ISSN 2278-2540 | DOI: 10.51583/IJLTEMAS | Volume XV, Issue V, May 2026

Bio Trace - A Blockchain and IPFS Based Traceability Platform for Secure Ayurvedic Herb Supply Chains

Mrs. CH. Sudha[1], P. Sarayu Rajkumar[2], K. Nidhish Dharma[2]

[1]Assistant Professor, IT Department, Mahatma Gandhi Institute of Technology Hyderabad, Telangana

[2]Student, IT Department, Mahatma Gandhi Institute of Technology Hyderabad, Telangana

DOI: https://doi.org/10.51583/IJLTEMAS.2026.150500031

Received: 02 May 2026; Accepted: 06 May 2026; Published: 25 May 2026

ABSTRACT

Ensuring transparency, authenticity, and regulatory compliance in Ayurvedic herb supply chains remains a major challenge due to the use of centralized and fragmented tracking systems. Traditional approaches are vulnerable to data tampering, poor traceability, and lack of trust among stakeholders. This paper proposes BioTrace, a blockchain and IPFS-based traceability platform designed to provide secure, transparent, and immutable tracking of Ayurvedic herbs from harvesting to consumer delivery. The system integrates Hyperledger Fabric for decentralized transaction management, Inter Planetary File System (IPFS) for tamper-proof document storage, and role-based access control for secure stakeholder interaction. Bio Trace supports automated compliance verification using geo-fencing, seasonal validation, species verification, and laboratory quality metrics. QR-code based consumer verification enables end users to access complete batch provenance information.

Index terms - Blockchain, Supply Chain Traceability, Ayurvedic Herbs, IPFS, Decentralized Storage, Role-Based Access Control, QR Code Verification.

INTRODUCTION

Voluntary supply chains that are both visible and verifiable has become a major need in the past few years especially in the industry where producers of raw materials have a direct implication on human health. One of such areas is the Ayurvedic medicine industry, the medicinal properties of a certain product are purely determined by the purity of the ingredients, the circumstances under which they were picked and the quality followed during the processing and distribution. The consumers who buy Ayurvedic products expect to be assured that whatever is written in the label matches what is in the pack. Regulators insist that documented records should be presented to show that all batches must have gone through certified areas, undergone laboratory tests, and met set quality standards before they can be introduced in the market. The companies that have businesses in this space require responsible records that will help them to withstand legal responsibility, recall and prove to be obedient during audits.

Nevertheless, the increasing requirement is accompanied by the fact that traditional supply chain systems used in the Ayurvedic industry still use centralized databases and manual records. Historical records held in disconnected systems by various stakeholders at the farm, at the processors, at the laboratories, at the distributors and at the retailers are seldom harmonized and then it becomes hard to create a comprehensive and reliable history of a particular batch. Storing data in a centralized way creates a single point of failure, in which information may be changed, lost or modified without being noticed. Paper records are susceptible to human errors, time wastage and inconsistency especially when records change hands of various individuals in

ISSN 2278-2540 | DOI: 10.51583/IJLTEMAS | Volume XV, Issue V, May 2026

different geographical regions. Such weaknesses leave loopholes in accountability that may be used either with the ulterior intention of adulteration or without any such intention but with negligence.

However, the results of these issues should not be taken lightly, as there have been cases of Ayurvedic medicine being linked to adverse health conditions due to contaminants and false labelling of products. It is also very difficult for the relevant authorities to trace the cause of the problem with the batch of Ayurvedic medicine. This has led to widespread adverse health conditions among the populace. The farmer who has been adhering to the quality standards has no means of differentiating his products from those of the farmer who has not. This eliminates the motivation for quality adherence. The consumer also has no means of verifying the claims made on the label of the Ayurvedic medicine. This makes him totally dependent on the integrity of the participants of the supply chain.

To overcome the structural challenges that are a part of the Ayurvedic supply chain, modern technology has been seen to be a viable option for enhancing the level of trust that is associated with the supply chain systems that are currently in place. The blockchain, which was initially developed for the purpose of transactions for the financial industry alone, has been seen to be extremely viable for supply chain management with the inherent properties that are a part of the blockchain. Once data is written to the blockchain, it cannot be changed without the entire chain of data that follows being considered invalid, thereby making any attempt at data tampering extremely easy to detect. The data that is written to the blockchain is not stored anywhere; therefore, it is not possible for any one entity to attempt to delete the data that has been written to the blockchain, as that would imply that the participant would have access to the blockchain itself, which is not possible due to the decentralized nature of the blockchain.

Complementing blockchain for data integrity, the InterPlanetary File System is an approach to storing large files such as laboratory certificates, quality reports, images of products in a decentralised way. Unlike normal file storage where a URL points to a server that can be taken offline or have its contents changed, IPFS refers to files by their content hash. This means that a link to a certificate stored on IPFS will always return exactly said certificate, or nothing at all -- it cannot silently return a different document. This property makes IPFS very suited to storing the documentary evidence of the compliance claims of regulated industries.

This paper introduces BioTrace - an integrated web-based platform made to integrate these technologies in a practical system for Ayurvedic herb supply chain. BioTrace simulates the supply chain as a sequence of batches and events, where each batch of product would stand for a specific quantity of a specific herb species, and each event would stand for a recorded action taken on a batch at a specific time. This system covers the entire ide-to-pharm process of a herb from when it is plucked from the field, processed, tested in the lab, packaged, shipped and sold. Every event is recorded with a timestamp, the identity of the actor responsible, the geographic location of the event and documentation supporting the event, if any, uploaded to IPFS.

Compliance checking is not a separate audit process but an integral part of the platform. Each batch is automatically evaluated against a list of regulatory parameters including geo-fencing parameters to ensure that the harvest location is within acceptable agriculture zones, seasonal restrictions ensure that the herb was harvested during the appropriate time of the year, species conservation parameters ensure that the herb is in the list of approved species to be harvested commercially and quality parameters flag batches with pharmaceutical manufacturing performance concerns that were produced under laboratory reported parameters for purity, moisture content or ash content outside of approved ranges. When a violation happens, it can be seen instantly by regulators via a special compliance monitoring interface with levels assigned to the severity to help prioritize the response.

The main contributions of this work are:

1. Design of a blockchain-based traceability framework for Ayurvedic herbs.

ISSN 2278-2540 | DOI: 10.51583/IJLTEMAS | Volume XV, Issue V, May 2026

2. Integration of Hyperledger Fabric and IPFS for secure storage and immutable audit trails.
3. Automated compliance verification using geo-fencing and quality metrics.
4. QR-code based consumer transparency mechanism.
5. Role-based access control for different supply chain stakeholders.

Related Work

Tiago M. Fernandez-Carames et al. [1], is an advanced warehouse management system using UAVs (drones) and blockchain technology. The drones automate the inventory monitoring process by scanning goods in real-time, while blockchain ensures the security of each update made so there is no issue or any doubt in the accuracy and traceability. This reduces human error and creates more efficiency in the industry 4.0 environment. However, the system is high in investment, has high reliability of network connectivity and complex infrastructure, which restricts its practical adoption.

