Hyperledger Fabric-Based Tea Supply Chain Production Data Traceable Scheme

Chin-Ling Chen 1,2,*, Wan-Bing Zhan 3,*, Der-Chen Huang 4, Ling-Chun Liu 4, Yong-Yuan Deng 2,* and Chin-Guo Kuo 5

1 School of Information Engineering, Changchun Sci-Tech University, Changchun 130600, China; clc@mail.xyut.edu.tw
2 Department of Computer Science and Information Engineering, Chaoyang University of Technology, Taichung City 413310, Taiwan
3 School of Computer and Information Engineering, Xiamen University of Technology, Xiamen 361024, China
4 Department of Computer Science and Engineering, National Chung-Hsing University, Taichung 40227, Taiwan; huangd@nchu.edu.tw (D.-C.H.); d110056604@mail.nchu.edu.tw (L.-C.L.)
5 Department of Industrial Education, National Taiwan Normal University, Taipei 10610, Taiwan; t07019@ntnu.edu.tw
* Correspondence: 2122031228@s.xmut.edu.cn (W.-B.Z.); allendeng@cyut.edu.tw (Y.-Y.D.)

Abstract: With the advent of Industry 4.0, blockchain is one of the emerging technologies that can be used in multiple fields, especially in supply chain networks, where it is considered a sustainable concept technology. Because of its decentralization, reliability, transparency, consistency, and traceability, blockchain can challenge existing conventional models in supply chain scenarios. Therefore, this study proposes a framework that integrates the technology of Blockchain 3.0 (Hyperledger Fabric) into the tea supply chain. The concept of data traceability driven by blockchain technology consists of documenting the tea supply chain system, in which the cultivation, processing, and retailing of tea leaves are documented, and optimizing the existing anti-counterfeiting mechanisms. The ECDSA algorithm is used to confirm the identity among the entities located in the Hyperledger Fabric channel, and IPFS technology is introduced to store tea traceability data to solve the problem of data increment in the tea production process. Only the hash value and traceability code of the traceability data are stored in the block. We analyze the relationship between the number of transactions and latency, and we can see the latency time of both write and read transactions. The system tested write transactions and read transactions with a minimum write speed of 0.97 s and a maximum of 6.26 s and a minimum read speed of 0.1 s and a maximum of 4.62 s via Caliper analysis. The experimental results show that the performance analysis sounds good. This study uses distributed theory and service-oriented thinking in its specific application to the tea supply chain system model and takes each entity through a B2B connection to achieve anti-counterfeit traceability in the tea supply chain of a regulatory nature.

Keywords: blockchain (BC); anti-counterfeit traceability; tea supply chain; ECDSA; hyperledger fabric

1. Introduction

1.1. Background

During periods of economic development, many supply chain industries adopt a linear economic model in which a large number of raw materials are extracted and turned into products that are not reused or recycled. This economic model can lead to the destruction of our environmental resources such as air, water, and land [1]. As a result, many supply chain industries are gradually moving towards a circular economy, where product design and manufacturing take into account sustainability and the longest possible period of high-value utilization. However, due to the involvement of multiple stakeholders in the supply chain, it is easy to encounter difficulties in information tracing, information falsification,
and trust crises during the various lifecycle stages of production [2]. Therefore, this study aims to use blockchain technology to address issues of product information authenticity and stakeholder trust in the tea supply chain and establish a recyclable model of the tea supply chain.

Blockchain technology is a decentralized ledger. Firstly, the ledger is transparent, and multiple users can verify the information recorded in the ledger, achieving data transparency within the blockchain [3]. Secondly, the blockchain is a distributed database maintained by multiple nodes and not owned by any individual, which makes the data in the blockchain immutable [4]. Thirdly, the data in the blockchain are stored in a Merkle tree structure and combined with cryptography to achieve accurate data verification and encryption of data information [5]. Finally, blockchain does not rely on a central authority for management, which can effectively avoid issues such as information leakage or data tampering caused by hacker attacks through its decentralized mechanism [6].

There are two reasons for studying the tea supply chain in this paper. Firstly, tea is popular worldwide, with a global tea market value of about USD 209.3 billion in 2022, expected to rise to USD 266.7 billion by 2025 [7]. Tea has a long history of popularity globally, originating in China, where approximately 3.12 million tons of tea were produced in 2021, up from about 2.74 million tons in 2020 [8]. India, China, Sri Lanka, and Kenya are the world’s largest tea exporting countries, with China exporting USD 1.6 billion, Sri Lanka exporting USD 1.5 billion, and Kenya exporting USD 1.4 billion in 2017 [9]. Secondly, there are many problems in the current tea supply chain network, such as poor information utilization, chaotic regulatory systems, and a lack of traceable monitoring systems [10].

1.2. Related Works

The usage of blockchain technology is currently a popular approach in the field of supply chain research to guarantee the traceability of each link in the supply chain process. Due to the limited storage space on the public chain, which is the format chosen for the study, it may be challenging to solve the resource access problem. Table 1 contains a list of the pertinent books, some of which are still difficult to understand. Treiblmaier et al. [11] suggest using blockchain technology to connect the food supply chain to address the problem of multiple information asymmetry, using it as a label that recognizes information based on a traceability system as a key factor in what consumers think of the product and their intent to purchase. Paul et al. [12] proposed a practical model to support a circular supply chain in the tea industry network, which completes the circular supply chain by using blockchain technology as a substrate to drive RFID technology. Paul et al. explored the possibility of combining multiple modules in the system with RFID technology by analyzing multiple existing system models, but they did not specify the specific combination process. Centobelli et al. [13] designed a circular blockchain platform that includes manufacturers, reverse logistics service providers, selection centers, recycling centers, and landfill applications in a supply chain scenario. However, the proposed blockchain platform was not analyzed for security. Helo et al. [14] proposed a pilot cloud-based portal system for real-time tracking and tracing of logistics and supply chains. And a detailed design of how the triple-loop framework of the system utilizes blockchain qualities is presented. Chang et al. [15] proposed the concept that blockchain and smart contract technology can help in business process re-engineering across enterprises and, through smart contract technology in their proposed system framework, ensure the intelligent advancement of business processes to be able to take advantage of the advantageous features of the blockchain platform. However, no logical description is given for the writing of smart contracts.
Table 1. Comparison of business data-sharing options that have been proposed and those that now exist.

<table>
<thead>
<tr>
<th>Authors</th>
<th>Year</th>
<th>Objective</th>
<th>Technologies</th>
<th>Merits</th>
<th>Demerits</th>
</tr>
</thead>
<tbody>
<tr>
<td>Treiblmaier et al. [11]</td>
<td>2023</td>
<td>Blockchain tagging as a signaling mechanism proves, through signaling theory, that blockchain can influence and perceive purchase intention.</td>
<td>Blockchain, Signaling theory</td>
<td>Blockchain can record the product flow while applying it as a tag to signal theory.</td>
<td>There is no good integration of signal theory with the underlying logic of the blockchain.</td>
</tr>
<tr>
<td>Paul et al. [12]</td>
<td>2022</td>
<td>A useful model has been developed using Radio Frequency Identification (RFID) technology and Blockchain Technology (BCT) to assist the tea industry’s web-based circular supply chain.</td>
<td>Blockchain, RFID</td>
<td>Various system models for integrating the supply chain with RFID are analyzed, and their possibilities are analyzed.</td>
<td>No specific supply chain system architecture process is indicated.</td>
</tr>
<tr>
<td>Centobelli et al. [13]</td>
<td>2022</td>
<td>Create a thorough triple-retesting framework that links three reverse elliptical supply chain procedures (such as recycling, redistribution, and remanufacturing) for circular blockchain platforms.</td>
<td>Blockchain, Distributed ledger, Reverse logistics service providers (RLSPs)</td>
<td>A detailed design of the system framework and how the triple loop framework leverages blockchain qualities.</td>
<td>No encryption mechanism is used, and the flow of information in the system may make it difficult to resist hacking attacks.</td>
</tr>
<tr>
<td>Helo et al. [14]</td>
<td>2020</td>
<td>Propose a pilot cloud-based portal system for real-time tracking and tracing of logistics and supply chains.</td>
<td>Blockchain, IoT, RFID</td>
<td>By combining RFID, IoT, and blockchain technologies into one integrated, real-time view.</td>
<td>No detailed description of the entire business logic is provided.</td>
</tr>
<tr>
<td>Chang et al. [15]</td>
<td>2019</td>
<td>It is suggested and investigated to automate business flows in tracking supply chain processes using a blockchain-based business process re-engineering (BPR) architecture.</td>
<td>Blockchain, Smart contract</td>
<td>The logic of how a smart contract works when multiple data interaction processes are given.</td>
<td>The detailed coding of smart contracts has not been elaborated.</td>
</tr>
</tbody>
</table>

