IEEE Access
Multidisciplinary ⋮ Rapid Review ⋮ Open Access Journal

Received 22 June 2023, accepted 8 July 2023, date of publication 13 July 2023, date of current version 19 July 2023.

Digital Object Identifier 10.1109/ACCESS.2023.3295210

RESEARCH ARTICLE

A Novel Resource-Saving and Traceable Tea Production and Supply Chain Based on Blockchain and IoT

XIAOFENG XU[1,2], **(Member, IEEE), XIANGLIN BAO**[1], **HAODONG YI**[1,3], **JUN WU**[1], **AND JINGLEI HAN**[1]

[1]School of Computer and Information, Anhui Polytechnic University, Wuhu 241000, China
[2]Industrial Innovation Technology Research Company Ltd., Anhui Polytechnic University, Wuhu 241000, China
[3]School of Computer Science and Engineering, South China University of Technology, Guangzhou 510640, China

Corresponding author: Xianglin Bao (baoxianglin@ahpu.edu.cn)

This work was supported in part by the Anhui Provincial Natural Science Foundation under Grant 2108085QF268 and Grant 2108085QF264, in part by the Advanced Research Project of Anhui Polytechnic University under Grant Xjky2020119, in part by the Research Start-Up Fund for Talent Introduction of Anhui Polytechnic University under Grant 2020YQQ062, and in part by the Anhui Future Technology Research Institute Enterprise Cooperation Project under Grant 2023qyhz14.

ABSTRACT To realize efficient cooperation among tea plantations, manufacturers, logistics, and sellers, the tea production and supply chain (PSC) benefits participating enterprises by coordinating tea planting, product processing, transportation, and product sales links. However, the current tea PSC lacks resource-saving automatic control and suffers from the effect of counterfeit tea products and inefficient supervision. To address these problems, in this work, blockchain and Internet of Things (IoT) technologies are applied to turn the tea PSC around with efficient automation and decentralized supervision. Specifically, we propose DeTea, a blockchain-IoT-empowered decentralized framework, for chain-wide tea counterfeiting supervision and automatic environment management. On the one hand, for the benefit of tea customers, an incentive scheme is designed based on blockchain technology to attract tea PSC participants and decentralized detectors to report dishonest participants, which can motivate the good behaviors of the participating enterprises for a healthier tea market. On the other hand, for the benefit of practitioners of tea products, we realize the automation of environment monitoring and equipment control via IoT technology. Moreover, we design an improved adaptive weighted data fusion algorithm for accurate IoT data and efficient resource allocation, and present an optimal irrigation strategy for automatic plantation environment adjustment. To evaluate the proposed solution, a prototype is implemented by designing a blockchain infrastructure with ten main smart contracts and constructing an IoT-based system sandbox for automatic environment monitoring and resource allocation. Experimental results demonstrate the high throughput of DeTea and the efficiency of resource-saving automation. This work introduces blockchain and IoT technologies to tea PSC for full-process traceability and automatic environment control, which is expected to extend to other agricultural products to ensure the safety, reliability, and efficiency of agricultural traceability systems.

INDEX TERMS Blockchain, Internet of Things, Resource-saving, Counterfeit detection, Automatic control.

I. INTRODUCTION

As a popular economic crop, tea has a high nutritional value for human health and has growing global demand [1]. Tea customers are showing increasing care about their fitness, and the quality and reputation of tea products have attracted more and more attention. The current tea production and supply chain (PSC) relies on experience-required manual control, which has high risk and low production efficiency. To produce high-quality tea products, plenty of experienced manpower is devoted to resource allocation and environment control. However, the oversight of manual-specified environment control

The associate editor coordinating the review of this manuscript and approving it for publication was Renato Ferrero.

causes great resource waste and enterprise losses. To relieve the high-quality tea product of the requirement of experience manpower and avoid the risk of human oversight, resource-saving automatic control must be achieved. With the rapid development of Internet of Things (IoT) technology, some research develops IoT-based agricultural information systems to enhance productivity and save human resources [2], [3].

Currently, most tea PSCs adopt IoT technology in the production process, while they often lack traceability throughout the entire process. Therefore, current tea PSCs are suffering from the effect of counterfeit tea products and inadequate supervision, which harms the tea market and receives considerable critical attention [4], [5], [6], [7]. Malicious enterprises that produce counterfeit and low-quality tea products are hidden in the tea market, and these counterfeit tea products could cause economic losses and health damage for tea consumers [3], [8]. It is worth noting that various enterprises are involved in the tea PSC but their information systems are isolated. Due to the information asymmetry problem in tea PSC [9], [10], it is difficult for tea customers to find trustworthy proof of tea quality and the indication of counterfeit tea products. Well-behaved enterprises devoting great resource costs to high-quality tea products are hard to build customer trust in the current unhealthy tea market. To protect the interests of tea customers and well-behaved enterprises, the problem of counterfeit tea products is urgent to be solved [11]. The joint efforts of tea PSC enterprises should be guaranteed to achieve information symmetry.

Recently, increasing researchers devoted themselves to achieving information symmetry for traceability of agricultural products, automotive, electronics, and aviation [12], [13], [14], [15], [16]. Cao et al. [17] explored the human-machine reconciliation mechanism of the beef supply chain and enabled shared responsibilities based on blockchain technology. Thakur et al. [18] designed a traceability system for the Norwegian hides supply chain based on the Radio Frequency Identification (RFID)-enabled hide tags. Biswas et al. [19] designed a blockchain-based traceability system for the wine supply chain to enable wine customers' verification and each blockchain transaction is visible to the relevant participants. Cao et al. [20] established a blockchain-based traceability system for steel products and eliminated the information islands. Tsai et al. [21] proposed a traceability model for tape management in semiconductor test companies and let information transfer transparently. However, there is no perfect chain-wide traceability solution to achieve information symmetry in the tea PSC and solve the problem of counterfeit tea products.

Taking the above problems into account, blockchain is introduced to break the information asymmetry and ensure decentralized supervision. Blockchain is a distributed and traceable ledger well-known for its transparency [22]. Multiple parties participate in the ledger updating, and each party is guaranteed to get the same data record of the blockchain ledger based on its consensus mechanism [23]. All the parties cooperate to manage and supervise the ledger records. As a blockchain component, the smart contract provides the programming API of the blockchain to achieve automatic execution without manual triggering [24]. Smart contracts are deployed and executed by all participating blockchain nodes. The blockchain participants can upload data to the blockchain and record it as ledger records, which are time-ordered, consistent, tramper-resistant, and transparent. The blockchain updating is under decentralized supervision, and the dishonest behaviors of blockchain nodes are all accountable [25].

Even if blockchain has features to achieve transparency and decentralized supervision, there are still some limitations when applying blockchain technology in tea PSC. The chain-wide tea product traceability needs the joint effort of the participants in the tea PSC. However, there are no sufficient incentives for chain-wide enterprises to participate in. Moreover, if all of the existing system modules of tea PSC rely on one blockchain, the cost will be quite high [26], [27]. We also observe that most processes of existing systems require plenty of human participation and lack automation [28], [29]. These human-participated processes make the malicious participants easily manipulate data and conduct tea counterfeiting [2]. Since the IoT is a landmark technology in automatic control, we apply IoT in tea PSC to avoid the risk of not only human oversight but also malicious data manipulation.

To sum up, in this work, we develop the DeTea, a blockchain-IoT-empowered platform, to achieve resource-saving automation and counterfeit detection for tea PSC. DeTea automates not only the resource allocation and environment control but also the data handling and incentive management of tea PSC. The data security of tea PSC is guaranteed from data collection to data exhibition. We design an improved adaptive weighted data fusion algorithm to guarantee the accuracy of the collected data. The resource-saving automatic control is achieved via IoT-based automatic plantation environment adjustment and the optimal irrigation strategy. DeTea can efficiently detect and track counterfeit products with its traceable blockchain record and incentive scheme. The malicious behaviors, such as uploading manipulated documents, revealing fake credentials, supporting the fake credentials, refusing valid credentials, and reporting invalid credentials, are accountable and deterred. The collusion of dishonest participants could be detected and punished.

In our prototype, we develop ten main smart contracts in Solidity for DeTea blockchain based on the FISCO-BCOS framework to achieve chain-wide traceability and decentralized supervision with incentives and deterrence. Inter Planetary File System (IPFS) is utilized to reduce the storage cost of the DeTea blockchain which enables the decentralized storage of the supplementary materials and records the supporting details of DeTea documents and credentials. For privacy, we encrypt the supplementary materials of DeTea documents and only the authorized

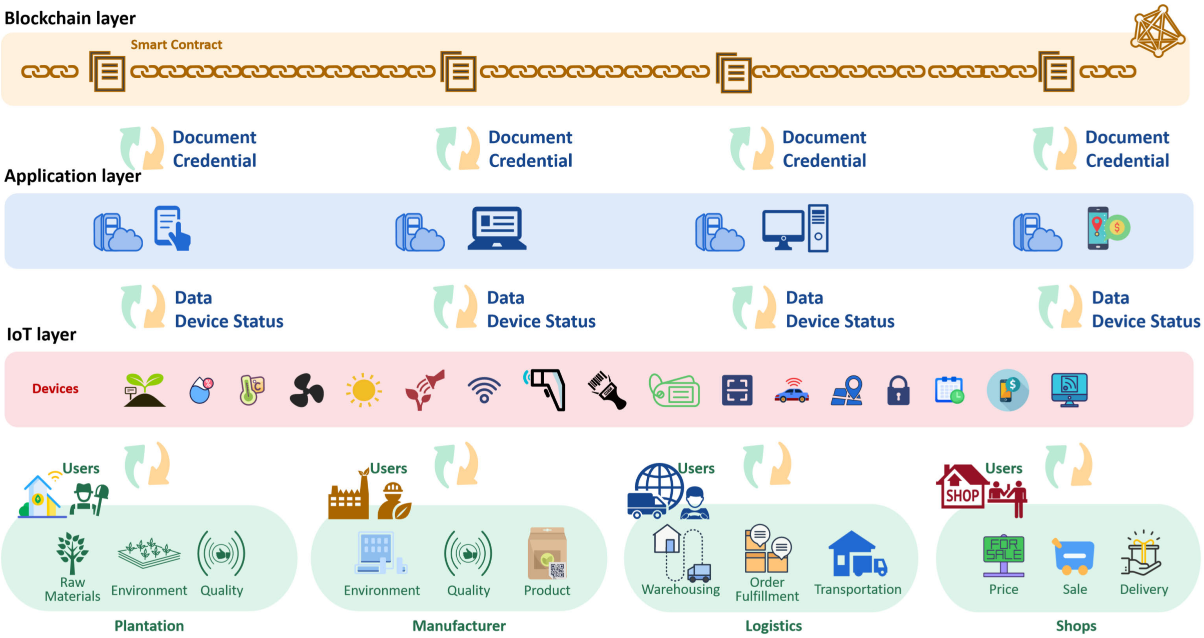


FIGURE 1. Overview of the DeTea architecture.

participants can access the details. We also build a sandbox model for DeTea to test the performance of autonomous environment monitoring and optimized equipment control. Experimental results demonstrate the high throughput of DeTea and the efficiency of data collection and environment control.

