SAD STATE OF DECENTRALIZED IDENTITY

AND WHAT TO DO ABOUT IT

- Host:
  - Christopher Allen
- Panelists:
  - Ryan Grant

THE BAD NEWS

- eIDAS captured by Apple & Google (mDL)
- US states following suit *(its cheap)*
- DHS funding for DID/VC has collapsed, team resigned
- KYC everywhere but insecure
- Web3/Nostr: progress but no key rotation

WHY DECENTRALIZED IDENTITY IS LOSING

- Technical standards met geopolitical reality
- Corporate capture of "decentralization"
- Builder's Dilemma: pure but irrelevant vs. adopted but compromised

MOST DANGEROUS

When systems **succeed** while **inverting their purpose**

Infrastructure for sovereignty becomes infrastructure for control

WHAT WE HAVEN'T ADDRESSED

SOME HOPE

- **Swiss e-ID**: Referendum passed, uses SSI DID/VS tech stack, potential transition path to LESS (legally enabled self-sovereign) Identity
- **Utah**: State Endorsed Identity experiments
- **Wyoming**: Law protecting private keys

THE DILEMMA

Technology alone? Not enough (failure of DID/VC proof)

Legislation alone? Not enough (failure of eIDAS proof)

SO YOU THINK YOU HAVE A SOLUTION?

DON'T WASTE MY TIME

- Persistent keys as identifiers
- Keys that can't rotate
- Using same key material for different purposes
- Naive BIP32 derivation tricks
- Rely on DNS or X.509
- KYC-centric strategies
- Global names or Global Proof-of-Personhood
- Monetization via tokens
- Over-identification (passports as root-of-trust, etc.)
- VCs that phone home
- Other solutions depending on centralized entities

DO YOUR HOMEWORK!

THESE MIGHT IMPRESS ME

- Self-revokable psuedoanonymity
- Authorization strategies over identification strategies
    - Such as object capabilities (not ACLs)
- Leverage multi-party computation (MuSIG2, FROST, FHE)
- Leverage BitTorrent mainline DHT
- Demonstrate understanding of Proof-of-Personhood (not a bot) vs Proof of Unique Personhood (not a bot and only represented once in this contextual domain)
- Incorporate Progressive Trust (reveal over time)

QUESTIONS FOR THE PANEL

- What's the path forward?
- Build alternatives or constrain platforms?
- Both?

RESOURCES

Musings of a Trust Architect:
https://www.blockchaincommons.com/musings/gdc25/

The Path to Self-Sovereign Identity:
https://www.lifewithalacrity.com/article/the-path-to-self-soverereign-identity/

Origins of Self-Sovereign Identity:
https://www.lifewithalacrity.com/article/origins-SSI/