Based on reading the literature combined with the research in this paper, it is concluded that the specific problems are:

1. Redundancy of information and information asymmetry in the process of tea farming until tea selling;
2. Because tea is a non-standardized product and the tea supply chain network’s standardization is low, it can only be identified by tea tasters and tea artists (experienced people), so there is personal subjectivity;
3. Complex distribution channels for tea, where the source is difficult to determine and the quality cannot be ascertained, can easily give rise to the problem of substandard or counterfeit products.
4. The traditional tea supply chain lacks digital management due to the low adoption of information technology across all stages. There is poor information exchange and interaction, making it difficult for consumers to access comprehensive information.

Given the above problems, this study will create a secure channel using Hyperledger Fabric, a blockchain 3.0 federation chain technology, to pull the stakeholders in the tea supply chain together.
supply chain into the channel. Due to the native nature of the Hyperledger Fabric channel, the various entities in the channel can share data securely, encrypt the required data using the private key generated by ECDSA, then use the algorithm known as Elliptic Curve Digital Signature Algorithm (ECDSA) to digitally sign the data at different stages of transmission. To solve the blockchain block capacity problem, an IPFS file storage system is introduced to store all the data recorded during the tea production process to ensure the quality of the tea and solve the tea anti-counterfeiting problem. Finally, all data will be hashed, the hash value will be uploaded to the chain, and the data will be made into a unique traceability code to follow the outer packaging of tea for identification between entities.

The research objectives of this study that can be achieved under the traditional tea supply chain model are as follows:

1. Solve the credit problem: There is more than one institution involved, and each institution supervises the other, thus ensuring the accuracy of the information and ensuring that the information on the chain cannot be tampered with, which greatly reduces the chance of cheating.

2. The whole record tracking: Relative to keeping the express logistics tracking open, transparent, and able to track the production, processing, testing, transportation, and warehousing of goods for sale, each link of time after the point is recorded in full.

3. Clear responsibilities and traceability of problems: The characteristics of blockchain, namely, openness and transparency, cannot be tampered with. Once a problem occurs at a certain link, it is timely and effective to find out where the problem link occurs.

4. Prevent commodity counterfeiting: After the information about the goods is put on the chain, the whole process is open and transparent, and the products from the source down to the hands of customers can be checked so that there is no problem of counterfeiting.

The format of this essay is as follows. The major technologies employed in this paper’s system are introduced in Section 2 of the text; Section 3 describes the main processes of the system operation as well as the architecture; Section 4 performs the security analysis; Section 5 discusses the performance analysis and comparison; finally, in Section 6, we conclude our scheme.

2. Preliminary

2.1. Blockchain

Blockchain is a decentralized, distributed ledger technology for recording and verifying transactions. It ensures the security and integrity of transaction data through cryptography and distributed consensus algorithms, making it impossible for transactions to be tampered with or forged. Due to its decentralized nature, blockchain technology is widely used in digital currency, smart contracts, supply chain management, asset management, and other fields [16].

Blockchain technology is a very promising technology when it comes to the tea industry since it can offer answers for transparency, safety, and traceability in the tea supply chain. Blockchain is a decentralized digital ledger that can keep track of transactions without requiring centralization [17]. The technology is unique in that it ensures transparency and security of transactions, as the record of transactions cannot be tampered with or deleted. In the tea supply chain, blockchain technology can be used to track the entire process of tea production, processing, packaging, and transportation and to ensure its authenticity and integrity [18]. Because the tea supply chain usually involves multiple participants, such as farmers, processors, retailers, and consumers, all of these participants can use blockchain to record and track the transaction records of tea. Through blockchain technology, participants in the tea supply chain can share the same transaction information, thus enabling real-time information sharing and collaboration and reducing un-necessary human intervention and errors.
In addition, blockchain technology can also ensure the quality and security of the tea supply chain. Through blockchain technology, the production and processing of tea can be traced, thus determining the quality and security of the beverage [19]. For example, if there is a problem with a batch of tea, the participants can use blockchain technology to determine where and when the problem occurred and find the source of the tea so that appropriate measures can be taken to prevent the problem from expanding.

2.2. Hyperledger Fabric

Hyperledger Fabric is an open source blockchain framework designed to provide a customizable, scalable, and highly secure blockchain solution for enterprise-class applications [20]. Unlike other public blockchains, Hyperledger Fabric has many customization features that can be configured to meet different business needs. It supports smart contracts that enable various forms of business logic while providing strict permission control to ensure the confidentiality and security of data and transactions.

In the past, the management of tea supply chains was usually conducted manually, which led to many problems, such as opaque information, frequent errors, difficulty tracking, and so on. This article uses Hyperledger Fabric technology to manage the supply chain for tea to address these issues. The enterprise-level blockchain system Hyperledger Fabric satisfies the supply chain for tea’s requirements for efficiency, dependability, and security.

(1) Data privacy and security: Hyperledger Fabric uses a multi-tier architecture and smart contracts to ensure data privacy and security [21]. All data in the tea supply chain are encrypted and can only be decrypted by authorized participants.

(2) Management and tracking: Hyperledger Fabric allows every participant in the tea supply chain to track every step of the tea’s transportation, processing, quality testing, and sales. This means that all participants in the tea supply chain can know the real-time status of the tea at all times, allowing them to better manage and plan the flow of tea [22].

(3) Transparency and trust: Hyperledger Fabric can also establish an environment of transparency and trust, and through blockchain technology [23], all participants in the tea supply chain can view and verify information on the origin, processing, inspection, and quality of tea, thus ensuring the authenticity and quality of tea.

2.3. Inter Planetary File System (IPFS)

The Inter Planetary File System (IPFS) is a peer-to-peer distributed file storage and sharing protocol. It is designed to create a decentralized global file system that enables users to share and access files over the Internet without relying on centralized servers [24]. IPFS guarantees data uniqueness and reliability through hash addresses and content addressing and uses peer-to-peer network protocols to transfer data, improving the speed and security of file transfers [25]. By using this technology, the proposed scheme has the following advantages:

(1) Data storage: the tea supply chain involves a large number of data, including production, processing, transportation, and quality inspection data. The use of IPFS can store these data on distributed nodes, avoiding the problem of a single point of failure, and can improve the reliability and security of the data.

(2) Traceability: Customers should be able to trace the origin and production process of their tea. To enhance trustworthiness, details such as where and how the tea is grown, harvested, and processed can be recorded on the blockchain using IPFS. This allows customers to easily verify the authenticity and traceability of the tea online.
2.4. Elliptic Curve Digital Signature Algorithm (ECDSA)

The elliptic curve digital signature algorithm (ECDSA) was standardized by IEEE and NIST in 2000 [26]. There is no sub-exponential time solution to the elliptic curve discrete logarithm problem (ECDLP), in contrast to the integer factorization problem (IFP). ECDLP has advantages, including shorter keys, shorter signatures, and quicker calculation times. With Hyperledger Fabric, ECDSA may be employed, partially resolving the issue of insufficient processing and storage resources.

Assume that role A signs the message with m in the signer’s capacity, role B evaluates the message’s legitimacy in the verifier’s capacity, and A selects the elliptic curve’s parameters as $y^2 = (x^3 + ax + b) \mod p$, p, and G. This generates the roles of an A key pair $(d_A, Q_A)$, a private key $d_A$, and a public key, each of which is $Q_A = d_A G$.