In conclusion, to improve the current tea SPC from traceability, quality, resource conservation, and automatic control for customers, practitioners, and policymakers, we propose a resource-saving and production-traceable framework based on blockchain and IoT technologies. The main contributions of this work are summarized as follows:

(1) We propose a novel framework DeTea for tea PSC to achieve resource-saving automation and counterfeit detection.

(2) For tea PSC automation, we propose IoT-based automatic control strategies to avoid abnormal data and reduce resource costs.

(3) We design an incentive scheme based on blockchain technology to deter malicious behaviors in the tea market.

The rest of this paper is organized as follows: Section II presents the literature review, Section III depicts the DeTea overview, Section IV proposes decentralized credential management and counterfeit detection, Section V proposes resource-saving automatic control, Section VI presents the DeTea implementation and performance, and Section VII draws the conclusion.

II. LITERATURE REVIEW

In recent years, some researchers have put forward solutions for product traceability. Thakur et al. [18] introduced a framework for automated traceability systems in the meat processing industry to improve data collection and exchange between the participants of a hide supply chain. With the proposed hide traceability system, the quality inspection data generated through the supply chain can be used as feedback to producers to improve farm processes and animal distribution and slaughtering. Cao et al. [17] implemented a cross-border beef supply chain between Australia and China based on blockchain technology to improve consumer trust. Based on the insights gained from discussions with supply chain stakeholders, they developed a human-machine coordination mechanism and deployed the mechanism into its traceability system, which has the trace responsibility of all supply chain stakeholders. Kumar and Tripathi [30] proposed a medical supply chain system based on blockchain to solve drug safety problems. They introduced a drug safety framework based on blockchain, which provides a transparent and safe channel among manufacturers, distributors, patients, hospitals, supervision, and other participants for drug safety. However, these works are faced with the high cost of data storage brought by blockchain and the open-access data records of blockchain can reveal private data to irrelevant parties. At the same time, these systems do not provide incentive schemes to attract honest participation and misbehavior detection. It is still challenging to guarantee efficient traceability when lacking chain-wide participation and supervision.

Several works applied blockchain as a data sharing and exchanging medium for IoT applications [31]. Li et al. [32] proposed BDDT for secure IoT data storage and trustworthy data transactions based on blockchain technology. Han et al. [33] designed an auditable access control system for IoT data. Feng et al. [34] proposed the access control framework for 5G-enabled industrial IoT based on the consortium blockchain. Li et al. [35] introduced a blockchain-based framework of the self-tallying voting system in decentralized IoT. These works provide novel strategies for IoT data storage and access control.

Furthermore, some research has focused on applying blockchain technology to the tea industry [10], [36], [37], [38], [39]. Mangla et al. [36] aimed to present a conceptual framework for the integration of blockchain technology to establish a sustainable tea supply chain, define possible actions, and prioritize the possible risks that may arise in this integration process. Wu et al. [37] analyzed the whole-process information of a tea supply chain from planting to sales, constructed the system architecture and each function, and designed a machine learning-blockchain-IoT-based tea credible traceability system. Paul et al. [10] extended the resource-based view and network theory by integrating blockchain technology into the tea supply chain and developed a conceptual model of a blockchain technology-driven tea supply chain. Paul et al. [38] developed a distributed and service-oriented system architecture that embraces a radio frequency identification-integrated blockchain technology-enabled circular supply chain practice model for a business-to-business tea industry network. Kumar and Dwivedi [39] provided a methodology for transforming traditional agriculture into smart farming, where all parties participating in the agricultural supply chain will be given an equal chance even if they are not related. IoT devices are incorporated to minimize human involvement in data collection, recording, and verification. These traceability systems use blockchain and IoT technologies, while they usually hard to guarantee the authenticity of product data required for traceability from the source. In this work, by effectively combining the advantages of blockchain and IoT technologies, we propose a blockchain-IoT-empowered platform DeTea with resource-saving automation and counterfeit detection for the tea PSC. DeTea automates the processes based on IoT technology to reduce human participation and guarantee data integrity from data collection to data exhibition. We also propose an adaptive weighted data fusion algorithm and an automatic plantation environment adjustment strategy to reduce resource costs and upgrade the tea product quality. Moreover, DeTea adopts an incentive scheme to attract more participants and incentive honest behavior.

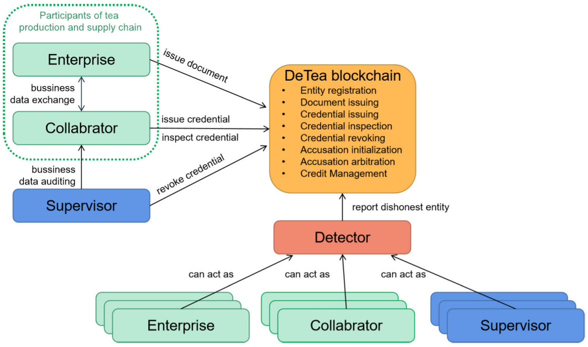


FIGURE 2. DeTea entities and interactions.

For tea PSC, there are different enterprises that manage their data in different ways and store their data on their own. The tea PSC data differed from formats is isolated and the enterprises in tea PSC are hard to be organized in a uniform way to trace the tea product based on the distributed and scattered data. Meanwhile, for tea products, the efficiency of the environment control influences the tea quality and requires much human effort. Therefore, Tea PSC requires a solution to automate and optimize its environment control. To meet the requirements of the chain-wide traceability and automation of tea PSC, this paper proposes DeTea, a chain-wide tea traceability system, with IoT-based automation and blockchain-empowered decentralized supervision. Compared to other existing traceability systems, Detea has two main contributions. On the one hand, the traceability of the DeTea covers the entire production process, including the plantation, manufacturer, logistics, and shops (as shown in Figure 1). On the other hand, Detea designs the incentives and deterrence schemes based on the participants' on-chain credit management. Therefore, DeTea can guarantee credit rewards to honest participants and credit deductions to dishonest participants, which also ensures the deterrence of corruption among malicious participants.

III. DeTea OVERVIEW

A. ARCHITECTURE

The architecture of DeTea, a chain-wide tea traceability system with IoT-based automation and blockchain-empowered decentralized supervision, is shown in Figure 1. DeTea has three layers, i.e. the IoT layer, blockchain layer, and application layer. It applies IoT and blockchain technology to achieve automatic and traceable process management for tea PSC. We also develop smart contracts for decentralized supervision and chain-wide tea traceability of DeTea.

The IoT layer collects the environmental information and product status with sensor devices, wireless sensor networks, GPS satellite positioning systems, and RFID technology. DeTea sensor devices monitor the illumination, temperature, humidity, water storage, air quality, CO2 concentration, battery voltage, and the invading creatures. The data fusion algorithm of DeTea improves the quality of the data collected by the IoT layer and the control parameters of IoT actuator equipment can be automatically decided by the fused IoT data and user preferences. DeTea also applies the optimal irrigation strategy to improve the environmental control of tea plantations. Moreover, the participants in tea PSC can trace the tea products circulated in DeTea with their RFID chip tags. Each circulated tea product is endowed with unique virtual identities and the digital identifier is written into its RFID chip tags. The participants collect chain-wide information about tea products and transmit the information to the downstream participants. The downstream participants enrich tea product information with the data generated by its links and transmitted to the next link. Only authorized parties can transmit data in the tea PSC via DeTea.

The blockchain layer provides open-access evidence of tea quality and indications of counterfeit tea products. The tea PSC participants can register as the blockchain network peers to maintain the blockchain ledger and trigger the smart contracts. Only the registered participants can get their key pairs and join the blockchain network to publish chain-wide data of tea PSC. The enterprises registered as DeTea blockchain nodes trigger DeTea smart contracts and upload the relevant documents of the tea products. Moreover, the published documents should be supported by the on-chain tea credentials. The enterprise's collaborators can register in the blockchain network and upload the tea credentials to the blockchain. The tea customer gets trustworthy proof of tea product quality by looking up the on-chain credentials that support the published documents of the tea product. Any registered participants can be misbehavior detectors and report the malicious entity by triggering the DeTea smart contract and uploading the accusations. The authorities register as a blockchain node to supervise the chain-wide activities and publish the arbitration results. And the credit of the registered participants is automatically updated by DeTea smart contract. Meanwhile, DeTea smart contracts eliminate human interactions and automatically conduct the management of documents, credentials, accusations, and arbitration.

