Blockchain and Self- Sovereign Identity

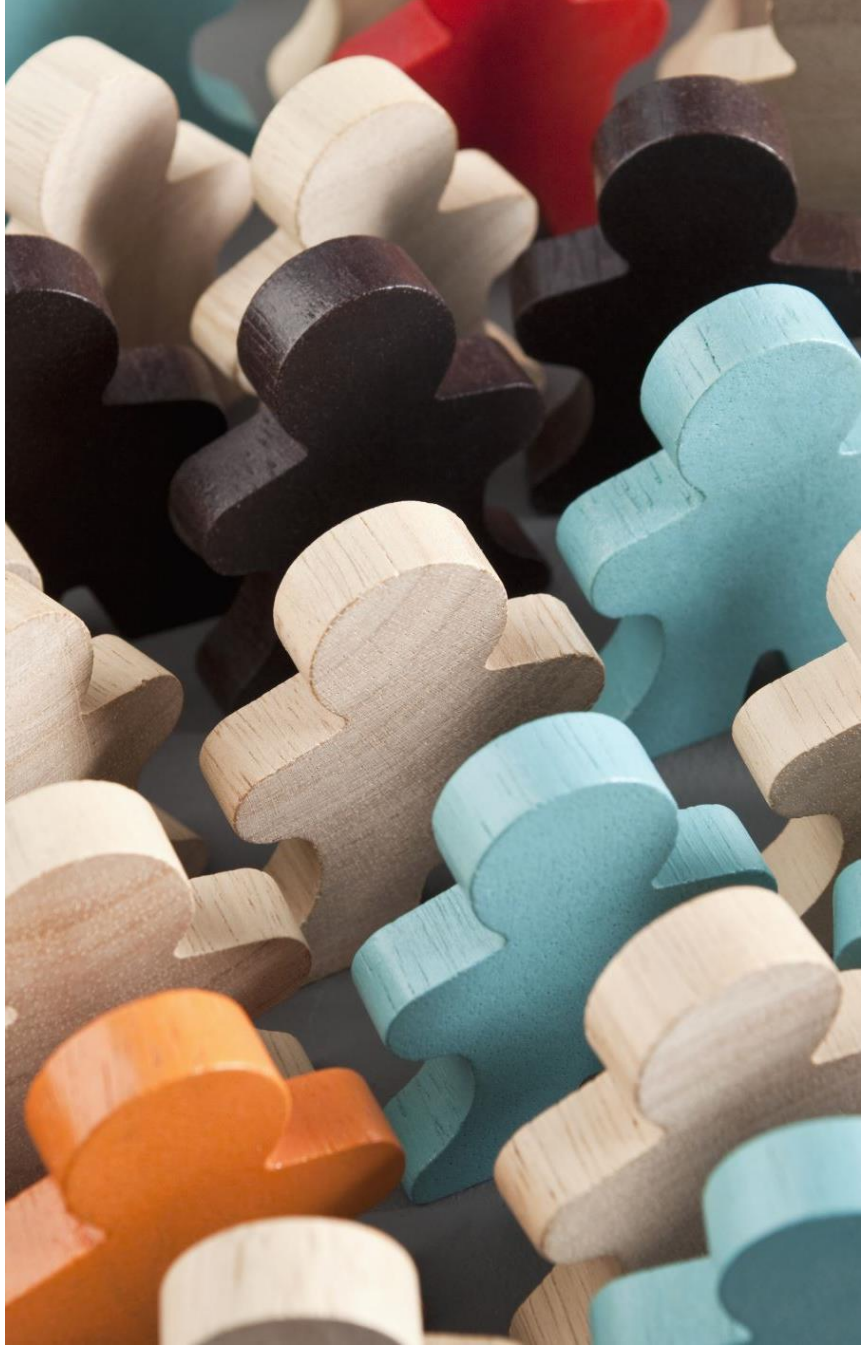
Biological Identity

- Biological identity means **the unique characteristics** that define an individual organism.
- Biological identity is often considered a consequence of our DNA, our genes, which demonstrate our relatedness to each other.
- **Carmen GRAVINO**, University of Michigan, explains that a **person's identity is the expression of an open process that is constantly in flux. The biological mechanisms of the body interact with the person's psychological and social life within this process. The construction of identity begins with our everyday connections to the people who are closest to us**

IDENTITY

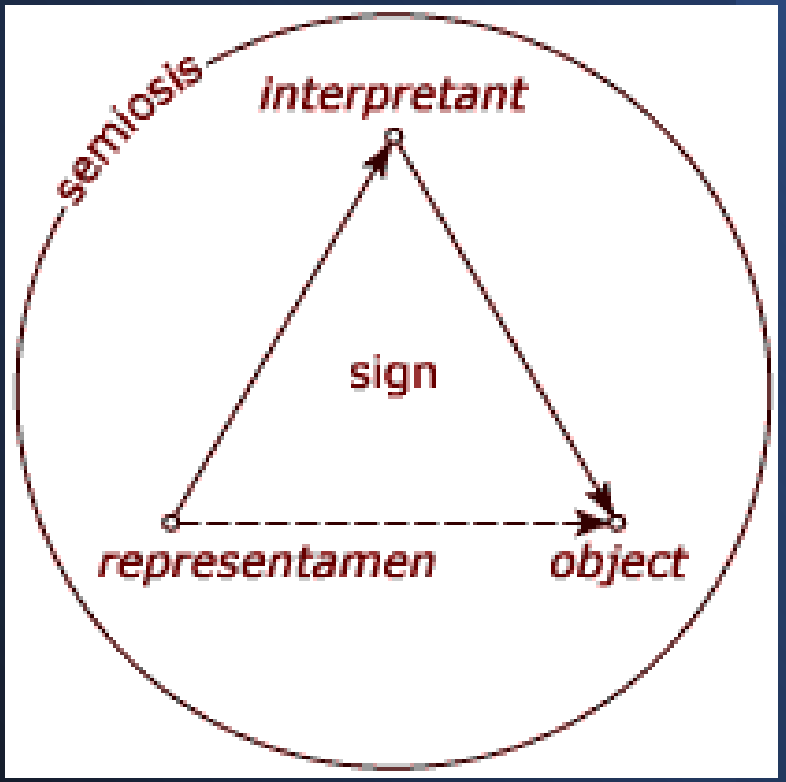
Sociology has shown that identity is the qualities, beliefs, personality traits, appearance, and/or expressions that characterize a person or group. In sociology, emphasis is placed on collective identity, in which an individual's identity is strongly associated with role-behavior or the collection of group memberships that define them.

Neuroscience has shown that identity is closely related to functioning of various brain regions and networks. For example, the prefrontal cortex, which is involved in decision-making and social behavior, has been implitheicated in processes related to self-awareness and self-reflection.



