TravelOK

Blockchain-Based Booking & Hospitality Review Platform

We're not selling crypto. We're fixing trust.

With a simple app backed by real-world tech, we can make Sri Lanka's tourism stronger, fairer, and smarter for both travelers and locals.

Team - Byte Chainers

Hashini Kaweesha Ranaweera

Vinu Kaveesha

Verosha Kriyanjala

Harith Maduranga

Table of Contents

1. What problems are we solving?

Traditional issues in Sri Lankan hospitality,

- High Online Travel Agency(OTA) fees – Hotels often pay 15–25% commission to Booking.com, Agoda, etc.
- Fake reviews – Manipulated or unverified feedback can damage trust.
- No Guest loyalty – Small/independent hotels can't offer cross-property rewards.
- Lack of transparency – Guests often don't know whether reviews are authentic or whether a property is legally registered or maintained.

2. Solutions we offer

2.1 Decentralized Identity for Hotels and Guests

- Each hotel/restaurant has a verifiable blockchain identity (DID – Decentralized ID).
- Registration is done once and recorded on-chain: name, license, ratings, payment address.
- This ensures only lawful businesses appear on the platform.

  Like a public digital registry for verified hotels.

2.2 Immutable Reviews

- Guests leave reviews as signed transactions linked to their stays (verified via smart contract).
- The review gets recorded permanently on-chain (or hashed and stored via IPFS).
  IPFS - Interplanetary File System (a distributed file storage protocol that allows computers all over the globe to store and serve files as part of a giant peer-to-peer network.)
- Hotel owners cannot delete, alter, or suppress reviews.

  This guarantees trust, because no central authority controls the data.

2.3 Tokenized Direct Booking System

- Guests pay in fiat or stablecoins (LKR-backed token or USDT).
- Smart contracts hold the deposit until check-in or post-stay confirmation.
- No need for OTAs, no 25% cut.
- Smart contracts can automatically,

    - Trigger cancellation refunds.
    - Release payments to hotel wallets.
    - Split income with agents or partners.

  Hotels get paid faster with less cost. Guests get more control and transparency.

2.4 Smart Loyalty / Tip Incentives

- The platform issues its own loyalty token.
- Guests earn tokens for,

    - Leaving honest reviews.
    - Booking directly.
    - Referring to others.
- These tokens can be,
    - Redeemed for discounts.
    - Tipped to staff.
    - Traded or staked.

2.5 Proof of Stay & Reputation

- Once a stay is completed, a "Proof of Stay" NFT or badge is issued to the guest.
- These can be reused for,

    - Building a travel reputation.
    - Earning higher-tier discounts or VIP benefits.
    - Proving experience for digital travelling visas.

  Guest trust and loyalty becomes portable and provable.

3. User-friendly app that allows

- Hotels to list rooms and accept bookings directly
- Guests to book rooms, leave verified reviews, and earn loyalty tokens
- All bookings, reviews, and tips are stored securely and transparently using blockchain

- Smart contracts reward users with tokens they can use for tips, discounts, or future travel

4. Market Plan

We keep the platform sustainable and scalable with multiple income streams:

- 2–5% booking fee (vs. 15–25% on OTAs)
- Hotel subscriptions for pro tools (analytics, marketing, loyalty)
- Boosted visibility and “verified” hotel badges (optional, paid)

5. Feasibility of our product

- Sri Lanka is rebuilding its tourism sector trust is key.
- Internet + mobile payments are growing rapidly.
- Government is open to innovation & blockchain trials.
- Travelers (especially Gen Z, digital nomads) care about authenticity and impact.

6. Tech Stack

Layer	Tool/Tech	Purpose
Smart Contracts	Aiken	On-chain Plutus V2 contract logic (bookings, reviews, reward logic)
Blockchain API	Blockfrost	Off-chain data fetch, wallet balances, tx details, asset metadata

Frontend SDK	Mesh SDK	Seamless wallet connection, transaction building/sending
Wallets	Lace, Eternal, Nami	User-side wallet integration
Metadata Store	IPFS + Arweave	Store review metadata, licenses, and hotel images
Backend Services	Node.js + PostgreSQL	Business logic, hotel/user profiles, admin dashboards

6.1 Microservices (with Cardano Integration)

Microservice	Cardano Integration	Purpose
Auth & Wallet Binding	Mesh SDK + Wallet APIs	Connect Lace/External wallet, store linked wallet address
Hotel Registry Service	Aiken + Blockfrost + IPFS	Onboarding verified hotels via DID, storing legal docs off-chain
Booking Service	Aiken smart contract + Mesh SDK	Booking contract to lock ADA/stablecoin until check-in; supports refund, split payout
Review Service	IPFS + Blockfrost + On-chain hash	Reviews signed by wallet, saved to IPFS, hash stored on-chain