The application layer processes the data collected from the IoT layer and manages the IoT equipment of the tea PSC. It enables data collection, data processing, automated equipment control, and chain-wide data transmission, along with new device addition, discarded device deletion, and automatic device control. The authorized participants of tea PSC can get the chain-wide IoT data and set the preference of equipment control via the DeTea mobile application. They can upload data produced in different links of tea PSC, and monitor the data of the tea products with the DeTea web application. If the malicious participants are detected, the detector can report the accusations via the DeTea web application. The tea customer can get trustworthy proof of tea product quality and discover the counterfeit product based on the on-chain data.

B. PARTICIPANTS

DeTea participants consist of the enterprises, the collaborators, the supervisors, and the decentralized detectors of the tea PSC.

1) ENTERPRISES

The enterprises that participated in DeTea include the tea plantation, the tea manufacturer, the tea seller, and the logistics provider. Each enterprise needs to provide its profile information to complete the registration. The chain-wide enterprises collect their data on tea PSC. They organize the data into supplementary materials and upload the abstract of the supplementary materials in the form of DeTea documents to the DeTea blockchain. The DeTea documents are required to prove the tea product quality and their supplementary materials are uploaded to the IPFS blockchain after encryption. Meanwhile, the registered enterprises of DeTea can also act as collaborators of other enterprises.

2) COLLABORATOR

Each collaborator needs to upload the list of its cooperative enterprise and its staff list for registration. The registered collaborators can inspect the enterprise documents if they have business cooperation in tea PSC. They upload the credential as blockchain records to support the honest enterprise documents. The collaborators upload the DeTea credential to the blockchain and get their credential addresses in the blockchain. Then they can upload their cooperation information to DeTea, which includes the cooperation time, the business data, the relevant staff, and the credential address. The collaborator can also manage its staff with the DeTea blockchain.

3) SUPERVISOR

The relevant authorities can participate in the DeTea blockchain and supervise the tea market based on the on-chain data. They get the accusation of dishonest participants from the DeTea blockchain and accept or deny the accusation after the supervision. DeTea will automatically execute the arbitration result and update the credit values.

4) DETECTOR

Any participant can act as the detector of the malicious participants. If the detectors find blockchain records conflict with the business activities of the participants in tea PSC, they can upload an accusation against the malicious participant along with the attachment.

C. OPERATIONS

We introduce the participant operations of DeTea in this section. The details of the relevant DeTea smart contracts will be introduced in Section IV.

1) ENTERPRISE REGISTRATION

An enterprise can register its profile information with DeTea. The fields of the enterprise profile consist of the enterprise name, the enterprise representative, the enterprise address, the enterprise type, the enterprise limit, and the business field. After successful registration, the enterprise can obtain the enterprise account address and enterprise contract address in the blockchain. They will also obtain their key pairs distributed by DeTea. The update of enterprise registration requires the signature of the enterprise.

2) DOCUMENT UPLOADING

After a registered enterprise log-in, it can select the local file to be uploaded as the supplementary materials and fill in the file hash with the DeTea application. DeTea slices and encrypts the file and then uploads it to the IPFS blockchain to reduce the storage pressure of the DeTea blockchain. The enterprises organize the file abstracts as DeTea documents and upload them to the DeTea blockchain. The DeTea documents contain the IPFS address of the supplementary materials of the document and the authorized participants can check the supplementary materials by downloading and decrypting the corresponding IPFS file.

3) COLLABORATOR REGISTRATION

The collaborator registers its information with the DeTea blockchain to inspect the enterprise document and adds the information of the relevant staff. After that, the collaborator can get its account address, the Collaborator contract address, and the StaffList contract address.

4) CREDENTIAL UPLOADING

A registered collaborator can inspect the enterprise document by looking up the blockchain records via the DeTea application. If the enterprise is honest, the collaborator can select the credential of the local file system and fill in the relevant staff ID and the credential hash. DeTea uploads the credential to the IPFS system and only records the IPFS address to reduce the storage pressure of the DeTea blockchain. After that, the collaborator can get the credential address in the blockchain and get detailed information about the uploaded credentials. The fields of the uploaded credential consisted of the inspected enterprise profile, the expiration time of the enterprise document, the credential status, the IPFS address of the uploaded document, the IPFS address of the uploaded credential, the collaborator name, and the relevant staff ID.

5) CREDENTIAL INSPECTION

To complete credential inspection, the registered collaborator can query the CredentialInspection contract address of the enterprise under cooperation via the DeTea application. The relevant staff can inspect the uploaded credential by providing the CredentialInspection contract address and the staff ID. Then, he can pass the valid credential and deny the invalid credential.

6) ACCUSATION UPLOADING

Any DeTea participants can look up the public key information of other DeTea participants, and query the detailed information of the uploaded data. They can act as detectors and upload the accusation against the malicious participants.

7) ARBITRATION UPLOADING

The supervisors can query the uploaded data to supervise the tea market activities. They can invoke the Arbitration contract and execute the arbitration result if the decentralized detectors discover the malicious participants. They can directly revoke the credentials of the problem enterprises if they find malicious participants by themselves.

D. CHAIN-WIDE MONITORING AND TEA TRACKING

During tea growth, the DeTea IoT layer monitors the plantation environment of the tea tree. Once the tea leaves are picked and packaged, the DeTea application layer collects the information about the picked tea. The information about the picked tea contains the plantation identification, the tea leaves category, the planting area, the batch number, the tea leaves quality, and the responsible staff. The tea plantation can organize the information of the picked tea as its enterprise document and upload it to DeTea. And the downstream enterprise, such as a tea manufacturer, can query the enterprise documents of tea plantations and order the target tea leaves. Then, the relevant tea plantation transmits the transaction identification code, the batch number, the downstream enterprise, the delivery address, and the logistics tracking number to the tea manufacturer. The tea plantation can upload the transmitted information as the credential via the DeTea application to support the document of the tea manufacturer.

When the tea leaves are delivered, the tea manufacturer processes the picked tea and packs it into the tea product. The DeTea IoT layer monitors the processing and packaging environment of the tea products. Each packaged tea product is labeled with an electronic RFID chip tag that is written into the product identification to capture the flow of the tea products circulated in DeTea. The tea manufacturer can organize the tea product information as its enterprise document and upload it to DeTea. The tea product information covers the manufacturer name, the tea processing parameters, the product weight, the product quality, the product identifications, and the responsible staff. The downstream enterprise, such as an enterprise of tea seller, can query the enterprise documents of tea manufacturers and order the target tea product. Then, the relevant tea manufacturer transmits the transaction identification code, the product identifications, the downstream enterprise, the delivery address, and the logistics tracking number to the tea seller. The tea manufacturer can upload the transmitted information as the credential via the DeTea application to support the document of the tea seller.

When the tea products are delivered, the tea seller updates the information on inventory and the on-sale product of its shop. The DeTea IoT layer monitors the inventory environment of the tea seller. The tea manufacturer can organize the sales information of the tea product as its enterprise document and upload it to DeTea. The sales information includes the seller identification, the seller address, the on-sale tea products, the product price, the discount rate, the available product amount, and the sold-out product amount. The tea customer queries the enterprise documents of tea sellers and orders the target on-sale product. Then, the relevant tea seller transmits the transaction identification code, the sale date of the tea product, the product identification, the delivery address, and the logistics tracking number to the tea customer. The tea customer can look up the chain-wide data of the tea product by uploading the tea product identification via the DeTea application.

During the delivery of tea leaves and tea products, the DeTea IoT layer monitors the logistics status. The logistics provider uses the GPS satellite positioning system to capture the position and logistics status of tea leaves and tea products. The tea manufacturer can organize the logistics information as the credential and upload it to DeTea to support its collaborator. The logistics information covers the logistics name, the logistics tracking number, the product weight, the product identifications, and the responsible staff.

The decentralized detectors can discover untrustworthy and problematic tea products conflicting with the chain-wide activities based on the uploaded documents and credentials recorded by the DeTea blockchain. They can upload the accusations against the malicious participants to DeTea and get detector incentives. The supervisor will upload the arbitration result and the DeTea smart contracts will automatically conduct punishment of the responsible enterprise and collaborator. The relevant tea products can be located and recalled in time based on the chain-wide data uploaded to the DeTea blockchain. The chain-wide monitoring and tea tracking achieve the trustworthiness of the tea PSC and improve the efficiency of dispute resolution of the relevant enterprises.

IV. DECENTRALIZED CREDENTIAL MANAGEMENT AND COUNTERFEIT DETECTION

A. MOTIVATION

We observe that an individual enterprise of traditional tea PSC cannot prove the authenticity of the tea product with convincing evidence. The chain-wide enterprises can issue documents for the tea product, but no one can guarantee the document's authenticity. Therefore, we design chain-wide credentials to make product authenticity provable. Collaborators upload credentials to support DeTea documents of the enterprises and refuse to support the illegal ones. Only the collaborator that the enterprise has trade relations with can upload credentials to prove the authenticity of the enterprise document. The collaborators can deny the illegal credential conflicting with their business activities in tea PSC. DeTea binds the authenticity proofs of tea products to the DeTea credential for no credential means a DeTea document is illegal.

However, the collaborator corrupted by a malicious enterprise will upload fake credentials for the illegal document. The decentralized detectors participating in DeTea can discover the malicious enterprise and the corrupted collaborator based on the on-chain records and chain-wide activities. The detectors can upload the accusation against the malicious participants to the DeTea blockchain along with the attachment and trigger the arbitration automatically via DeTea smart contracts. To guarantee fairness, the participants in arbitration are selected randomly by DeTea and the arbitration result can be trustworthy. Then DeTea changes the credential status to revoked after arbitration.

Moreover, the DeTea credential status lets the malicious participants and the impacted tea product be public based on blockchain technology. It makes the tea market more friendly to honest enterprises and tea customers. No downstream enterprises and tea consumers are willing to order the impacted tea leaves and products. The malicious participants have to recall the impacted tea leaves and products. And DeTea can provide efficient problematic link location and product recalls based on traceable chain-wide data.