Devraj V. Rajput et al. [2], the study deals with applications of blockchain in the food supply chain for better transparency, traceability and sustainability. By documenting all steps of the supply process on an immutable ledger, this helps prevent fraud, ensure product authenticity and help to build trust from consumers. It also promotes ethical sources of production. However, use of such systems is difficult because of high implementation costs, integration complexity, and resistance to change.

C. Vijj et al. [3], this research aims at the application of smart contracts on automating supply chain operations. These contracts automate predefined actions based on conditions without incurring much manual intervention, delays and errors. The approach is useful in improving the efficiency and authenticity of data across transactions. Despite these benefits, the system has issues with scalability when working with large files of transactions, and also risks for security if contracts are not carefully designed.

Sidra Malik et al. [4], the authors propose PrivChain, a blockchain-based framework for achieving secure traceability services while maintaining data privacy. Unlike traditional systems, it enables sensitive business information to be held in confidence, yet with transparency maintained in those places where it needs to be. This makes it suitable for supply chains that require privacy. However, the approach leads to an increase in the computational overhead and adds complexity in system design and implementation.

Peng Zhao et al. [5], in this paper proposes a blockchain-based traceability model that helps improve data integrity and visibility between supply chain participants. It handles the access of consistent tamper-proof data to all interested parties, which will result in better coordination and trust. While effective in strengthening transparency, the model suffers from a lack of scalability for applicability in large systems, and the check and good enough monitoring of supply chain activities in real time.

Zibin Zheng et al. [6], this study is a comprehensive overview of the blockchain technology and its application in many different sectors, including supply chains. On the one hand, it highlights how blockchain leads the way to better transparency, decentralisation and security, which makes it valuable for the purposes of tracking and verification. However, the paper also highlights some important limitations like issue of scalability, slow transaction speeds, or high energy consumption that are limiting widespread adoption.

Marco Conoscenti et al. [7], the research is focused on the use of the blockchain in achieving better trust and verification of data in supply chains. By keeping a shared and unaltered ledger, it ensures that all the stakeholders are working on the same verified information that will reduce disputes and enhance collaboration. However, the complexity of the system and the challenge of integrating it with existing infrastructure are still significant challenges.

ISSN 2278-2540 | DOI: 10.51583/IJLTEMAS | Volume XV, Issue V, May 2026

Kamanashis Biswas et al. [8], in this paper a framework for secure data sharing in distributed systems is proposed which can be used in supply chains, and is based upon blockchain. It enhances the data protection, prevents unauthorized access, and ensures the integrity of data. But these improvements to security often come with tradeoffs, such as increased latency and heightened computational resources requirements.

Feng Tian. [9], the blockchain technology is coupled with the radio frequency identification systems to develop a powerful solution for food traceability. RFID tags take product information in their data automatically at each stage, and blockchain keeps this data secure and unable to alter. This has the positive effects of improving tracking efficiency and food safety. However, it is a system that needs a lot of investment in the set-up of the infrastructure for the use of RFI as well as the technological aspects.

Dylan Yaga et al. [10], this paper provides a detailed overview of the basics of blockchain, including blockchain architecture, consensus mechanisms, and security features. For supply chains and other areas, it comes down to explaining how blockchain can be used for secure and transparent data management. At the same time, it points out some key challenges like scalability limitations, regulations, absence of standardization, etc.

METHODOLOGY

Farmer → Processor → Lab → Regulator → Consumer

Step 1- User registration and role assignment

Each agent involved in the supply chain registers on the platform and is given a function: farmer, processor, laboratory, regulator or consumer. Role assignment defines what modules, types of events and data fields are available to that user. Permissions are stored in the user record and enforced at any point for any API endpoint.

Step 2 - Creation of a Batch by Farmer

A registered farmer triggers the traceability process by establishing a new batch of the herb. Farmer supplies data of herb species, quantity, unit, date of harvest and the harvest location coordinates. On submission, the system validates all the fields, and performs a preliminary compliance check that includes geo-fencing, seasonal rules, and writes the batch record to the MongoDB system. Simultaneously, a block chain transaction of type CREATE_BATCH is created, mined into a new block and the resulting block hash and transaction ID are stored against the batch record. The batch is now live in the system with its own one of a kind batch id.

Step 3 - Supply Chain Event Recording

As the batch progresses through the supply chain, individual stake holders log their activity as an event against the batch ID. A processor logs processing event with location & description. A recording of a lab test event is made by a user in the laboratory and can upload a certificate file. Each event subdivided passes through the input validation process, authorization check and business rule check before being written in the events array of the batch in the Mongo database. A corresponding blockchain transaction of type ADD_EVENT is mined with the batch linked together.

Step 4 - Upload Certificate to IPFS

When a laboratory user submits a lab test event along with a certificate file, the server reads the file from the temporary upload directory, calls the Pinata API to email the file to the IPFS and, in return, it receives a content hash. This hash is saved in the event record and the batch record. The frontend write a direct link to access the file stored on the IPFS gateway and any authorized user can open this link by authenticated users and verify original certificate.

ISSN 2278-2540 | DOI: 10.51583/IJLTEMAS | Volume XV, Issue V, May 2026

Step 5 - Quality Metrics Submitting and Evaluating Compliance

When a lab user runs a quality test event the following are included in the request: purity, moisture content and ash content values. The server parses these values and stores them in the quality metrics fields of the batch, and immediately performs a complete evaluation of compliance. The evaluation verifies the validity of geo-fencing (using haversine distance calculations and comparing against approved zone coordinates), seasonal validity (comparing the harvest month), species approval (checking against a predefined list of species) and quality thresholds (checking against the submitted metric values). The result - pass or fail for each dimension - is stored to the batch compliance status record with a list of specific violation descriptions. This update is used by the direct update of the database to make sure that the result is persisted without any interference from any middleware.

Step 6 - Regulatory Compliance Monitoring by Regulator

Regulators have access to the compliance monitoring dashboard, which is used to query all the batch records and aggregate the compliance outcome. Non-compliant batches are displayed in a violations table ordered by last updated giving the batch ID, Violation description, Severity level and date. Severity is determined by violation type with quality violations labelled critical, geo-fencing and species violations labelled high, and seasonal violations labelled medium. The dashboard refreshes automatically, so the regulators see the state should not have to refresh the page.

Step 7 - QR Code generation and consumer verification

Once a batch is created, a QR code (encoding the batch id) is created and linked to the batch record. This QR code can be printed on the packaging of the product. When the consumer scans the QR code using the platform's scanner, the system fetches the complete batch record with all the events, compliance status, and IPFS certificate links and the platform presents it in a readable timeline. The consumer can check the origin of the herb, the laboratory results, and if the batch passed all the compliance checks, without any account and login requirements.

Step 8 - Blockchain used for Verification

At any given point, any user who has access to the Blockchain Explorer is able to see the list of all the blocks that have been mined, as well as the hash of each block, the hash of the block before it, and the transactions that are in each block. The validity of the chain is continually checked by re-computing the hash of each block and checking that it is as stored and that each block has the correct reference for its predecessor. This provides a separate proof that the recorded history of the supply chain has not been tampered with since it was written.

