Ethereum Citizen: Embracing Self-Sovereign Digital Identity

Vid Kersic (kersic.eth)

Researcher & Founder,

University of Maribor & Lutra Labs

Citizen

“A person who is a member of a particular country …,
or a person who lives in a particular town or city”
— Cambridge Dictionary

Citizen in 21st century

“A person who is a member of a particular country or a network state …,

or a person who lives in a particular town or city

or is part of any other kind of digital community”

Who is Ethereum Citizen?

Who is Ethereum Citizen?

Ethereum Citizen is a person who is participating in the Ethereum ecosystem or using the Ethereum technology to achieve its goals, while promoting the Ethereum's values

- There is no real hard definition (similar to Ethereum alignment)
- But you can tell "by feeling" to certain degree

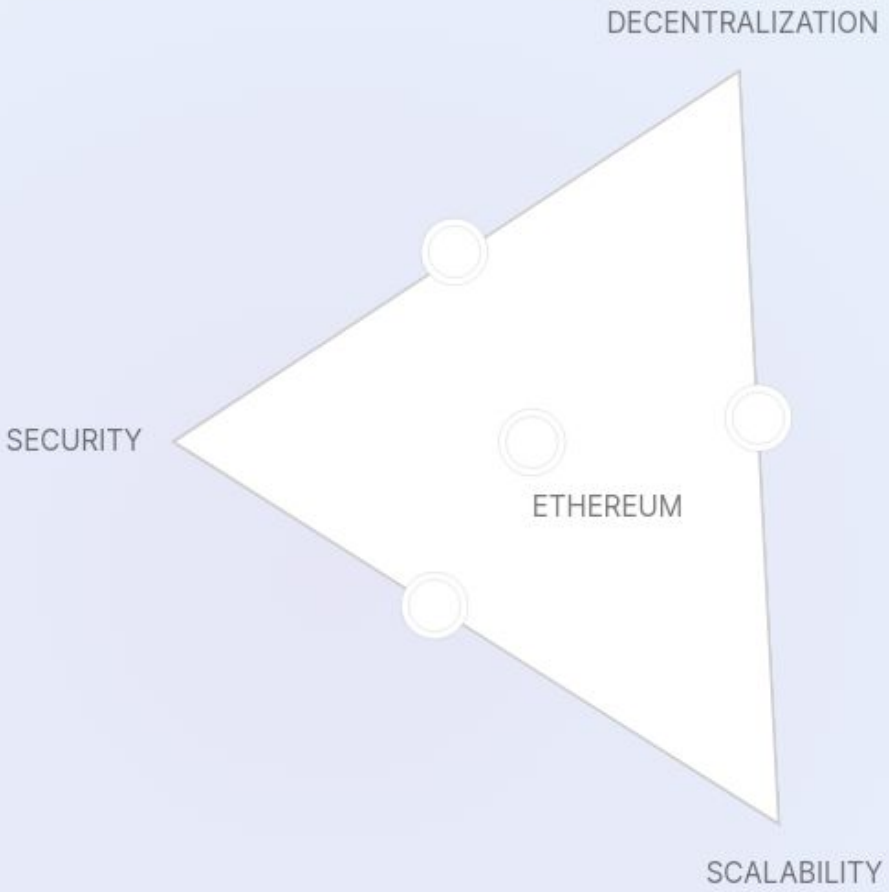
What are Ethereum values?

From technology perspective:

- Decentralization
- Security
- Scalability

From Citizen perspective:

- Self-sovereignty
- Censorship resistance
- Ownership
- Permissionless
- Privacy



Where are we today?

Financial assets

Control your assets with your private key - not your keys, not your crypto.

ใช่

Smart contracts

Smart contracts can only be upgraded through governance process of decentralized community.

เลขที่

Website

Frontend is hosted in a decentralized way - decentralized storage network.

เลขที่

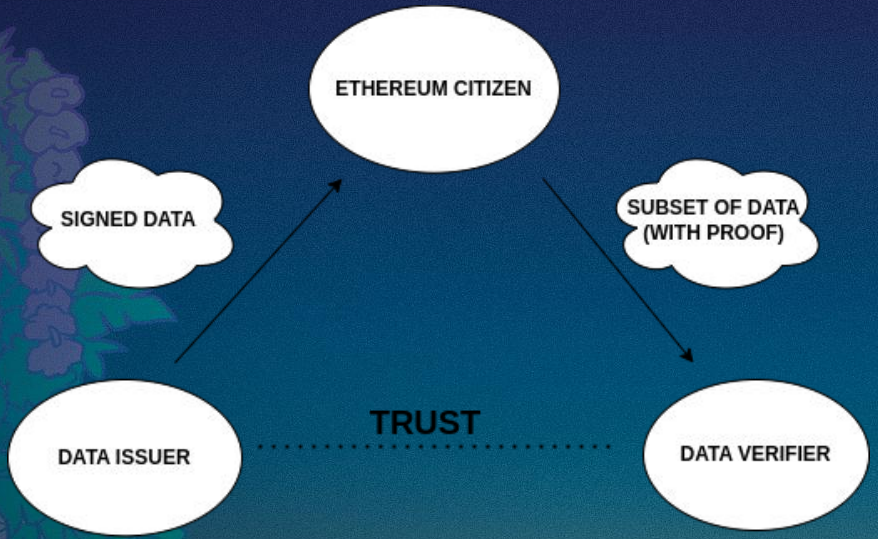
Identity & data

Identity and data is owned and fully controlled by Citizens.

เลขที่

Identity & Data

- *As an Ethereum Citizen, I want to control my identifier so no one can take my identity*
  - Ethereum address, ENS, DID, Semaphore identifier in Zupass …
  - Currently most adopted: EOA/smart contract wallet + ENS
  - But we also want privacy
- *As an Ethereum Citizen, I want to control my data and share/disclose it only to people I want and only what's really necessary when it's necessary*
  - Data in my wallet, personal server, or encrypted somewhere else
  - For that, we need verifiable data



Verifiable Data

- Data is digitally signed, so we always know where it comes from (don't forget about self-signed data)
- Users decide with whom they want to share their data
- Data verifier can verify the data without contracting the issuer (but needs to have the public key of the data issuer) - better privacy

Reality

While financial assets are in full control of the users, additional data is most often still stored on centralized databases:

- List of favorite NFTs and tokens on trading dapps
- On every platform, I have to connect my social accounts and prove that I'm owning them
- KYC

But it's not all that bad!

Things have drastically improved in the last 1-2 years:

- Just look at the tickets for Devcon :)
- Farcaster and Lens Protocol
- DIDs and Verifiable Credentials, PCD - proof-carrying data
- ZK solutions, e.g., zkTLS

How would the perfect world look like?

User visits her favorite dapp. He/she fills out some information - social profiles, favorite NFTs/memecoins/DAOs, site preferences … . This data is signed by issuer or user and stored somewhere.

User visits another dapp. This dapp also requires social profile information, but user already provided that information and the dapp can automatically get these data and verify it was indeed provided by the user.

Challenges

User friendliness

Data sharing and (ZK) proof generation takes a long time.

Developer experience (DevEx)

No unified SDKs and tools for different solutions (requiring specialized knowledge).

Adoption & Standards

Need more common standards (especially on wallet side) for better interoperability and easier adoption.

Ethereum Citizens will become self-sovereign when all of their assets, data, and identities are completely self-sovereign without any centralized point of failure.


Thank you!
Vid Kersic (kersic.eth)
R&D, founder - UM, Lutra Labs
vid.kersic@yahoo.com
@vidkersic