Parameters selection:

1. Elliptic curve equation $y^2 = (x^3 + ax + b) \mod p$: This represents an elliptic curve that has a definite shape.
2. Base point: A point $G$ on the curve is chosen as the base point.
3. Large prime number: A random number is chosen as the modulus n, which is usually a very large prime number.
4. Private key: A random number $d_A$ is chosen as the private key.
5. Public key: The public key $Q_A$ is calculated as the product of the base point $G$ and the private key $d_A$.

Role A uses the following steps to complete the signature:

1. Role A chooses a base point $G$ and an elliptic curve $E_p(a, b)$.
2. Role A picks the numbers $k \in [1, N - 1]$ and $N$, which are in the order of $G$ at random.
3. Role A does the $H = \text{hash}(m)$ information hash calculation.
4. Role A figures out a point $(x, y) = kG$.
5. After role A calculates $r = x \mod n$ and $r \neq 0$, it sends role B the result of its ECDSA signature, which is $s = k^{-1}(H + rd_A) \mod n$ and $(r, s)$.

Role B uses the following steps to complete the verification:

1. Role B calculates the $m, H' = \text{hash}(m)$ hash.
2. Role B determines $u_1 = s^{-1}H' \mod n$ and $u_2 = s^{-1}r \mod n$.
3. Role B determines $(x', y') = u_1G + u_2Q_A$.
4. The verification of the signature is successful if $x' = r$.

3. System Overview

3.1. System Architecture

As illustrated in Figure 1, we propose an architecture for a consortium blockchain network in this study. The system design consists of three key components that make up the architecture of the consortium’s distributed ledger service center: the blockchain network component, the application development and service component, and the data storage module. User entities joining the federation chain store data in the Data Storage Component via a client in the Application Component and subsequently interact with the Hyperledger Fabric Network with the address information it returns along with other transaction-required information.
Figure 1. The consortium blockchain service architecture.

1. **Tea Planting Enterprise (PE)**

   The whole tea supply chain starts with tea farmers planting tea leaves, and the professional inspectors monitor their air temperature and humidity, light level, soil temperature, humidity, pH value, planting location, and other environmental data during the planting cycle. At the same time, we collect records of agricultural operations such as plot sowing, fertilization, and irrigation and take high-definition pictures of the whole growth cycle. After ensuring the quality of the picked tea leaves, they are transported to the tea processing facility.

2. **Processing Mechanism (PM)**

   The tea processing process broadly consists of various steps such as killing, withering, kneading, fermentation, drying, etc. Different processing steps are carried out by different types of tea leaves. In the overall processing chain, professionals monitor the operation process to control the details of each operation, record all the operation data, and write the operation data and all the planting data of the planting enterprise into the tea traceability code. Finally, the processed tea leaves are transported to the distributors along with the traceability code.

3. **Retailers (R)**

   After receiving the processed tea leaves, dealers verify the quality of the tea leaves through the traceability code to ensure the standardized production process of tea installation, and after confirmation, they can distribute the tea leaves to multiple platforms for retailing. A record of the sale is made and uploaded to the Hyperledger Fabric Network for subsequent review by consumers and market regulators for complaints.
(4) Consumers (C)

Consumers can view the entire production process and detailed data of tea through the traceability code when purchasing tea and provide feedback to market supervision if they find quality problems with tea. The feedback process concludes with the need to submit feedback to the Hyperledger Fabric Network, which facilitates regulatory logging by market regulators.

(5) Market Supervision (MS)

Market supervision can verify the whole process of the tea supply chain through the feedback information and evidence provided by consumers and carry out supervision operations if there is a problem.

3.2. Application Scenario

We describe the transaction flow of the tea supply chain as shown in Figure 2 below.

Figure 2. A flowchart of the transactions in the tea supply chain.

Step 1: Each entity in the system must register at this level. To join the blockchain network as a node, all entities—including producers, processors, distributors, market supervisors, and consumers—need to be certified by CA. After the authentication, the CA node will issue digital certificates, and all entities can share data through the blockchain network.

Step 2: All production-related data are recorded by the PE, who then uploads the finished product to the blockchain hub with an electronic signature and a hashing method. There, it is added to the ledger by the sorted nodes and updated on the local ledger. The raw materials and transaction information will be delivered to the PM after the production is finished.

Step 3: When the PM receives the transaction request, it verifies the legitimacy of the signature through the ECDSA algorithm to confirm the origin of the transaction and verifies the hash value to ensure that the transaction information and production data are not tampered with to ensure the quality of the raw materials. After the production is completed, it generates product information and order information, as well as its processing process, and uploads it to the blockchain center, which is converted into traceability code through coding and transported to the R with the product.

Step 4: After the R receives the products, they verify the data in the chain by scanning the traceability code and comparing the product information and order information, and can start selling after confirming all data sources and data integrity.
Step 5: C can access the data in the chain by scanning the traceability code on the products through the client and obtaining all the production data of the intended products. If they find any problems with the data after verification, they can report them to the MS and send the reporting information to the blockchain center.

Step 6: The MS can access two parts of the data in the chain through the client: one is all the product information and order information of the products to supervise whether there are crude and falsified orders in the market, and the other is to check whether there is any information reported by consumers, to realize the supervision of the whole market operation through the blockchain-shared data.

3.3. Notations

The notation of this article is as follows:

<table>
<thead>
<tr>
<th>Symbol</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>ID_X</td>
<td>The Identity of X</td>
</tr>
<tr>
<td>d_X</td>
<td>Party X’s private key for the ECDSA</td>
</tr>
<tr>
<td>Q_X</td>
<td>Party X’s public key for the ECDSA</td>
</tr>
<tr>
<td>Cert_X</td>
<td>A user X’s digital certificate</td>
</tr>
<tr>
<td>k_i</td>
<td>The user selects the i-th random number</td>
</tr>
<tr>
<td>Data_X</td>
<td>Data at the heart of each transaction</td>
</tr>
<tr>
<td>M_Pe</td>
<td>PE indicates the transactions uploaded to Hyperledger Fabric</td>
</tr>
<tr>
<td>M_PM</td>
<td>PM indicates the transactions uploaded to Hyperledger Fabric</td>
</tr>
<tr>
<td>M_R</td>
<td>R indicates the transactions uploaded to Hyperledger Fabric</td>
</tr>
<tr>
<td>M_C</td>
<td>C indicates the transactions uploaded to Hyperledger Fabric</td>
</tr>
<tr>
<td>(r_i,s_i)</td>
<td>The signature that user X created</td>
</tr>
<tr>
<td>H_Xi</td>
<td>The i-th hash that user X produced</td>
</tr>
<tr>
<td>C_X</td>
<td>Information encrypted by user X</td>
</tr>
<tr>
<td>E_{Puk}(M_X)/D_{PRK_X}(C_X)</td>
<td>Use the party X’s public key or private key to encrypt or decode the message M.</td>
</tr>
<tr>
<td>T_i</td>
<td>The i-th timestamp</td>
</tr>
<tr>
<td>ΔT</td>
<td>The standard for determining whether a timestamp is correct</td>
</tr>
</tbody>
</table>

3.4. Transaction Information Flow

Figure 3 depicts the transaction format used by the Hyperledger Fabric-based blockchain system.

![Figure 3. Transaction information format.](image)

If Entity A and Entity B need to communicate and exchange information within the supply chain, they will each establish an organization (Organization A and Organization B), register with a Certificate Authority (CA), and obtain their corresponding public–private key pairs and digital certificates. Peer nodes are the components that comprise an organization, including endorser nodes, orderer nodes, anchor nodes, and leader nodes. When Organization A interacts with Organization B, it encrypts the transaction data with its public key and then submits the transactions to the blockchain through its orderer node. Organization B receives the transaction data from Organization A over the channel and updates its local copy of the blockchain ledger to store the data by invoking chaincode functions. Each peer node in the network can deploy one or more chaincodes and maintain...
a copy of the ledger for the channel. The ordering node collects and packages the trans-
actions and information exchange generated within the channel, before submitting to the
Hyperledger Fabric network.