II. Proposed Architecture

The proposed system uses a four-tier distributed architecture to help provide transparency, immutability, and role-based access throughout the Ayurvedic herb supply chain. The architecture combines a React-based frontend, a node JS/express backend, a permissioned blockchain network using Hyperledger Fabric along with a hybrid storage layer that contains MongoDB and IPFS. Each tier is designed to promote certain functional and non-functional requirements of the traceability system, respectively.

Architectural Layers

i. **Presentation Layer:** The frontend layer is built using React 18 with Tailwind CSS as a means of rendering a responsive UI, and Zustand being a small state management. It connects with the backend using Restful API using Axios and gets real-time updates using Socket.IO. The interface is dynamically adapted according to the role that the authenticated user has, so that the interface only renders the features and data

ISSN 2278-2540 | DOI: 10.51583/IJLTEMAS | Volume XV, Issue V, May 2026

that are relevant to be used by that stakeholder.

ii. **Application Layer:** The backend is developed on the Node.js platform using the Express.js framework. It represents the central orchestration layer, which covers authentication with the help of the JWT, password hashing with bcrypt, and role-based authorization middleware. It exposes the batch management, events tracking and QR code operations, compliance reporting and blockchain queries through the exposed endpoints to the users using the Rest. Socket.IO is built-in for broadcasting of real-time events on connected clients.

iii. **Blockchain Layer:** Implementation of the blockchain is the permissioned distributed ledger system for enterprise supply chain applications. The network contains a single organization, one node for consensus and one node for transaction endorsement and ledger maintenance. The smart contract is coded in the Go programming language and deployed on the herb-channel recording all batch creation and lifecycle events in an un-manipulable transaction.

iv. **Storage Layer:** A mix of storage strategy is used. MongoDB stores mutable application data such as user profile, batch metadata, event logs, etc. MongoDB supports fast querying and indexing capabilities. IPFS - by way of the Pinata gateway is a storage for large off-chain artifacts such as quality certificate, compliance documents, and laboratory reports. Files stored onto IPFS are referenced on-chain by the content hash, allowing it to have tamper-evidence without ledger bloat. The API Server Layer is also based on Node.js using the Express module as the primary hub to communicate between the client and all of the back-end systems. It does the request processing, enforces authentication with the help of the middleware of the JSON Web Tokens, applies permission every time at every endpoint according to the roles of the users, validates all the incoming data, manages file uploading with Multer middleware, coordinates the logic that handles the evaluation aberrations whenever new batch or quality data is submitted.

System Data Flow

When an action is initiated by a stakeholder, the request will come from the React frontend and is sent over secure type http to the Express backend. The backend performs validation, business logic and persistence of relevant metadata to the MongoDB. At the same time, the blockchain service builds and sends a transaction to the Hyperledger Fabric peer which endorses and commits the transaction to the herb-channel ledger. For document-heavy operations, content of files will be uploaded to IPFS and the content-addressable-hash of these files will be stored on-chain. Clients that are connected and successfully confirmed transaction real-time notification are pushed to all connected clients using socket.io.

Role-Based Access Control

The system enforces a multiple role access control model in order to restrict operations based on stakeholder identity. A summary of the roles and their respective permissions is given in the table I.

Table I: Role Based Access Control Matrix

Role	**Permissions**
Farmer	Create batches, add harvest events
Processor	Add processing and transformation events
Laboratory	Submit quality test results and certifications

ISSN 2278-2540 | DOI: 10.51583/IJLTEMAS | Volume XV, Issue V, May 2026

Regulator	Access compliance reports and complete audit trail
Retailer	Add events related to retail and distribution
Consumer	Read-only access to batch provenance history

Compliance Verification Mechanism

Each batch of herbs undergoes an automated compliance validation on the backend before a transaction gets on to the blockchain. The validation checks include: (i) geo-fencing of the geo-location of harvest to check if it falls within permitted geographical boundaries (ii) seasonality restriction enforcement by species specific harvest window (iii) quality threshold check related to purity percentage, moisture content, ash content (iv) species identity check by database of registration. The resulting compliance status is recorded on-chain which gives regulators an immutable and auditable compliance trail for each batch in the system.

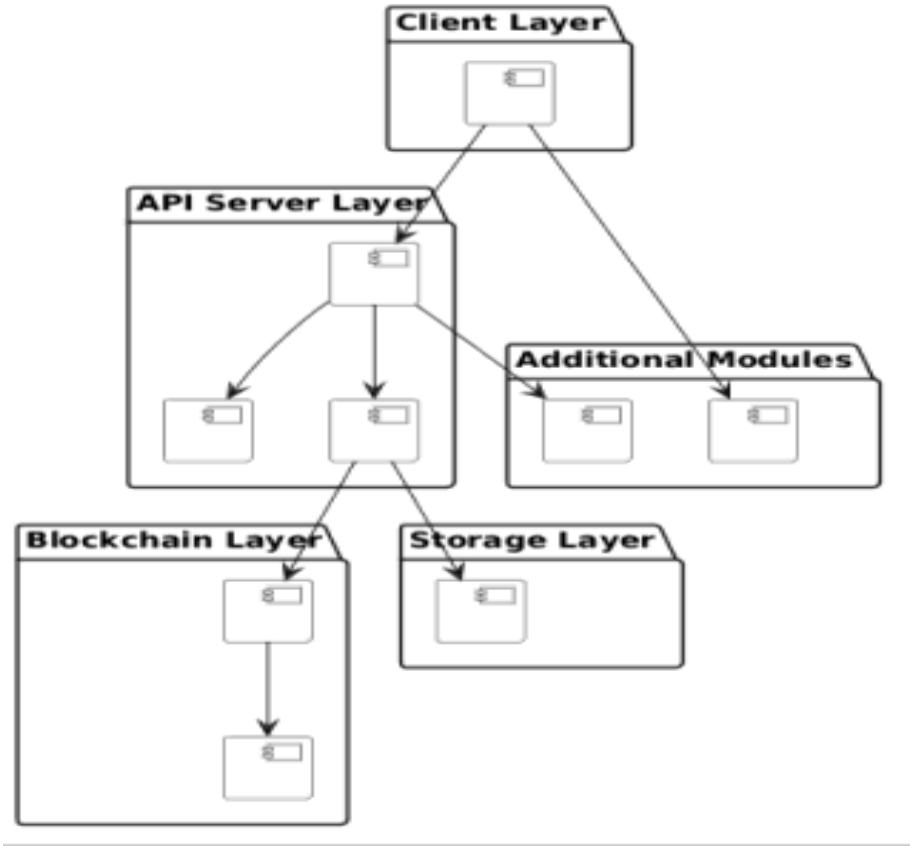


Fig. 4.1: Proposed architecture

Proposed Work

The proposed work focuses on developing BioTrace, a blockchain-integrated traceability system for the Ayurvedic herb supply chain. The system records every stage of a herb batch lifecycle — from harvesting and processing to laboratory testing and retail — as immutable transactions on a blockchain, ensuring that no record can be silently altered once written. Automated compliance checks run against each batch using predefined regulatory parameters, flagging violations without requiring manual audits. Laboratory certificates are stored permanently on IPFS, giving every document a verifiable and tamper-proof address. A role-based

ISSN 2278-2540 | DOI: 10.51583/IJLTEMAS | Volume XV, Issue V, May 2026

access model ensures each stakeholder interacts only with the functionality relevant to their position in the supply chain, while consumers can verify any product's complete history by scanning a QR code. The following section describes the algorithms and methodology that drive the core functionality of the system.

