The Coders

Shreyash Telsang (TL)
Manthan Thakare
Om Thigale

PROBLEM STATEMENT – 3

LANPay Solution for Smart Offline Payments:

COMPREHENSIVE AGENDA FOR OFFLINE PAYMENTS

01 Introduction & Problem Statement

– Overview of the current challenges in offline payment systems.

02 Proposed Offline Payment Solution

– Introduction to the new offline payment solution designed to address existing issues.

03 System Architecture Diagram

– Working model architecture of the system

04 Workflow Pipeline and System Architecture

– Overview of the current challenges in offline payment systems.

05 Overview of Offline Blockchain Wallet

– Its importance in the system

06 Realtime Use-case

– How the system will work for the end user. User-experience

07 Limitations

– Limitations that can occur in the system

08 Future Scope

– Future scope of the system

PROBLEM STATEMENT

PROBLEM STATEMENT

In areas with limited or no internet connectivity, digital payments are often inaccessible, leaving residents and businesses unable to benefit from cashless transactions. This challenge focuses on building an offline payment system that enables secure transactions without requiring continuous internet access.

Examining connectivity and financial exclusion

- Connectivity issues limit internet access in rural areas.
- Financial exclusion leads to cash dependency and inefficiencies.
- Economic growth is hindered by reduced connectivity.

SOLUTION

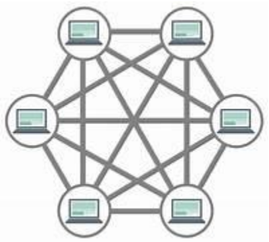
Enabling secure, offline blockchain-based digital transactions that redefine how we handle payments without internet connectivity.

Key Parameters to Consider here

- Offline Blockchain Wallet.
- Network Infrastructure.
- Authentication Methods.
- Data Storage Model.

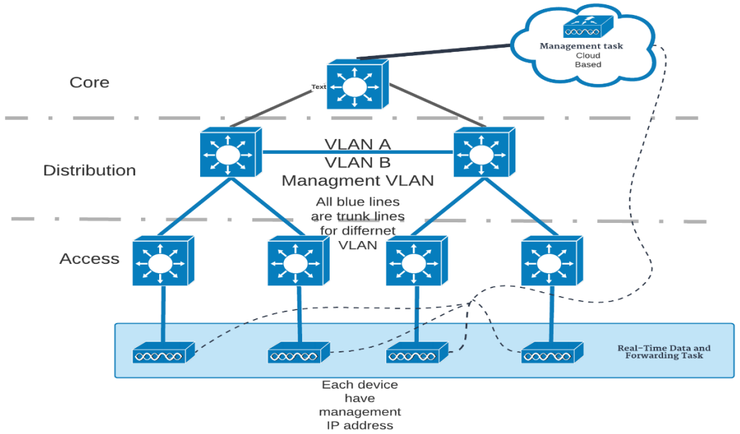
1. Network Infrastructure Overview

Detailed insights into network components and coverage

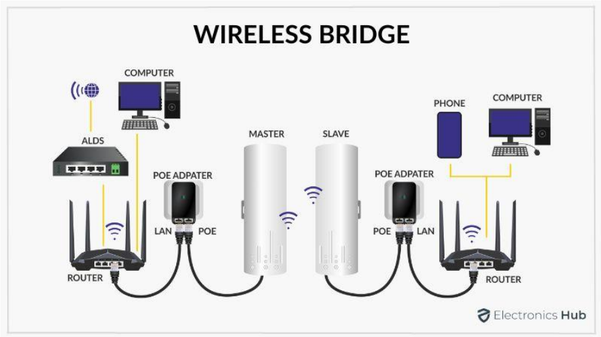


Mesh Topology

- Utilizes the below node systems to ensure seamless handoff during device movement.



1. **Wi-Fi Access Points & Backbone Connectivity (Close-range) (Node)**
   - Stable coverage achieved through APs instead of simple repeaters for better performance.
   - Utilizes wired Ethernet & fiber optics where available for robust connectivity.



Wireless Bridges (Node) (Long-range)

- Utilizes local area network for secure and efficient transactions without internet dependency.

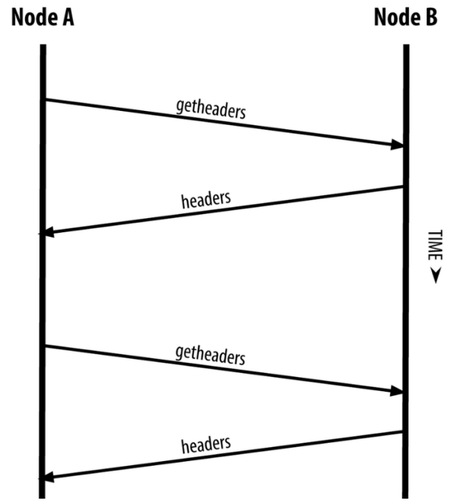
2. Blockchain Infrastructure Overview

SPV Nodes on Smartphones

- Allow verification of transactions without needing full blockchain data.

