LSDS – Re-decentralization – Wicked Problem

Jon Crowcroft,5.6.25

Localisation: physical v. legal

- Databox/hat/personal data stores
  - Databox principles (human data interaction) at Aarhus 2015
  - Lots of examples (Solid, Bluesky PDS, (Matrix, Mastodon), Estonian digital citizen, EU, open wallet etc)
- Data lakes and data trusts
  - Alternatively, legislate/jurisdictional limits (not just GDPR)
  - Enforcement depends, and tends to be reactive where PDS proactive

Three technical challenges

– Trustworthiness

– Availability

– Deployability

– And one use case

=> *Expectations (convenience)* ***set today by central (cloud) systems***

=> Claim: we can do better for latency, resilience, sustainability

Trustworthiness

- Resource pooling between friends
- How do we know they really are our friends?
- Identity is key

⇒Trustchain minimized root of trust compared to today

⇒Requires new mechanism for global verifiable timestamps

Availability #1

– Replication and Consistency in heterogenous, assymetric nets

⇒ Cloud alrea[illegible]countered

⇒ Leaderless, Adaptive, Tunable

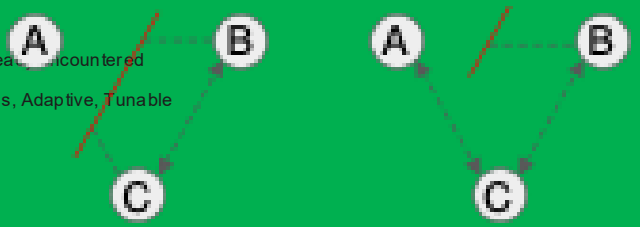
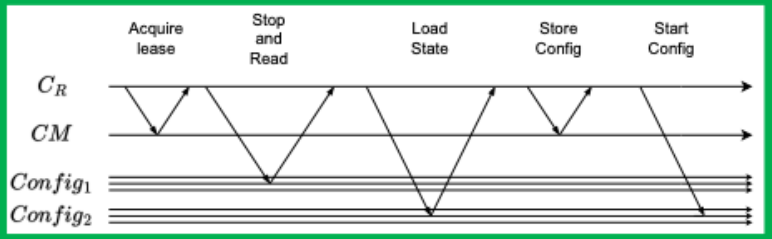
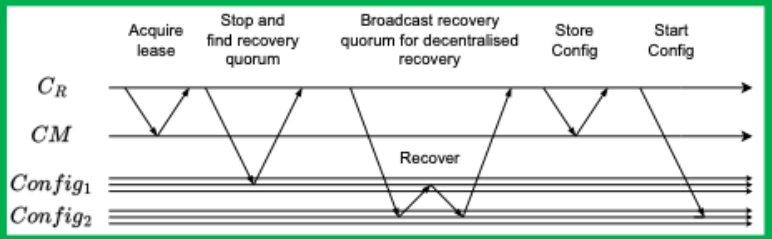


Figure 2. Full (left) vs partial (right) partition.



(a) Centralised recovery.



(b) Decentralised recovery.

Availability #2

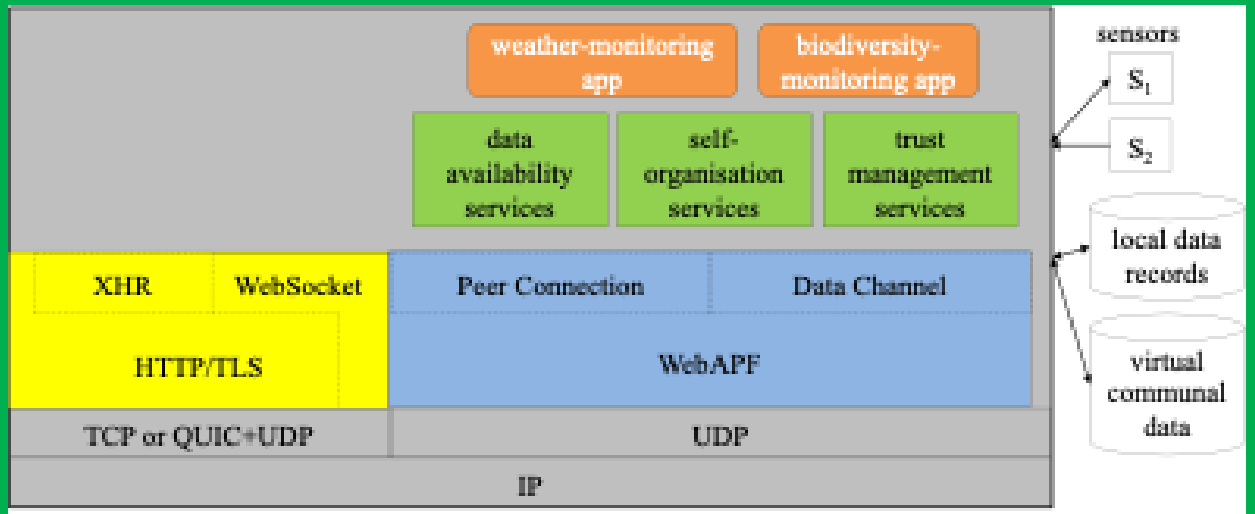
- Replica update convergence
  - Form DAG between (large) connected components, with fastest edges
  - Use these for majority consensus
  - Trickle updates to edges..
- Hybrid with CRDTs & Append only data for common cases…
- Tooling to pick right replica mech/param