SHA-256 Hashing Algorithm

SHA-256 (Secure Hash Algorithm 256-bit) is a cryptographical function that produces a fixed-length (256-bit) output in its output based on whatever is thrown in as argument. In BioTrace, it provides immutability to the blockchain by creating a unique hash for each block that is based on the index, timestamp, transactions, previous hash and nonce that this block contains. Even if slight changes are made in the data, it generates a whole new hash and therefore it is immediately obvious that tampering has taken place. And because it is a one-way function, the data cannot be reconstructed and information can be indicated without revealing sensitive information.

```
Algorithm: Block Hash Generation
Input: block (index, timestamp, transactions, previousHash, nonce)
Output: hash string

1. Concatenate block.index + block.timestamp +
   JSON(block.transactions) + block.previousHash + block.nonce
2. Apply SHA-256 cryptographic hash function to the concatenated string
3. Return the resulting 64-character hexadecimal hash string
```

```
calculateHash(block) {
  const data = block.index + block.timestamp +
    JSON.stringify(block.transactions) +
    block.previousHash + block.nonce;
  return crypto.createHash('sha256').update(data).digest('hex');
}
```

Fig. 5.1.1: SHA-256 Hashing Algorithm

Raft Consensus Mechanism

Raft is the consensus mechanism used in Hyperledger Fabric for maintaining consistency and reliability across the blockchain network. In BioTrace, the ordering service uses the Raft protocol to ensure that all transactions are received, ordered, and committed to the ledger in the same sequence across all participating nodes. Unlike Proof of Work systems, Raft does not require computational mining, making it more efficient and suitable for enterprise applicationss.

ISSN 2278-2540 | DOI: 10.51583/IJLTEMAS | Volume XV, Issue V, May 2026

```
Algorithm: Proof of Work Mining
Input: pendingTransactions, difficulty (d)
Output: valid mined block

1. Create newBlock with index, timestamp, transactions, previousHash
2. Set newBlock.nonce = 0
3. REPEAT:
     a. Calculate newBlock.hash = SHA256(newBlock)
     b. IF hash starts with d leading zeros THEN
          EXIT loop
     c. ELSE increment newBlock.nonce by 1
4. Append newBlock to blockchain
5. Clear pendingTransactions
6. Persist blockchain to disk
7. Return newBlock
```

```
async mineBlock() {
  const newBlock = {
    index: this.blocks.length,
    timestamp: new Date().toISOString(),
    transactions: [...this.pendingTransactions],
    previousHash: this.getLatestBlock().hash,
    hash: '', nonce: 0
  };
  while (newBlock.hash.substring(0, this.difficulty) !==
         '0'.repeat(this.difficulty)) {
    newBlock.nonce++;
    newBlock.hash = this.calculateHash(newBlock);
  }
  this.blocks.push(newBlock);
  this.pendingTransactions = [];
  this._save();
}
```

Fig. 5.2.1: Proof of Work Algorithm

Haversine Algorithm

The Haversine formula is a formula for calculating the shortest distance between two geographical points by using the latitude and the longitude of the two points. In BioTrace, it is used for geo-fencing in order to verify whether a batch is harvested from approved agricultural zones. The system compares the location of the harvest with predefined centers of the zones the harvest belongs to, and if the distance is longer than a predefined limit (as an example 500 km), then a violation is marked. This method takes into account the curvature of the Earth, and because of that, real-life distance calculation is no longer off.

ISSN 2278-2540 | DOI: 10.51583/IJLTEMAS | Volume XV, Issue V, May 2026

```
Algorithm: Blockchain Integrity Verification
Input: blocks[]
Output: true (valid) or false (tampered)

1. FOR i = 1 TO length(blocks) - 1 DO:
     a. currentBlock  = blocks[i]
     b. previousBlock = blocks[i-1]
     c. IF currentBlock.hash ≠ SHA256(currentBlock) THEN
          RETURN false  // block content was altered
     d. IF currentBlock.previousHash ≠ previousBlock.hash THEN
          RETURN false  // chain linkage broken
2. RETURN true
```

```
isChainValid() {
  for (let i = 1; i < this.blocks.length; i++) {
    const curr = this.blocks[i];
    const prev = this.blocks[i - 1];
    if (curr.hash !== this.calculateHash(curr)) return false;
    if (curr.previousHash !== prev.hash) return false;
  }
  return true;
}
```

Fig. 5.3.1: Haversine Algorithm

b. Compliance Evaluation Algorithm

This algorithm forms the core logic of BioTrace and runs whenever quality data is submitted. It evaluates four aspects: geo-fencing (location validation), seasonal checks (harvest between March–November), species validation (approved herbs), and quality parameters (purity, moisture, ash content). Any failure generates a violation record, while full compliance is confirmed only if all checks pass. The results are directly stored in the database to maintain accuracy and consistency.

```
Algorithm: Automated Compliance Check
Input: batch (location, harvestDate, species, qualityMetrics)
Output: complianceStatus (flags + violations[])

1. violations = []
2. IF harvest location outside approved zones → ADD violation
3. IF harvest month < 3 OR > 11 → ADD violation
4. IF species NOT in approved list → ADD violation
5. IF purity < 95%  → ADD violation
6. IF moisture > 12% → ADD violation
7. IF ashContent > 8% → ADD violation
8. overall = (violations.length == 0)
9. UPDATE batch.complianceStatus
10. RETURN complianceStatus
```

ISSN 2278-2540 | DOI: 10.51583/IJLTEMAS | Volume XV, Issue V, May 2026

```
const inZone = approvedZones.some(z =>
  calcDistance(loc.latitude, loc.longitude, z.lat, z.lng) <= z.r);
const inSeason = month >= 3 && month <= 11;
const speciesOk = approvedSpecies.includes(batch.species.toLowerCase());
let qualityOk = true;
if (purity < 95)    { violations.push('Purity below 95%');    qualityOk = false; }
if (moisture > 12)  { violations.push('Moisture above 12%');  qualityOk = false; }
if (ashContent > 8) { violations.push('Ash content above 8%'); qualityOk = false; }
const overall = inZone && inSeason && speciesOk && qualityOk;
```

Fig. 5.4.1: Compliance Evaluation Algorithm

JWT Authentication Algorithm

BioTrace uses the That Authentication Method for Secure access of API By using the JSON Web Token (JWT) authentication. When a user logs in, a signed token containing his or her identity, role and permissions is created and returned to the client. This token will be sent in the future whenever it requests and will be checked by the server. Access control is enforced on the basis of user roles and only authorized actions and allowed to be done. Tokens also have an expiry time for the sake of security.

```
Algorithm: JWT Token Verification
Input: HTTP request with Authorization header
Output: authenticated user object or 401 error

1. Extract token from Authorization header (Bearer <token>)
2. IF token is missing THEN RETURN 401 Unauthorized
3. Verify token signature using SECRET_KEY
4. IF verification fails THEN RETURN 401 Invalid token
5. Decode payload to extract userId, role, permissions
6. Attach user object to request
7. Check if user.role is in allowedRoles for this endpoint
8. IF not authorized THEN RETURN 403 Forbidden
9. ELSE proceed to route handler
```

```
const decoded = jwt.verify(token, process.env.JWT_SECRET);
req.user = await User.findOne({ userId: decoded.userId });
if (!req.user) return res.status(401).json({ error: 'Unauthorized' });
```

Fig. 5.5.1: JWT Authentication Algorithm

QR Code Generation Algorithm

QR codes in BioTrace contain a batch ID or URL coded into a scannable image for people to access the product's traceability identification. The system employs Reed-Solomon error correction so that it is still readable if partly damaged. The encoded data is organized in a matrix pattern and saved into the database as a PNG image. A blockchain record is also made of the generation event of the QR code for its verification.