Identity as semiotic Concept

- Semiotics holds that identity is formed through the use of signs and symbols that are associated with specific meanings or representations. The use of a national flag, for example, can represent a sense of national identity, whereas the use of specific clothing styles or music genres can be associated with specific subcultures or identity groups.
- Semiotics also suggests that identity is not a singular or static concept, but rather can be multiple and fluid.. **Individuals can have multiple identities that are created and maintained through different contexts and interactions, and these identities can also change over time as a result of new experiences or cultural shifts**
- **The semiotic concept of identity emphasizes the role of signs and symbols in creating and communicating identity, and highlights the social and cultural processes involved in shaping and negotiating identity.**
- **The identity of the semiotic object depends on the context and the interpretation of the receiver or audience**. Different people may interpret the same sign or symbol differently, based on their cultural background, personal experiences, and individual perspectives.

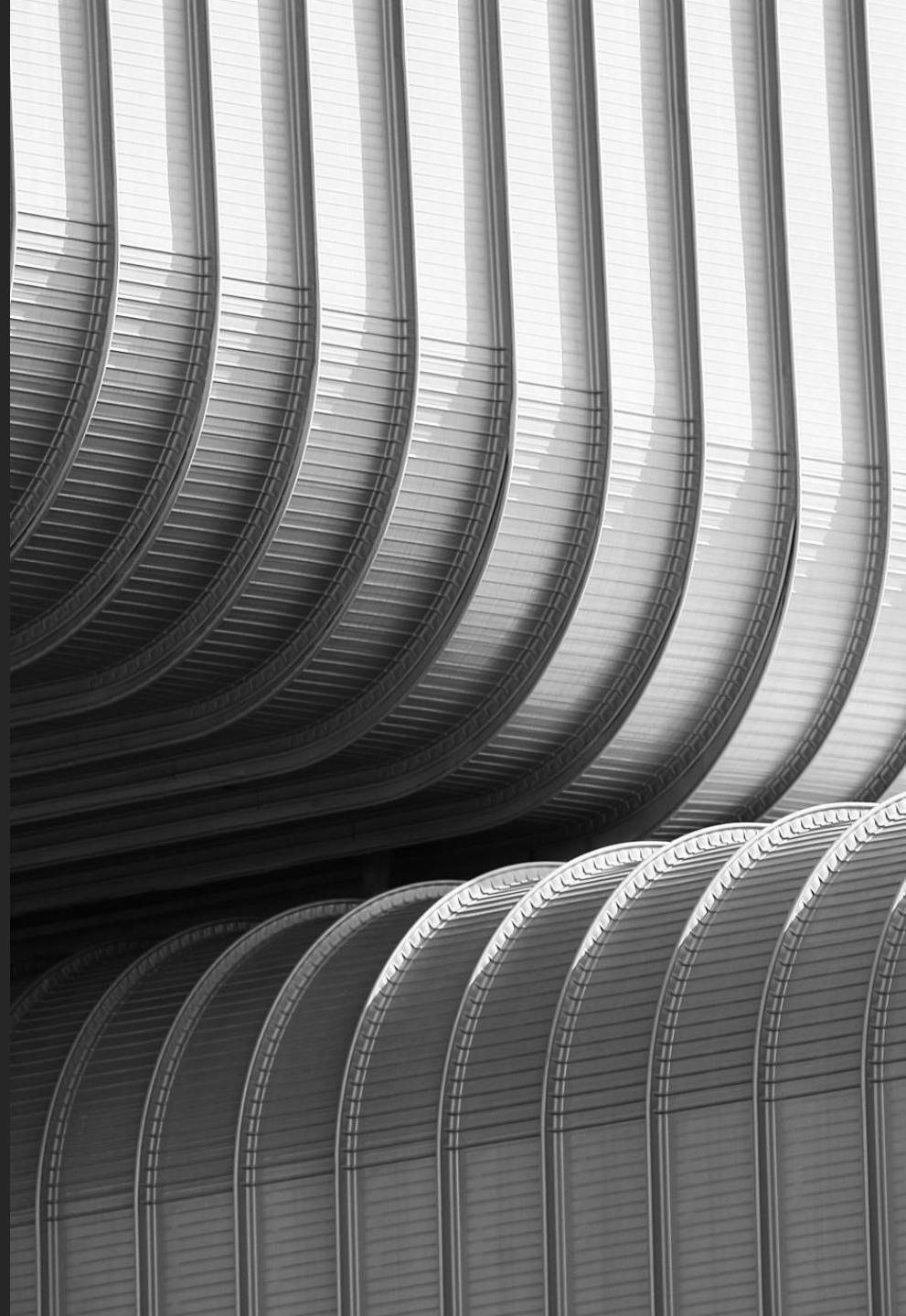


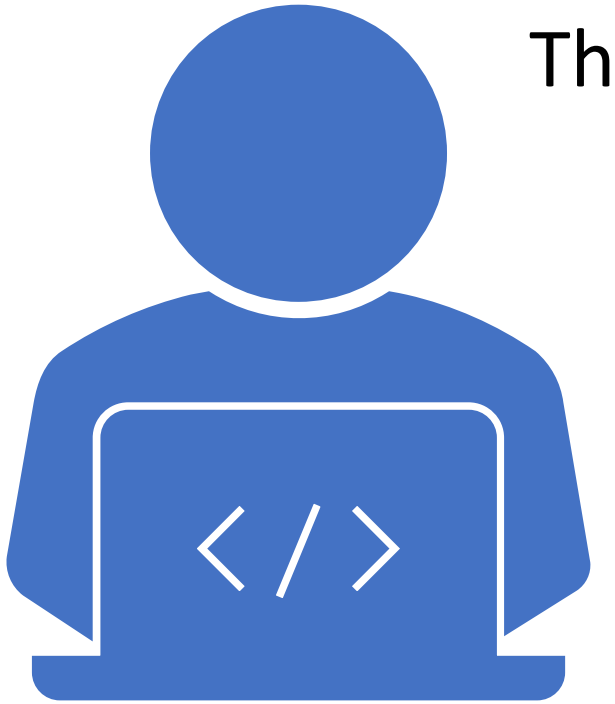
Digital Identity

Digital identity means information used by computer systems to represent an external agent(a person, organization, application, or device). In Digital Univers, identity is formalized into following two components:

The **identifier**: a unique set of characters or numbers that identifies a subject(Ex. SID in a Directory services, S-1-5-21-1004336348-1177238915-682003330-512)