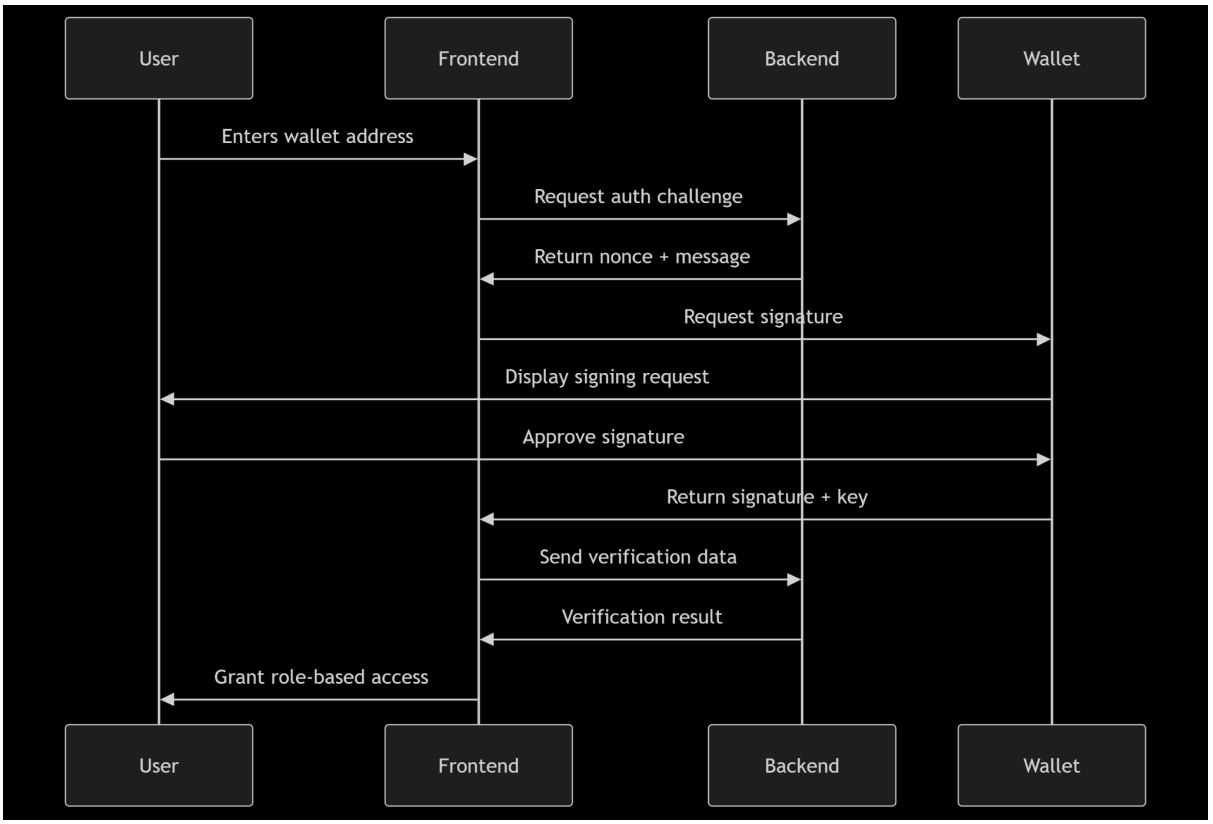
NFT Issuer Service	Aiken contract + Mesh SDK	Mint “Proof of Stay” NFT after stay confirmation
Admin Dashboard	REST API + Wallet Auth	Approve hotel applications, revoke listings, view flagged content

6.2 Functionalities of each microservice

6.2.1 Auth & Wallet Binding

The authentication system uses Cardano wallet addresses as decentralized identifiers (DIDs) for passwordless login. Users prove wallet ownership through cryptographic signing, eliminating traditional credentials. This enables,

- Non-custodial identity management
- Tamper-proof verification of wallet ownership
- Role-based access control (admin/traveler)
- Session-based authentication workflow



Core Components

1. Challenge Generation Service (/api/auth-challenge)
    - Validates Cardano address format (Bech32/hex)
    - Generates cryptographic nonce
    - Creates session with { address, nonce, timestamp }
    - Returns signable message,
        "Sign this message to authenticate: {nonce}"
2. Signature Verification Service (/api/verify-wallet)
    - Validates session expiration (5-minute TTL)
    - Verifies message matches original nonce
    - Executes cryptographic signature verification

```
verifySignature(
  address,
  signature,
  key,
  message
)
```

