SOFTWARE REQUIREMENTS SPECIFICATION

Organic Food Traceability System Using Blockchain

Project Title: Organic Food Traceability System Using Blockchain

Developed by-

DEVNEST

Department: CSE(IOT CS BT)

Date: 31/07/2025

Table of Contents

1. Introduction

1.1 Purpose

Defining the requirements and specifications for the creation and deployment of a "Organic Food Traceability System Using Blockchain" is the aim of this document. By ensuring strong, impenetrable traceability throughout the organic food supply chain, this system seeks to improve operational efficiency, transparency, trust, and regulatory compliance. By enabling them to transparently confirm the origin and authenticity of organic food products, it caters to the needs of producers, certifiers, distributors, retailers, and most importantly, consumers.

1.2 Scope

This project offers a comprehensive way to track the flow and change of organic food items through every phase of the supply chain:

1. **Farm**
   Product creation, batch tracking, and initial certification.
2. **Processing**
   Batch updates, processing, packaging.
3. **Logistics**
   Tracking transport, warehousing.
4. **Retail**
   Product arrival, sales.
5. **Consumer**
   Verification of product origin and authenticity via QR code scanning.

Farmers, processors, distributors, retailers, regulatory agencies, certification authorities, and final consumers are all considered stakeholders. For safe and decentralized event recording, the system will be offered as a web and mobile application with backend integration into a permissioned blockchain.

1.3 Definitions, Acronyms, Abbreviations

- **Blockchain**: A distributed ledger technology that maintains transparent, decentralized, and unchangeable records of transactions.
- **Traceability:** The capacity to track a food product's processing and movement through the entire supply chain.
- **QR Code (Quick Response Code):** A machine-readable, two-dimensional code that contains product-specific information for traceability is called a QR code.
- **Certification Authority (CA):** An organization that verifies and certifies organic compliance at different phases is known as a Certification Authority (CA).
- **Batch:** A grouping of product units for supply chain tracking; they may be divided or combined depending on processing.
- **Regulator:** The government or legal body in charge of ensuring the safety and quality of food.
- **Stakeholder:** Anybody participating in the supply chain, including producers, certifiers, handlers, etc., is considered a stakeholder.2. Overall Description
-

2.1 Product Perspective

The supply chain for organic food will be supported digitally by the traceability system. Data fragmentation, a lack of transparency, and ease of tampering are the results of existing practices, which are usually paper-based or employ siloed digital systems. The suggested solution makes use of blockchain technology to guarantee:

Immutable event logging

for every batch/product.

Real-time data sharing

between all participants.

Rapid consumer verification

at point-of-sale.

Integration:

- Can connect to old supply chain software and certification platforms using APIs.
- Can be used as both software as a service (SaaS) for small businesses and on-premises for big businesses.

2.2 Product Functions

Key functions provided by the system are:

1

Stakeholder registration and authentication

Secure, role-based onboarding of all chain participants.

2

Batch creation and lifecycle management

Each organic product batch is registered at the farm and tracked through splits, merges, processing, transport, and sale.

3

Immutability of events

Every supply chain event (harvest, certification, transfer, sale) is cryptographically recorded to the blockchain for proven authenticity.

4

Certification document management

Upload, verify, and link organic/food safety certificates with each batch.

5

QR code generation and assignment

Unique QR codes for each product/batch, encoding blockchain event IDs and summary trace data.

6

Consumer verification interface

Publicly accessible web/mobile page for consumers to instantly verify product origin, journey, and certification by scanning QR.

7

Administrative controls

Monitoring, reporting, and analytics tools for regulatory authorities and system admins.

2.3 User Classes and Characteristics

- **Farmers:** Enter information about crops and harvests, start batches, ask for certification, and keep track of product transfers. Usually, they need a simple mobile interface and the ability to use their own language.
- **Processors/Manufacturers:** Update product state, split/merge batches, upload processing certificates.
- **Distributors/Retailers:** Distributors and retailers should keep track of when they ship, receive, and store things, and they should also update the locations of their batches.
- **Certification Authorities:** Check certification requests, upload scanned documents, and approve or deny organic claims.
- **Consumers:** Use mobile or web interfaces to scan QR codes and see full product histories in formats that are easy to read and understand.
- **Admin users (system, regulatory):** Keep an eye on user accounts, set up the system, and make reports for compliance and audits.

