

Business Requirements Document

Project: aetherlink-docs

1. Executive Summary

- **Project Overview:** AetherLink is a decentralized privacy layer for real-world payments, enabling tap-to-pay transactions without revealing identity, location, or amount. It aims to make crypto as private as cash and as instant as thought.
- **Business Objectives:** To create a seamless and sovereign financial experience by bridging the gap between real-world usability and cryptographic privacy.
- **Expected Outcomes:** A robust, user-friendly platform that facilitates private, offline-first transactions, enhancing privacy and convenience for users.

2. Project Scope

- **In-scope Features and Functionalities:**
 - Tap-to-pay transactions using NFC or Bluetooth Low Energy (BLE).
 - Offline-first protocol for transactions.
 - Verifiable consensus layer for global synchronization.
 - Integration with existing blockchain for security and transparency.
 - Staking and governance mechanisms for token holders.
- **Out-of-scope Items:**
 - Development of the main blockchain infrastructure.
 - Integration with specific third-party payment systems.
- **Key Assumptions:**
 - Users have basic familiarity with cryptocurrency and blockchain technology.
 - The platform will be used in environments with varying internet connectivity.

3. Business Requirements

- **Functional Requirements:**
 - **User Authentication:** Secure login and registration for users.
 - **Transaction Processing:** Ability to initiate and complete transactions offline and sync with the network when online.
 - **Privacy Features:** Zero-knowledge balance proof protocol to ensure transaction legitimacy without identity exposure.
 - **Staking and Rewards:** Mechanism for users to stake \$AETH and earn rewards for verifying transactions.
 - **Governance:** Token holders can propose and vote on protocol upgrades and privacy parameters.

- **Non-Functional Requirements:**
 - **Performance:** The system should handle a large number of transactions with minimal latency.
 - **Security:** Robust security measures to protect user data and transactions.
 - **Scalability:** The system should be scalable to accommodate a growing user base.
 - **Usability:** Intuitive user interface for easy navigation and transaction processing.
- **User Stories:**
 - As a user, I want to initiate a tap-to-pay transaction offline so that I can make payments without an internet connection.
 - As a user, I want to sync my transactions when I reconnect to the network so that my transactions are verified and added to the global ledger.
 - As a token holder, I want to stake \$AETH to earn rewards for verifying transactions and participate in governance.

4. Technical Architecture Overview

- **High-level System Architecture:**
 - **Client Layer:** Mobile application for users to initiate and manage transactions.
 - **Network Layer:** LumenMesh for offline verification and sync.
 - **Consensus Layer:** ZK-Aura for zero-knowledge balance proof.
 - **Blockchain Layer:** Integration with compatible main chains for security and transparency.
- **Technology Stack:**
 - **Frontend:** Mobile application (platforms not specified).
 - **Backend:** Offline-first protocol, ZK-Aura, LumenMesh.
 - **Blockchain:** Compatible main chains for security and transparency.
- **Integration Points:**
 - Integration with NFC and Bluetooth Low Energy (BLE) for offline transactions.
 - Integration with compatible main chains for transaction verification and security.

5. User Personas & Use Cases

- **Target Users:**
 - **Tech-savvy Individuals:** Users familiar with cryptocurrency and blockchain technology.
 - **Privacy-conscious Users:** Individuals who value privacy and want to avoid surveillance.
 - **Users in Low-connectivity Environments:** Users in rural areas or regions with unstable internet infrastructure.
- **Primary Use Cases:**
 - **Offline Transactions:** Initiating and completing transactions without an internet connection.
 - **Syncing Transactions:** Syncing transactions with the network when reconnecting.

- **Staking and Governance:** Staking \$AETH to earn rewards and participate in governance.
- **User Journey Flows:**
 - **Offline Transaction Flow:**
 1. User initiates a tap-to-pay transaction using NFC or BLE.
 2. Transaction is processed offline.
 3. User syncs transactions with the network when reconnecting.
 - **Staking and Governance Flow:**
 1. User stakes \$AETH to earn rewards.
 2. User participates in governance by proposing and voting on protocol upgrades.

6. Success Criteria

- **Key Performance Indicators:**
 - Number of active users.
 - Transaction volume.
 - User satisfaction scores.
- **Acceptance Criteria:**
 - Successful deployment of the platform.
 - Positive user feedback and adoption.
 - Compliance with security and privacy standards.
- **Business Value Metrics:**
 - Increased user privacy and convenience.
 - Enhanced trust in the platform due to robust security and privacy features.
 - Growth in the number of active users and transactions.

7. Implementation Timeline

- **High-level Milestones:**
 - **Phase 1: Research and Planning (2 months)**
 - Conduct market research.
 - Define project scope and requirements.
 - **Phase 2: Development (6 months)**
 - Develop the mobile application.
 - Implement the offline-first protocol.
 - Integrate with NFC and BLE for offline transactions.
 - **Phase 3: Testing (2 months)**
 - Conduct unit and integration testing.

- Perform user acceptance testing.
- **Phase 4: Deployment (1 month)**
 - Deploy the platform.
 - Monitor and address any issues.
- **Phase 5: Maintenance and Updates (Ongoing)**
 - Provide ongoing support and updates.
 - Address user feedback and make improvements.
- **Dependencies:**
 - Compatibility with NFC and BLE hardware.
 - Integration with compatible main chains.
- **Risk Considerations:**
 - Security vulnerabilities.
 - Compatibility issues with different devices and operating systems.
 - Regulatory challenges related to cryptocurrency and privacy.