We also observe that malicious detection is labor-consuming and the decentralized detectors have little incentive to report the illegal document. Moreover, the participants in tea PSC require more motivation to join in DeTea and behave honestly. Therefore, we design an incentive scheme for DeTea decentralized supervision to provide incentives for honest participants and decentralized detectors along with deterrents for malicious participants. The DeTea incentive scheme guarantees the deductions of the credit of the malicious participants and the increases of the credit value of the honest detector who first uploads the accusation.

B. DeTea SMART CONTRACT MODELING

The smart contracts of DeTea consist of 10 contracts, including `Enterprise`, `Collaborator`, `StaffList`, `Credential`, `CredentialInspection`, `Accusation`, `Arbitration`, `Management`, `Credit`, and `PublicQuery`. The DeTea participants(e.g., enterprise, collaborator, supervisor, or the decentralized detectors) are the one who can interact with the blockchain and invokes contract function deployed in the blockchain network. Here we introduce the functionalities of DeTea smart contracts.

1) ENTERPRISE CONTRACT

It provides document interfaces for enterprises to upload their documents on-chain. The enterprises in tea PSC can register their accounts from DeTea and get their key pairs. The DeTea application client processes the selected documents with slicing and encryption before being issued to DeTea participants, and the encrypted documents are uploaded to the IPFS, a decentralized file system. It triggers `Enterprise` contract to upload the profile information and the document data of the enterprises to the DeTea blockchain. Moreover, DeTea protects the decryption key of the uploaded documents with the Shamir secret sharing scheme and distributes the key shares to the DeTea supervisors for accusation arbitration. The variables of `Enterprise` contract are listed in Table 1. The functions defined in `Enterprise` contract are presented in Table 2.

2) COLLABORATOR CONTRACT

It implements collaborator management and provides credential interfaces. The DeTea participants should register as collaborators via `Collaborator` contract before uploading the credentials. DeTea collaborators can upload

TABLE 1. **Variables in enterprise.sol.**

Type	Name	Description
string	name	Enterprise name
string	representative	Enterprise representative
string	addr	Enterprise address
string	enterpriseType	Enterprise type
string	enterpriseLimit	Enterprise business scope
string	encryptedDataIpfs	Encrypted document ipfs address
string	encryptedDataHash	Encrypted document hash value
string	encryptedDataHash	Credential ipfs address
string	credentialHash	Credential hash value
address	credentialAddress	Credential contract address
CredentialInspection	inspection	Credential inspection contract

TABLE 2. **Enterprise contract functions and descriptions.**

Function	Description
setInformation	Set enterprise basic information
updateData	Upload the document hash and document IPFS address
update	Upload credential and get CredentialInspection contract address
setCredential	Set Credential contract address
getInformation	Get enterprise basic information
getCredential	Get IPFS address of Credential contract
getCredentialAddress	Get Credential contract address

TABLE 3. **Variables in collaborator.sol.**

Type	Name	Description
address	staList	StaffList contract address
string	collaboratorCert	Collaborator certificate data
struct	businessInfo	Business information
uint	time	Struct member of businessInfo
address	credentialAddr	Struct member of businessInfo
string	businessType	Struct member of businessInfo
businessInfo[]	businessList	Business information list
address	creditAddr	Credit contract address
int	credit	Credit value

TABLE 4. **Collaborator contract functions and descriptions.**

Function	Description
setCollaboratorCert	Set collaborator certificate
setStaListAddr	Set StaffList contract address
confirm	Submit inspection confirmation to ContractInspection contract
deny	Submit inspection denial information to ContractInspection contract
addBusiness	Add business record of collaborator staffs
setCreditAddr	Set Credit contract address
updateCredit	Update collaborator credit value
getCollaboratorCert	Get collaborator certificate
getStaListAddr	Get StaffList contract address
showBusiness	Return collaborator business list
getCreditAddr	Get Credit contract address
getCredit	Get collaborator credit value

the credentials that support the documents uploaded by the enterprises in the tea PSC based on their business information. They can also refuse credentials that conflict with real-world business activities. The variables of `Collaborator` contract are listed in Table 3. The functions defined in `Collaborator` contract are presented in Table 4.

3) STAFFLIST CONTRACT

It provides the interfaces to manage the staff relevant to the business activities in tea PSC. The collaborator can add information about the new staff, including the staff name, staff certificate ID, staff business field, staff certificate data, and the collaborator for whom the staff working. The variables of `StaffList` contract are listed in Table 5. The functions defined in `StaffList` contract are presented in Table 6.

TABLE 5. **Variables in stafflist.sol.**

Type	Name	Description
struct	staffInfo	Staff information
string	name	Struct member of staffInfo
string	field	Struct member of staffInfo
string	inspectionCertificate	Struct member of staffInfo
string	collaborator	Struct member of staffInfo
int	credit	Struct member of staffInfo
businessInfo[]	businessList	Struct member of staffInfo
struct	businessInfo	Business information
uint	time	Struct member of businessInfo
address	credentialAddr	Struct member of businessInfo
string	businessType	Struct member of businessInfo
mapping	staffMap	Map certificate id to staffInfo
address	creditAddr	Credit contract address

TABLE 6. **StaffList contract functions and descriptions.**

Function	Description
addStaff	Add the information of the new staff
deleteCollaborator	Delete the collaborator attribute of the specified staff
setCollaborator	Set the collaborator attribute of the specified staff
addBusiness	Add the business information of the specified staff
setCreditContractAddr	Set the Credit contract address
updateCredit	Update the credit value of the specified staff
getStaff	Get the specified staff information
getCreditContractAddr	Get the Credit contract address
getCredit	Get the credit value of the specified staff

TABLE 7. **Variables in credential.sol.**

Type	Name	Description
string	name	Enterprise name
string	representative	Enterprise representative
string	addr	Enterprise Address
string	enterpriseType	Enterprise type
string	enterpriseLimit	Enterprise business scope
string	credential	Credential data
string	dataIpfs	IPFS address of encrypted document
string	credentialIpfs	IPFS address of credential
address	collaborator	Collaborator contract address
string[]	staff	Relevant staff id
uint	expiration	Credential expiration time
string	credentialStatus	Credential status

4) CREDENTIAL CONTRACT

It provides the interfaces for the collaborator to upload the credential information and manage the credential information, the relevant staff ids, the expiration time of the credential, and the credential status. The collaborator can revoke the problematic credential via `Credential` contract, and the DeTea blockchain will update the status of the problematic credential to ‘Revoked’. The variables of `Credential` contract are listed in Table 7. The functions defined in `Credential` contract are presented in Table 10.

5) CredentialInspection CONTRACT

It generates a random number from the Oracle and chooses collaborators randomly based on the generated random number to inspect the uploaded credential. The selected collaborator should confirm or deny the credentials after credential inspection. If the collaborator denies the credential, the DeTea blockchain will invoke the arbitration and return the address of `Arbitration` contract. If no collaborator denies the credential, the DeTea blockchain will update the credential status from ‘Pending’ to ‘Valid’. The variables of `CredentialInspection` contract are listed in Table 8. The functions defined in `CredentialInspection` contract are presented in Table 9.

TABLE 8. Variables in CredentialInspection.sol.

Type	Name	Description
address	credentialAddress	Credential contract address
mapping	resultMap	Map uint256 randomness to uint
Management	systemManagement	Management contract instance
uint256[]	randomCollaboratorIndex	Randomly selected collaborator index
address[]	randomCollaboratorAddress	Randomly selected collaborator address
string[]	randomCollaboratorName	Randomly selected collaborator name
string[]	pubKey	Collaborator public key list
address[]	allCollaborator	Collaborator contract address list
string[]	allCollaboratorName	Collaborator name list
address	enterprise	Enterprise contract address
address	relatedCollaborator	Credential relevant collaborator address
string[]	relatedStaff	Credential relevant staff
string	business	Business name
uint	start	Inspection status
uint	confirmTimes	Credential comfirmation times
address	randomNumberAddress	Randomness generation address
randomNumber	randGen	Randomness generation instance

TABLE 9. CredentialInspection contract functions and descriptions.

Function	Description
addCollaborator	Add the specified Collaborator Contract address to Collaborator Contract address list
addCollaboratorList	Add the specified Collaborator Contract addresses to Collaborator Contract address list
genNextRand	Generate the sequence of the randomness
randomCollaborator	Randomly select the collabortators to inspect the credential
startInspection	Update the random selected collaborator address list and start inspection
confirm	Collaborator confirms the credential
deny	Collaborator denies the credential and generates the Arbitration Contract
getCollaboratorList	Get Collaborator Contract address list from Management Contract
showCollaboratorList	Query all of the Collaborator Contract addresses
getCredentialAddr	Get the address of Credential Contract whose status is 'Pending'
randFromOracle	Get randomness from Truora
businessUpdate	Update business list of collaborator and staffs

TABLE 10. Credential contract functions and descriptions.

Function	Description
addCredential	Add the credential data and the Credential contract address of relevant enterprise
revokeCredential	Set the credential status to 'Revoked'
updateStatus	Update credential status
getInfo	Get the basic data of enterprise
showInfo	Get the data of credential, document Ipfs, credential Ipfs, collaborator, and staff

6) ACCUSATION CONTRACT

It provides the interfaces to handle the accusation of the public (decentralized detectors) and the query of the accusation information. The information about the accusation consists of the detector's name, the accusation abstract, and the attachment. The variables of `Accusation` contract are listed in Table 11. The functions defined in `Accusation` contract are presented in Table 12.

7) ARBITRATION CONTRACT

It executes arbitration when the decentralized detectors upload accusations and the supervisors upload the arbitration result. `Management` contract randomly selects these supervisors based on the random number getting from Oracle. Then, `Arbitration` contract gets the selected supervisor list from `Management` contract. The variables of `Arbitration` contract are listed in Table 13. The functions defined in `Arbitration` contract are presented in Table 14.