The **data** associated with that subject





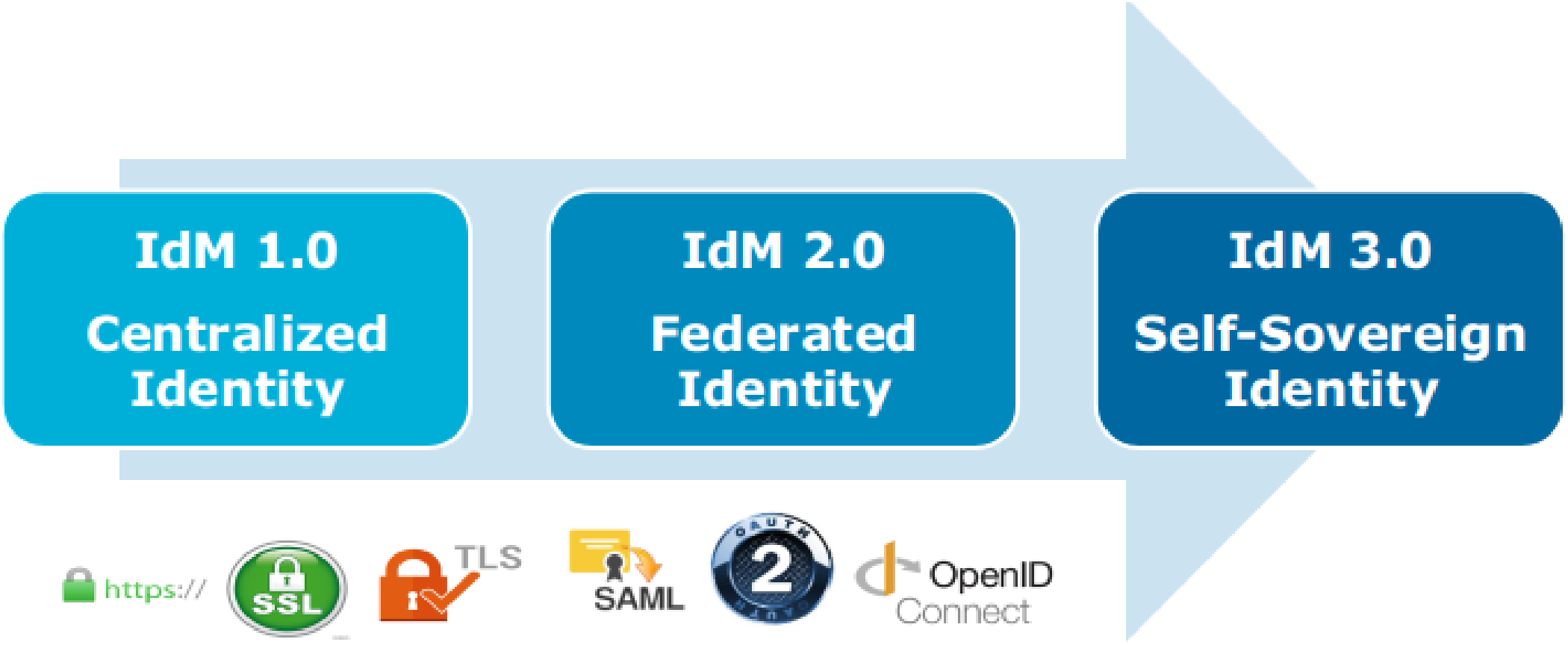
The Internet was created without an identity layer.

Kim Cameron, Former Chief Architect of Identity for Microsoft

Identity Data Management

- The organizational process of ensuring individuals have appropriate access to technology resources is known as identity management (IdM). This includes identifying, authenticating, and authorizing a person or people to gain access to applications, systems, or networks
- Initially, IdM systems were designed to provide solutions to small and close environments, relying on a **central authority**, e.g. **directory services(NDS eDirectory, Active Directory, LDAP etc.)** or a public key infrastructure with registration/validation authorities to manage the identity lifecycle
- Directory-as-a-Service(DaaS) with the popularization of the cloud, the business flow environments started to become bigger and needed more interconnections; it was clear that an evolution of this initial approach was necessary – SSO Federation Identity with protocols Kerberos, SAML(**Security Assertion Markup Language)**, OpenID, OAuth 2.0 –JWT, JSON Web Token)

Identity Management Evolution

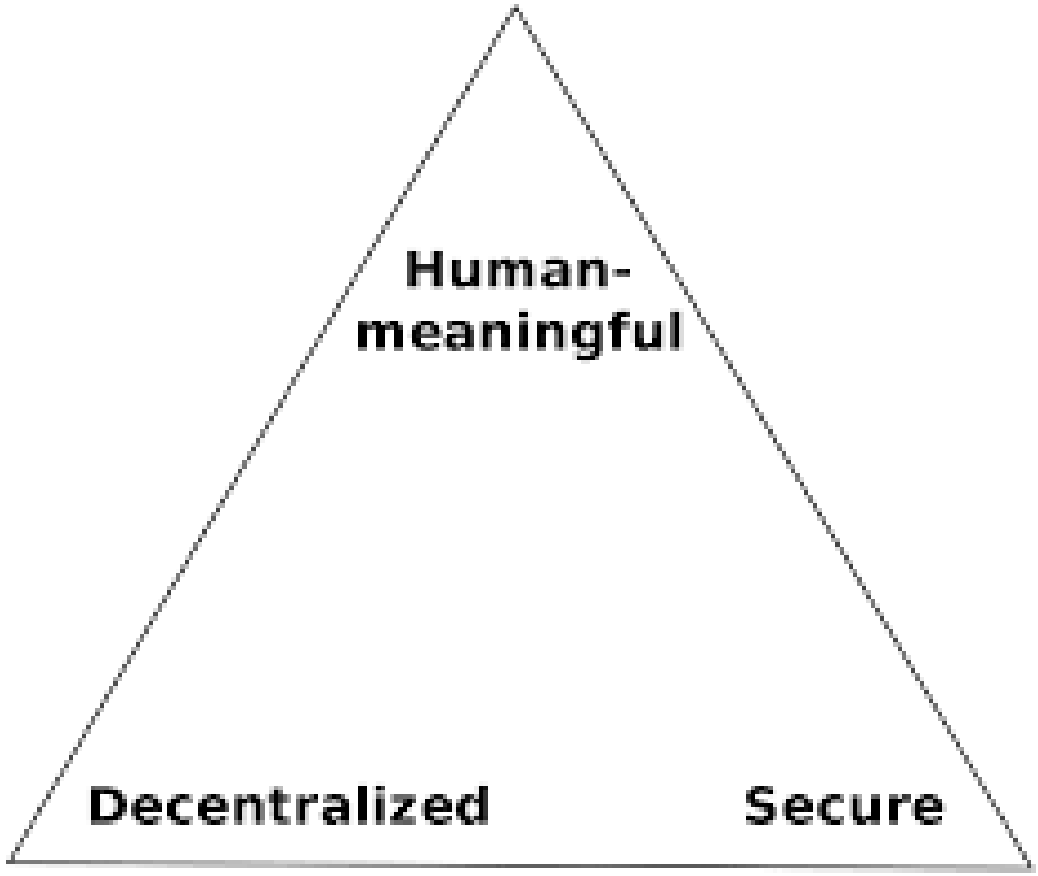


The Beginning

- In 2005, Philip Windley, Kaliya Hamlin, and Doc Searls founded the **Internet Identity Workshop** at the **Computer History Museum,CA** in Mountainview, to discuss the issue of Internet identity.
- Eitgtheen years later, the Internet Identity Workshop is still going looking for better solutions to **Internet Identity**
- An Internet-like identity system would allow any person, organisation, or thing to have an **identity relationship** with any other
- An Internet-like identity system has been a long time coming , but I'm excited that recent developments in distributed computing have allowed truly **self-sovereign identity systems** to be realised