ISSN 2278-2540 | DOI: 10.51583/IJLTEMAS | Volume XV, Issue V, May 2026

```
Algorithm: QR Code Generation
Input: batchId
Output: QR code image (base64 PNG)

1. data = CLIENT_URL + "/batch/" + batchId
2. Apply Reed-Solomon error correction on data
3. Encode data into QR matrix with finder patterns
4. Convert matrix to base64 PNG image
5. Store QR reference in batch record
6. Record blockchain transaction: GENERATE_QR
7. Return base64 image to client
```

```
async function generateQRCode(batchId) {
  const data = `${process.env.CLIENT_URL}/batch/${batchId}`;
  const qrImage = await QRCode.toDataURL(data, {
    errorCorrectionLevel: 'H', width: 300
  });
  await HerbBatch.updateOne({ batchId },
    { $set: { qrCodeGenerated: true, qrCodeHash: data } });
  await blockchainService.generateQRCode(batchId);
  return qrImage;
}
```

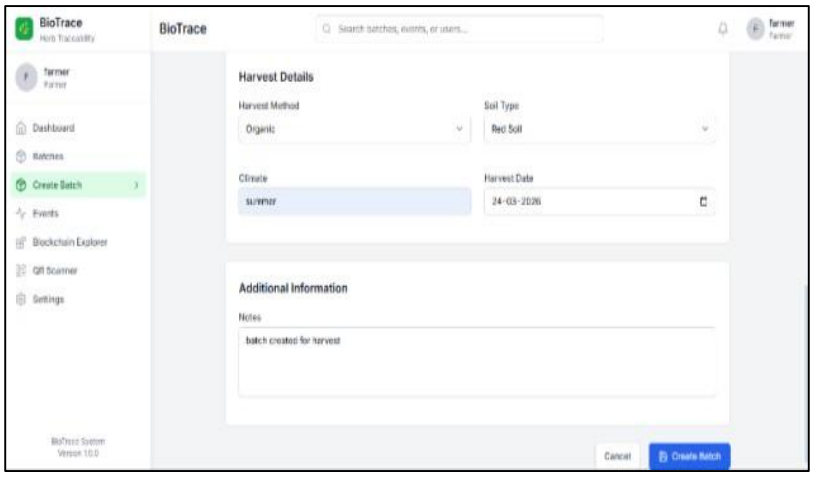
Fig. 5.6.1: QR Code Generation Algorithm

RESULTS AND DISCUSSION

The utilization of the proposed blockchain-based traceability system for ayurvedic herbs was successfully chosen and implemented to ensure transparency, security, and efficiency in the supply chain. The system proved to be a good tracking system of herb batches from harvesting to final distribution, with everything happening being recorded properly.

Farmer Creating A Batch:

Fig. 3. The system starts with the farmer doing a new batch of herb through the application interface. This step includes vital information such as species name, amount and geographic location. The creation of a successful batch proves the ability of the system to accurately record origin data, as it should form the basis for full traceability. This stage makes certain that all the products hitting the supply chain are uniquely identifiable and digitally recorded.



ISSN 2278-2540 | DOI: 10.51583/IJLTEMAS | Volume XV, Issue V, May 2026

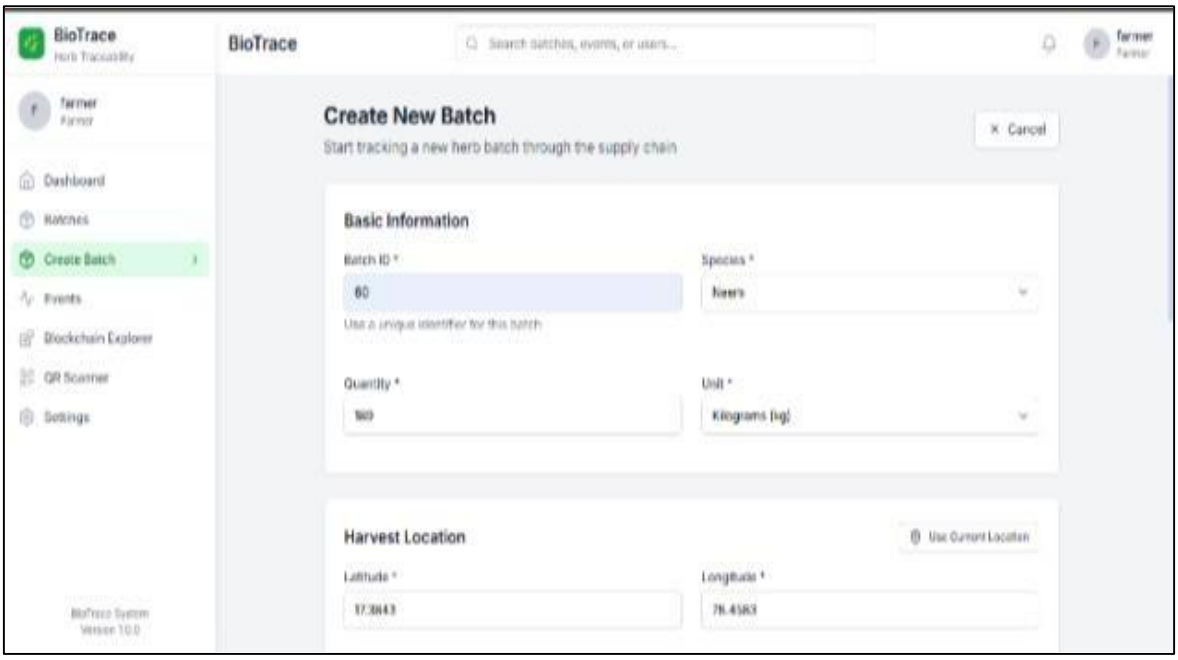


Fig. 6.1.1: Farmer Creating a New Herb Batch

Add Event (Lab Role – Quality Test):

Fig. 4. In this stage, it is achieved by providing a quality test by a laboratory user by entering quality parameters such as purity and moisture levels. When wrong or poor quality values (e.g. purity = 50%) are submitted, the system processes the data but flags it as non-compliant. This is an example of the efficacy of automated validation and compliance monitoring detecting quality problems early in the supply chain.