2.4 Operating Environment

- **Front-end platforms (Web and Mobile):** Web (built with React.js or Angular) and a cross-platform mobile app (built with Flutter or Kotlin for Android).
- **Backend/API Layer:** Node.js or Python REST API—handles user requests, checks data, and talks to the blockchain and databases.
- **Blockchain Network:** A permissioned blockchain like Hyperledger Fabric or, optionally, a private Ethereum instance for keeping records that are secure, controlled, and easy to audit.
- **Database:** For storing data that isn't on the blockchain, like user profiles and cached summary data, we have to use NoSQL (MongoDB) or relational (PostgreSQL) databases.
- **Hosting:** Deployed on cloud services (AWS, Azure) or the institution's own datacenter for sensitive or local data needs.

2.5 Design and Implementation Constraints

- **Security Compliance:** Encryption is required for all user information, certificates, and event logs both during transmission and storage.
- **Privacy Regulations:** Made to comply with the GDPR in Europe, the FSSAI in India, and other comparable food and data privacy laws across the globe.

- **Scalability & Performance:** Needs to be able to manage thousands of users at once and real-time blockchain writes while keeping response times short (less than three seconds for trace-back queries).
- **Offline Support:** Users, particularly farmers, must be able to enter data offline; synchronization should happen automatically as soon as device connectivity is restored.
- **Localization:** Multilingual support and user-friendly visual interfaces for users with limited literacy.

3. Specific Requirements

3.1 Functional Requirements (FR)

- **FR1:** All user types (farmers, processors, certifiers, distributors, retailers, admins) can register and log in with authentication/authorization based on their role.
- **FR2:** Farmers can create new product batches, add harvest details, request certification, and initiate product transfer events.
- **FR3:** Processors/Manufacturers can split/merge batches as per processing steps, attach certificates, and update batch status.
- **FR4:** All events (creation, certification, transfer, receipt, storage, sale) must be cryptographically committed to the blockchain.
- **FR5:** QR codes must be generated for each product and batch, linking to full trace data retrievable from blockchain logs.
- **FR6:** Certification documents can be securely uploaded, validated by certifiers, and permanently linked with batch histories.
- **FR7:** Consumers can scan a QR code and immediately view a human-readable product journey (farm, certification, processing, retail, etc.) with attached certifications.
- **FR8:** System administrators must be able to monitor logs, user activity, and generate traceability/compliance reports.

3.2 Non-Functional Requirements (NFR)

- **NFR1:** System must provide at least 99.9% uptime, with robust disaster recovery for all critical data.
- **NFR2:** Any product trace request from the consumer must respond within 3 seconds under expected peak load.
- **NFR3:** All transmissions and data (including those on the blockchain) must use strong encryption (e.g., TLS, AES-256).

- **NFR4:** The system must be fully responsive—work on all current browsers, tablets, and modern smartphones.
- **NFR5:** System operations (even by non-technical users) should require no more than 30 minutes training.

3.3 External Interface Requirements

3.3.1 User Interface

- **Dashboards:** Intuitive dashboards for all roles—showing key actions, alerts, and batch status.
- **Traceability UI:** Consumer-facing single-page view of a product's journey (with clickable/expandable events and image of certification).