- **Bryce Wilcox-O'Hearn** published a widely cited article on namespaces in computer systems in 2001
- According to his assessement it was impossible that someone would be able to design a system in which **identifiers could** be chosen in a distributed fashion but at the same time being both secure and human-readable
- **Namecoin** was the first fork of Bitcoin and still is one of the most innovative "altcoins". It was first to implement merged mining and a decentralized DNS.
- Namecoin was also the first solution to Zooko's Triangle, the long-standing problem of producing a naming system that is simultaneously secure, decentralized, and human-meaningful.

Zooko's Triangle



A new step ”Self-soverereign Identity”

- **Identity as Endpoint** - The Internet was built without a standard, explicit way of identifying machine (**not people**) or **networks**(not organisations)
- The next step in the evolution of the Internet will be the development of a common identity layer that will allow people, organizations, and things to have their own Self-Sovereign Identity—a digital identity that they own and control that cannot be taken away.
- **Self-sovereign identity is the natural evolution of an ecosystem which has moved faster than its supporting capabilities**

The Impacts of the Missing Identity Layer

- Businesses have to develop and manage different security architectures for each platform they deploy
- **CTRL-Shift** estimates the total costs of **identity assurance processes** in the UK exceed £3.3bn. They estimate that this could fall to as little as £150m if people are given control of their own identity data
- The average retailer cost for each **stolen record** containing sensitive and confidential information is **165 USD**
- 30-40% of contact center call volume is related to password and account recovery
- **25 people/minute** in the US **fall victim to identity theft.**
- 18% of shoppers abandon their shopping cart due to username and password issues

The Evolution of Internet Identity

Christopher Allen presents a comprehensive analysis of the online identity landscape and traces its development in his iconic paper **"The Path to Self-Sovereign Identity.“** He identifies four stages of development in his analysis:

- **Security** - the identity information must be protected from **unintentional disclosure**
- **Control** - The **owner of the identity** must manage who has access to their data, how it is used, and who may see it.
- **Portability** - The **user must not be bound to a particular supplier** and must be allowed to utilize their identity data anywhere they choose.

User-Centric

- In a iconic paper from **2008, Kim Cameron** , Reinhard Posch and Kai Rannenberg describes "**A User-Centric Identity Metasystem**" It details an abstracted design for a system which puts the user in control of their own data, the accumulation of that data, and its release to third parties
- The essential criterion for user control is that information is only transferred from "Claims Providers" to "Relying Parties" at the user's request.
- **The most common manifestations of user-centric identity are independent personal data stores on one end of the spectrum and large social networks on the other.**

Self-Sovereign Identity

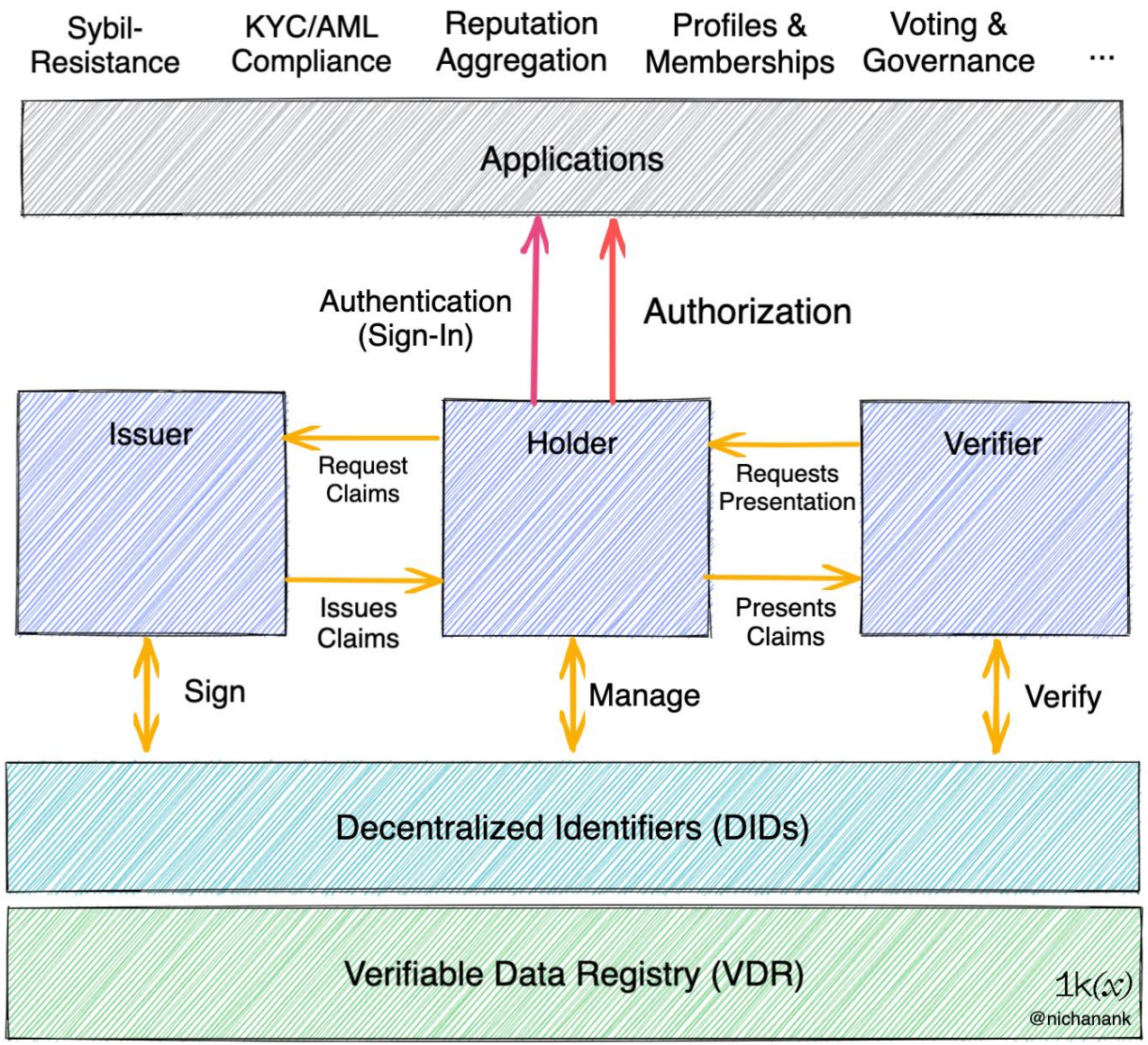
- **Self-Sovereign Identity refers to a concept in which the person is the ultimate decider of who can access and use their data and personal information. Individual control, security, and full portability are all provided, and it is independent of any particular silo.**
- Self-sovereign identity is the final step in this evolution
- The individual to whom the identity pertains completely owns, controls and manages their identity
- In this sense the individual is their **own identity provider**-there is no external party who can claim to "provide" the identity for them because it is intrinsically theirs
- **Phil Windley** describes self-sovereign identity as an "**Internet for identity**" which, like the Internet itself, has three virtues: **no one owns it, everyone can use it, anyone can improve it**