3.5. Registration Phase

The CA, which generates the key pairs required to issue the relevant digital certifi-
cates, must first receive registration information from all entities that intend to join the
Hyperledger Fabric network. We use ‘Users X’ to denote each entity in the proposed
network.

Step 1. Using his client, the user sends the registration data ID_x to the CA node of
the Hyperledger Fabric Network; if the registration information is legal, the CA node will
enter the second step of operation; if not, the client will give the corresponding prompt.

Step 2. The CA node creates a unique private key d_x and determines the corresponding
public key.

\[ Q_X = d_X G \] (1)

Using the ECDSA algorithm with G as the base point, it generates a private digital
certificate Cert_x based on the registration information provided by ‘Users X’, and finally
sends it back to the user.

Step 3. The client saves the key pair and certificate IDX provided by CA after user
registration.

\[ \text{ID}_X, d_X, Q_X, \text{Cert}_X \] (2)

The registered chaincode is shown in Algorithm 1:

\begin{algorithm}
\caption{Physical information sign up chaincode}
\begin{algorithmic}
\Function{RegisterUser}{contractapi.TransactionContextInterface, userID string}{error}
\State //Obtain the client’s identity
\State \text{clientIdentity, err} := \text{ctx.GetClientIdentity()}
\If{err != nil}
\State \Return fmt.Errorf("failed to get client identity: ", err)
\EndIf
\State //Create a new user
\State \text{newUser} := \&\text{User}
\State \hspace{1em} ID: \hspace{1em} userID, \hspace{1em} Balance: 0, \hspace{1em} Owner: clientIdentity.GetID(),
\State \hspace{1em} \}
\State //Write the user to the ledger
\State \text{err} = \text{ctx.GetStub().PutState(userID, newUser.ToBytes())}
\If{err != nil}
\State \Return fmt.Errorf("failed to put user: ", err)
\EndIf
\State \Return nil
\EndFunction
\end{algorithmic}
\end{algorithm}

3.6. Production Phase

The start of the tea supply chain is handled by the production phase, which is mainly
the interaction between the two entities, the grower and the manufacturer, to which the tea
farmer belongs, through Hyperledger Fabric with the following specific process:

Step 1. In the production phase, the PE first monitors the environmental data of the
planting site, such as air and soil humidity, illumination, pH value, etc., and the records of
various farming operations, such as sowing, right and wrong, irrigation, etc., and makes
detailed records of the tea growth cycle, collectively referred to as production data Data_PE,
and then stores the Data_PE in IPFS, which will return the corresponding address \text{ads}_{Data}_{PE}.
Step 2. The PE chooses a random number $k_1$ at random and calculates the hash value

$$h_{Data_{PE}} = hash(Data_{PE})$$

(3)

of $Data_{PE}$, and generates a message containing $h_{Data_{PE}}$ and the timestamp $T_1$.

$$M_{PE} = (ID_{PE} || ID_{PM} || h_{Data_{PE}} || ads_{Data_{PE}} || T_1)$$

(4)

PE generates the signature $(r_{PE}, s_{PE})$ by calling the signature function of Algorithm 2.

$$(r_{PE}, s_{PE}) = Sign(M_{PE}, k_1, d_{PE})$$

(5)

The PE encrypts the data and generates an encrypted message using a public key issued by the PM at the center of the blockchain:

$$C_{PE} = E_{Puk_{PM}}(M_{PE})$$

(6)

PE encapsulates the encrypted data into transaction information and then uploads the transaction information to the Hyperledger Fabric network center by invoking Algorithm 3. PE sends the successful upload message to PM via the client and finally transports the tea to the processing machinery via logistics.

---

**Algorithm 2. ECDSA’s process**

```go
func Signature(k string, d string, H string) (r string, s string) {
    (x, y) = k * G
    r = x / n
    if (r != 0)
        s = (H + r * d) / k mod n
    else
        return false
    return r, s
}
```

```go
func Verify(H string, r string, s string) (res string) {
    u1 = (H mod n) / s
    u2 = (r mod n) / s
    Q ← cert.PublicKey
    (x, y) = u1 * G + u2 * Q
    if (x == r)
        return true
    else
        return false
}
```

Algorithm 3. Upload the transaction information link code

```go
func addTransaction(stub shim.ChaincodeStubInterface, args []string) pb.Response {
    // Check input arguments
    if len(args) != 5 {
        return shim.Error("Incorrect number of arguments. Expecting 5")
    }
    // Create a new transaction
    transaction := Transaction{
        ID: args[0],
        Signature: args[1],
        Timestamp: args[2],
        Address: args[3],
        Message: args[4],
    }
    // Marshal the transaction into bytes
    transactionBytes, err := json.Marshal(transaction)
    if err != nil {
        return shim.Error("Failed to marshal transaction into bytes")
    }
    // Store the transaction on the ledger
    err = stub.PutState(transaction.ID, transactionBytes)
    if err != nil {
        return shim.Error(fmt.Sprintf("Failed to store transaction with ID %s: %s", transaction.ID, err.Error()))
    }
    // Return a successful response
    return shim.Success(nil)
}
```

3.7. Process Phase

Step 1. The PM receives the notification from the PE client at T2 and receives the material at the same time. The PM then accesses the Hyperledger Fabric Network Center to query the records uploaded by PE and decrypts them with his private key.

\[
M_{PE} = D_{PRK_{PM}}(C_{PE}) \tag{7}
\]

The PM then verifies the timeliness of the data by timestamp.

\[
\text{Check}(T2 - T1) \leq \Delta T \tag{8}
\]

PM verifies the validity of the signature by using the verification function in Algorithm 2.

\[
h'_{Data_{PE}} = \text{hash}(Data_{PE}) \tag{9}
\]

\[
\text{Verify}\left(h'_{Data_{PE}}, r_{PE}, s_{PE}\right) \tag{10}
\]

If the signature is legitimate, the PM obtains the production data \(M_{PE}\) through the IPFS address \(Data_{PE}\).

Step 2. The PM compares the quality of tea raw materials with the obtained \(Data_{PE}\). After ensuring the quality, the data \(Data_{PE}\) as part of the traceability code will be encapsulated into retrospective source code (RSC) by using Algorithm 4. At the same time, the processing mechanism will process and package the raw material and encapsulate the relevant proof of technological operation \(Data_{TO}\) into the RSC together. During the processing and packaging process, PM chooses the number \(k2\) at random and calculates the hash value

\[
h_{Data_{TO}} = \text{hash}(Data_{TO}) \tag{11}
\]
of $Data_{TO}$, and generates a message containing $h_{Data_{TO}}$ and the timestamp $T3$.

$$M_{PM} = \langle ID_{PM} || ID_{R} || h_{Data_{TO}} || T3 \rangle$$  \hspace{1cm} (12)

PM generates the signature $(r_{PM}, s_{PM})$ by using the signature function in Algorithm 2.

$$(r_{PM}, s_{PM}) = \text{Sign}(M_{PM}, k2, d_{PM})$$  \hspace{1cm} (13)

R’s public key

$$C_{PM} = E_{Puk_{R}}(M_{PM})$$  \hspace{1cm} (14)

encrypts the resulting encrypted message by PM.

PM encapsulates the data as transaction information and uploads them to the Hyperledger Fabric Network Center. Finally, the RSC is printed on the processed tea package and transported to R via logistics.

---

**Algorithm 4. Generate retrospective source code.**

```python
import qrcode
import cv2 as cv

data_img = cv.imread("img path")
data_video = cv2.VideoCapture("video path")
data_word = "message"

rsc = qrcode.QRCode(version = 1,
    error_correction = qrcode.constants.ERROR_CORRECT_L,
    box_size = 8,
    border = 8,
)

rsc.add_data(data_img,data_video,data_word)
rsc.make(fit = True)
img = rsc.make_image()
img.save('tsc_code.png')
```

---

### 3.8. Sale and Purchase Phase

This phase is mainly composed of the retailing of tea by distributors and the purchase of tea by customers, and the physical interaction is between R and C.

