Team Details

a. **Team Name: Aura**
b. **Team Leader name: Chetan Wakde**
c. **Problem statement: AI agents require total access to sensitive data, forcing users to give up all privacy for any real utility. This fundamental flaw prevents millions from trusting and adopting powerful Web3 and AI-driven services**

Problem that you are solving

Current Web3 and AI-driven services face a fundamental flaw that blocks mass adoption: to gain real utility (like undercollateralized loans), users must sacrifice their data privacy.

- **The Broken Trade-off:** Existing protocols demand invasive, total access to sensitive financial history for risk assessment.
- **The Trust Barrier:** This requirement for total data exposure erodes user trust, preventing millions from adopting powerful decentralized services.
- **The Lending Gap:** Users cannot prove creditworthiness without "doxxing" their entire financial life on-chain or to centralized servers.

Problem: What's wrong with traditional banks?

High Interest

Slow Approval

Unsecured Data

Brief about your solution

The project delivers a **decentralized lending platform on Cardano** that enables users to apply for loans while preserving their financial privacy. Instead of sending raw KYC or income information to a centralized server, the system performs **client-side encryption and decentralized storage on IPFS**, ensuring that **sensitive data never leaves the user's control in plain form**.

Eligibility is validated through **deterministic proof generation (ZK-style)** that evaluates income, debt ratio, and compliance checks **without exposing personal details**. This proof is then analyzed by the **Aura Agent**, which calculates a risk score and recommends loan terms. The **Lender Agent** finalizes the approval, interest rate, and tenure with a clear explanation for transparency.

Once the user accepts the offer, **settlement proceeds on the Cardano blockchain**, disbursing ADA directly to the borrower's wallet and storing an **immutable hash of the loan agreement** for auditability. Throughout the process, the **user remains in control via the connected wallet**, and backend systems operate without access to unencrypted personal data.

The solution blends:**Decentralized storage (IPFS)**

- **Privacy-preserving verification**
- **AI-driven credit assessment**
- **On-chain loan settlement**

This results in a **secure, transparent, and regulation-ready decentralized lending MVP**, built to showcase financial privacy, blockchain trust, and automated lending intelligence.

Technologies used and their use cases (Musami/Midnight)

Frontend Technologies

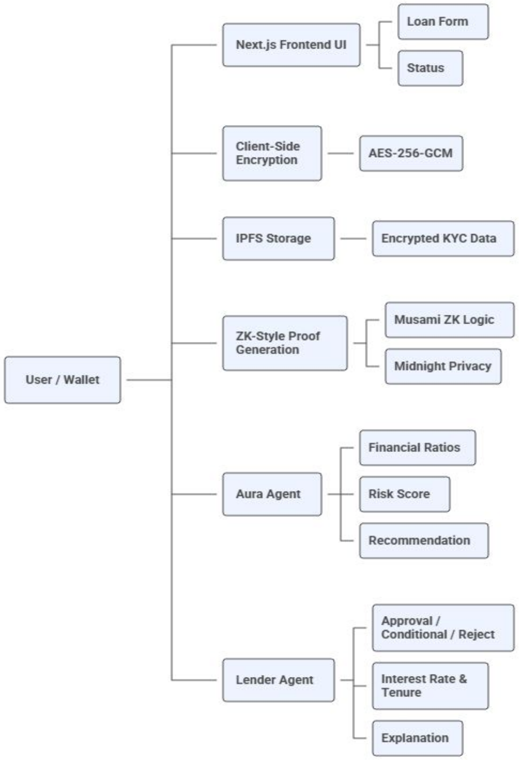
- **Next.js 14** – Used to build the main UI, loan application form, status pages, and client/server components.
- **TypeScript** – Adds strong type safety across the UI and API interactions.
- **Tailwind CSS v4** – Provides fast and responsive UI styling.
- **Web Crypto API** – Performs client-side encryption of sensitive KYC/financial data before sending it anywhere.

Backend / Core Logic

- **IPFS / Web3.Storage (Mock MVP)** – Stores encrypted user and document data in a decentralized location instead of centralized servers.
- **ZK-style Deterministic Proof Logic** – Verifies financial eligibility conditions without exposing raw data.
- **Aura Agent** – Performs AI-based risk assessment and recommends loan terms.
- **Lender Agent** – Finalizes approval decision, interest rate, tenure, and provides a readable explanation.
- **Blockfrost API** – Handles blockchain interactions: transaction creation, submission, confirmations, and status checks.

