SDG BLOCKCHAIN ACCELERATOR

MENTORSHIP FEEDBACK FORM

Project / Company: Cladfy
Project Title: Blockchain-Enabled CRF Fund Disbursement System

Mentor: ELV (Technical Lead)
Dates: September – October 2025
Number of Sessions: 2

Executive Summary

Cladfy delivered a working PoC on Cardano Preprod for a cooperative loan platform: beneficiary onboarding with DID registration, loan creation, disbursement, and repayment recorded end-to-end. A Flask backend orchestrates lifecycle operations; pycardano and Blockfrost handle UTxO construction, submission, and monitoring; a Tailwind/JS dashboard provides operational visibility; the beneficiary web app supports DID registration, loan submission, status tracking, and repayment history. Conceptual Aiken-based Plutus validators per loan are defined (Disburse / Repay / Committee approval), with metadata linking transactions to Loan ID and Borrower DID. Preprod success rate reported at ≥95%; typical confirmation ~30–45s.

Mentorship focused on:

- clean DID → contract integration patterns,
- validator evolution from "conceptual" to "auditable,"
- off-chain/on-chain reconciliation and multi-cooperative support, and
- a roadmap for security (HSM/multi-sig), state persistence (PostgreSQL), throughput benchmarking, and mobile-money integration.

Session 1: Architecture Review & DID–Contract Integration

Session Date: September 2025
Session #: 1

Discussion Points

- Reviewed end-to-end flow: DID registration → loan application → committee approval → disbursement UTxO → repayment UTxOs.
- Validator responsibilities: Escrow/Disbursement, Repayment, CommitteeApproval (conceptual Aiken specs).
- Flask service boundaries (member/loan APIs), pycardano UTxO build/sign/submit, Blockfrost monitoring.
- Frontend (Tailwind/JS dashboard) + beneficiary web app for DID ops and loan UX.
- Metadata strategy: embed LoanID + DID refs; keep PII off-chain; evidences pinned off-chain (hashes in datum/metadata).

Key Findings

- Hybrid pattern (off-chain dashboard + on-chain transparency) is feasible and reproducible.
- Deterministic build pipeline demonstrated (success ≥95%); UTxO conventions respected.
- Validators are well-scoped conceptually but require edge-case semantics and authorization rules to move toward auditability.

Recommendations

1. DID Binding Pattern:
    - Require Borrower DID and Cooperative DID references in datum; verify Committee DID (or role badge) in approvals.
    - Maintain a DID→role cache off-chain with hash in datum for quick on-chain verification.
2. Validator Hardening (Aiken):
    - Define strict state machine per loan: `Requested → Approved → Disbursed → Repaid|Default`.

    - Enforce monotonic state transitions; check policy IDs and role signatures on each path.

3. Reconciliation:
    - Emit event logs from Flask after each on-chain confirmation; reconcile dashboard state with confirmed tx hashes.
4. Data Layer:
    - Move from in-memory to PostgreSQL (loans, committees, DID bindings, tx logs).
5. Security Prep:
    - Plan multi-sig/HSM for cooperative keys; rotate API keys; secrets management policy.

Risks / Cautions

- Committee participation and defaults need contract-level safeguards.
- Mobile-money integration reliability and fallback paths must be validated.

Action Items (before Session 2)

- Draft Aiken state machine per loan (types, datums, redeemers, invariants).
- Add PostgreSQL persistence and migration scripts.
- Extend Flask to emit reconciliation webhooks post-confirmation.

Engagement & Openness (1–5): Openness 5 | Preparedness 5 | Responsiveness 5 | Implementation 4 | Team Cohesion 5

Session 2: Validator Semantics, Security & Scale Readiness

Session Date: October 2025
Session #: 2

Discussion Points

- Walkthrough of Aiken validator pseudocode (Disburse/Repay/Approve).
- Authorization model: committee approvals (quorum), cooperative signer, borrower signer.
- Throughput and latency targets; provider limits and fallback infra.
- Key management: multi-sig thresholds for high-value disbursements; HSM plan.
- Multi-cooperative registry: isolate namespaces (LoanID prefixes / policy segregation).

Progress Observed

- Preliminary Aiken specs drafted; datum includes Borrower DID, LoanID, principal/interest, state.
- Flask emits tx event logs; dashboard reconciliation improved.
- PostgreSQL schema drafted (members, DIDs, loans, states, txs, committees).

Recommendations

1. Committee Quorum Contract:
    - Introduce CommitteeBadge reference inputs; quorum check in CommitteeApproval validator.
2. Disbursement Controls:
    - Require Cooperative multi-sig for `Disburse`; disallow bypass from `Requested`.
3. Repayment Rules:
    - Verify Borrower DID or Delegated Payer DID; prevent over-repayment; close loan on zero balance.
4. Defaults / Dispute:
    - Add `Defaulted` transition (timeout + committee resolution); define dispute evidence hash in metadata.
5. Ops & SRE:
    - Add retry/backoff and provider failover; health checks; latency SLOs; alerting on stuck UTxOs.
6. Security Posture:

- Key ceremonies; HSM evaluation; secret rotation cadence; least-privilege service accounts.

Risks & Mitigations

- Scaling throughput: batch repayments, queue back-pressure, parallel UTxO builders.
- Network downtimes: failover to secondary provider; idempotent job design.

Action Items (Next 4–6 Weeks)

- Implement committee quorum and multi-sig paths in validators.
- Bench disbursement TPS and 95p/99p latency on Preprod; record SLO baselines.
- Integrate mobile-money callbacks into repayment flow (idempotent handlers).

Engagement & Openness (1–5): Openness 5 | Preparedness 5 | Responsiveness 5 | Implementation 5 | Team Cohesion 5

Mentor's Overall Evaluation

Progress: Strong; PoC validated on Preprod; DID and loan lifecycle tested E2E; validator hardening underway.
Trajectory: Promising → Strong; With committee quorum, multi-sig, PostgreSQL persistence, and throughput benchmarking, the system is on track for pilot readiness.
Additional Observations: Keep PII off-chain; prefer hashes/refs in datum/metadata; document key ceremonies and role assignments; finalize defaults/dispute flows before field pilot.

Post-Accelerator Continuation

Agreed areas for ongoing technical mentorship:

- Finalize Aiken validators (state machine, quorum, multi-sig paths) and run edge-case tests.
- Security audit prep (HSM, key rotations, permissioning), and operational SLOs with failover.
- Mobile-money production integration and idempotent callback handling.
- Multi-cooperative registry enablement and namespace isolation for scale.