users control over what personal information is shared, with whom, and for which purposes. But eliminating an "omniscient" authority that verifies trust also creates many technical challenges.

Enter Self-Sovereign Identity

> *Self-Sovereign identity (SSI) is an idea, a movement, and a decentralized approach for establishing trust online.*
> — Lacity & Carmel, 2022

Jolocom gives a succinct definition for self-sovereign identity:

> *Self-Sovereign Identity refers to a particular model of identity in which subjects of identity are able to express their identities autonomously and to control their identities on their own terms when interacting & communicating with other subjects irrespective of context.*
> — Jolocom whitepaper, 2019

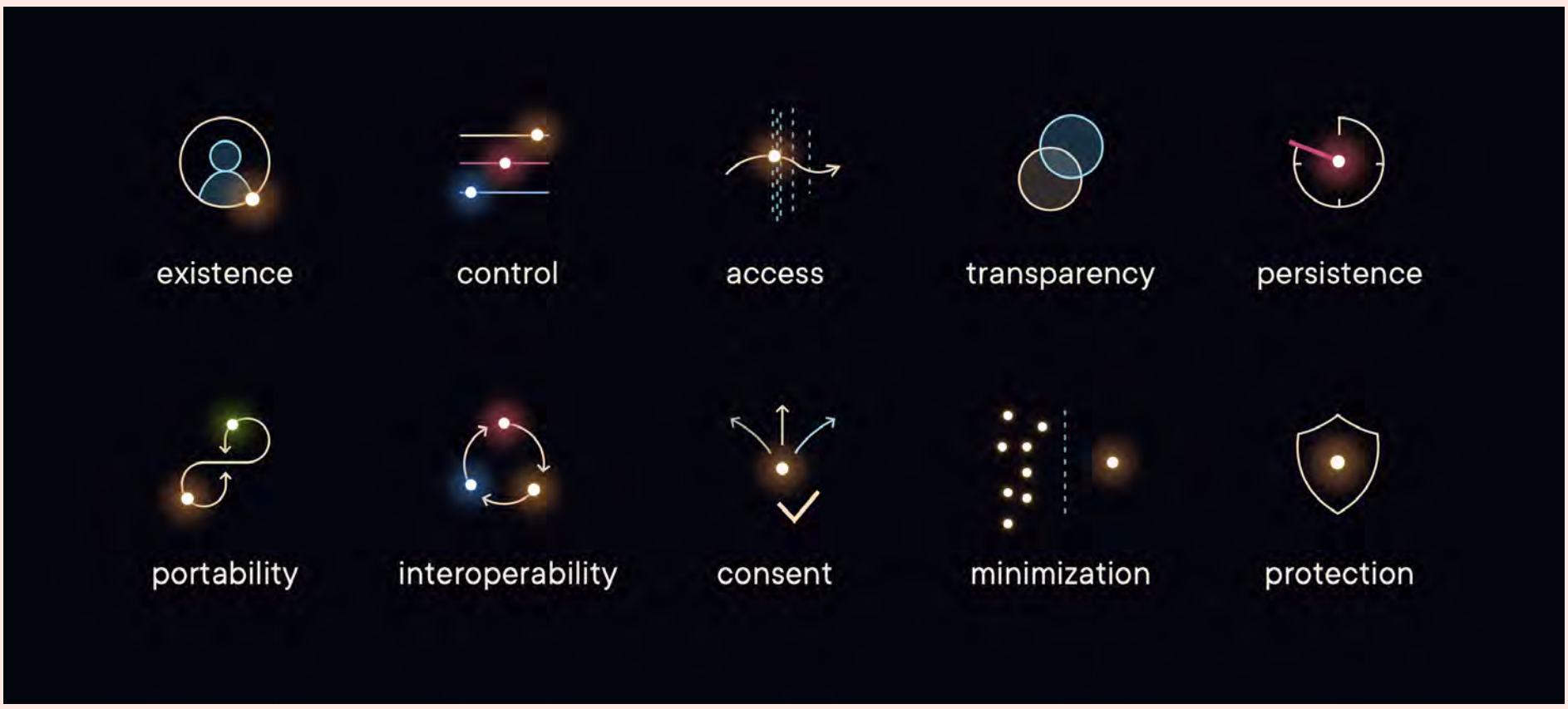
In other words, self-sovereign identity is a system where users themselves-and not centralized platforms or services like Google, Facebook, or LinkedIn-are in control and maintain ownership of their personal information.