SSI - Core Concepts

- **Decentralized Identifiers(DIDs)** are a type of identifier that is designed to be **globally unique** and resolvable without the need for a central authority. DIDs are based on decentralized technologies such as blockchain, and they allow individuals or entities to create and manage their own digital identity.
- **Atestation** in the context of DIDs, refers to the process of verifying the authenticity of a DID and the associated identity. Attestation involves a trusted third-party or authority, who verifies the information provided by the DID holder and issues a digital certificate that confirms the validity of the identity. Attestation is an important component of DIDs as it helps to establish trust and ensure the integrity of the digital identity. It also enables DIDs to be used in a variety of applications, such as in the financial sector for identity verification and KYC (Know Your Customer) purposes, or in the healthcare sector for managing patient data and records.
- **DIDs and attestation**, **represent a promising technology for creating a more decentralized and secure digital identity system that is controlled by the individual or entity themselves, rather than by centralized authorities or intermediaries**.

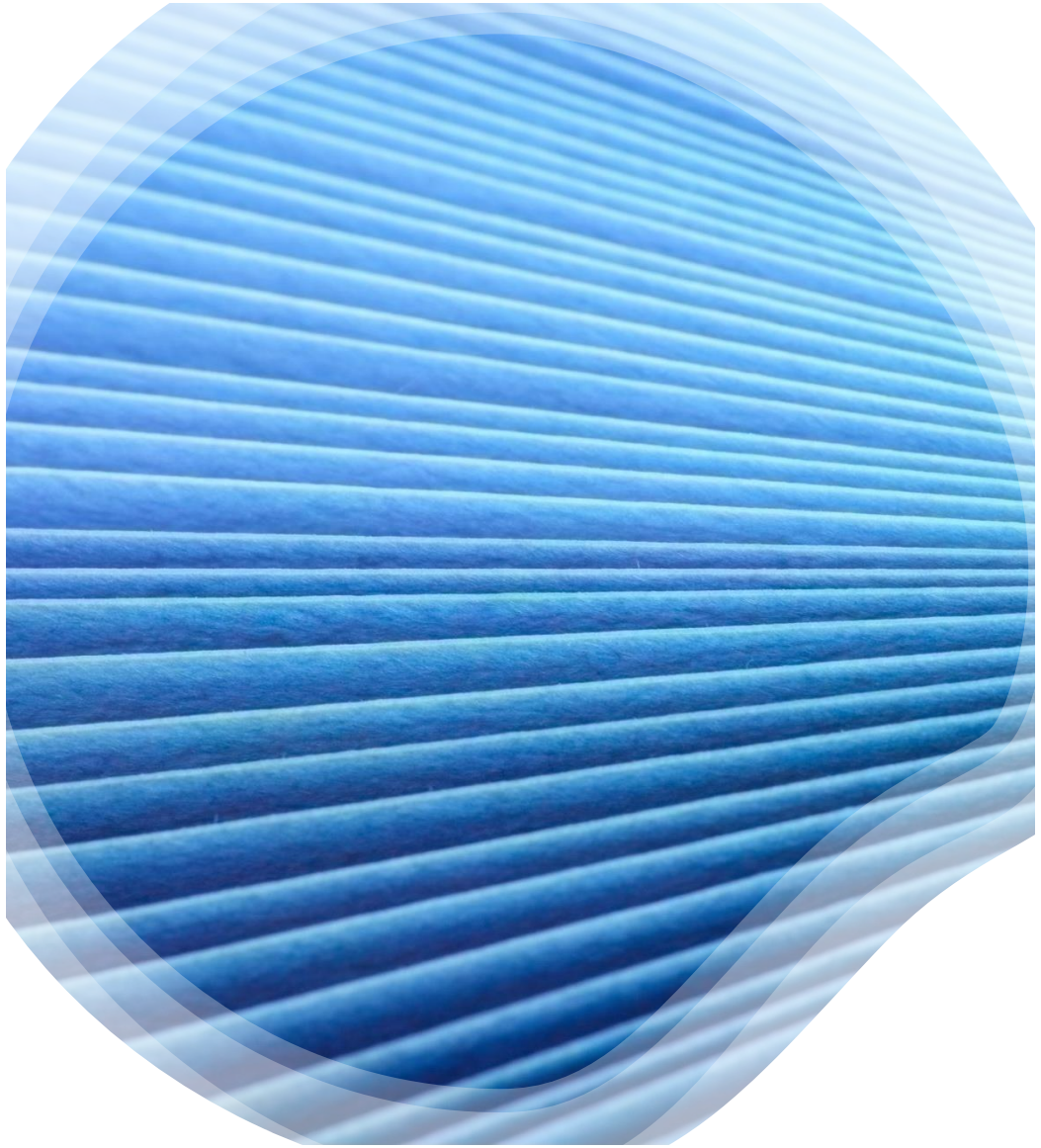
SSI as a Technology Package

- Self-sovereign identity encapsulates a set of technologies, tools, and governance models designed to outline and facilitate the transition to a new paradigm for digital identity systems.
- The technical architecture that is emerging defines three distinct transactional roles that entities within an SSI system can engage in:
  - **Holder:** creates their decentralized identifier with a **digital wallet app and receives Verifiable Credentials**.
  - **Issuer:** authority to issue Verifiable Credentials**.**
  - **Verifier:** checking the credential**.**
- The most mature is the **Verifiable Credential Data Model**, **a W3C recommended standard** for the structure of the credential data object that issuers sign
- The **W3C DID** specification is designed to be technology and protocol agnostic, instead defining a common syntax that can be used to understand all DIDs and a generic set of requirements for create, read, update, and deactivate operations of DID Documents


Sybil-Resistance
KYC/AML Compliance
Reputation Aggregation
Profiles & Memberships
Voting & Governance
...
Applications
Authentication (Sign-In)
Authorization
Issuer
Holder
Verifier
Request Claims
Issues Claims
Requests Presentation
Presents Claims
Sign
Manage
Verify
Decentralized Identifiers (DIDs)
Verifiable Data Registry (VDR)
1k(x)
@nichanank

W3C DID specifications

- **Schema:** The prefix “did” tells other systems that it is interacting with a DID and not other types of identifiers like a URL, email address, or product barcode.
- **DID Method:** specifies to other systems **how to interpret the identifier**. There are over **100 DID Methods listed** on the W3C website, often associated with its own VDR and with differing mechanisms for creating, resolving, updating, and deactivating identifiers.
- **Unique Identifier:** a unique ID specific to a DID method. For example an address on a specific blockchain(Ethereum Adress).
- **DID Document:** The aforementioned three components come together to form a DID Document, which includes the methods by which the entity can authenticate itself, any attributes or claims made about it, and pointers ("service endpoints") to locations where more information about the entity is stored.



