What Goes in a Wallet?

Daniel Hardman — CCG, July 14 2020 — https://j.mp/3e4HuAw

Physical wallets are not general-purpose containers

- A convenient entrée into a larger world.
- Hold small, flat, valuable, common items
- Never shared - one owner
- Enough to unlock identity in key situations

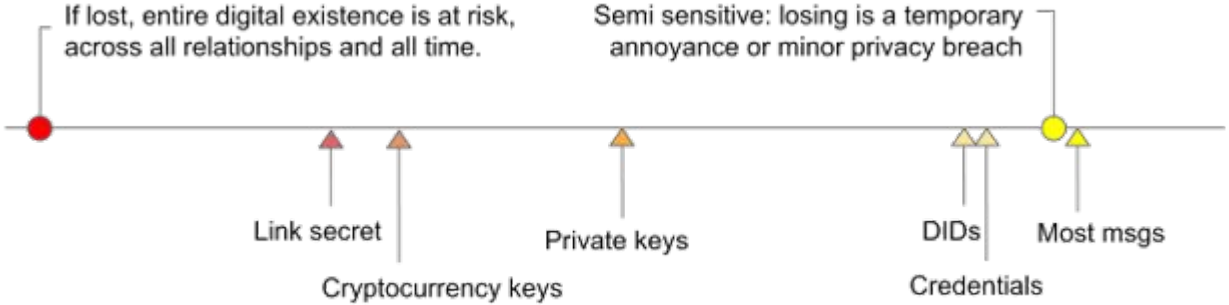
- Don’t hold:
  - all assets
  - transaction history
  - bank accounts
  - proofs given to you

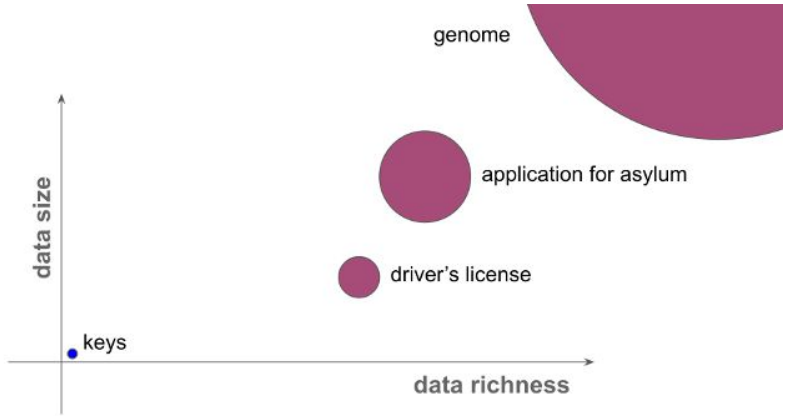
Charles Kremenak, Flickr, CC-BY 2.0

Putting the wrong stuff into a wallet doesn’t work very well.

Different types of data

1. encryption and signing keys
2. payment keys
3. link secrets
4. PII about self or others
5. held credentials
6. presented credentials
7. biometric templates
8. metadata about relationships (what Alice knows of Bob)
9. configuration
10. personal docs (last year's taxes, journal, love letters)
11. digital breadcrumbs (purchase history, browse history)
12. photos and videos
13. receipts
14. health records

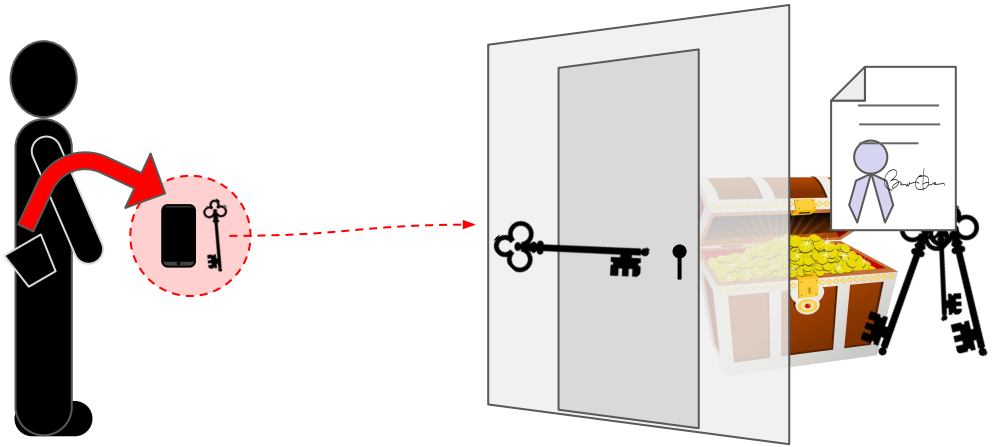




Some keys MUST be local...

...Otherwise you can’t prove you deserve access to remote.

These become the root of trust for any other keys or secrets you store, since they let you fetch them.



Notice where a wallet or mobile device is stored...

Other observations: a wallet is...

1. Not just a mobile app (enterprise, paper)
2. Locus of control (in the DID control sense)
3. Unit of backup and replication (repl != backup; multidevice w/ no key copying)
4. Unit of identity portability
5. Subdivided by personas (work vs. personal) and multi-identity (parent as self, parent for child)
6. Hacking target
7. Not necessarily the container (difference between “in” versus “referenced in” or “known to”)

Local, small, simple, sensitive

Sweet spot

wallet

1. encryption and signing keys
2. payment keys
3. link secrets
4. PII about self or others
5. held credentials
6. presented credentials
7. biometric templates
8. metadata about relationships (what Alice knows of Bob)
9. configuration
10. personal docs (last year's taxes, journal, love letters)
11. digital breadcrumbs (purchase history, browse history)
12. photos and videos
13. receipts
14. health records

hub, EDV, etc