Deployability #1

- Browser extensions WebAPF Analogous to WebRTC
  - Enormously successful getting video tools (zoom, teams) deployed
  - Cross platform
  - Offers security hooks (isolation/verification)
  - Offers Other use cases (FL = the Flower project)

  - Brave/Chrome
  - Use standards (AP or AT protocol, DIDs etc)

Deployability #2



Re-use Bsky id (W3C DiDs)

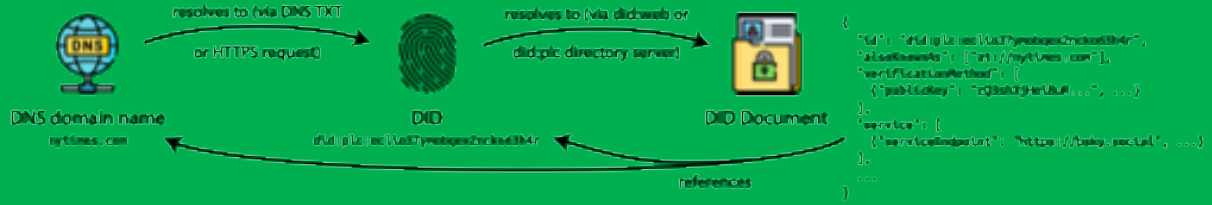


Figure 2: A handle resolves to a DID, and a DID resolves to a DID document, which in turn references the handle, DID, and the user's public key. Icons from Flaticon.com.

Use case

– Biodiversity crowdsensing

Various novel Privacy Concerns
No (especial) profit motive
Gain empirical data

=>Experiment with choice of algorithm
⇒And parameter tuning/adaptation

⇒5 apps with a million users, versus
⇒1 million apps with 5 users

Trustworthiness

- **Key management**
  - **Who creates & stores keys**
- **Exfiltration detection and redress**
  - **Spotting bad actors can be hard – maybe inference**
- **Redress?**
  - **Ostracism was a thing in medieval society☹**

Reflections on Distrusting Decentralization

- **Why trust CryptoBros?**
  - **Don't trust anyone. Unsurprisingly, we shouldn't trust them – toxic eco-systems**
- **Why trust Real Decentralized (aka community) networks?**
  - **There is no "thing" - trust in decentralized systems is a social construct.**
- **Can you trust a commons (to persist?)**
  - **Ostrim wrote 8 useful rules for such a society to last (also antonidadis& martignoni)**

Usability

- Federation v. Decentralisation

  FL is not decentralised

- Coordination

  But FL or DL both need coordination which is hard.

- Flower et al

  FL platforms need to somewhat decentralise for scale anyhow ☺

License models (and Governance)

- Both software and governance can be licenses

  You want multiple implementations (c.f. IETF)

- BSD v. GPL

  For profit tend (but not 100%) avoid GPL – so why not just mit/bsd/ etc?

- Free Ride v. No Ride?

  For profit sometimes take it and run (can give evidence☹) interfer with dual governance model

Towards Governance 2.0

- Whereby public infrastructure

  Somehow, the Internet exists – why did that work?

- Wherefore profit/non-profit

  They didn't just fence and steal the commons. They stole your personal data..

- Sustainability

  Retaking and Retaining decentralised ownership is going to be hard☺

Governance 2.0 Challenges

- Asymmetric Power

  Hyperscalers are larger than countries/regulators; capture is almost total

- Asymmetric Expertise

- Without the expertise how is the lay person supposed to even understand..

- Asymmetry of Motive

  As the Ais increase in agency, even their owners/keepers will cease to comprehend☺

Governance 2.0 is a Wicked Problem

- Unpredictable growth rates
  - Bluesky AT Protocol use, for example
- Adversaries
  - at state actor scale..
- Political
  - e.g. just look at Open Wallet Foundation & Global Digital Collaboration

Questions?