Ethereum where **did:ethr:<public key>** represents Ethereum accounts as an identity

Cosmos,where **did:cosmos:<chainspace> : <namespace>: <unique-id>** represents a Cosmos interchain-compatible asset

Bitcoin, where **did:btcr:<btcr-identifier>** represents a TxRef encoded transaction id, in reference to a transaction position within the UTXO-based Bitcoin blockchain

Chain-Agnostic did:pkh:<address> where generative DID method designed for interoperability across blockchain networks. <address> is an account according with CAIP-10(HEDERA)

W3C DID techniques exist for a variety of public blockchains

Blockchain Protocols and Platforms

- **Fractal ID** is an **online service for identity provisioning and verification**. It implements the OAuth2 protocol for user authentication, authorization and resource retrieval. Fractal is the digital identity solution provider for Web3 projects2. Their vertically integrated decentralized identity stack offers **cross-chain identity verification, GDPR compliance, and seamless user verification via KYC/AML(Know Your Customer/Anti-Money Loundring)** and human liveness checks.

- **Kilt, Dock, and Sovrin** are application-specific blockchains for self-sovereign identity. All of them are primarily being used by enterprises to issue identities and credentials to end users. To participate in the network, nodes are required to based on native tokens in order to process transactions such as **DID/credential issuance, define credential schemas, and perform revocation updates**.


The Web3 Identity Stack

Web3 Identity Stack

1k(x) @nichanank

Foundations & Standards Bodies

TRUST Over IP FOUNDATION
DIF
W3C
HYPERLEDGER FOUNDATION

Profiles & Memberships

LENS
CyberConnect
prysm
PASSAGE PROTOCOL
SpringRole
Unlock
Disco
Backdrop
Mazury
Link3
semaphore
profile

Compliance KYC/AML

KYCDAO
keyring
burrata
Verite
QUADRATA
parallel MARKETS
QUDOS
noxx
Violet
BLOCKPASS
SYNAPS
notebook
AllianceBlock
ZKPASS

Reputation & Credentials

POAP
orange
Disco
ARCx
DEGENSCORE
Proved
MintKudos
101
noox
karma
coinvise
RabbitHole
UniRep Social
Indicio
SISMO
SourceCred
Offerspace
GALXE
Krebit
lvl protocol
KLEOVERSE
Quest
LAYER3
rep3
Portabl
Gateway
SealCred
zCloak Network

Authentication

SIGN IN WITH ETHEREUM
SSX
moralis
Magic
WalletConnect Auth
web3auth
dynamic

Aliases & ID Aggregators

ENS
Gitcoin Passport
.bit
UNSTOPPABLE DOMAINS
SPACE ID
Litentry

Proof-of-Personhood

brightID
WORLDCOIN
Gitcoin Passport
PROOF OF HUMANITY
IDENA

Wallets & Key Management

walt.id
ESSENTIALS
FRACTAL
UNIPASS
MATTR
Lit
METAMASK
Qredo
polygon ID
ONTO
zCloak
nuggets
Safe
argent
Pillar
Frame

DID Issuance, Tooling & Frameworks

Spruce
ONT ID
iden3
Bluesky
evernym
dock
trinsic
cheqd
.ID
MATTR
Elastos
everest
polygon ID
FRACTAL
ANIMA
HYPERLEDGER ARIES
sovrin
KILT

Access Control & Authorization

Lit
kepler
Privy
Guild
Unlock
token proof
Collab.Land
MintGate

Oracles

Chainlink
flux
API3
DECO
DIA
PYTH

Chain Data Index & Query

Covalent
goldsky
Coherent
basement
Dune
pnl
the graph
Bitquery
Transpose
KYVE
Luabase
moralis

Data Pipelines

kamu
SPACE AND TIME

Data Mutation & Composability

ceramic
TABLELAND

Blockchains

ethereum
polygon
AVALANCHE
NEAR
Polkadot
Tezos
STARKNET
HYPERLEDGER INDY
zkSync
GnosisCHAIN
SOLANA
celo
COSMOS
ARBITRUM
Moonbeam
CONCORDIUM

Decentralized Data Storage

arweave
swarm
sia
Filecoin
IPFS
STORJ

SSI stack inspired by the ISO Model

Layer	Examples
Application	Selective disclosure, music app, rideshare service, extensions, etc.
Implementation	DIF Hubs, Indy Agents, uPort app, etc.
Payload	JSON-LD, JWT, CWT
Encoding	ProtoBuf, Cap'n Proto, MessagePack, JSON, CBOR, etc.
Encryption	Ciphersuites, JWE, etc.
DID AuthN	Key ownership, verification, challenge/response, etc.
Transport	QR Code, HTTP, BLE, NFC, FTP, SMTP, etc.
DID Resolution	DID -> DID Doc / service and key resolution
DID Operations	CRUD support for a DID Doc
Storage	Optional, separate storage of DID metadata, e.g., IPFS
Anchor	Bitcoin, Ethereum, Veres.One, Sovrin, etc.

Decentralized Data Storage

- In a blockchain-based decentralized data storage system, data is typically stored in a series of blocks that are distributed across the network. Each block contains a hash of the previous block, creating a chain of blocks that cannot be altered without the consensus of the network. This makes it virtually impossible for anyone to tamper with the data stored on the network without being detected.
- There are several blockchain-based platforms that provide decentralized data storage solutions, including **Arweave**, **Filecoin**, and **Storj**. Each platform uses a different consensus mechanism and incentive structure to encourage users to participate in the network and provide storage space.
- By incorporating blockchain technology into cloud storage and combining the security and transparency of blockchain technology with the fault-tolerance and scalability of cloud storage, blockchain-based cloud storage solutions offer a promising alternative to traditional centralized cloud storage services.
- One example of a blockchain-based cloud storage solution is Storj, which uses a decentralized network of computers to provide secure, private, and affordable cloud storage. Storj allows users to store and retrieve data from its network using its own cryptocurrency, STORJ, which can be used to pay for storage space and network fees.
- Another example is Filecoin, which incentivizes users to provide storage space on their computers to the network in exchange for Filecoin tokens, which can then be used to access storage on the network. Filecoin is designed to be highly scalable, allowing it to handle large amounts of data storage.

