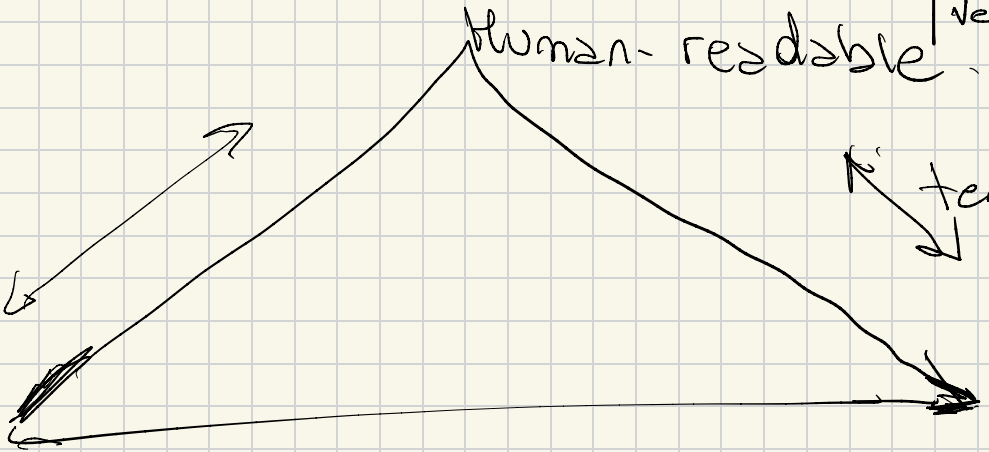
IDENTIFIERS → Security → collision-free.
↳ no fake id.
↳ no stealing id.
→ HUMAN READABLE.
→ DECENTRALIZED → No central authority for ID creation/verification.



Security.

ZOOKO'S TRIANGLE (2001)

"It is impossible (or highly unlikely) to design a system that simultaneously achieve the three properties"

ID → random generated number hash.. (A)
→ Registration Authority.. (B)
→ Hybrid solution combining (A) & (B) (Blockchain).

1980s Universally | Unique Identifier UUID.
Globally U.
→ MAC address.

→ large address space 2^{122}. w/ pseudo random number generator.

EXAMPLE:
X.509. : Name ⟷ Public | Private Key.
certificate. MAP
Central Authority.

PGP : e-mail ⟷ Public key.
quasi centralized MAP
↳ ICANN Centralized Authority.

2011 → Blockchain → "square" the Zooko's triangle.

(Name, Number).

↳ this mapping is Unique.

Method is decentralized

- it's revocable.

→ time.

Name coin (fork of Bitcoin). → "squatting" names.

PROBLEM.

- Human-readable IDENTIFIERS are scarce.

ENS (Ethereum) → Solution for squatting.

→ bidding for a name.

DID example did::example::12345678...
random number

Decentralized infrastructure.

control.
→ private key.

12 mnemonic words → seed.
to recover key..

Blockchain → public key.