    - Returns authentication success/failure

3. Wallet Integration
    - Dynamic wallet detection via window.cardano
    - Multi-wallet support (Lace/Nami/Eternl/etc.)
    - Address verification against wallet's own addresses

4. Role Management
    - Admin wallet whitelisting
    - Automatic role assignment,

```
isAdmin = adminWallets.includes(walletAddress)
role = isAdmin ? 'admin' : 'traveler'
```

Security Measures

- HTTPS-Only - All endpoints enforce TLS
- Session Binding - Nonce tied to session ID
- Time Validation - 5-minute challenge expiration
- Signature Verification,

    - ❖ Cardano-Serialization-Lib for Ed25519 verification
    - ❖ CBOR decoding of COSE_Sign1 structures
    - ❖ Message integrity checking

Technical Stack

Component	Technology
Wallet interface	CIP-30 Standard
Cryptography	@emurgo/cardano-serialization-lib
Session Management	express-session
Message Encoding	CBOR
Security Headers	HSTS, CSP, X-Content-Type-Options

Error Handling

- Invalid Address - Format validation failures
- Wallet Connection - Browser extension detection
- Signature Rejection - User declines signing
-

- Session Expiry - 5-minute timeout enforcement
- Message Tampering - Nonce mismatch detection

This authentication system provides secure, decentralized identity verification while maintaining UX simplicity through wallet-based authentication.

6.2.2 Hotel Registry Service

The Hotel Registry Microservice is responsible for managing the registration and verification of hotels on the TravelOK platform. It allows hotel owners to register their business by submitting necessary metadata and documents. Admins can verify hotels, and verified hotels are linked to an NFT transaction recorded on Cardano.(This will be handled through NFT Issuer service)

Functionalities

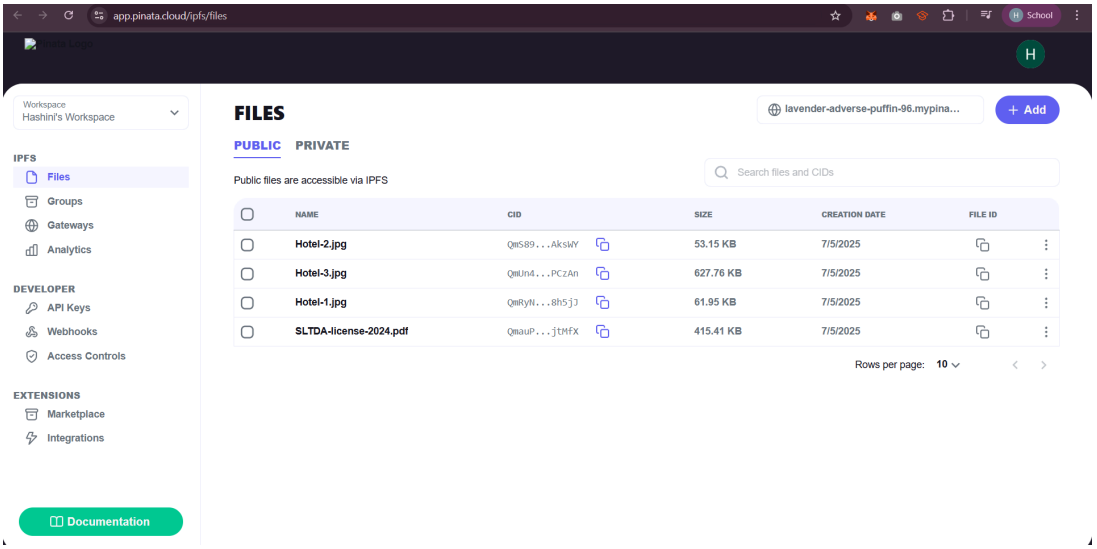
- Accept hotel registration data (name, location, documentations)
- Upload documents (license and images) to IPFS
- Store hotel records in MongoDB
- Verify hotels and record verification status
- Provide API access to list or filter hotels (all, verified, pending)

Tech stack

Component	**Tech Used**
Backend Framework	Node.js + Express
Database	MongoDB (Atlas)
Storage (Docs)	IPFS via Pinata
Blockchain	Cardano + Blockfrost API
Environment Mgmt	dotenv (`.env` file)