Wallet & Blockchain Settlement

- **Nami Wallet / Eternl Wallet -** Used for wallet login, identity verification through address ownership, and receiving loan disbursement.
- **Cardano Testnet / Preprod -** Executes ADA transfer on-chain and stores an immutable record of the loan agreement/transaction



User / Wallet

Next.js Frontend UI
Loan Form
Status

Client-Side Encryption
AES-256-GCM

IPFS Storage
Encrypted KYC Data

ZK-Style Proof Generation
Musami ZK Logic
Midnight Privacy

Aura Agent
Financial Ratios
Risk Score
Recommendation

Lender Agent
Approval / Conditional / Reject
Interest Rate & Tenure
Explanation

Features of the solution

◆ User Layer

➔ **Wallet Login:** Authenticate using Cardano wallets.
➔ **Loan Application:** Simple form with live auto-validation.
➔ **Status Tracking:** Follow steps — Proof → Review → Approval → Settlement.

◆ Privacy Layer

➔ **Client-Side Encryption:** All KYC/financial data encrypted before upload.
➔ **IPFS Storage:** Only encrypted files stored on IPFS.
➔ **Private Verification:** Income & DTI verified using ZK-proofs (no raw data shared).

◆ Intelligence Layer

➔ **Aura Agent:** Generates eligibility & risk score using private data.
➔ **Lender Agent:** Final approval + calculates loan amount & interest.

◆ Settlement Layer

➔ **On-Chain Transfer:** Loan amount paid to user on Cardano testnet.
➔ **Transaction Tracking:** Confirms transaction status in real time.
➔ **Audit Log:** Stores hash of loan decision for transparency.

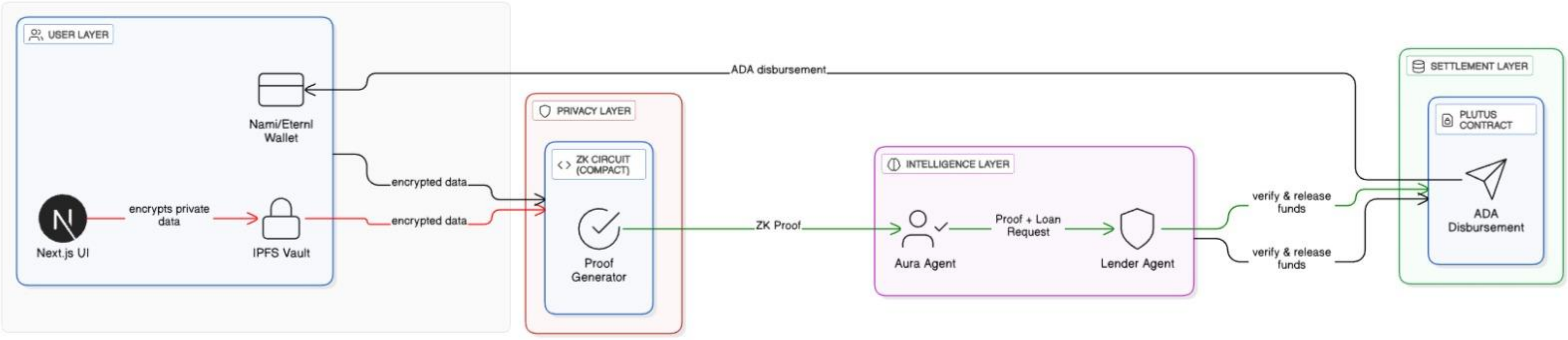
◆ Security

➔ **Proof Integrity:** Ensures ZK-proofs cannot be tampered.
➔ **Wallet Identity:** Wallet = secure digital identity.
➔ **Zero Server Exposure:** Backend never stores sensitive data.