3.3.2 Software Interfaces

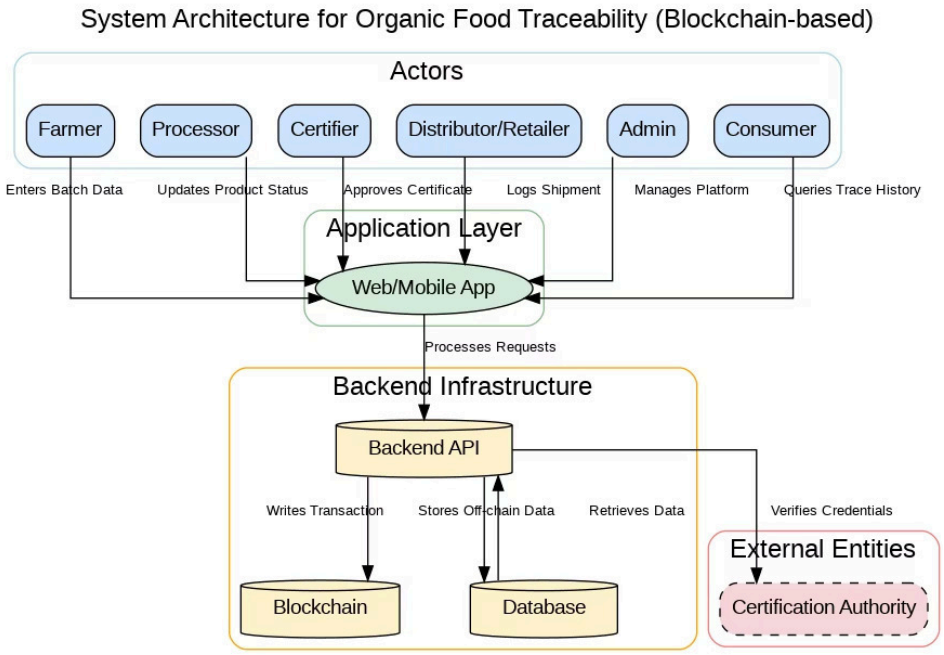
- **REST APIs** for external platform integration (government certification sites, ERP/SCM solutions, etc.).
- **Blockchain node** (Hyperledger/Ethereum) APIs for system-side event commitment and retrieval.
- **Notification integrations** (SMS, email, WhatsApp) for important status changes.

3.3.3 Hardware Interfaces

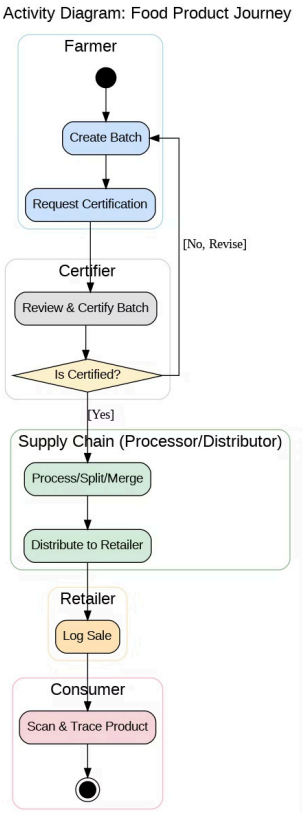
- **QR code/scanner interface** support for mobile/tablet devices.
- **(Optionally) Thermal printer compatibility** for on-premise QR code label generation.