Step 1. R receives the tea that has been processed and packaged at the moment. R accesses the Hyperledger Fabric Network Center to query the records uploaded by the PM and, at the same time, decrypts them using its private key:

$$M_{PM} = D_{PRK_{R}}(C_{PM})$$  \hspace{1cm} (15)

R uses the timestamp to confirm the accuracy of the data:

$$\text{Check}(T3 - T2) \leq \Delta T$$  \hspace{1cm} (16)

R uses Algorithm 2’s verification function to check the signature’s validity.

$$h'_{Data_{TO}} = \text{hash}(Data_{TO})$$  \hspace{1cm} (17)

$$\text{Verify}\left(h'_{Data_{TO}} , r_{PM}, s_{PM}\right)$$  \hspace{1cm} (18)

R will then scan the RSC to verify all the production and processing processes of the tea, and if there is no problem, R will put it on the shelves for sale.

Step 2. C can scan the RSC of the tea to identify the authenticity of the tea before purchase, and after the purchase is complete, the system will generate the order. All the
order information is available \((\text{Data}_{\text{Order}})\); R will randomly select a random number \(k3\) and calculate the hash value
\[
h_{\text{Data}_{\text{Order}}} = \text{hash}(\text{Data}_{\text{Order}})
\]
of \(\text{Data}_{\text{Order}}\), and then generate transaction information containing \(h_{\text{Data}_{\text{Order}}}\) and timestamp \(T4\):
\[
M_R = (\text{ID}_R \mid \text{ID}_C \mid h_{\text{Data}_{\text{Order}}} \mid T4)
\]
R generates a signature \((r_R, s_R)\) by invoking the signature algorithm.
\[
(r_R, s_R) = \text{Sign}(M_R, k3, d_R)
\]
The public key of C is used to encrypt the message it generates in encrypted form.
\[
C_R = E_{\text{Puk}_C}(M_R)
\]
R encapsulates all the data into a transaction message and uploads them to the Hyperledger Fabric hub, where the transaction ends.

### 3.9. Supervision Phase

After the generation of tea transaction records, customers will enter this stage only if they need to defend their rights and interests, and the main interaction objects of this stage are C and MS. The supervision flow chart is shown in Figure 4.

![Supervision flow chart](image)

**Figure 4.** Supervision flow chart.

Step 1. The customer can file a complaint about his order with the market supervisor through the client. C edits the complaint and the evidence of the complaint \(\text{Data}_{\text{Appeal}}\), then chooses a random number \(k4\) at random and calculates the hash value
\[
h_{\text{Data}_{\text{Appeal}}} = \text{hash}(\text{Data}_{\text{Appeal}})
\]
of \(\text{Data}_{\text{Appeal}}\), and generates a transaction message containing \(h_{\text{Data}_{\text{Appeal}}}\) and the timestamp \(T5\):
\[
M_C = (\text{ID}_C \mid \text{ID}_M \mid h_{\text{Data}_{\text{Appeal}}} \mid T5)
\]
C generates a signature \((r_C, s_C)\) by invoking the signature algorithm.
\[
(r_C, s_C) = \text{Sign}(M_C, k4, d_C)
\]
C’s public key encrypts the message
\[
C_C = E_{\text{Puk}_M}(M_C)
\]
it generates in encrypted form.
C sends the complaint message to MS.
Step 2. At time \(T6\), when MS receives the complaint message from C, it decrypts it with the use of its private key.
\[
M_C = D_{\text{PRK}_M}(C_C)
\]
MS uses the timestamp to confirm the accuracy of the data.
\[
\text{Check}(T6 - T5) \leq \Delta T
\]
R uses Algorithm 2’s verification function to check the signature’s validity.

\[ h'_{Data\text{Appeal}} = hash\left(Data\text{Appeal}\right) \]  

(29)

\[ Verify\left(h'_{Data\text{Appeal}}, r_C, s_C\right) \]  

(30)

After confirming the authenticity of the complaint information, MS will intervene in the market to regulate fake and inferior tea.

Step 3. MS will first collect the signature information of each stage, such as the signature information of PE, PM, and R. If one or more of the signatures is faulty, it means there is counterfeiting at that stage. MS will regulate the entities involved in counterfeiting.

4. Security Analysis

4.1. Data Integrity

The suggested study subject employs the ECDSA method to sign the data used in the supply chain process for tea to ensure the integrity and tamper resistance of the information in the transmission process. We take the example of the production stage added to the blockchain tea supply chain and verify the signature process of its production data as follows:

\[
(r_{PE}, s_{PE}) = Sign(M_{PE}, k_1, d_{PE})
\]

(31)

\[
= (rG, r + hash(M_{PE} || ID_{PE} || ID_{PM} || h_{Data_{PE}} || ads_{Data_{PE}} || T1))
\]

The validation process is as follows:

\[ h'_{Data_{PE}} = hash(Data_{PE}) \]  

(32)

\[ u_1 = s_{PE}^{-1}h'_{Data_{PE}} \mod n \]  

(33)

\[ u_2 = s_{PE}^{-1}r_{PE} \mod n \]  

(34)

\[
(x'_{PE}, y'_{PE}) = u_1G + u_2G
\]  

(35)

When \( x'_{PE} = r_{PE} \), the data have not been altered, the validity of the data source can be confirmed, and the signature is recognized to be legitimate. If the data integrity has been damaged, \( x'_{PE} \neq r_{PE} \) will appear. The hash value validation of each stage is shown in Table 2.

**Table 2. Validation of each stage’s hash value.**

<table>
<thead>
<tr>
<th>Phase</th>
<th>Hash Value</th>
<th>Integrity Check</th>
</tr>
</thead>
<tbody>
<tr>
<td>Process phase</td>
<td>( h'<em>{Data</em>{PE}} = hash(Data_{PE}) )</td>
<td>( Verify\left(h'<em>{Data</em>{PE}}, r_{PE}, s_{PE}\right) )</td>
</tr>
<tr>
<td>Sale and Purchase phase</td>
<td>( h'<em>{Data</em>{TO}} = hash(Data_{TO}) )</td>
<td>( Verify\left(h'<em>{Data</em>{TO}}, r_{PM}, s_{PM}\right) )</td>
</tr>
<tr>
<td>Supervision phase</td>
<td>( h'<em>{Data</em>{Appeal}} = hash(Data_{Appeal}) )</td>
<td>( Verify\left(h'<em>{Data</em>{Appeal}}, r_C, s_C\right) )</td>
</tr>
</tbody>
</table>

Scenario: False data will be signed and posted to the blockchain center if an unethical merchant attempts to tamper with the production data to use it as a stand-in for actual goods.

Analysis: After receiving the tea raw materials, the entity at the center of the blockchain network, such as the processing company, employs the verification function in Algorithm 2 to confirm their authenticity. If the verification is successful, the processing organization
parses the data, obtains the detailed IPFS address, and submits a request to view the data. The hash value of the data is then calculated, and if it differs from the hash value recorded in the blockchain ledger, either the batch of tea has poor quality, or the businessman has lied about his identity.

4.2. Tamper-Resistant

The security of the on-chain data is guaranteed by federated blockchain technology. A binary tree integrated with a Merkle tree structure will be constructed using all the chain data stored in a block. As illustrated in Figure 5, the hash value between every two data records in the Merkle tree will be concatenated as the input to the next binary tree node. If an attacker attempts to tamper with any data record, the root node of the Merkle tree will change dramatically due to the property of the SHA-256 cryptographic hash. If you arbitrarily change the left side of the data, the corresponding right hash value will be completely different. Just like in SHA-256 encryption, as long as the input is slightly changed, the output hash value will be substantially different.

![Merkle tree structure](image-url)

Figure 5. Merkle tree structure.

So, if an attacker tries to modify the blockchain data, the hash of the corresponding Merkle tree leaf nodes will change. The root hash is calculated recursively based on all leaf nodes; any leaf node changes will lead to a completely different root hash. As a result, when others who participated check the block information, they will see that the content has been altered [27].