In his article "The Path to Self-Sovereign Identity," Christopher Allen notes these core requirements:

> *The user must be central to the administration of identity. That requires not just the interoperability of a user's identity across multiple locations, with the user's consent, but also true user control of that digital identity, creating user autonomy. To accomplish this, a self-sovereign identity must be transportable; it can't be locked down to one site or locale.*
>
> *A self-sovereign identity must also allow ordinary users to make claims, which could include personally identifying*

> *information or facts about personal capability or group membership*[18]*. It can even contain information about the user that was asserted by other persons or groups.*
>
> *In the creation of a self-sovereign identity, we must be careful to protect the individual. A self-sovereign identity must defend against financial and other losses, prevent human rights abuses by the powerful, and support the rights of the individual to be oneself and to freely associate*[19]*.*

Allen goes on to identify a series of ten guiding principles — captured in the illustration below.



↑ "Ten Principles of Self-Sovereign Identity" by Christopher Allen (2016), illustrated by Jolocom (2019).

In sum, (Bluesky Community, 2020) self-sovereign identity allows a person to:

- control an account and access private data
- communicate with another actor
- establish visible reputation and credibility
- allow authentication and migration between services
- allow communication across services
- create an identity that is unique, global, and memorable.

The Building Blocks of SSI

01 Key Management

SSI puts control in the hands of the user, but that means users must handle technical steps including *cryptographic* key management. If you forget your keys or passwords, it's not possible to recover them because there is no third party to rely on.

Today, many people are trading cryptocurrencies using hardware wallets and third party services like Coinbase that require key management. These systems use private keypairs that are usually very secure, but too hard to use for casual web applications like social media.

Other decentralized applications use Web wallets such as the Metamask browser extension to authenticate your identity. The Metamask wallet is tied to Ethereum and serves its decentralized apps.

In the future, your browser may have built-in tools to manage your cryptographic keys for services across the web.

Some peer-to-peer protocols that already use keypairs for identity include Gun, Secure Scuttlebutt (SSB), and Peergos.

02 Blockchain-based DNS

Today, most centralized identity systems rely on a *DNS*, or *Domain Name System*, that translates human readable domain names (for example, www.archive.org) to numeric IP addresses that computers use to connect to each other. But since the advent of *blockchains*, many projects have created blockchain-based naming systems that are decentralized, understandable by humans and secure. Namecoin, ENS (Ethereum Name Service), Blockstack, and Handshake all use blockchains to assign and verify names.

03 Decentralized Identifiers (DIDs)

DIDs are a new type of globally unique identifier (URI) that does not require a centralized registration authority like a DNS because *control of the identifier can be proved using cryptography*. This could be the core infrastructure of decentralized identity and the concept is being formalized into an emerging W3C standard, which would make DIDs interoperable.

DIDs require a global key-value database in which the database is a blockchain, distributed ledger, or decentralized network.

Some applications using DIDS:

- Jolocom - an open source SSI protocol & smart wallet using DIDs and DID documents built on Ethereum and IPFS.
- 3ID/Ceramic - 3ID is an identity system that links a user's Ethereum address to a DID. They are in the process of migrating to a blockchain-agnostic DID network called Ceramic.

- Sovrin - Sovrin is a permissioned blockchain identity network that implements DIDs. Consensus in the Sovrin network is maintained by approved validator nodes.
- uPort - Uport is a DID implementation built on Ethereum.
- ION is a Microsoft-led DID system. It is an implementation of Sidetree, a blockchain-agnostic DPKI protocol, that runs on Bitcoin.

04 Verifiable Credentials (VCs)

Every time you produce a driver's license, vaccine card, or passport, you are using a physical document to verify who you are and other personal attributes. But these documents can be forged, stolen and are hard to verify by a machine. The digital era requires new types of credentials.

Verifiable Credentials (VCs) *are a standard format for the digital representation of credentials that are cryptographically secure, verifiable through machines, and that guarantee privacy by enabling methods such as minimum disclosure*. They obey a common structure regardless of the attributes contained, making it possible, perhaps, to one day have a single identity credential.