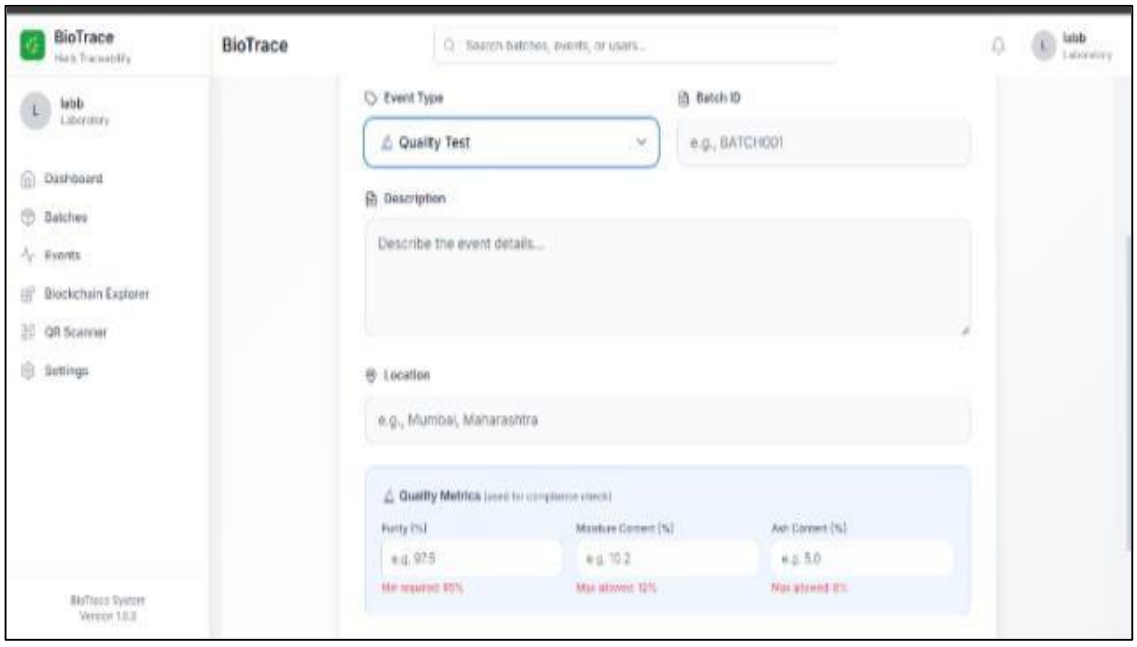


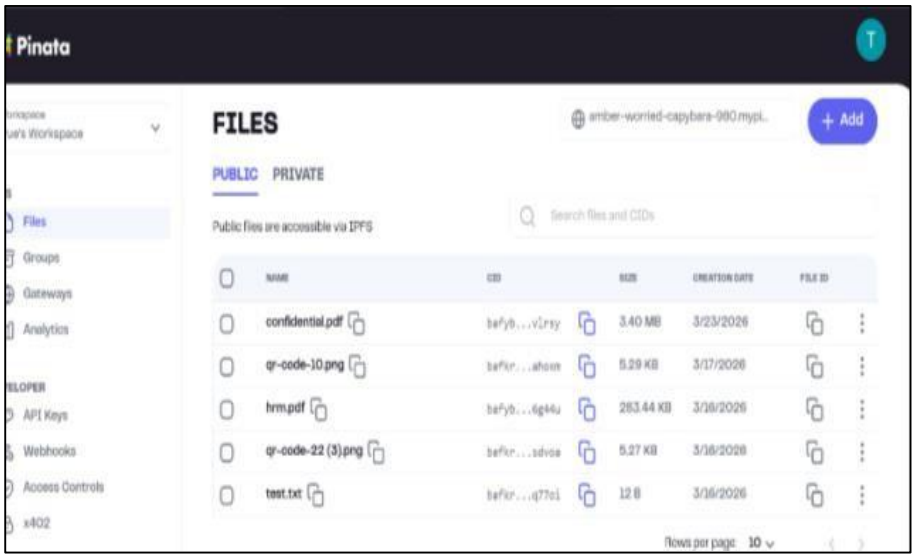
Fig. 6.2.1: Laboratory Quality Test Entry with Non-Compliant Values

Batch Detail Page with IPFS Integration:

Fig. 5. The batch detail page gives a time-based sequential view of all the recorded events. It has built into it

ISSN 2278-2540 | DOI: 10.51583/IJLTEMAS | Volume XV, Issue V, May 2026

a function to access the supporting documents (such as lab reports) via decentralized storage. The link "View Certificate on IPFS" verifies that documents are fetched and stored safely ensuring transparency and corruptibility. This integration draws to the lucidity of the system to manage volatile files efficiently.



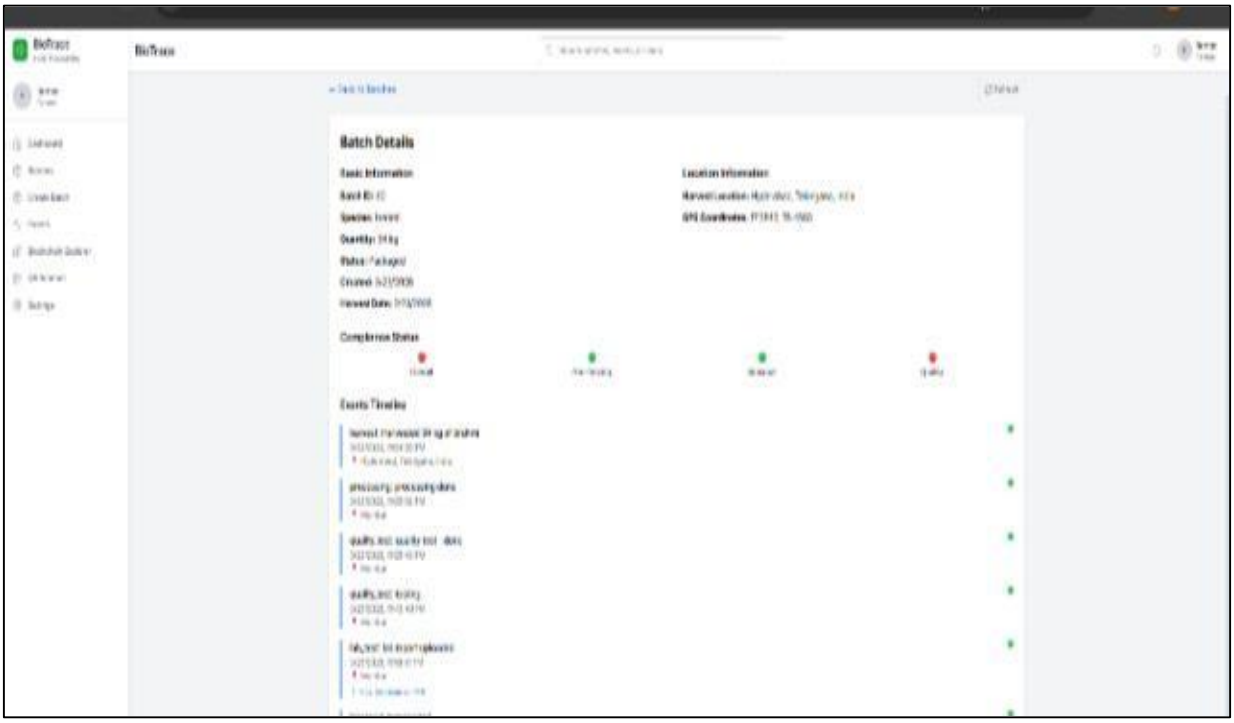


Fig. 6.3.1: Batch Detail Page with IPFS Certificate Access

Compliance Monitoring Dashboard (Regulator View):

Fig. 6. The compliance monitoring page gives regulators a centralised view of all violations. The table points out important factors such as purity or moisture in the ingredients, which are then able to make a quick decision. Step One: Discover the strengths of a system and its capacity to manage oversight by regulators by presenting insights actionable by the regulators in the regulated environment and presents concepts of action in an organized manner.