4.3. Traceability

Since blockchain is employed as the fundamental technology, all transactions conducted by members of the federated blockchain will be acknowledged as valid transactions recorded on-chain, safeguarding them from malicious tampering [28]. Owing to the immutability of data, the system can enable reliable traceability and prevent fraud at the source. For instance, in the stage of producing tea, the information about tea in the ledger will be permanently maintained in the blockchain after uploading the information relevant to the production of tea to the blockchain.

Situation: PE discovers a flaw in the tea’s quality but is unable to identify which link in the production process is at fault.

Analysis: To compare and verify the data in the blockchain and assure their traceability by signature, utilize the blockchain’s immutability and traceability. If we wish to verify and track how PM interacts with PE, we can assess whether the data between PE and PM are accurate using the following formula:

\[
(r_{PE}, s_{PE}) = \text{Sign}(M_{PE}, k_1, d_{PE})
\]
\[(r_{PM}, s_{PM}) = \text{Sign}(M_{PM}, k2, d_{PM})\]  
(37)

4.4. Non-Repudiation

ECDSA signature verification is necessary at every level; therefore, data non-repudiation can be achieved by checking it. The recipient needs the public key for verification since every data transmission requires the participant’s secret key signature. After verifying that the sender’s message content is correct and authentic, the receiver will not reject it. The non-repudiation of each level is displayed in Table 3.

Table 3. Non-repudiation of the suggested plan.

<table>
<thead>
<tr>
<th>Phase</th>
<th>Item</th>
<th>Signature Value</th>
<th>Sender</th>
<th>Receiver</th>
<th>Signature Verification</th>
</tr>
</thead>
<tbody>
<tr>
<td>Production phase</td>
<td>((r_{PE}, s_{PE}))</td>
<td>PE</td>
<td>PM</td>
<td>(x_{PE} \equiv r_{PE} \mod n)</td>
<td></td>
</tr>
<tr>
<td>Process phase</td>
<td>((r_{PM}, s_{PM}))</td>
<td>PM</td>
<td>R</td>
<td>(x_{PM} \equiv r_{PM} \mod n)</td>
<td></td>
</tr>
<tr>
<td>Sale and Purchase phase</td>
<td>((r_{R}, s_{R}))</td>
<td>R</td>
<td>C</td>
<td>(x_{R} \equiv r_{R} \mod n)</td>
<td></td>
</tr>
<tr>
<td>Supervision phase</td>
<td>((r_{C}, s_{C}))</td>
<td>C</td>
<td>MS</td>
<td>(x_{C} \equiv r_{C} \mod n)</td>
<td></td>
</tr>
<tr>
<td></td>
<td>((r_{MS}, s_{MS}))</td>
<td>MS</td>
<td>Hyperledger Fabric</td>
<td>(x_{MS} \equiv r_{MS} \mod n)</td>
<td></td>
</tr>
</tbody>
</table>

4.5. Privacy Protection

At the ledger level, a Hyperledger Fabric offers a channel-like structure for data privacy protection. A channel’s function in a blockchain network is to enable business isolation, where a business correlates to a channel and entities outside of that channel are unable to access the data within that channel. Participants in the same Hyperledger Fabric network can create multiple channels according to their business needs, ensuring that data are exchanged only within that channel. The creation of channels significantly protects data privacy. Participants send their ID\(_X\) to the CA node, which will then return the associated public–private key pair \((d_{X}, Q_{X})\) for that entity if the CA confirms that the information is accurate.

4.6. Resist Known Attacks

Every node in the tea supply chain can participate in a decentralized platform that is constructed using Hyperledger Fabric applied to the tea supply chain. Every transaction on the platform will be recorded in a tamper-proof distributed ledger that can be verified and audited by every node in the tea supply chain. In this approach, issues like data manipulation and man-in-the-middle attacks may be prevented, ensuring the reliability and security of transactions throughout the tea supply chain.

Hyperledger Fabric provides the following capabilities to successfully ward off blockchain attacks:

- Byzantine Fault Tolerance (BFT): Hyperledger Fabric makes use of the BFT algorithm, which keeps the platform’s dependability and accuracy even if a few nodes are attacked or fail.

- Protection from data leakage and tampering with encryption: Hyperledger Fabric supports a variety of encryption techniques, including hash algorithms, symmetric encryption algorithms, and asymmetric encryption algorithms.

- Scalability: Hyperledger Fabric has a high degree of scalability and can dynamically change the network’s size and capacity to meet changing demands.
4.6.1. Man-in-the-Middle Attack

A man-in-the-middle assault occurs when a perpetrator can alter messages in transit to ask particular queries or make requests as part of their attack if they have control over the communication channel [29].

Scenario: For instance, during PM and PE communication, an attacker might intercept data about tea production or might try to manipulate the assessed price of tea after intentionally interfering with the data sent by the PM.

\[ C_{PE} = E_{Puk_{PM}}(M_{PE}) \] (38)

\[ M_{PE} = D_{PRK_{PM}}(C_{PE}) \] (39)

4.6.2. Replay Attack

In a replay attack, the attacker repeatedly requests the same packets that were previously received from the server side. If it is not effectively avoided, the server side can successfully pass the authentication because the packets have already been verified as legitimate [30]. To guard against replay attacks, each transaction message has a timestamp that is set as it is posted and received. The time difference between when the transaction message was transmitted and when it was received can be calculated by the receiver. As an illustration, consider how PM and PE interacted. The verdict is as follows:

If an attacker intercepts a transaction message sent by a sender in the tea supply chain, they could launch a replay attack by resending the identical message to the intended recipient.

Analysis: To establish a distinctive timestamp, the recipient decrypts the encrypted message they have just received. They then subtract the time stamp from when the message was sent from the time they are currently receiving it. If the timestamp verification is incorrect, the receiver can be recognized as a replay attack.

\[ M_{PE} = \left( ID_{PE} || ID_{PM} || h_{Data_{PE}} || ads_{Data_{PE}} || T1 \right) \] (40)

\[ C_{PE} = E_{Puk_{PM}}(M_{PE}) \] (41)

\[ M_{PE} = D_{PRK_{PM}}(C_{PE}) \] (42)

\[ \text{Check}(T2 - T1) \leq \Delta T \] (43)

5. Performance Evaluation
5.1. Performance Analysis

This section assesses the chain code contract calls’ performance for the scenarios put forth in this study. The testing tool uses Hyperledger Caliper version 0.42, whereas the blockchain platform utilizes Hyperledger Fabric version 2.3. A benchmarking tool called Hyperledger Caliper was created to evaluate the blockchain platform’s scalability and performance. Caliper can be used to create and run a range of benchmark tests, including ones for transaction speed, latency, resource usage, and other metrics. It was developed by 30 founding corporate members, including IBM, and is headed by the Linux Foundation. We tested transaction throughput (number of transactions per second: the performance bottleneck of the system in processing transactions), latency (average response time: the response time and performance bottleneck of the system), and resource utilization (the resource utilization and performance bottleneck of the system in processing transactions) on our Intel Core i9-11900K, RAM: 32GB DDR4 configuration. The results are displayed in Figures 6–9.
We examine the connection between transaction volume and CPU and memory consumption in Figures 6 and 7. The progressive increase in CPU and memory usage as the number of transactions rises suggests that the system’s processing power may be constrained as the workload rises. Figures 8 and 9 illustrate how the system’s performance degrades as the number of transactions rises, resulting in increased latency and decreased throughput. When there are 3500 transactions, the CPU and memory use spike dramatically because the system has hit its processing capacity and cannot effectively handle any more requests.