TABLE 11. Variables in accusation.sol.

Type	Name	Description
struct	accusationInfo	Accusation Information
string	detector	Struct member of accusationInfo
string	accusationAbstract	Struct member of accusationInfo
string	attachment	Struct member of accusationInfo
mapping	accusationMap	Map supervisor name to accusation information

TABLE 12. Accusation contract functions and descriptions.

Function	Description
addAccusation	Add accusation information
getAccusation	Query the accusations submitted by the specified supervisor

TABLE 13. Variables in arbitration.sol.

Type	Name	Description
mapping	resultMap	Map uint256 randomness to uint
address	credentialAddress	Credential contract address
address	enterpriseAddress	Relevant enterprise contract address
address[]	allSupervisor	All supervisor account address
uint256[]	randomSupervisorIndex	Index of the randomly selected supervisor
address[]	randomSupervisorAddress	Randomly selected supervisor account address list
string[]	allSupervisorName	All supervisor name
string[]	randomSupervisorName	Randomly selected supervisor name list
Enterprise	newEnterprise	The enterprise instance
Management	systemManagement	Management contract instance
uint	confirmTimes	Supervisor confirm times
uint	start	Arbitration status
address	randomNumberAddress	Randomness generation address
randomNumber	randGen	Randomness generation instance

TABLE 14. Arbitration contract functions and descriptions.

Function	Description
addSupervisor	Add account address of supervisor
addSupervisorList	Supervisor account address list
randFromOracle	Get randomness from Truora
genNextRand	Generate the sequence of randomness
randomSupervisor	Select the supervisor randomly
startSupervision	Start supervising the arbitration
confirm	Accept the arbitration
deny	Deny the arbitration
getSupervisorList	Get supervisor account address list from Management contract

TABLE 15. Variables in management.sol.

Type	Name	Description
struct	entityInfo	Entity Information
address	accountAddr	Struct member of entityInfo
address	contractAddr	Struct member of entityInfo
string	pubKey	Struct member of entityInfo
string	field	Struct member of entityInfo
mapping	supervisorMap	Map supervisor name to supervisor information
mapping	collaboratorMap	Map collaborator name to collaborator information
mapping	enterpriseMap	Map enterprise name to enterprise information
string[]	supervisorList	Supervisor name list
string[]	collaboratorList	Collaborator name list
string[]	enterpriseList	Enterprise name list
address[]	supervisorAddressList	Supervisor address list
address[]	collaboratorAddressList	Collaborator address list

8) MANAGEMENT CONTRACT

It provides the interfaces to manage DeTea participants and store their information. The information of the DeTea participant consists of the account address, the contract address, the public key, and the participant's responsibility. The variables of `Management` contract are listed in Table 15. The functions defined in `Management` contract are presented in Table 16.

9) CREDIT CONTRACT

It calculates and updates the credit value for the DeTea participants based on the on-chain events and arbitration results. The functions defined in `Credit` contract are presented in Table 17.

10) PublicQuery CONTRACT

It provides interfaces for the public query of the DeTea participants and tea customers. They can get the information of DeTea credentials, the public key of DeTea participants, the

TABLE 16. Management contract functions and descriptions.

Function	Description
addSupervisor	Add supervisor and update the supervisor list and supervisor address list
addCollaborator	Add collaborator and update the collaborator list and collaborator address list
addEnterprise	Add enterprise and update the enterprise list
getSupervisorAccountAddr	Get the account address of the specified supervisor
getSupervisorPubkey	Get the public key of the specified supervisor
getSupervisorField	Get the business field of the specified supervisor
getCollaboratorAccountAddr	Get the account address of the specified collaborator
getCollaboratorContractAddr	Get the contract address of the specified collaborator
getCollaboratorPubKey	Get the public key of the specified collaborator
getCollaboratorField	Get the business field of the specified collaborator
getEnterpriseAccountAddr	Get the account address of the specified enterprise
getEnterpriseContractAddr	Get the contract address of the specified enterprise
getEnterprisePubKey	Get the public key of the specified enterprise
getEnterpriseField	Get the business field of the specified enterprise
getSupervisorList	Get the supervisor list and supervisor address list
getCollaboratorList	Get the collaborator list and collaborator address list
getEnterpriseList	Get the enterprise list

TABLE 17. Credit contract functions and descriptions.

Function	Description
computeEnterpriseCredit	Calculate the credit value of the specified enterprise
computeCollaboratorCredit	Calculate the credit value of the specified collaborator
computeStaffCredit	Calculate the credit value of the specified staff
computeSupervisorCredit	Calculate the credit value of the specified supervisor
computeParticipantCredit	Calculate the credit value of the specified participant

TABLE 18. Variables in PublicQuery.sol.

Type	Name	Description
address	accusationAddr	Accusation contract address
address	managementAddr	Management contract address
address	creditAddr	Credit contract address

TABLE 19. PublicQuery contract functions and descriptions.

Function	Description
getCredential	Call Management contract and get the specified enterprise credential address
getPubkey	Call Management contract and get the public key of the specified entity
getStaCredit	Call Management and Stafflist contract, get the specified staff credit value
getCollaboratorCredit	Call Management and Collaborator contract, get the specified collaborator credit value

staff credit, and the collaborator credit via `PublicQuery` contract. The variables of `PublicQuery` contract are listed in Table 18. The functions defined in `PublicQuery` contract are presented in Table 19.

C. INCENTIVE SCHEME

The scheme of incentives and deterrence of DeTea are designed based on the on-chain credit management of DeTea participants. DeTea guarantees credit rewards to honest participants and credit deductions to dishonest participants. It also ensures the deterrence of corruption among malicious participants. Table 20 states that the DeTea participants can earn credit value with honest behavior and lose credit if they behave dishonestly. We use the following notation: E denotes the enterprise that issues the document, C denotes the collaborator that uploads the credential to support the document issued by E, D denotes the decentralized detector who initializes the accusation of a DeTea participant and any DeTea participant can be the detector, S denotes the supervisor who issues the arbitration result of the accused participants, P denotes the DeTea participant, the prefix d denotes the dishonest participant, the prefix h denotes the honest participant, no prefix denotes the honesty of the participant is uncertain.

TABLE 20. List of credit value changes for each event.

Event	P.	increase	P.	decrease
Enterprise registration	E	m_1	-	-
Document Uploading	-	-	E	n_1
Collaborator registration	C	m_2	-	-
Credential uploading	C	m_3	-	-
Credential inspection	C	m_4	-	-
Supervisor registration	S	m_5	-	-
Accusation uploading	-	-	D	n_2
Accusation arbitration	S	m_6		
Arbitration execution	h.D	m_7	d.D	n_3
			d.C	n_4
	-	-	d.S	n_5
	-	-	d.E	n_6

TABLE 21. Incentive and deterrence for each entity in different scenarios.

Scenario	P.	unreported	reported+h.	reported+d.
issuer	E	$m_1 - n_1$	$m_1 - n_1$	$m_1 - n_1 - n_6$
- with d.C	E	$m_1 - n_1$	$m_1 - n_1$	$m_1 - n_1 - n_6$
- with d.S	E	$m_1 - n_1$	$m_1 - n_1$	$m_1 - n_1 - n_6$
issuer	C	$m_2 + m_3$	$m_2 + m_3$	$m_2 + m_3 - n_4$
- with d.C	C	$m_2 + m_3$	$m_2 + m_3$	$m_2 + m_3 - n_4$
- with d.S	C	$m_2 + m_3$	$m_2 + m_3$	$m_2 + m_3 - n_4$
inspector	C	$m_2 + m_4$	$m_2 + m_4$	$m_2 + m_4 - n_4$
- with d.S	C	$m_2 + m_4$	$m_2 + m_4$	$m_2 + m_4 - n_4$
accuser	D	-	$-n_2 + m_7$	$-n_2 - n_3$
approver	S	m_5	m_5	$m_5 - n_5$
revoker	S	$m_5 + m_6$	$m_5 + m_6$	$m_5 + m_6 - n_5$

To analyze the incentive and deterrence of DeTea, we consider the possible scenarios of each DeTea participant and list them in Table 21. We assume that DeTea has more than half honest participants and the on-chain arbitration can pick out the dishonest ones, and let $n_1 < m_1 < n_6$, $m_2 + m_3 < n_4$, $m_2 + m_4 < n_4$, $m_5 + m_6 < n_5$, $n_2 < m_7$. First, we consider an enterprise acting as the document issuer that (1) has no report of his misbehavior, (2) has the report of misbehavior but is honest (reports are issued by the dishonest detector), (3) has the report of misbehavior and is dishonest. We observe that no matter whether any other participants are honest or the collaborator is dishonest or the supervisor is dishonest, the honest enterprise will earn $m_1 - n_1$ credit if he registers and issues his document. If the enterprise is dishonest, he will lose $n_1 + n_6 - m_1$ credit. Second, we consider a collaborator acting as a credential issuer in the (1)-(3) situations. We can see that the honest collaborator will earn $m_2 + m_3$ credit if he registers and issues the credential for enterprise and will earn $m_2 + m_3$ if the dishonest detector issues a report. If the collaborator or a supervisor is dishonest and does not revoke the invalid credential, then the dishonest collaborator will lose $n_4 - m_2 - m_3$ credit. Third, we consider a collaborator acting as a credential inspector in the (1)-(3) situations. The honest collaborator will earn $m_2 + m_4$ credit if he registers and inspects the credential for enterprise, and earn $m_2 + m_4$ if the dishonest detector issues a report. If the collaborator is dishonest, he will lose $n_4 - m_2 - m_4$ credit. If the supervisor is dishonest and does not revoke the invalid credential, then the dishonest enterprise will also lose $n_4 - m_2 - m_4$ credit. Fourth, we consider a detector accuses the credential in the

(1)-(3) situations. The honest detector will earn $m_7 - n_2$ credit, and the dishonest detector will lose $n_2 + n_3$ credit. Fifth, we consider a supervisor approving the credential in the (1)-(3) situations. The honest supervisor will earn m_5 credit if he registers and approves the credential for enterprise, and the dishonest supervisor will lose $n_5 - m_5$ credit. Sixth, we consider a supervisor revoking the credential in the (1)-(3) situations. That the honest supervisor will earn $m_5 + m_6$ credit if he registers and revokes the invalid credential for enterprise, and the dishonest supervisor will lose $n_5 - m_5 - m_6$ credit.