4. System Models

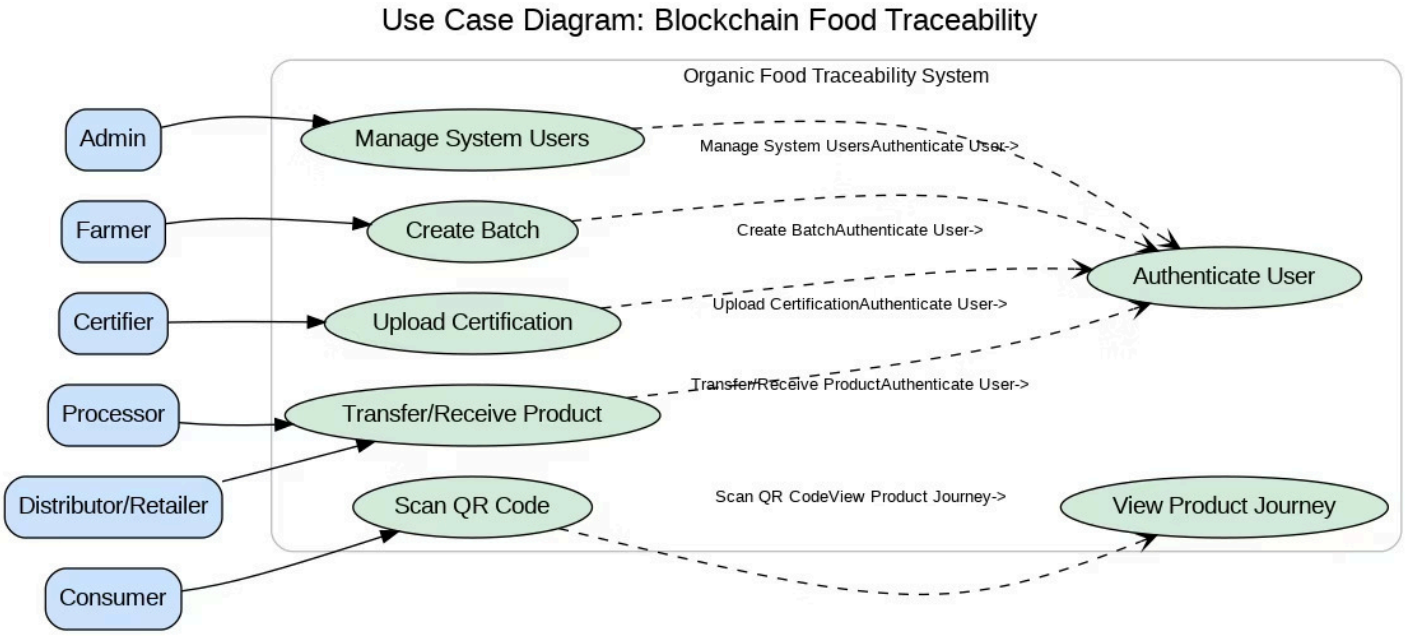
4.1 Architecture Diagram



4.3 Activity Diagram



4.2 Use Case Diagram



5. Appendices

5.1 Tools Used

- **Frontend:** React.js / Angular for web app Flutter / Kotlin for mobile app
- **Backend/API:** Node.js or Python (Django/Flask/FastAPI)
- **Blockchain:** Hyperledger Fabric (preferred for enterprise/consortium) (OR) Ethereum (private/consortium network)
- **Database:** MongoDB (JSON/event store) OR PostgreSQL (relational)
- **QR Code:** Open-source generation/decoding libraries, e.g., qrcode.js for web, Zxing for mobile apps
- **Hosting:** Amazon Web Services (AWS) Microsoft Azure (OR) On-premise VM/cloud for regulated deployments

5.2 Dataset

For pilot/prototyping: Use simulated or open datasets:

- Example: Food and Agriculture Organization (FAO) supply chain data
- Sample organic crop records from local government/NGO trials
- Data fields: (Batch ID, Product Type, Origin Farm, Harvest Date, Certification Status, Event Timestamps, Actor Logs, etc.)

Real-world deployment: Data from participating co-operatives, certification bodies, or public domain spice/fruit traceability datasets.

5.3 SDG Goals Supported

SDG 2: Zero Hunger

Ensures food safety, reduces fraud, increases trust in organic labeling.

SDG 9: Industry, Innovation, and Infrastructure

Integrates advanced IT (blockchain, web/mobile, cloud) into agriculture & food sectors.

SDG 12: Responsible Consumption and Production

Enables consumers to make informed choices and supports compliance with ethical and sustainability practices.

5.4 References

Technical Standards:

- GS1 (Global Standards 1) for food traceability
- ISO 22005:2007 Food traceability standard
- IEEE 2410-2019, Blockchain technology overview

Key Papers & Reports:

- Tian, F. (2016). An agri-food supply chain traceability system for China based on RFID & blockchain.
- Galvez, J.F., et al. (2018). Future challenges on the use of blockchain for food traceability analysis.
- Casino, F., et al. (2019). Blockchain-based food supply chain traceability system: A survey.

Web Resources:

- IBM Food Trust blockchain platform whitepapers
- FAO Guidelines on food traceability
- FSSAI (India) regulations and circulars
- European Union General Data Protection Regulation (GDPR)
- (Add your own country/local standards as relevant.)