Advantages of SPV Nodes

Lower resource usage on mobile devices, enhancing accessibility.

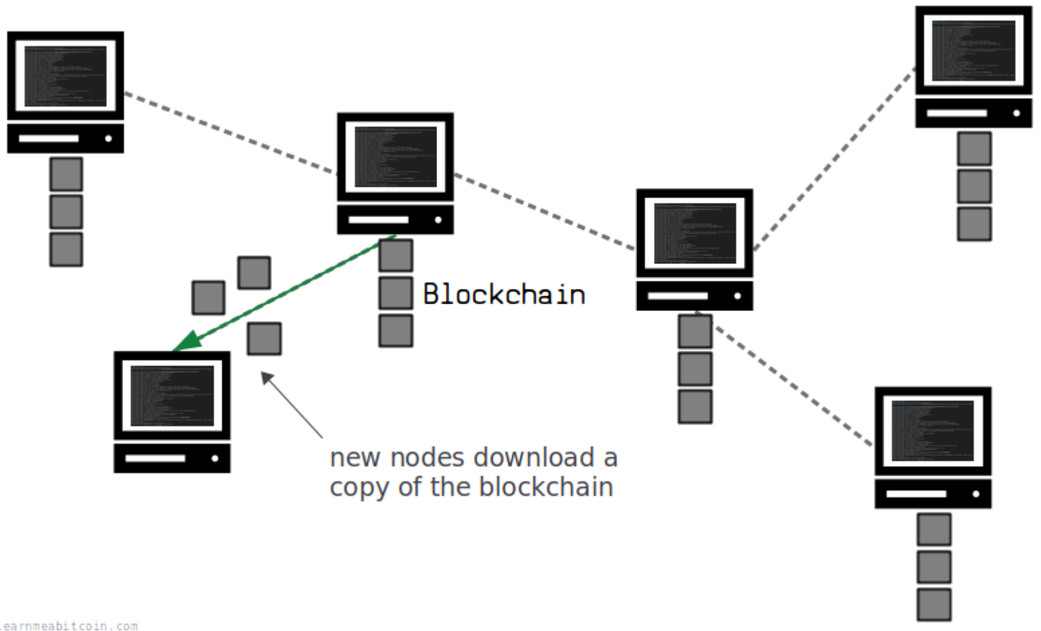


Full Nodes on Village Servers

- Allow verification of transactions without needing full blockchain data.

Advantages of Full Nodes

Provide high security through complete transaction validation and ledger storage.



Server Types and Their Responsibilities

Overview of server roles and their placements

	Description	Location
Main Ledger Server	Centralized full node at the village hub	Village Hub
Edge Servers	Partial nodes to reduce load and process local transactions	Local Areas
Local DB Server	Stores user profiles, ration card, transaction metadata (SQL-based)	Local Server
Backup Server	Provides redundant storage in a separate location	Offsite Location

Blockchain for Transaction Ledger

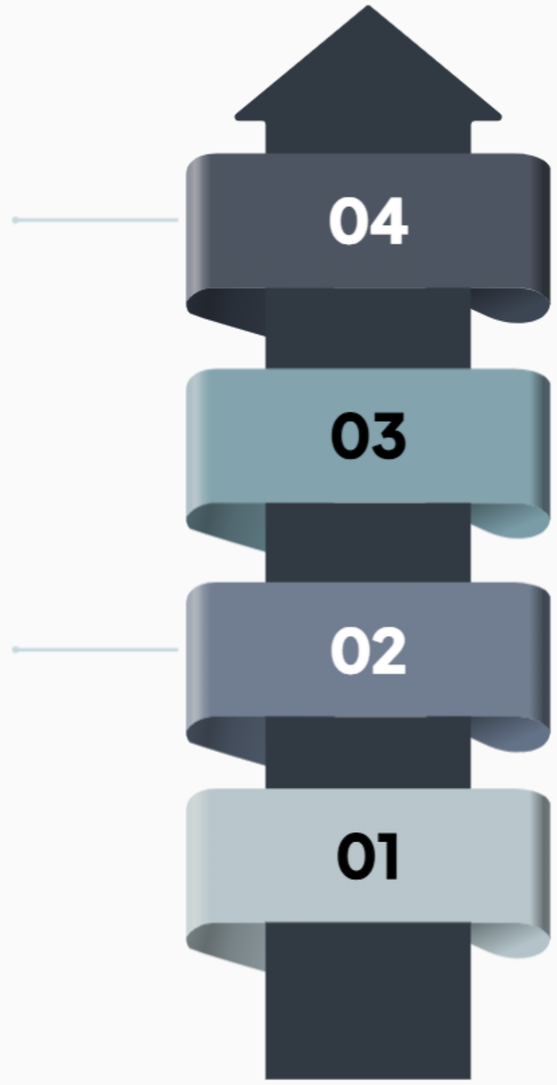
Overview of server roles and their placements

Cryptographic hashing

Employs cryptographic hashing to secure transaction data, making it tamper-proof and verifiable.