ISSN 2278-2540 | DOI: 10.51583/IJLTEMAS | Volume XV, Issue V, May 2026

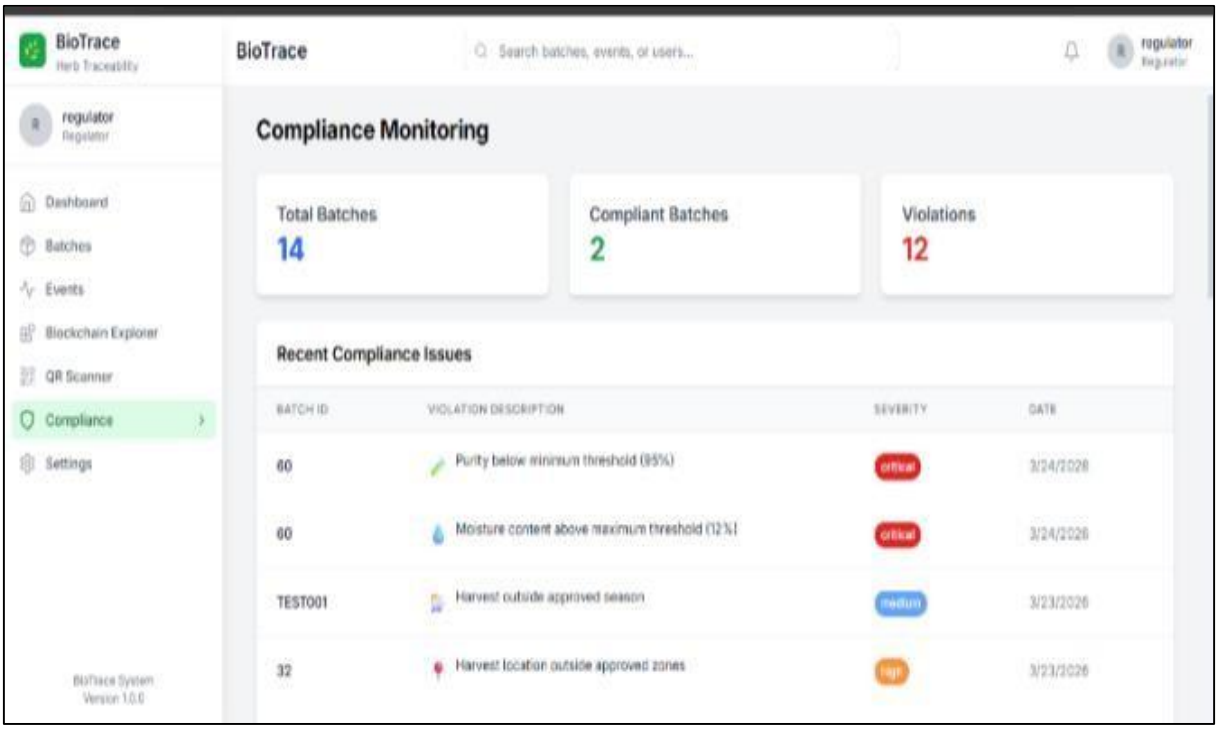


Fig. 6.4.1: Compliance Monitoring Dashboard Showing Violations

Blockchain Explorer – Proof of Immutability:

Fig. 7. The explorer of blockchain presents mined blocks with details of transactions and their correspondences of their hashes respectively. This is to prove that everything that are recorded are unchangeable and can no longer be changed after they have been stored. The work of the block hashes makes the trust and data security or validation the reliability of the system.

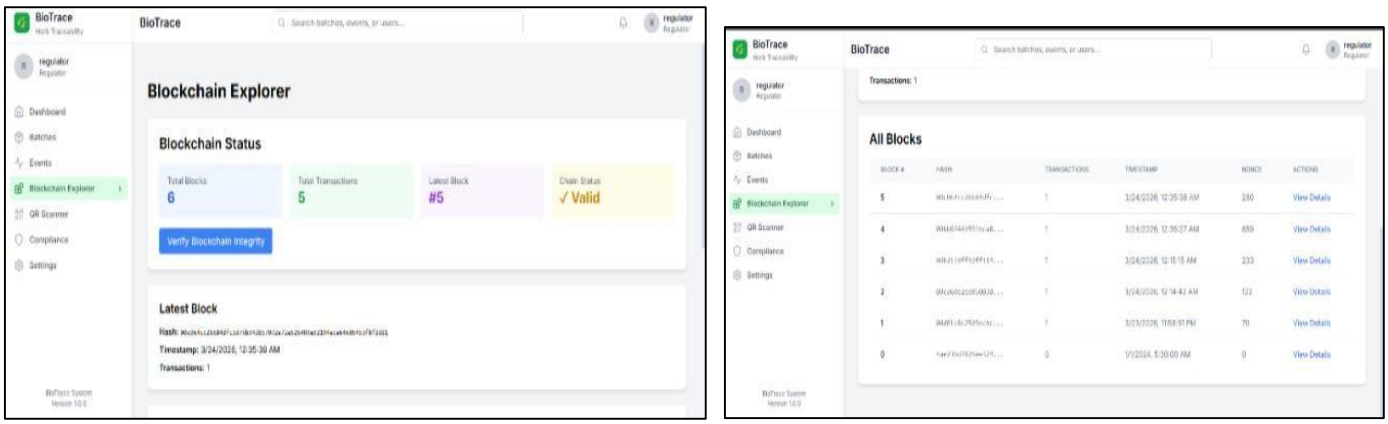


Fig. 6.5.1: Blockchain Explorer Displaying Transaction Blocks and Hashes

Consumer Dashboard Interface:

Fig. 8. Consumer dashboard is the entry point for the end users. It offers various options such as scanning the QR code and browsing the available batches. It is a user-friendly interface for the consumers and makes the product easy to authentic.

ISSN 2278-2540 | DOI: 10.51583/IJLTEMAS | Volume XV, Issue V, May 2026

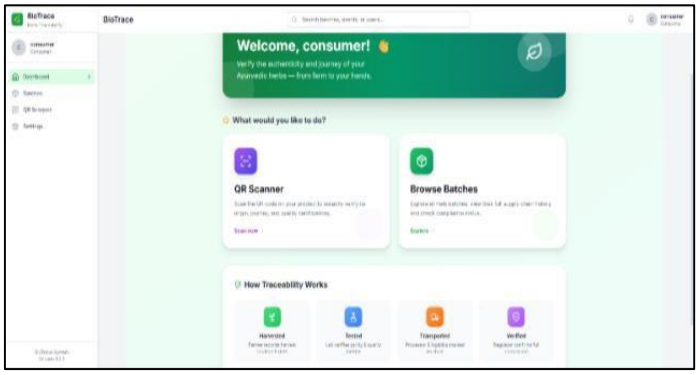


Fig. 6.6.1: Consumer Dashboard with QR Scanner Interface

QR Code Scan Result – Full Traceability:

Fig. 9. If a consumer scans a QR code of a product that he or she wants to buy, this system will show him or her the entire history of supply chain management of that product. It will show him or her information from the harvesting process all the way to the processing process. That is complete transparency in order for him or her to make a decision that can be verified.