Impact of the solution

Key Feature & Category	Strategic Impact & Outcome
Reg-DeFi Capability	Opens compliant markets by verifying eligibility (Income/DTI) without exposing raw data.
Automated Agents	Drastically reduces overhead and boosts yields via automated risk assessment (Aura/Lender).
Structured Risk Logic	Attracts institutional liquidity by enforcing standardized safety checks (e.g., Income ≥ 3x Repayment).
ZK-Style Proofs	**Data Minimization:** Breaches yield only useless hashes, protecting user identity completely.
Client-Side Encryption	**Self-Custody:** Users hold decryption keys (AES-256), ensuring GDPR/CCPA compliance.
Immutable Audit Trail	Stores loan agreement hashes on Cardano for tamper-proof auditing without data exposure.
Modular Architecture	**Scalability:** Allows independent upgrades of Intelligence layers without disrupting the core system.
Cardano Integration	Validates Cardano for complex, multi-stage financial settlements beyond simple transfers.
Deterministic Logic	**Bias Mitigation:** Credit decisions are based purely on math, not subjective judgment.
Explainable Decisions	**Transparency:** Builds trust by providing human-readable reasons for every loan outcome.
Financial Inclusion	Empowers unbanked users to access global capital using digital reputation instead of banks.

Architecture diagram of the proposed solution



How is this solution different from others

Feature	Legend dApp Approach	Typical DeFi Lending Protocol
KYC/Eligibility	**Zero-Knowledge (ZK)-Style Proofs:** Proof is generated client-side to verify conditions (e.g., *Income $\geq 3\times$ repayment*) without exposing the raw financial data.	**Permissionless/Overcollateralized:** No KYC required, but loans must be heavily overcollateralized (e.g., $150 in ETH for a $100 loan).
Sensitive Data	**Client-side AES-256-GCM Encryption** and storage on **IPFS**. Sensitive data *never* hits the server unencrypted and is not stored on a centralized database.	**Centralized Database (Web2-style):** If KYC is implemented, raw data is typically collected, stored, and managed by a centralized intermediary.
Risk Model	**Agent-based, Deterministic Risk:** Uses output from the ZK proof (validity, condition results) as the primary input for the **Aura Agent** risk score.	**Collateral-based Liquidation:** Risk is managed purely by the collateral-to-debt ratio and automated liquidation mechanisms.

uture scope

Scope Area	Current MVP (Diagram Components)	Future Enhancement (Focus)	Rationale/Goal
II. Governance & Control	**Config Variables** and **Supported Networks** managed centrally; implicit **Deployment Manager** control.	**DAO Governance Integration:** Connect the governance model to the **Access Control** and **Configuration** flows.	Enable decentralized, community-driven voting on interest rates, risk parameters, and protocol upgrades (Voltaire era).
III. Security & Verification	**Security** flow points to basic access; **Testing and Assurance** phase.	**Formal Verification & Security Oracles:** Rigorous, mathematical proof of **Smart Contract** correctness and real-time transaction monitoring.	Mitigate high-risk exploits (e.g., reentrancy, overflow) and ensure regulatory compliance (**Audit-logging**).
I. Core Automation & Settlement	Server-side disbursement logic (LENDER_PRIVATE_KEY likely stored in **Environments**).	**Plutus Smart Contract Automation:** Implement the full disbursement and repayment logic on-chain.	Achieve true **trustlessness**; eliminate reliance on a centralized, sensitive private key for fund transfers.

II. Governance & Control	**Config Variables** and **Supported Networks** managed centrally; implicit **Deployment Manager** control.	**DAO Governance Integration:** Connect the governance model to the **Access Control** and **Configuration** flows.	Enable decentralized, community-driven voting on interest rates, risk parameters, and protocol upgrades (Voltaire era).
III. Security & Verification	**Security** flow points to basic access; **Testing and Assurance** phase.	**Formal Verification & Security Oracles:** Rigorous, mathematical proof of **Smart Contract** correctness and real-time transaction monitoring.	Mitigate high-risk exploits (e.g., reentrancy, overflow) and ensure regulatory compliance (**Audit-logging**).
IV. Data & Privacy	**Data Pipes** and **Data Storage** (likely IPFS mock); **Web Flow**.	**Native ZK and Off-Chain Compute:** Integrate actual ZK proof systems and leverage off-chain computation frameworks (e.g., Hydra) for complex risk analysis.	Maximize user privacy while enabling complex, cost-effective risk modeling that is too heavy for the main chain.
V. Liquidity & Expansion	Single, assumed lender source (funded by `LENDER_PRIVATE_KEY`).	**Multi-Signature Lender Pool/DeFi Integration:** Develop contracts to manage pooled liquidity from multiple providers.	Increase Total Value Locked (TVL) and the capacity of the lending protocol; create a more robust **Enterprise** product.

Cardano HACKATHON ASIA IBW Edition 2025

Innovation partner HACK2SKILL

Thank you