Tech examples

Notable blockchain technologies include Hyperledger Fabric, Go-Quorum, and Tendermint, each offering unique features.



Merkle Trees

Utilises Merkle Trees for efficient data verification, enabling quick checks of transaction integrity.

Secure storage of transactions

Blockchain provides a secure, immutable way to store financial transactions, ensuring data integrity and trust.

3. Authentication & User Access Solutions

Smart Ration Cards: NFC/QR-based

Utilises NFC and QR codes for offline user authentication for ration access.

Smartphone Apps for Transactions

Digital wallet applications allow transactions over a local area network (LAN).

Fallback Options for Authentication

Includes PIN and OTP via local SMS as backup authentication methods if supported.

4. Data Storage Model:

01 Blockchain Ledger

Stores immutable transaction records using Merkle Trees and cryptographic hashing.

02 SQL Database

Enables fast lookup for non-financial data, such as user profiles

03 Distributed Storage

Overview of the IPFS

Facilitates LAN-synced data sharing and intra-village communication.

User Authentication Management

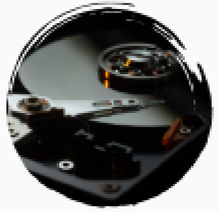
SQL databases are ideal for storing and managing user authentication data with secure access controls.

Ration Card Data Storage

Storing ration card information in SQL DB ensures structured data management and easy access for verification.

User Profiles Storage

SQL databases efficiently handle user profiles, enabling quick retrieval and updates as needed.

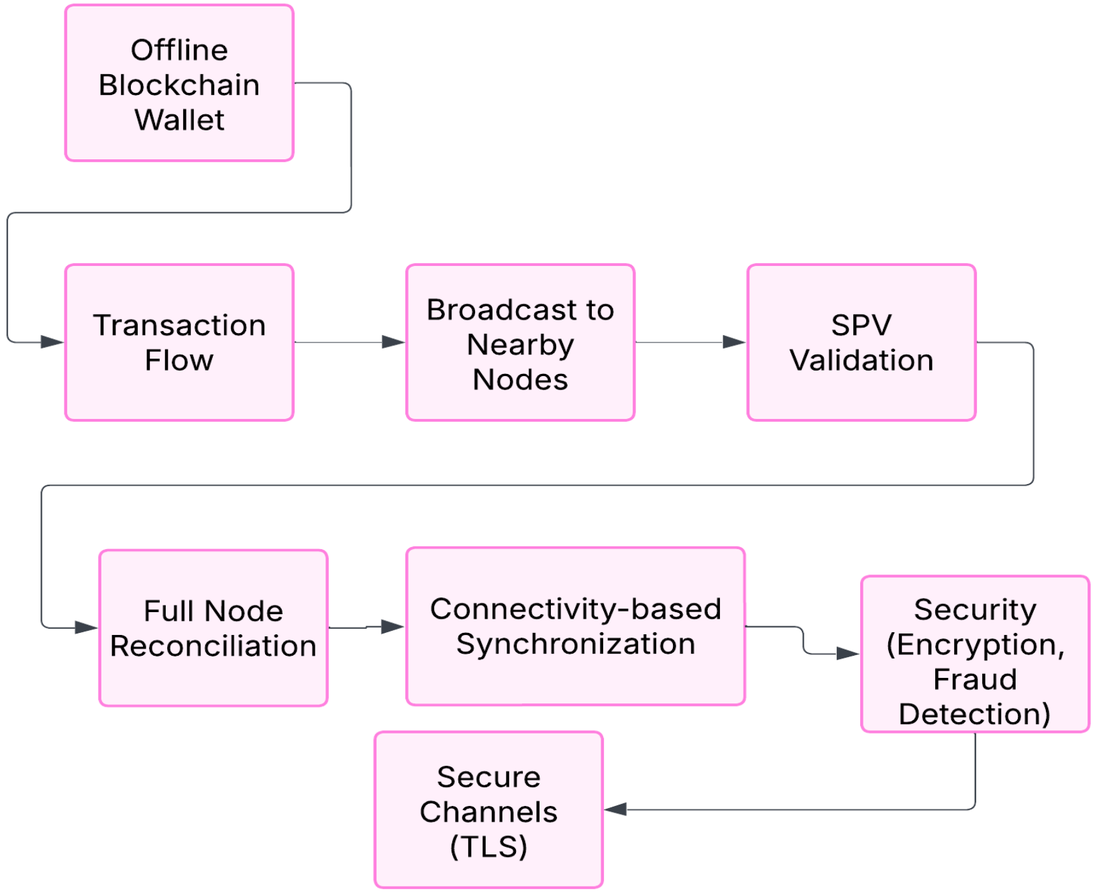


Speed of Query Processing

SQL databases provide fast query processing, essential for applications requiring real-time data access.