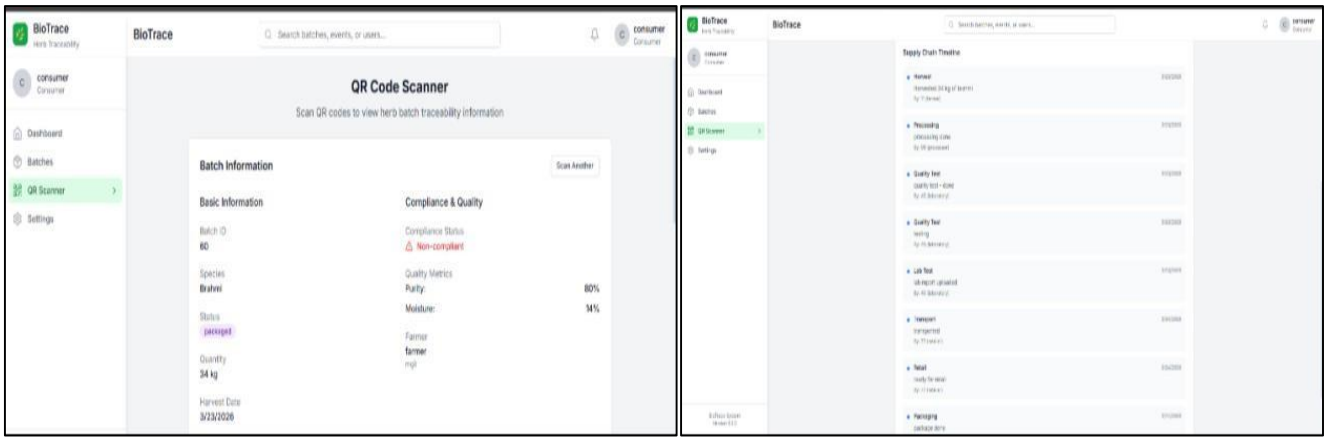


Fig. 6.7.1: QR Code Scan Result Showing Complete Supply Chain Traceability

Table II. System Modules and Roles

Module	Farmer	Processor	Laboratory	Regulator	Consumer
Create Batch	✓	✗	✗	✗	✗
Add Event	✓	✓	✓	✗	✗
Upload Certificate	✗	✗	✓	✗	✗
Quality Test	✗	✗	✓	✗	✗
View	✗	✗	✗	✓	✗

ISSN 2278-2540 | DOI: 10.51583/IJLTEMAS | Volume XV, Issue V, May 2026

Compliance					
Scan QR	✓	✓	✓	✓	✓

Table III Compliance Check Parameters

Parameter	Threshold	Violation Condition
Purity	≥ 95%	Below 95%
Moisture Content	≤ 12%	Above 12%
Ash Content	≤ 8%	Above 8%
Geo-fencing	Within approved zones	Outside India zones
Harvest Season	March – November	Outside this range
Species	Approved list only	Unlisted species

Table IV. Blockchain Vs Traditional System

Feature	Traditional System	BioTrace System
Data Storage	Centralized Database	Blockchain + MongoDB
Tamper Detection	Not possible	Hash verification
Certificate Storage	Physical / Local	IPFS (permanent storage)
Compliance Check	Manual audit	Automated real-time
Traceability	Partial	Full farm-to-retail
Consumer Access	Not available	QR code-based access

Table V. Test Results Summary

Test Case	Input	Expected Outcome	Result
Quality violation	Purity = 50%	Compliance = Red	✓ Pass
IPFS upload	PDF certificate	Pinata link generated	✓ Pass
QR scan	Valid batch ID	Full timeline displayed	✓ Pass
Geo-fencing	Outside Violated Area	Violation flagged	✓ Pass
Role restriction	Consumer adds event	Access denied	✓ Pass

ISSN 2278-2540 | DOI: 10.51583/IJLTEMAS | Volume XV, Issue V, May 2026

CONCLUSION

This paper presented BioTrace, a block chain-based traceability system, conceived to solve age-old authenticity, quality-due to the lack of quality assurance and regulatory set-up challenges, and the authentication problems of the Ayurvedic herb supply chain. By combining blockchain, which is based on Node.js, backend, frontend written in React, MongoDB and IPFS the system becomes an end-to-end solution that stores all phases of the lifecycle of each herb batch -- from herb harvest at the farm to its distribution at the end consumer's smartphone -- on the same platform and in the form of immutable cryptographic transactions. In terms of system functionality, the access control mechanism for seven types of stakeholders is implemented with role-based access control (RBC), the verification of compliance with geo-fencing rules, seasonal use, quality, species conservation automatically validation is achieved, and consumers can check batch provenance under real time verification through QR code. The use of a permissioned blockchain to maintain the sensitivity of supply chain data so that only authorized participants always have access, and the hybrid storage strategy, which is based on a combination of MongoDB for operational queries and IPFS for off-chain document storage to balance performance with data integrity data. Future work includes integration of IoT sensors for automated environmental monitoring, advanced analytics for anomaly detection, and deployment on multi-organization blockchain networks for large-scale industrial adoption

REFERENCES

1. Tiago M. Fernandez-Carames et al.” Towards an autonomous industry 4.0 warehouse: A UAV and blockchain-based system for inventory and traceability applications in big data-driven supply chain management.” arXiv, 2024
2. Devraj V. Rajput et al. “Blockchain technology in the food supply chain: a way towards circular economy and sustainability.” Sustainable Food Technology (RSC Publishing), 2025
3. C. Vijj, Aniket Kuntal, Aryan Bhardwaz & Darshan Bandari. ” Blockchain Based Traceability in Supply Chain Using Smart Contracts.” IJRASET, 2022
4. Sidra Malik et al. “PrivChain: Provenance and Privacy Preservation in Blockchain enabled Supply Chains.” arXiv, 2021
5. Peng Zhao & Shiren Ye. ” A Supply Chain Traceability Scheme Based on Blockchain.” Academic Journal of Computing & Information Science, 2022
6. Zibin Zheng et al. “Blockchain Applications and Challenges in Industry and Supply Chains.” IEEE Access, 2019
7. Marco Conoscenti et al. “Blockchain for Supply Chain Traceability and Data Verification.” IEEE Conference, 2016
8. Kamanashis Biswas et al. “Blockchain-Based Framework for Secure Data Sharing in Distributed Systems.” IEEE Conference, 2017
9. Feng Tian. “Blockchain-Based Food Supply Chain Traceability Using RFID.” IEEE Conference, 2017
10. Dylan Yaga et al. “Blockchain Technology Overview and Security Applications.” NIST, 2018