![CPU occupancy variation graph.](image)

![Memory occupancy variation graph.](image)

In Figure 8, we analyze the relationship between the number of transactions and the throughput, and we can see that the number of write transactions and read transactions show a gradual increase as the number of transactions increases. At a transaction count of 500, the number of write transactions is 456 TPS and the number of read transactions is 1042 TPS, while at a transaction count of 5000, the number of write transactions increases to 3713 TPS and the number of read transactions increases to 3930 TPS.
In Figure 9, we analyze the relationship between the number of transactions and latency, and we can see that the latency time of both write and read transactions increases as the number of transactions increases, with a minimum write speed of 0.97 s and a maximum of 6.26 s, and a minimum read speed of 0.1 s and a maximum of 4.62 s. This performance system’s processing capacity may be limited as the load increases. For the same number of transactions, the latency of write transactions is usually longer than that of read transactions because write transactions require more computation and storage operations. As the number of transactions increases, the gap between the latency times of write and read transactions gradually shrinks, which may indicate that the processing capacity of the system has reached a bottleneck and cannot efficiently handle more requests.

When combined, these statistics offer helpful details on load management and system performance that can be used to improve the system’s performance. We are effective when compared to the functionality of current Hyperledger Fabric application solutions [31]. Decisions must be taken based on the unique system architecture and application scenarios if particular optimization tactics are still required. System performance enhancement will probably be required, including expanding hardware resources, streamlining the code, and changing load-balancing tactics.
5.2. Communication Cost

The communication scenario analyzed in this study is summarized in the following table: The highest transmission speed in a 4G network environment is 100 Mbps, while in a 5G network environment, it is 20 Gbps. The length of the ECDSA signature is 160 bits, 160 bits is the length of the key, 256 bits is the length of the hash function, 1024 bits is the length of the request information, 1024 bits is the length of the transaction information, and 160 bits is the length of other information (such as the identifying timestamp, etc.).

As an illustration, let us use the selling and purchase phase, which has the largest communication cost. First, R needs to verify the decrypted PM message, which contains a decrypted message, a hash value, and another message with a total size of 160 bits + 256 bits + 160 bits = 576 bits. R purchases the tea operation, which contains an encrypted message, a hash value, a signature, another message, and a transaction message, with a total size of 160. R uploads the order data after verifying it, which has a total size of 160 bits + 160 bits + 2*256 bits + 160 bits + 1024 bits + 160 bits = 2176 bits and includes a decryption message, an encryption message, two hash values, a signature, a transaction message, and another message. Speed is therefore necessary in diverse network contexts, as indicated in Table 4.

Table 4. Cost of communication.

<table>
<thead>
<tr>
<th>Phase</th>
<th>Item</th>
<th>Message Length</th>
<th>4G (100 Mbps)</th>
<th>5G (20 Gbps)</th>
</tr>
</thead>
<tbody>
<tr>
<td>Registration phase (X-HFN)</td>
<td>736 bits</td>
<td>7.4 µs</td>
<td>0.037 µs</td>
<td></td>
</tr>
<tr>
<td>Production phase (PE-PM)</td>
<td>1760 bits</td>
<td>17.6 µs</td>
<td>0.088 µs</td>
<td></td>
</tr>
<tr>
<td>Process phase (PM-R)</td>
<td>2016 bits</td>
<td>20.2 µs</td>
<td>0.101 µs</td>
<td></td>
</tr>
<tr>
<td>Sale and Purchase phase (R-C)</td>
<td>4032 bits</td>
<td>40.3 µs</td>
<td>0.202 µs</td>
<td></td>
</tr>
<tr>
<td>Supervision Phase (R-C-MS)</td>
<td>3232 bits</td>
<td>32.32 µs</td>
<td>0.162 µs</td>
<td></td>
</tr>
</tbody>
</table>

Notes: Any user in the alliance chain (X); planting enterprise (PE); processing mechanism (PM); retailers (R); consumers (C); market supervision (MS); hyperledger fabric network (HFN).

5.3. Computation Cost

The costs connected with each stage of the approach for this article are listed in Table 5 below. The asymmetric decryption and encryption processes in ECDSA, along with the hashing operation, provide the basis for the cost analysis.

Table 5. Computation cost.

<table>
<thead>
<tr>
<th>Phase</th>
<th>Party</th>
<th>( T_{\text{Enc}} + 2T_{\text{Sig}} + T_H )</th>
<th>( 2T_H + T_{\text{Enc}} + T_{\text{Sig}} + T_{\text{Dec}} + T_{\text{Ver}} )</th>
<th>( 4T_H + 2T_{\text{Enc}} + 2T_{\text{Sig}} + 2T_{\text{Dec}} + 2T_{\text{Ver}} )</th>
<th>( 3T_H + T_{\text{Enc}} + 2T_{\text{Sig}} + 3T_{\text{Dec}} + 3T_{\text{Ver}} )</th>
</tr>
</thead>
<tbody>
<tr>
<td>Production phase (PM)</td>
<td></td>
<td>( T_{\text{Enc}} + 2T_{\text{Sig}} + T_H )</td>
<td>( 2T_H + T_{\text{Enc}} + T_{\text{Sig}} + T_{\text{Dec}} + T_{\text{Ver}} )</td>
<td>( 4T_H + 2T_{\text{Enc}} + 2T_{\text{Sig}} + 2T_{\text{Dec}} + 2T_{\text{Ver}} )</td>
<td>( 3T_H + T_{\text{Enc}} + 2T_{\text{Sig}} + 3T_{\text{Dec}} + 3T_{\text{Ver}} )</td>
</tr>
<tr>
<td>Process phase (PE)</td>
<td></td>
<td>( 2T_H + T_{\text{Enc}} + T_{\text{Sig}} + T_{\text{Dec}} + T_{\text{Ver}} )</td>
<td>( 4T_H + 2T_{\text{Enc}} + 2T_{\text{Sig}} + 2T_{\text{Dec}} + 2T_{\text{Ver}} )</td>
<td>( 3T_H + T_{\text{Enc}} + 2T_{\text{Sig}} + 3T_{\text{Dec}} + 3T_{\text{Ver}} )</td>
<td></td>
</tr>
<tr>
<td>Sale and Purchase phase (R and C)</td>
<td></td>
<td>( 4T_H + 2T_{\text{Enc}} + 2T_{\text{Sig}} + 2T_{\text{Dec}} + 2T_{\text{Ver}} )</td>
<td>( 3T_H + T_{\text{Enc}} + 2T_{\text{Sig}} + 3T_{\text{Dec}} + 3T_{\text{Ver}} )</td>
<td></td>
<td></td>
</tr>
<tr>
<td>Supervision Phase (MS)</td>
<td></td>
<td>( 3T_H + T_{\text{Enc}} + 2T_{\text{Sig}} + 3T_{\text{Dec}} + 3T_{\text{Ver}} )</td>
<td></td>
<td></td>
<td></td>
</tr>
</tbody>
</table>

Notes: \( T_{\text{Enc}} \): encryption operation, \( T_{\text{Dec}} \): decryption operation, \( T_{\text{Sig}} \): signature operation, \( T_H \): hash function operation, and \( T_{\text{Ver}} \): verify operation.

5.4. Comparison

Treiblmaier et al. [11] suggested applying blockchain technology to the food supply chain to address the problem of multiple instances of information asymmetry by using it as a label to identify blockchain-based traceability systems as a primary driver of perceived product quality and purchase intentions. Paul et al. [12] proposed a workable architecture to support a circular supply chain for the tea industry network that uses blockchain technology as a substrate to drive RFID technology to complete the circular supply chain operation, despite the fact that they did not specify the precise integrated procedure. The circular blockchain platform developed by Centobelli et al. includes manufacturers, reverse
logistics service providers, selection centers, recycling facilities, and landfill applications in a supply chain scenario (ref. [13]). However, the security of the proposed blockchain platform was not investigated. Helo et al. [14] developed a cloud-based portal pilot system for real-time logistics and supply chain tracking and tracing. Chang et al. [15] proposed that blockchain and smart contract technology can support cross-enterprise business process re-engineering and ensure the intelligent advancement of business processes through smart contract technology within the framework of their proposed system in order to benefit from the advantages of the blockchain platform. However, there is no logical justification for the creation of smart contracts. A comparison of the proposed scheme’s functionality to earlier designs is shown in Table 6.