Imagine your passport in a secured, digital ID wallet that you can use to travel, open a bank account, or check into a hotel.

Use Cases

→ ConDIDI

ConDIDI — *Conference Digital Identifier Integration* - aims to use SSI technology to make it easier for academic conference organizers and participants to track credentials and reputation. It is a collaboration of the Leibniz Information Center for Science and Technology (TIB) and Jolocom.

→ Xride

Xride — a showcase for the future of ridesharing, where scooters employ processes for payment, identity and re-charging that are completely decentralized. This month-long experiment in Bonn and Berlin aimed to prototype a less costly, more secure and more efficient scooter sharing system. It was a collaboration between Deutsche Telekom's T-Labs and Jolocom.

Recommended Resources

Identity in the Decentralized Web (2019), a blog post by Jim Nelson, Internet Archive

Self-Sovereign Identity (SSI) Explainer, an 8-minute video explaining Self-Sovereign Identity (SSI) using a real world example of renting a property.

SSI Essentials: Everything you need to know about Decentralized Identity. Blog post by Gataca.io, 2021

Self-Sovereign Identity (SSI) 101: Decentralized Identifiers (DIDs) & Verifiable Credentials (VCs). Blog post by Gataca.io, 2021.

Try it out!

The Jolocom SmartWallet enables you to create and manage your own self-sovereign digital persona, giving you the ability to provide verifiable credibility for your personal attributes.

Super Skills learning app (2021). The Lego Foundation and the Learning Economy Foundation create a gamified learning app for kids which showcases all the key components of the decentralized identity stacks, with an emphasis on DIDs, Verifiable Credentials, and wallets.

Dive Deeper

Self-Sovereign Identity: Decentralized Digital Identity and Verifiable Credentials is a 2021 book by Alexander Preukschat and Drummond Reed.

The Decentralized Identifiers (DIDs) v1.0. Standard, a Proposed Recommendation at W3C, 2021.

A Decentralized Open Source Solution for Digital Identity and Access Management, Jolocom Whitepaper, 2019.

A Brief History of SSI: Where Does It Come from? A Timeline by Hannah Loskamp, from Jolocom, 2022.

SELF-SOVEREIGN IDENTITY: The Future of Identity: Self-Sovereignty, Digital Wallets, and Blockchain. White Paper by the Inter American Development Bank, 2020.

What Does the Decentralized Identity Landscape Look like in 2022?. Tweet from @affinidi.

Implementing Self-Sovereign Identity (SSI) for a digital staff passport at UK NHS. Research paper about real-world implementation of self-sovereign identity, by Mary Lacity and Erran Carmel.

Panel: Decentralized Identity. Video recording of a panel discussion at the Decentralized Web Summit 2018, featuring representatives from SSI projects around the globe.

The path to Self-sovereign identity (SSI) in research. Video presentation by Lambert Heller at the 2nd international Conference on Blockchain For Science, Research and Knowledge Creation, 2019

Community Resources

GetDWeb.net - web site of the DWeb Community, a global network of meetup groups working to build a better web, following these core principles

Redigest - Monthly newsletter by Redecentralize.org

Stories from the Decentralized Web - Medium Channel with event recaps, articles & reposts of fundamentals of the Decentralized Web

DWeb Community Calendar

You can find links to other great information resources on the DWeb Website!

Past and upcoming webinar sessions

Jan 27	**The Decentralized Web: An Introduction** Watch the recording →
Feb 24 4 pm EST	**Using Decentralized Storage to Keep Your Materials Safe** Watch the recording →
Mar 31 4 pm EST	**Keeping Your Personal Data Personal: How Decentralized Identity Drives Data Privacy** Register →
Apr 28 4 pm EST	**Goodbye Facebook, Hello Decentralized Social Media? Can Peer-to-Peer Lead to Less Toxic Online Platforms?** Register →
May 26 4 pm EST	**Decentralized Apps, the Metaverse and the “Next Big Thing”** Register →
June 30 4 pm EST	**Ethics of the Decentralized Web & Uses for the Law, Journalism and Humanitarian Work** Register →