Sample API Flow

1. Hotel owner submits name, location, wallet + license + image
2. System,
    - Uploads license & image to IPFS



- Stores metadata in MongoDB


```
_id: ObjectId('686a23192e1adb5e3e9d18c8')
name : "Galle Face Hotel"
location : "2, Galle Road, Colombo 03, Sri Lanka 00300"
walletAddress : "addr_test1vzpwq95z3xyum8vqndgdd9mdnmafh3djcxnc6jemlgdmswcve6tka"
licenseIPFSHash : "QmauPcZ2aAtjEvxYsQbhjcywr8Uvf4W3rCB6Hr5KjjtMfX"
imageIPFSHash : "QmUn4CZLQqvrMsTJMn1SwvziCTNTbP6bDviYVfZ2APCzAn"
isVerified : false
createdAt : 2025-07-06T07:17:45.633+00:00
__v : 0
```


3. Hotel is in "pending" state

6.2.3 Booking Service

The Booking Microservice is responsible for managing hotel room reservations on the TravelOK platform. It handles booking creation, availability checks, date validations, and integrates with the Cardano blockchain to lock user funds through smart contracts until the booking is fulfilled or canceled. It also maintains booking records and provides endpoints to manage and retrieve bookings.

Create a booking

- Accept user input for hotel, room, check-in/check-out dates, number of guests.
- Validate availability based on date ranges.
- Generate and interact with smart contract on Cardano testnet for fund locking.
- Save the booking in the database with a status (pending, confirmed, canceled).

View bookings

- Get bookings by user
- Get bookings by hotel

- Get single booking by ID

Update booking status

- Mark booking as confirmed, canceled, or completed.
- Trigger fund release or refund from the smart contract (handled via blockchain integration).

Check room availability

- Validate whether a given room is available for the selected date range.

Tech stack

Component	**Tech Used**
Backend Framework	Node.js + Express
Database	PostgreSQL (Hosted in Aiven.io)
Storage (Docs)	IPFS via Pinata
Blockchain	Cardano + Blockfrost API
Environment Mgmt	dotenv (`.env` file)

Future Work

- **Plutus Smart Contract Deployment**
    - Transition from testnet Aiken scripts to production-ready **Plutus V2 smart contracts**.
    - Full deployment of booking logic on-chain (e.g., using `TxBuilder`, `Plutus script address`, `Datum/Redeemer` models).
    - Allow booking finalization and cancellation purely via blockchain transactions.

6.2.4 Review Service

The Review Microservice is responsible for handling guest reviews of hotels on the TravelOK platform. It enables verified users to submit feedback and ratings after a completed stay. Each review is stored on IPFS for immutability and referenced on the Cardano blockchain for verifiability. This service manages review submission, validation, storage, retrieval, and blockchain registration.

Submit a review

- Accept user input including hotel ID, rating, review content, and guest wallet address.
- Validate if the guest has a confirmed booking for the hotel (optional: Proof-of-Stay check).
- Upload the review JSON to IPFS via Pinata.
- Create a metadata transaction with the IPFS CID and record it on the Cardano blockchain using Lace wallet or a backend wallet (testnet/mainnet).
- Save the review in the database with metadata: `reviewCID`, `walletAddress`, `txHash`, `rating`, `timestamp`.

View reviews

- Get reviews by hotel.
- Get reviews by user wallet.
- Get single review by ID.
- Fetch and display original review content from IPFS using the stored CID.

Verify review authenticity

- Use stored `txHash` to verify the on-chain metadata.
- Check if the review was submitted from the same wallet used during booking.
- Optionally show badges or NFT rewards if integrated.

Tech stack

Component	**Tech Used**
Backend Framework	Node.js + Express
Database	Mongo DB
Storage (Docs)	IPFS via Pinata
Blockchain	Cardano + Blockfrost API
Wallet Interaction	Lace Wallet + Mesh SDK (Frontend)
Smart Contract TX	Lucid (for backend wallet TX signing)
Environment Mgmt	dotenv (`.env` file)

7. Future Work

- NFT minting on verification

  Automatically mint an NFT on the Cardano blockchain for verified hotels. NFT will include hotel metadata(name, wallet, license hash, image hash) and viewable on Cardano explorers

- Admin Dashboard

  Dashboard UI to preview IPFS docs before verification. Display NFT mint status, link to blockchain explorer.

- Notifications & Webhooks

  Notify hotel owners on registration status via email or wallet alerts.Webhooks for when hotels are verified or NFTs are minted.

- Hotel Profile page with reputation metrics

  Reputation score derived from reviews, bookings, proof-of-stay NFTs.Display average ratings, total verified stays, loyalty engagement.