Workflow System Architecture

Understanding the Steps in the System Architecture



Workflow Pipeline Overview

Understanding the Steps in the Workflow Pipeline

User Registration & Authentication

The initial step where users create accounts and log in securely to access services.

Currency Issuance & Wallet Funding

Users receive currency and fund their wallets, enabling transactions within the platform.

Transaction Initiation at PoS

Users initiate transactions at Point of Sale (PoS) locations, marking the start of the transaction process.

Local Validation via Edge Node & Blockchain Entry

Transactions are validated locally by edge nodes before being recorded on the blockchain, ensuring security.

Receipt Generation & Local Storage

Upon successful transaction, receipts are generated and stored locally for user reference.

Data Synchronization When Online

When online, data is synchronized to ensure all transactions and information are up-to-date across systems.

Overview of Offline Blockchain Wallet

Exploring a secure and efficient digital wallet system

- **Offline Blockchain Wallet System**
  - A secure digital wallet operating offline, leveraging blockchain technology for transactions.
- **Security Benefits**
  - Offers robust security measures against hacking and fraud, ensuring user data protection.
- **LAN-based Networking**
  - Utilizes local area network for secure and efficient transactions without internet dependency.
- **Scalability**
  - Designed to grow with increased user demand, maintaining performance and efficiency.
- **Hybrid Blockchain Approach**
  - Combines features of both public and private blockchains
- **Offline Capability**
  - Allows users to conduct transactions without an internet connection, ensuring accessibility.

Realtime Usecase

Ramesh’s Offline payment journey

Understanding Ramesh’s Transaction Process

Setup: One-Time Preparation

Ramesh downloads the Offline Wallet App, registers, links bank account, and pre-loads digital rupees.

Initiating Offline Transaction

Ramesh scans Raju’s QR code and enters the amount for seeds using a local LAN connection.

Secure Offline Transaction Signing

Ramesh’s wallet signs the transaction and broadcasts it to nearby SPV nodes via local mesh network.

Local Validation Without Internet

Raju verifies the transaction signature and balance check offline before recording it locally.

Reconciliation When Internet is Back

The village server syncs with the main blockchain once internet is available, updating transaction records.

Raju Converts Virtual Currency

Raju redeems digital rupees for cash by connecting to the internet and withdrawing to his bank account.

Advantages

- **Simple Setup Process**

  Users easily set up a wallet and load virtual money while online.

- **Offline Payment Capability**

  Users can sign transactions and broadcast them locally without the internet.

- **Local Validation**

  Transactions are validated within a local area network, ensuring speed and security.

- **Syncing with Blockchain**

  Village server updates the main blockchain when it regains online connectivity.

- **Merchant Cash Out**

  Merchants can withdraw funds to their bank accounts when connected to the internet.

- **No Internet Required**

  Transactions can occur in remote areas without internet access, increasing accessibility.

- **Enhanced Security**

  Blockchain technology prevents fraud, making the system secure for users.

- **Remote Area Functionality**

  The mesh network allows the system to function effectively even in isolated regions.

Limitations

01 Battery & Device Dependency

Users need charged smartphones with sufficient storage for SPV nodes. Power outages in rural areas could disrupt access.

02 Physical Security Risks

While blockchain is secure, offline transactions could be vulnerable to double-spending attacks if malicious users exploit synchronization delays.

03 Delayed reconciliation

If too many transactions occur offline, the sync process could become slow, causing backlogs.

04 Banking System Dependencies

- Bank Liquidity Issues: If the linked bank faces cash shortages (e.g., rural bank runs), users cannot withdraw "virtual" money as real currency.
- Mitigation: Integrate multi-bank support or stablecoin backups.

05 Irreversible scams

Future Scope

01 Integration with IoT Devices

Enable payments via wearables (smartwatches) or NFC-enabled feature phones for users without smartphones

02 Decentralized Recovery

Allow users to recover wallets via social keys (e.g., split among trusted contacts).

03 Offline Dispute Resolution

Embed smart contracts for conditional payments (e.g., release funds only if both parties confirm post-sync).

04 Tamper-Proof Hardware

Distribute low-cost hardware wallets (e.g., NFC cards) for users without smartphones.

05 Insurance Partnerships

Offer micro-insurance against theft/fraud for offline transactions.

THANKYOU