Decentralized Storage Solutions

1k(x) @nichanank

	General-Purpose Blockchains	Arweave	Filecoin	Crust	Sia	Storj
Persistence Mechanism	Blockchain-based (L1/L2s)	Blockchain-based (L1)	Contract-based (L2 to IPFS)	Contract-based (L2 to IPFS)	Contract-based (L1)	Contract*-based P2P network
Consensus	Depends	**Proof-of-Access**	**Proof-of-Spacetime**	**PoW** (of storage) **& PoS** Parachain	**PoW**	(Non-BFT) **PoW & Proof-of-Retrievability**
Incentive Structure	Nodes are paid fees and/or block rewards for processing txns	AR paid to miners for storing data. Also to an endowment which will pay miners when fees fail to cover storage costs	FIL gets paid to storage nodes as rent	CRUST gets paid to storage nodes as rent	SIA gets paid to storage nodes as rent	STORJ gets paid to storage nodes as rent. *Not a time-bound contract, but assumes indefinite storage paid month by month
Payment	**Per-transaction fees** to deploy smart contracts and alter state	**One-time** payment to store forever. **Dynamic pricing** based on demand	**Ongoing** payment to ensure data persistence. **Dynamic pricing** based on demand	**Ongoing** payment to ensure data persistence. **Dynamic pricing** based on demand	**Ongoing** payment to ensure data persistence. **Dynamic pricing** based on demand	**Ongoing** payment to ensure data persistence. **Dynamic pricing** based on demand
Notable Features	All data persists as long as the network persists. Good for limited use cases like on-chain games and generative art	Novel consensus and incentives mechanism to optimize for permanent storage	Incentivizes data persistence on IPFS via a storage market	Interoperable with other parachains, can become go-to solution for projects in the Polkadot/ Kusama ecosystem	All files are private by default using Threefish algorithm for high performance and secure encryption	Focus on web2 infra support e.g. sync option with AWS S3 buckets. backups on MongoDB

uPORT

- it is a **self-sovereign identity platform** that allows users to control their digital identity and personal data.
- it is an open-source identity management system that is built on blockchain technology
- it is **built on the Ethereum blockchain platform**.
- is a decentralized identity platform that allows users to create and manage their own digital identity, which can be used to access a variety of services.
- uPort has split into two new projects, Serto and Veramo, both of which carry on the mission of decentralizing the internet and returning control of data to individuals.

Polygon

- **Polygon has launched Polygon ID**, a WEB3 identification service on its Ethereum sidechain that authenticates user credentials without revealing personal information. It will use zero-knowledge proofs (ZKPs), which eliminate the need for sensitive information to be uploaded publicly to the blockchain.
- **Polygon ID** is the first identity solution that allows users to use zero-knowledge proofs to interact with smart contracts, based on rich Verifiable Credential documents issued off-chain. Polygon ID meets “Verifiable Credentials” (VC) and “Decentralized Identifiers” (DID) W3C standards, allowing you to increase interoperability of your dApp
- dAccess-as-a-Service. Polygon ID enables trust issuers to connect with trust verifiers. Individuals receive and store claims like a KYC check in a personal wallet, and use zero-knowledge (ZK) proofs to privately verify the statements made about them.
- Polygon ID can securely interact with smart contracts and other identities without revealing personal information

Hyperledger Indy

- **Hyperledger Indy is a public**, permissioned distributed ledger that uses RBFT(Redundant Byzantine Fault Tolerant) to establish a consensus between upfront well-authenticated nodes. The security mechanisms by **indy-node** and **indy-plenum** guarantee the correct processing of requests and transactions according to the rules, which are themselves part of the consensus on the ledger. In particular, this enables the creation and update of schemas, credential definitions and DIDs by their owners by authenticating with the corresponding public keys stored on the ledger.
- **Hyperledger Indy vs. Fabric** is a completely different kind of topic. Although they may seem like similar projects, in reality, they are not. Fabric is more suited for a wide-ranging of use cases and industries. On the other hand, Indy is specifically **created for self-sovereign identity management**. So, any industry dealing with identity management can use it.
- Anyone with read access to the ledger can verify signatures made by issuers on credentials, or their presentations
- As **Indy has been designed solely for the purpose of identity management** and supports anonymous credential cryptography, it stores unique data in contrast to other ledgers that store decentralised identifiers, such as the Bitcoin or Veres One Blockchain

Tranzacții(1)

- **NYM**—These transactions write a **new DID and related DID Document to the ledger**
- **ATTRIB**—Transactions that update existing **DID Documents on** the ledger, such as rotating keys or changing service endpoints
- SCHEMA—These transactions define a schema name, version, and list of attribute names for a specific credential
- **CLAIM**_DEF—Often referred to as a credential definition, these transactions write the public key from a generated key pair of an CL-RSA signature for a specific credential schema
- REVOC_REG_DEF—Transactions that define a revocation registry for a certain credential definition transaction meaning that credentials signed by this public key can be revoked
- REVOC_REG_ENTRY—Whenever an issuer issues or revokes a credential, they must author a transaction that updates the revocation registry keeping them up to date so they can be used to construct and verify proofs of non-revocation

Tranzacții(2)

- Only **NYM and ATTRIB** transactions are analogous to other ledgers storing and maintaining DIDs
- The reason Indy ledgers include SCHEMA and CLAIM_DEF transactions is likely determined by the need to efficiently support CL-RSA signatures
- The revocation transactions are similarly unique to Indy ledgers, to our knowledge the only ledger attempting to support anonymous revocation of credentials
- This leads to a hierarchical structure whereby all DIDs must first be authored to the ledger in a nym transaction signed by the key of another DID before they can themselves write transactions to the ledger

Verifiable claim

- Any **Indy-based ledger** is initiated with a number of genesis **nym transactions** and all other nym transactions can be traced to a nym transaction signed by one of these DIDs
- **Sovrin** is a public ledger intended solely for privacy-preserving self-sovereign identity. The international non-profit **Sovrin Foundation** governs the **Sovrin Ledger**. Sovrin is optimized for **DIDs** and **DID Documents** as the only public ledger designed exclusively for SSI.
- DIDs are generated, stored, and used in conjunction with verifiable claims.
- A **verifiable claim** is a piece of data that is cryptographically reliable. In Sovrin, a verifiable claim is shared as proof and is anchored to the public ledger by the credential issuer's credential definition and public DID. This proof is typically in the form of a digital signature. A Sovrin Verifiable Claim can be validated using a public key linked to the Issuer's DID. A digitally issued driver's license is an example of a verifiable claim.