Based on the above analysis, we can summarize that the DeTea participants have incentives to behave honestly and DeTea provides deterrence of dishonest behavior and collusion with others.

V. RESOURCE-SAVING AUTOMATIC CONTROL

A. DATA COLLECTION AND TRANSMISSION

DeTea IoT layer applies Internet of Things technologies such as wireless transmission and RFID technology to realize autonomous data capture from tea planting to tea selling. DeTea IoT devices for environment sensing have the built-in STM32L031F6 MCU and SX1278 RF chip to automate the environment data capture of DeTea and the data transmission to the gateway. The DeTea application layer collects the data from the IoT layer and the DeTea participants to provide the data service and achieve chain-wide product tracking. With the DeTea applications, DeTea users can query the IoT data, the documents, the credentials, the accusations, and the arbitrary results. DeTea participants can log in to the DeTea applications to update tea product data by sweeping the product chip and interacting with the DeTea blockchain. They can trace the chain-wide data of the circulated tea product by querying the blockchain record with product identification via the DeTea application.

B. MULTI-SOURCE DATA FUSION

To achieve efficient environment sensing of tea plantations, DeTea adopts the adaptive weighted fusion on the original data collected by the IoT devices to guarantee the accuracy of environmental data. The plantation gateway carries out the adaptive weighted fusion on the device data and uploads the fused data to the DeTea application layer. The algorithm of the adaptive weighted data fusion is demonstrated in Algorithm 1. Firstly, the algorithm obtains the initial acquisition value of the plantation devices and calculates the corresponding variance. Then the algorithm adaptively obtains the corresponding optimal weight according to the total mean square deviation. Finally, the algorithm gets the optimal value after multiplying the initial value and the optimal weight.

Because devices are deployed in different places of the tea plantation and the external environment causes noise in the collected data, the data fusion result should reduce the impact of the external noise to increase the accuracy of the estimated environmental data. The algorithm of the improved adaptive weighted data fusion is given in Algorithm 2. The improved algorithm computes and considers the mean values obtained by multiple iterations to increase the amount of data and optimize the collected data of devices. Compared to Algorithm 1, Algorithm 2 computes the optimized data weights based on the variances of the data updated with the obtained mean values, whose total mean square deviation becomes smaller, and the data fusion result becomes more accurate.

Algorithm 1 Adaptive Weighted Data Fusion

```
Input: Original data collected by m devices and independent
    of each other $x_1, \ldots, x_i, \ldots, x_m$
Output: Optimal data fusion result $\overline{X}$
Calculate the variance of original data collected by m
    devices $\sigma_1^2, \ldots, \sigma_i^2, \ldots, \sigma_m^2$
Calculate the optimal weight $w_i^* = \frac{1}{\sigma_i^2 \sum_{i=1}^{m} \frac{1}{\sigma_i^2}}$, subject to
    $f(w_i)_{min} = \sum_{i=1}^{m} w_i^2 \sigma_i^2$, $\sum_{i=1}^{m} w_i = 1$
Calculate the mean value of data collected by $i^{th}$ device
    in $l$ times: $\overline{X}_i = \frac{1}{l} \sum_{k=1}^{l} x_k$
Get the optimal data fusion value $\overline{X} = \sum_{i=1}^{m} w_i \overline{X}_i$
return $\overline{X}$
```

Algorithm 2 Improved Adaptive Weighted Data Fusion

```
Input: Original data collected by m devices and independent
    of each other $x_1, \ldots, x_i, \ldots, x_m$
Output: Optimal data fusion result $\overline{X}$
Sort and compare the data collected by the devices
    deployed in the tea plantation, find out the maximum
    value $x_{max}$ and minimum value $x_{min}$
Calculate the median value of the data collected by the
    devices $x_0 = \frac{x_{min}+x_{max}}{2}$
Calculate the average $E[x|x \geq x_0] = \frac{\sum_{x_i \geq x_0} x_i w_i}{\sum_{x_i \geq x_0} w_i}$
Calculate the average $E[x|x < x_0] = \frac{\sum_{x_i < x_0} x_i w_i}{\sum_{x_i < x_0} w_i}$
Update data $x_1 = \frac{E[x|x \geq x_0]+E[x|x < x_0]}{2}$
Let $m = 1$
while $x_m \neq x_{m-1}$ do
    Calculate the average $E[x|x \geq x_m] = \frac{\sum_{x_i \geq x_0} x_i w_i}{\sum_{x_i < x_m} w_i}$
    Calculate the average $E[x|x < x_m] = \frac{\sum_{x_i \geq x_m} x_i w_i}{\sum_{x_i < x_m} w_i}$
    Update data $x_{m+1} = \frac{E[x|x \geq x_m]+E[x|x < x_m]}{2}$
    Let $m = m + 1$
end while
Calculate the updated data variance $\sigma_1^2, \ldots, \sigma_i^2, \ldots, \sigma_m^2$
Calculate the optimal weight $w_i^* = \frac{1}{\sigma_i^2 \sum_{i=1}^{m} \frac{1}{\sigma_i^2}}$, subject to
    $f(w_i)_{min} = \sum_{i=1}^{m} w_i^2 \sigma_i^2$, $\sum_{i=1}^{m} w_i = 1$
Calculate the mean value of data collected by $i^{th}$ device
    in $l$ times: $\overline{X}_i(l) = \frac{1}{l} \sum_{k=1}^{l} x_k$
Get the optimal data fusion value $\overline{X} = \sum_{i=1}^{m} w_i \overline{X}_i(l)$
return $\overline{X}$
```

Algorithm 3 Automatic Plantation Environment Adjustment

```
Input: Optimal data fused results $\overline{X}_1, \ldots, \overline{X}_i, \ldots, \overline{X}_s$
Output: Device status $d_1, \ldots, d_i, \ldots, d_s$
Get the maximum value of environment parameters $M_1, \ldots, M_i, \ldots, M_s$
Get the minimum value of environment parameters $N_1, \ldots, N_i, \ldots, N_s$
for all $\overline{X}_i$ in $\overline{X}_1, \ldots, \overline{X}_i, \ldots, \overline{X}_s$ do
    if $\overline{X}_i > M_i$ then
        Get the set of device ID $R$ to decrease $\overline{X}_i$
        Change the status of the device in $R$
        Update the device status $d_1, \ldots, d_i, \ldots, d_s$
    end if
    if $\overline{X}_i < N_i$ then
        Get the set of device ID $I$ to increase $\overline{X}_i$
        Change the status of the device in $I$
        Update the device status $d_1, \ldots, d_i, \ldots, d_s$
    end if
end for
return $d_1, \ldots, d_i, \ldots, d_s$
```

Algorithm 4 Optimal Irrigation Strategy

```
Input: The tea tree height $h_{tea}$, the wind speed $u_2$, the field moisture content $\overline{\theta}_f$, the moisture content at the withering point $\overline{\theta}_w$, the root depth $d_{root_i}$
Output: The irrigation water volume $V_{water}$
Initialize the irrigation water volume $V_{water} = 0$
Calculate the estimated crop evapotranspiration at the $i^{th}$ day $ET_{0_i}$ (Eq. (1))
Calculate the tea tree evapotranspiration at the $i^{th}$ day $ET_{c_i}$ (Eq. (3))
Calculate the water deficit value at the $i^{th}$ day $D_i$ (Eq. (4))
Calculate the allowed water deficit value at the $i^{th}$ day $R_{a_i}$ (Eq. (5))
if $D_i > R_{a_i}$ then
    The irrigation water volume $V_{water} = D_i$
    Update the water deficit value $D_i = 0$
end if
return $V_{water}$
```

C. RESOURCE-SAVING AUTOMATIC CONTROL

DeTea users can also set the required environmental parameter range through the DeTea application. In DeTea, all the devices are assigned the device ID and the DeTea blockchain records the device description through the smart contracts. The plantation sensor devices share the collected environmental data with the gateway and the DeTea applications get the fused environmental data from the gateway. Then, the DeTea application automatically adjusts the plantation environment based on the fused environmental data, the latest meteorological data, and the suitable parameter range of the plantation environment. Algorithm 3 demonstrates the process regarding the automatic tea plantation environment adjustment of DeTea. First, judge whether the fused environmental data is within the suitable parameter range of the plantation environment. If the fused environmental data is out of the suitable parameter range of the plantation environment, query the actuator devices that can adjust the environmental parameter of the plantation and get their device ID by triggering the DeTea smart contract. Then, change the status of the corresponding actuator devices to adjust the plantation environment within the suitable parameter range.

DeTea makes use of Algorithm 4 to obtain the optimal irrigation strategy and reduce water waste, which illustrates the process of computing the optimal irrigation volume. The Penman-Monteith model is used to estimate crop evapotranspiration ET_0 and the model is recommended by FAO (Food and Agricultural Organization), which combines the physical characteristics with the physiological characteristics in the process of tree surface water vapor evaporation [40]. Penman-Monteith model expression is demonstrated in equation 1, where λ is the latent heat of vaporization (MJ/kg), δ is the slope of saturated vapor pressure curve (kPa/°C), R_n is net radiation (MJ/(m^2·d)), G is the soil heat flux (MJ/(m^2·d)), ρ_a is the air density (kg/m^3), C_p is the specific heat of air under ordinary pressure, e_s is the saturated vapor pressure (kPa), e_a is the actual vapor pressure (kPa), γ is the hygrometer constant, r_a is the aerodynamic impedance (s/m), r_c is the reference daily average canopy resistance (s/m). In the DeTea plantation greenhouse, C_p is 1.013*10^{-3}, γ is 0.067, r_c is 70.

