“Logins, Wallets, and Identity”
Half-Good Notes by Jamie Pitts

Upgrade path if you do not want to yet deal with private key

At status, users screen snap the 12 words

Company as custodian

How much metadata are you leaking with custodian

We are trying to operate in trustless environments

At Golem introducing an arbitrage-based system

How to educate users to the right path to security

Users are not thinking about security

UPort white paper, throw out proposals about KYC to verify

Believe some are capable, some are not

Different levels assigned, teach best best practices, have recovery options

---

There may be reluctance to write it up as an EIP, first implementation, perhaps no support for this

---

How do we help people working together?

Working group answers that question.

EIP may be too structured for the idea phase

When we were talking about multisigs, private key sharding, we need to have more awareness of those.

One idea is to downgrade the weight of the private key, so that there is no ether on it, multiple devices each with private key

---

If I come up with identity concept, interact from those systems, just get my certificate for this or that status

--

RE: private key sharding, this is similar to ether key recovery

---

We've been talking about wallet and identity, there is another side of it, when systems are talking to each, not about persons but one machine proving that it is machine A vs. machine B

If one machine talks to another and exchange ether, these are wallets

---

EIP 725, smart contract with attestations

UPort says that EIP 725 is not GDPR compatible

If we want to make it feasible, we need compatibility

--

Separate identity and wallet

Process to reclaim identity

“Entity” and “Identity”

Wallets, smart contracts, etc are “Entities”

“Identity” is the sum of the attention being paid to you

Leverage the multiple accounts to collectively act as a claim to identity

---

Can be represented as a “claim”

Entity vs. Identity is related to the Horizontal vs. Vertical relevance (these are context-dependent)

Reputation w/ Third parties

Aggregates reputation, simplifying the navigation of the interaction

---

How can this be made more fluid

Anybody can issue a claim

We can reduce fake claims by using staking on claims

How do we turn this into an objective metric

Staking adds in the effect of large amounts of capital

Offers notion of “proof of intention”

What about those cases where we may want to allow people to fake an identity

---

What should we call this working group?

Let’s call this “Self-sovereign identity”

--

We should make this Ethereum-centric

We drifted from the UX component

How do we want people to interact with it

We don’t know what to call it?

It is not private key management

Proxy contracts is one item the group is taking on

Interesting to create a challenge about how to use private keys

Incentivizing the user to explore the community and implications

Fun experience about the wallet, before we even worry about identity

---

Mobile

How do we welcome people to the community? How open can we be to allowing other groups to participate?