Trust Provided by Stewarts

- **Stewards**, trusted organizations within the ecosystem that have agreed to abide by the requirements in the Sovrin Trust Framework and are responsible for operating the nodes that maintain the Sovrin distributed ledger, operate the Sovrin ledger.
- All stewards agree to the requirements specified by the Governance Framework and sign the Sovrin Stewards Agreement
- This paper uses visualisations of a subset of MainNet transactions retrieved using the IndyScan API

Analysis

- Analysis of the data held within a Hyperledger Indy network may be useful for answering questions from many different perspectives within an SSI system
- This presentation focuses on one in detail, that of a verifier attempting to determine whether to accept a proof of a set of attributes presented by a credential holder
- While this decision will be tied to the semantic context of the interaction and is largely subjective for each verifier, we focus our analysis specifically on the syntax, the information contained within the ledger that might influence the decision of a verifier

Hyperledger Aries

- Hyperledger Aries is the infrastructure for blockchain-based, peer-to-peer interactions as defined by the **Trust over IP** Technical Stack, Layers 2 (secure peer-to-peer communications) and 3. (data exchange protocols). It defines messaging protocols and puts them into shared, reusable, interoperable toolkits for initiatives and solutions focused on creating, transmitting, and storing verifiable digital credentials.
- The presentation of indy-backed credentials is specified by Aries-rfc-0037 , a protocol involving two entities, a **holder** and a **verifier**, that have previously exchanged peer DIDs to establish a DIDComm channel across which encrypted, digitally signed messages can be exchanged, authenticated, and decrypted
- The holder then constructs a proof object from a set of credentials that have previously been issued to them and sends this to the verifier

Indy includes support for zero-knowledge proofs (ZKP) to avoid unnecessary disclosure of identity attributes — a privacy-preserving technology long pursued by IBM Research (Idemix) and Microsoft (UProve), but now made possible at scale by a public ledger for decentralized identity.

From proof, the verifier is able to use:

- The attribute values presented
- The identifiers of the scheme the attributes were issued in
- The identifiers of a set of claim definitions
- The mathematical proof of the integrity of the attributes
- The mathematical proof of a common master secret attribute known to the holder and signed by the issuer of each credential involved in the presentation
- The identifiers for the revocation registries of credentials if applicable

Public and Private Claims

For reasons of privacy, Sovrin claims architecture distinguishes between:

1. On-ledger (public) claims are stored directly on the Sovrin ledger. Public claims may or may not be in plain text, but whether they are in plain text or encrypted, their existence (and thus any correlation that can be derived from them) is publicly visible on the ledger. Whether encrypted or not, public claims should not contain personally identifiable information (PII).

2. Private claims are claims that are stored off-ledger in a private container that is not publicly visible, searchable, or correlatable by the associated Sovrin agent. Any claims containing PII or whose posting on the public Sovrin ledger may raise a correlation risk should be submitted as private claims.

- Another potentially useful insight can be gained from the ledger by querying all CLAIM_DEF transactions that reference the schema used within the presentation
- The analysis of these patterns can be derived from the SCHEMA transaction identifier, information that is included in a presentation request so available to all verifiers
- The importance of the author of the NYM transaction that initially wrote this DID to the ledger has already been emphasised, however, other information may be equally useful

MainNet Endorser DID

- A Sovrin MainNet Endorser DID enables writing to Sovrin MainNet, a production network used to scale live SSI applications and services.
- Transaction Endorsers on the Sovrin MainNet can authorize transactions to be written to the Sovrin MainNet. An Endorser may add their authorization as a digital signature to transactions created by them or others.
- When one of these signed transactions is written to Sovrin MainNet, the Endorser is responsible for paying the transaction fees.

Some considerations

- This presentation provides an overview of the data available in Hyperledger Indy-based ledgers, with a focus on the "Sovrin MainNet," an established public ledger designed for production.
- Many more public networks based on Hyperledger Indy are expected to emerge for production use cases in the future; as this occurs, the ability to assess the trust placed in the specific ledger itself will become increasingly important.
- This presentation try how metrics can be used to evaluate different Indy nodes, ledgers, and networks in order to improve solutions-based Sovrin.

Web3 Identity Stack

1k(x) @nichanank

Foundations & Standards Bodies

Profiles & Memberships

LENS · CyberConnect · prysm · PASSAGE PROTOCOL · SpringRole · Unlock · Disco · Backdrop · Mazury · Link3 · Semaphore · profile

Compliance KYC/AML

KYCDAO · keyring · burrata · Verite · QUADRATA · parallel MARKETS · QUEDO · noxx · Violet · BLOCKPASS · SYNAPS · notebook · AllianceBlock · ZKPASS

Reputation & Credentials

POAP · orange · Disco · ARCx · DEGENSCORE · Proved · MintKudos · 101 · NOOX · karma · COLLVISE · RabbitHole · UniRep Social · Indicio · SISMO · SourceCred · Offerspace · GALXE · Krebit · lvl protocol · KLEOVERSE · Quest · LAYER3 · rep3 · Portabl · Gateway · SealCred · zCloak Network

Authentication

SIGN IN WITH ETHEREUM · SSX · moralis · Magic · WalletConnect Auth · web3auth · dynamic

Aliases & ID Aggregators

ENS · Gitcoin Passport · .bit · UNSTOPPABLE DOMAINS · SPACE ID · Litentry

Proof-of-Personhood

brightID · WORLDCOIN · Gitcoin Passport · PROOF OF HUMANITY · IDENA

Wallets & Key Management

walt.id · ESSENTIALS · FRACTAL · UNIPASS · MATTR · Lit · METAMASK · Qredo · polygon ID · ONTO · zCloak · nuggets · Safe · argent · Pillar · Frame

DID Issuance, Tooling & Frameworks

Spruce · ONT iD · iden3 · Bluesky · evernym · dock · trinsic · cheqd · .ID · MATTR · Elastos · everest · polygon ID · FRACTAL · ANIMA · HYPERLEDGER ARIES · sovrin · KILT

Access Control & Authorization

Lit · kepler · Privy · Guild · Unlock · token proof · Collab.Land · MintGate

Oracles

Chainlink · flux · API3 · DECO · DIA · PYTH

Chain Data Index & Query

Covalent · goldsky · Coherent · basement · Dune · pnl · the graph · Bitquery · Transpose · KYVE · Luabase · moralis

Data Pipelines

kamu · SPACE AND TIME

Data Mutation & Composability

ceramic · TABLELAND

Blockchains

ethereum · polygon · AVALANCHE · NEAR · Polkadot · Tezos · STARKNET · HYPERLEDGER INDY · zkSync · GnosisCHAIN · SOLANA · celo · COSMOS · ARBITRUM · Moonbeam · CONCORDIUM

Decentralized Data Storage

arweave · swarm · sia · Filecoin · IPFS · STORJ

Many thanks for your attention!

Discussion & Questions