Hybrid Backup Service with Decentralised Sovereignty

UCSB Capstone 2025

Motivation

Traditional backup systems

- **Lock-in:** Providers may shut down, increase prices, or alter policies (e.g., reduce encryption guarantees), leaving users with limited options.
- **Regulatory pressure:** Centralised providers may be compelled to compromise security measures.
- **Data loss:** If the central service fails, users may permanently lose access to backups.

How to fix it?

Hybrid System

- **Centralised component:** convenience + performance
- **Decentralised component:** retain user control

WALRUS

Technical Ingredients

Centralised component

- Caching
- BW-heavy sync with Walrus
- Complex coins conversions
- Data lifecycle management

Decentralised component

- Store encrypted data
- Long-term persistence
- Complex coins conversions
- Failsafe for retrieval

Design Goals

- User Sovereignty
- Service Portability
- Usability without compromise
- Sustainable ecosystem adoption

- Week 1 — Research & Setup
- Week 2 — Basic Walrus Integration
- Week 3 — Encryption Layer
- Week 4 — Caching Layer
- Week 5 — Performance
- Week 6 — Client Interface
- Week 7 — Resilience & Direct Recovery
- Week 8 — Testing & Final Presentation