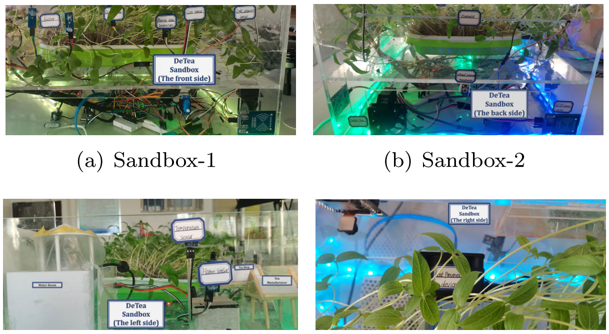
$$ET_0 = \frac{1}{\lambda}\frac{\delta(R_n - G) + \rho_a \frac{e_s - e_n}{r_a}}{\delta + \gamma(1 + \frac{r_c}{r_a})}) \tag{1}$$

DeTea uses equation 2 to calculate the aerodynamic impedance, which has high accuracy under high or low wind speed [41]. In equation 2, r_a is the aerodynamic impedance (s/m), Z is the measured height for wind speed (m), d is the zero_plane displacement length (m), Z_0 is the soil surface roughness length (m), u_2 is the measured wind speed (m/s), h_{tea} the tea tree height (m).

$$r_a = \frac{4.72[ln(\frac{Z-d}{Z_0})]^2}{1 + 0.54u_2} \tag{2}$$

In the DeTea plantation greenhouse, the measured height for wind speed Z is 2, the soil surface roughness Z_0 can be estimated as $0.13h_{tea}$, and the zero_plane displacement d can be estimated as $0.64h_{tea}$. After calculating the estimated evapotranspiration ET_0 under full irrigation, DeTea calculates the tea tree evapotranspiration under full irrigation ET_c based on the estimated crop evapotranspiration ET_0 and the crop parameters K_c. Different growth stages of the tea tree have different crop parameters and the tea tree evapotranspiration under full irrigation is calculated based on equation 3.

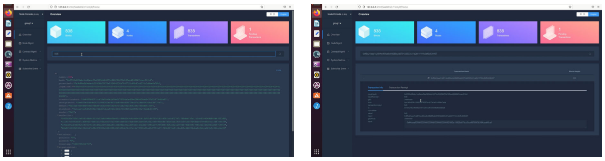
$$ET_c = K_c \cdot ET_0 \tag{3}$$


DeTea Sandbox (The front side)
DeTea Sandbox (The back side)
DeTea Sandbox (The left side)
DeTea Sandbox (The right side)

(a) Sandbox-1 (b) Sandbox-2

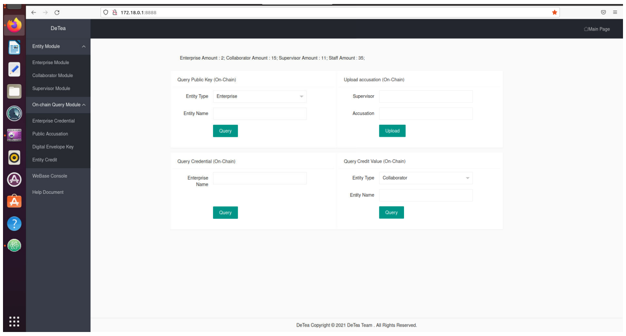
(c) Sandbox-3 (d) Sandbox-4

FIGURE 3. DeTea sandbox model.



(a) Console-1 (b) Console-2

FIGURE 4. The console snapshots of DeTea blockchain.



172.18.0.1:8888

DeTea

Main Page

Entity Module
- Enterprise Module
- Collaborator Module
- Supervisor Module

On-chain Query Module
- Enterprise Credential
- Public Accusation
- Digital Envelope Key
- Entity Credit

WeBase Console

Help Document

Enterprise Amount : 2; Collaborator Amount : 15; Supervisor Amount : 11; Staff Amount : 35;

Query Public Key (On-Chain)
Entity Type: Enterprise
Entity Name:
Query

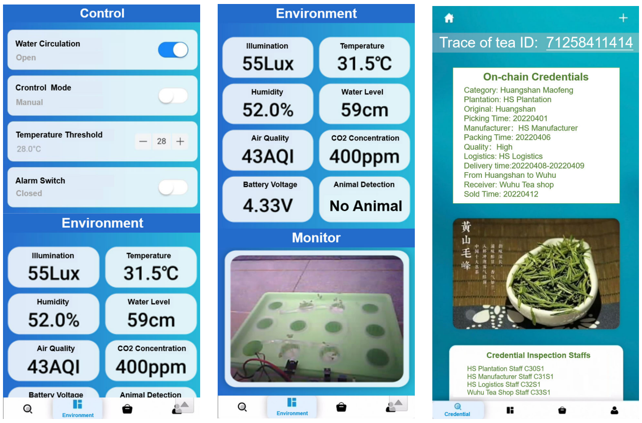
Upload accusation (On-Chain)
Supervisor:
Accusation:
Upload

Query Credential (On-Chain)
Enterprise Name:
Query

Query Credit Value (On-Chain)
Entity Type: Collaborator
Enity Name:
Query

DeTea Copyright © 2021 DeTea Team . All Rights Reserved.

FIGURE 5. The main page snapshot of DeTea web app.



Control

Water Circulation: Open

Crontrol Mode: Manual

Temperature Threshold: 28.0°C (− 28 +)

Alarm Switch: Closed

Environment

Illumination 55Lux | Temperature 31.5℃
Humidity 52.0% | Water Level 59cm
Air Quality 43AQI | CO2 Concentration 400ppm
Battery Voltage | Animal Detection

Environment

Environment

Illumination 55Lux | Temperature 31.5℃
Humidity 52.0% | Water Level 59cm
Air Quality 43AQI | CO2 Concentration 400ppm
Battery Voltage 4.33V | Animal Detection No Animal

Monitor

Environment

Trace of tea ID: 71258411414

On-chain Credentials
Category: Huangshan Maofeng
Plantation: HS Plantation
Original: Huangshan
Picking Time: 20220401
Manufacturer: HS Manufacturer
Packing Time: 20220406
Quality: High
Logistics: HS Logistics
Delivery time:20220408-20220409
From Huangshan to Wuhu
Receiver: Wuhu Tea shop
Sold Time: 20220412

Credential Inspection Staffs
HS Plantation Staff C30S1
HS Manufacturer Staff C31S1
HS Logistics Staff C32S1
Wuhu Tea Shop Staff C33S1

Credential

(a) Interface-1 (b) Interface-2 (c) Interface-3

FIGURE 6. The user interfaces of DeTea mobile app.

DeTea calculates the water deficit value (cm) based on the following equation:

$$D_i = D_{i-1} + ET_{c_i}eq : Di \tag{4}$$

where D_i is the water deficit value of the i^{th} day, D_{i-1} is the water deficit value of the $(i-1)^{th}$ day, and ET_{c_i} is the tea tree evapotranspiration value of the i^{th} day. The allowed water deficit value at i^{th} day R_{a_i} (cm) is calculated based on equation 5. In equation 5, A is the recommended value of the allowed deficit ratio, $\overline{\theta}_f$ is the field moisture content (cm^3/cm^3), $\overline{\theta}_w$ is the moisture content at the withering point (cm^3/cm^3), d_{root_i} is the root depth at the i^{th} day (cm, i.e., the estimated root depth according to tea tree growth stage and plant height). DeTea irrigates water for tea trees if the water deficit value of the i^{th} day D_i is larger than the allowed water deficit value at i^{th} day R_{a_i}, and the irrigation quantity is D_i.

$$R_{a_i} = A \cdot (\overline{\theta}_f - \overline{\theta}_w) \cdot d_{root_i} \tag{5}$$

VI. IMPLEMENTATION, RESULTS AND DISCUSSION

A. SIMULATION SETUP

To emulate the real-world environment of DeTea, we build a sandbox model as shown in Figure 3. We deploy the DeTea sandbox using Raspberry Pie, ESP32, Arduino, and multiple IoT sensors, such as temperature, humidity, light intensity, CO2, PH, and IR sensors using MQTT protocol to communicate with software. Meanwhile, DeTea adopts the alliance chain to achieve controllable decentralization and openness. The misbehavior can be detected if a blockchain record conflicts with other on-chain records or real-world business events.

We build the DeTea blockchain based on FISCO-BCOS v2.8.0.[1] It is an open-source, stable, efficient, and secure blockchain platform and many institutions and applications have tested FISCO BCOS in the production environment. WeBase is a toolset for managing the FISCO-BCOS chain and provides a graphical management interface for the DeTea blockchain. It improves the development efficiency of DeTea applications with node pre-processing, node management, transaction query, and data export. The WeBase snapshots of the DeTea blockchain are presented in Figure 4. We use the Ubuntu20.04 LTS, 64-bit Linux operating system to host the DeTea blockchain network with 16 GiB memory, 1.1 TB disk capacity, and an Intel core i7-5700HQ processor. We write the DeTea smart contracts in Solidity language and install the smart contracts on each node within the DeTea blockchain network.

We use FISCO-BCOS RPC interfaces and develop decentralized applications based on the FISCO-BCOS SDK to communicate the DeTea blockchain network. The main page snapshot of the DeTea web application is presented in Figure 5 and the user interfaces of the DeTea mobile application are presented in Figure 6. The DeTea application users can initiate an RPC request to the DeTea blockchain participant through the SDK to initiate a transaction. Then, the data packets are communicated between blockchain participants. After receiving the transaction, the DeTea blockchain participants attach the transaction to the trans-

[1] https://github.com/FISCO-BCOS/FISCO-BCOS

TABLE 22. Configuration parameter for evaluation of blockchain network.