Table 6. Comparison of the proposed scheme’s functionality to that of earlier schemes.

<table>
<thead>
<tr>
<th>Authors</th>
<th>Year</th>
<th>Objective</th>
<th>1</th>
<th>2</th>
<th>3</th>
<th>4</th>
<th>5</th>
</tr>
</thead>
<tbody>
<tr>
<td>Treiblmaier et al.</td>
<td>2023</td>
<td>As a signaling mechanism, a blockchain tag proves that blockchain can influence and perceive purchase intention through signal theory.</td>
<td>Y</td>
<td>Y</td>
<td>N</td>
<td>Y</td>
<td>N</td>
</tr>
<tr>
<td>Paul et al.</td>
<td>2022</td>
<td>An operational model supporting the network cycle supply chain of the tea sector is created by radio frequency identification (RFID) technology, which is driven by blockchain technology (BCT) encryption based on policies.</td>
<td>Y</td>
<td>Y</td>
<td>Y</td>
<td>Y</td>
<td>N</td>
</tr>
<tr>
<td>Centobelli et al.</td>
<td>2022</td>
<td>For the circular blockchain platform, the objective was to construct a thorough triple retry architecture to link three circular supply chain reverse operations (such as recycling, redistribution, and remanufacturing) technologies and establish a reward system between the two.</td>
<td>Y</td>
<td>N</td>
<td>N</td>
<td>Y</td>
<td>Y</td>
</tr>
<tr>
<td>Helo et al.</td>
<td>2020</td>
<td>Proposed a cloud-based portal pilot system for real-time tracking and traceability of logistics and supply chains.</td>
<td>Y</td>
<td>N</td>
<td>Y</td>
<td>N</td>
<td>N</td>
</tr>
<tr>
<td>Chang et al.</td>
<td>2019</td>
<td>A blockchain-based business process re-engineering (BPR) framework was proposed and explored to automate business flows in tracking supply chain processes.</td>
<td>Y</td>
<td>N</td>
<td>Y</td>
<td>N</td>
<td>N</td>
</tr>
<tr>
<td>Ours</td>
<td>2023</td>
<td>A fabric-based production data sharing and storage model system for the tea supply chain was proposed.</td>
<td>Y</td>
<td>Y</td>
<td>Y</td>
<td>Y</td>
<td>Y</td>
</tr>
</tbody>
</table>

Notes: 1: Blockchain architecture, 2: Encryption key, 3: Authorization, 4: Scalability, 5: Off-chain storage; (Y) Yes; (N) No.

5.5. Architecture Comparison

The three main types of blockchain architectures available now are public, private, and federated blockchains. While public blockchains allow open data visibility for anyone, they are not ideal for preserving confidential business data. On the other hand, private blockchains concentrate data access, which is unfavorable for inter-enterprise data sharing. Table 7 compares the three systems: Bitcoin [32], Ethereum [33], and Hyperledger Fabric [34]. The figure below illustrates Hyperledger Fabric, which can be applied to various application scenarios, including the one discussed in this study, and has more flexible and pluggable modules than Bitcoin and Ethereum. Additional benefits of Hyperledger Fabric are confidentiality, improved performance, and higher throughput.
Table 7. Comparison between Ethereum and Hyperledger Fabric.

<table>
<thead>
<tr>
<th>Description</th>
<th>Bitcoin</th>
<th>Ethereum</th>
<th>Hyperledger Fabric</th>
</tr>
</thead>
<tbody>
<tr>
<td></td>
<td>Platform for quantitative blockchains</td>
<td>Platform for a modular blockchain</td>
<td>Platform for a generic blockchain</td>
</tr>
<tr>
<td>Scene</td>
<td>Public chain</td>
<td>Public chain</td>
<td>Federation chain</td>
</tr>
<tr>
<td>Consensus algorithm</td>
<td>Proof of Work (POW)</td>
<td>Proof of Work (POW)</td>
<td>Practical Byzantine Fault Tolerance (PBFT)</td>
</tr>
<tr>
<td>Throughput</td>
<td>7 TPS</td>
<td>25 TPS</td>
<td>5000 TPS</td>
</tr>
<tr>
<td>Decentralization</td>
<td>Completely decentralized</td>
<td>Completely decentralized</td>
<td>Partial de-centralization</td>
</tr>
<tr>
<td>Smart contract</td>
<td>No</td>
<td>YES</td>
<td></td>
</tr>
<tr>
<td>Scalability</td>
<td>No</td>
<td>No</td>
<td>YES</td>
</tr>
<tr>
<td>Authentication</td>
<td>No</td>
<td>No</td>
<td>YES</td>
</tr>
<tr>
<td>Privacy</td>
<td>No</td>
<td>No</td>
<td>YES</td>
</tr>
<tr>
<td>Pluggability</td>
<td>No</td>
<td>No</td>
<td>YES</td>
</tr>
</tbody>
</table>

6. Conclusions

In this paper, we provide a Hyperledger Fabric-based method for tracking manufacturing data along the tea supply chain. We employ ECDSA and IPFS storage as well as smart contracts to guarantee data confidentiality, integrity, non-repudiation, storage performance, and automatic transaction triggering throughout the system to increase system efficiency. The contributions that can be achieved are as follows:

1. The addressing of the credit issue. The involvement of multiple institutions, each of which oversees the others, ensures the accuracy of the information. Additionally, the chain of information cannot be altered, considerably reducing the possibility of cheating.

2. The tracking of all records. Regarding the open, transparent, and capable express logistics tracking of the manufacturing, processing, testing, transportation, and warehousing to the shelves of items for sale, each link in time following the point is fully recorded.

3. The definition of roles and the ability to track down issues. The open and transparent features of blockchain cannot be altered. Finding the problematic link as soon as it manifests itself in one link is both timely and efficient.

4. The stopping of product counterfeiting. Since the products can be checked from the source all the way to the customer’s hands when the information about the goods is posted on the supply chain, there will not be a problem with counterfeiting.

In the future, we will focus on practical system application landing research. Blockchain technology can help enterprises in the tea supply chain to achieve more accurate inventory management and logistics distribution, thus improving their operational efficiency and reducing costs. At the same time, blockchain technology can also help tea enterprises to achieve reductions in carbon emissions and increased energy savings, so as to better fulfill their social responsibility and environmental protection obligations. In summary, the application of blockchain technology in the tea supply chain has a very broad prospect. In the future, with the continuous development of technology and the continuous expansion of the tea market, we believe that blockchain technology will play an increasingly important role in the tea supply chain and contribute to the sustainable development of the tea industry.
Author Contributions: C.-L.C.: Conceptualization, Investigation, Methodology, Writing—review and editing, Formal analysis, Funding acquisition, and Supervision. W.-B.Z.: Conceptualization, Investigation, Methodology, Data curation, Software, and Writing—original draft. D.-C.H.: Investigation, Validation, and Supervision. L.-C.L.: Investigation, Validation, and Formal analysis. Y.-Y.D.: Formal analysis, Investigation, and Methodology. C.-G.K.: Investigation and Validation. All authors have read and agreed to the published version of the manuscript.

Funding: This work was supported by the National Science and Technology Council, Taiwan, R.O.C., under contract NSTC 112-2410-H-324-001-MY2.

Institutional Review Board Statement: This study is only based on basic theoretical research. It does not involve humans.

Informed Consent Statement: This study is only based on basic theoretical research. It does not involve humans.

Data Availability Statement: The data used to support the findings of this study are available from the corresponding author upon request.

Conflicts of Interest: The authors declare no conflict of interest.

References


28. Tian, F. A supply chain traceability system for food safety based on HACCP, Blockchain Internet of Things. In Proceedings of the International Conference on Service Systems and Service Management, Dalian, China, 16–18 June 2017. [CrossRef]


Disclaimer/Publisher’s Note: The statements, opinions and data contained in all publications are solely those of the individual author(s) and contributor(s) and not of MDPI and/or the editor(s). MDPI and/or the editor(s) disclaim responsibility for any injury to people or property resulting from any ideas, methods, instructions or products referred to in the content.