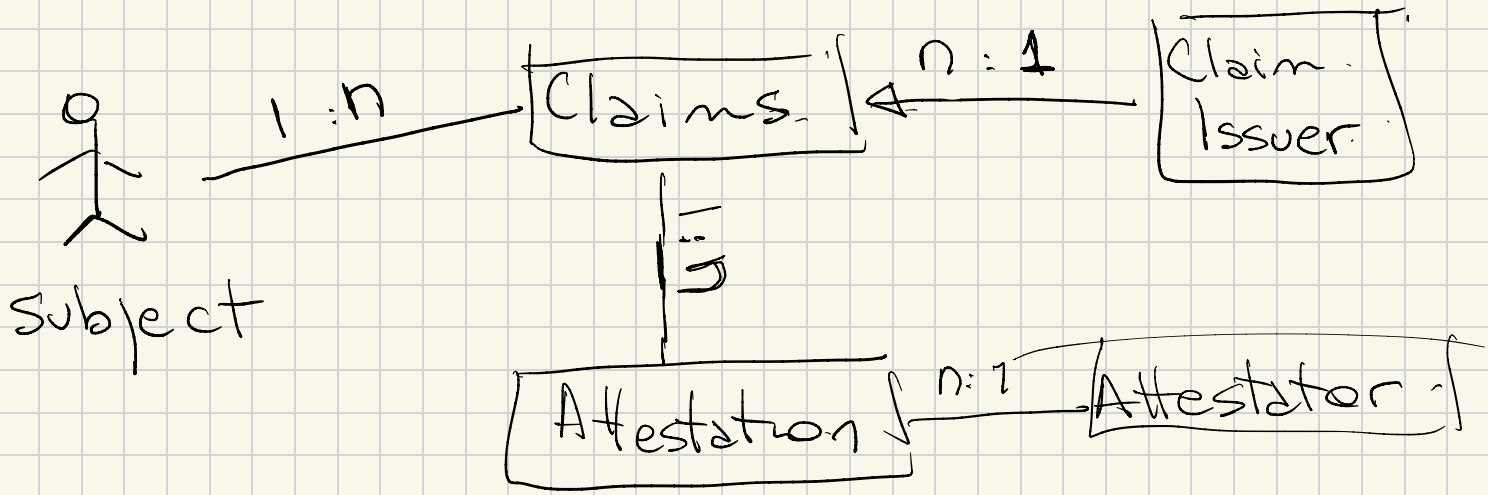
→ self-sovereign identity..

"Verifiable Claim"

- Claims → I have more than 18 years old. >18
  → I finished my bachelor course.
- Credentials → many claims that identify a person,
  → contain meta data (example validation expiration).

- Verifiable claims:

  There is an attestation (proof or signature) that says that the claim is valid.
  - (correctness of the claim).



Storage of credentials

- Public? (blockchain).
- Private (off-chain).
  - Centralized storage (Dropbox, cloud-based storage).
  - decentralized storage (IPFS).

Who ~~watches~~ verifies the ~~watchmen~~ verifiers?

- Proof of stake → one-dollar-one vote.
- Proof of work → one-CPU-one vote

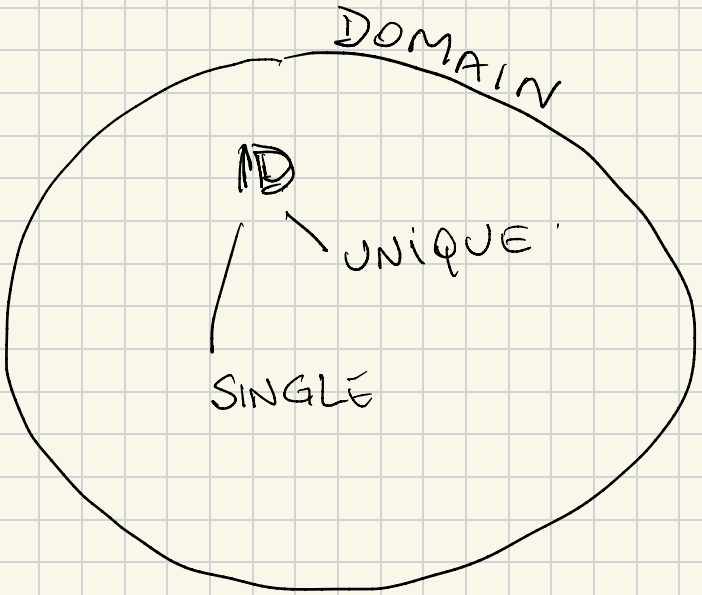
~~democratic system~~ → PLUTOCRACIES.

one-PERSON-one-vote.

- unique HUMAN identity (eliminate Sybil attacks)

→ How do we identify a human from a machine?

SOLUTION, ~~AIMS~~ AIMS AT HAVING A STRONG NOTION OF PERSONHOOD



1:1

ID ⟷ PERSON

Properties
- Sybil-resistance
- Privacy-preserving
- Self-sovereig—

- Voting / interpreting sth
- being present (regularly)
in time & in space

economic incentives (UBI)