Experiment Parameters	Values
Number of peers	4
Number of channels	1
Number of clients that fire transactions	5
Minimum block generation time	500ms
Maximum number of transactions per block	1000
Transaction expiration time	600s
Maximum memory size used for block sync	512MB
Maximum number of nodes that broadcast txs status to	4
Transaction pool memory size limit	512MB
Block consensus timeout	3s
The number of generated blocks each epoch	1000

action pool. The blockchain participant constantly takes the transaction out of the transaction pool and packages the taken transaction into a block. When the block is generated, the consensus engine verifies and executes the consensus. After verifying that the block is correct and the consensus is reached among participants, the block is put on the chain. When a DeTea blockchain participant downloads a missing block from another participant through the synchronization module, it will also execute and verify the block.

When the simulation is started, the DeTea sandbox devices need to be at work so that our IoT platform can communicate with the devices to get the sensing data and send a control command to actuators. Once the devices work, the DeTea blockchain and its smart contracts are deployed and initiated. Then, the DeTea application is at work. The DeTea users can supervise the tea product chain widely via the web application, and monitor the collected data and device status of DeTea IoT devices via mobile application.

B. BLOCKCHAIN PERFORMANCE EVALUATION

We use Hyperledger Caliper, a blockchain performance benchmark framework, to measure the implementation of the DeTea blockchain with a predefined configuration. We configure the DeTea blockchain with parameter settings listed by Table 22 and measured the read throughput and transaction throughput with different send rates of transaction. Throughput, namely the number of transactions processed per second (tps), indicates the performance of the blockchain in processing transactions. The number of valid transactions processed by the blockchain within a specified time is measured by transaction throughput. The total number of read operations handled by the blockchain in a specified period is indicated by read throughput. In addition, the proportion of invalid transactions in our evaluation is less than 1% and our evaluation results are meaningful. We set the send rate of DeTea transaction from 500 tps to 3500 tps and the evaluation of average read throughput is shown in Figure 7. We found that the highest point of DeTea read throughput is 2770.1 tps at the 3000 tps send rate and the read throughput started decreasing at 3500 tps. It shows that 3000 tps is the optimal value of the send rate for DeTea read throughput when the larger send rate decreases the DeTea read throughput. We found that the highest point of DeTea transaction throughput is 573.2 tps at the 600 tps send rate and the transaction throughput started decreasing at 700 tps. It shows that 600 tps is the optimal value of the send rate for DeTea transaction throughput.

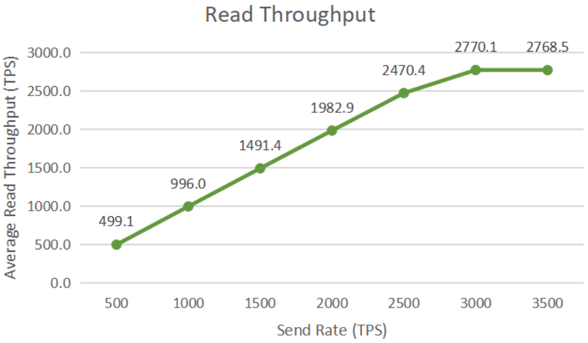


FIGURE 7. Impact of varying send rate on DeTea read throughput.

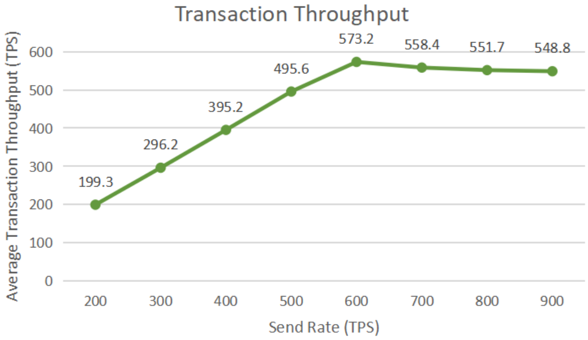


FIGURE 8. Impact of varying send rate on DeTea transaction throughput.

We also measure the average read latency and average transaction latency at different sending rates to evaluate the transaction time spent by the DeTea blockchain. The time spent by the DeTea blockchain to handle a read request of a client is measured by read latency. The time spent by the DeTea blockchain to process a transaction is indicated by transaction latency. Our measurement includes the broadcast time required by the PBFT consensus mechanism of the DeTea blockchain. We set the send rate from 500 tps to 3500 tps when we evaluated the average read latency of the DeTea blockchain. As shown in Figure 9, the average read latency of the DeTea blockchain increased slightly when the send rate varied from 500 tps to 3000 tps, and the slope of read latency increased significantly when the send rate is set larger than 3000 tps. As shown in Figure 10, the average transaction latency of the DeTea blockchain increased slightly when the send rate varied from 200 tps to 600 tps, and the slope of transaction latency increased significantly when the send rate is set larger than 600 tps.

C. ENVIRONMENT CONTROL EVALUATION

The evaluation of the IoT-based temperature control of DeTea is shown in Figure 11. The DeTea temperature can be controlled between the lowest temperature set by the user and the highest temperature set by the user. It can be seen from

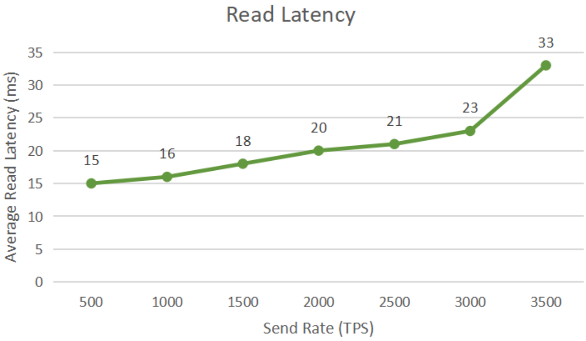


FIGURE 9. Impact of send rate on DeTea read latency.

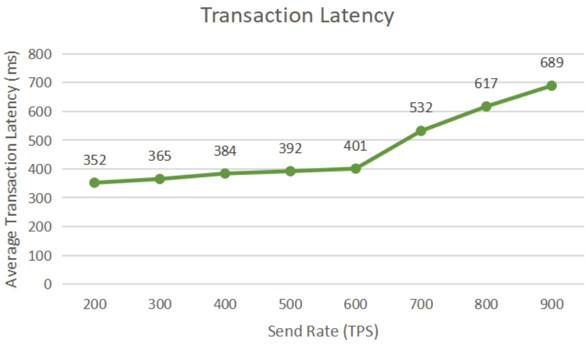


FIGURE 10. Impact of send rate on DeTea transaction latency.

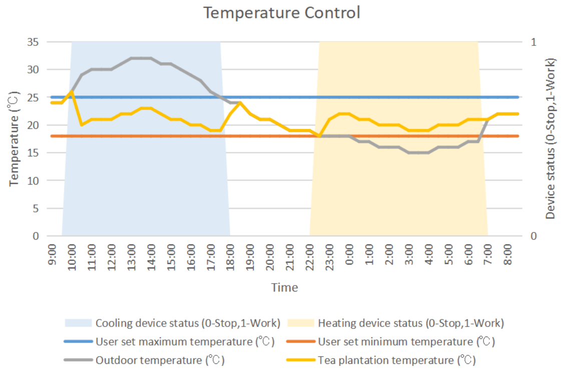


FIGURE 11. Evaluation of DeTea temperature control.

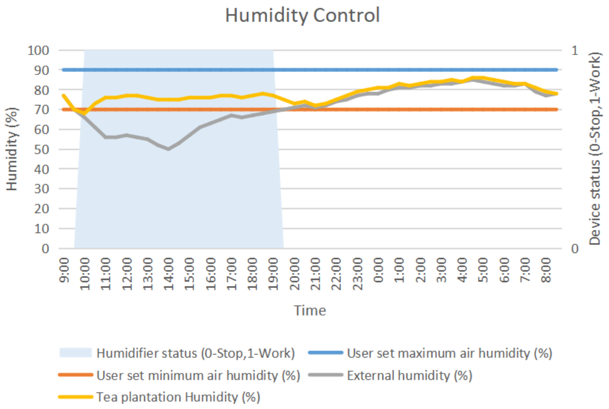


FIGURE 12. Evaluation of DeTea humidity control.

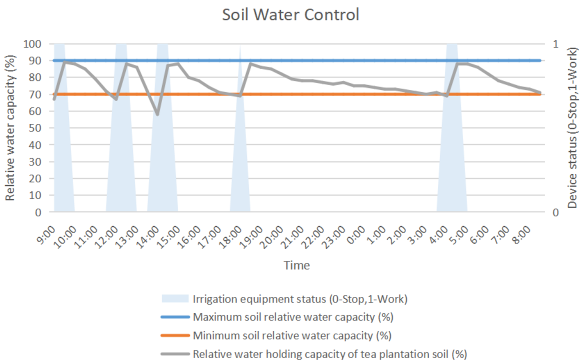


FIGURE 13. Evaluation of DeTea soil water control.

Figure 11 that when the temperature is higher than the user-set maximum temperature, the DeTea cooling device will work to decrease the temperature of the tea plantation. When the temperature is lower than the user-set minimum temperature, the DeTea heating device will work to raise the temperature of the tea plantation. When the outside temperature is between the user-set minimum temperature and the user-set maximum temperature, the cooling device and heating device stop working. Additionally, the environmental temperature of DeTea is calculated based on the data collected from several IoT devices via Algorithm 2, and the status of IoT devices is adjusted via Algorithm 3.

The IoT-based humidity control evaluation of DeTea is shown in Figure 12. The DeTea humidity is controlled between the minimum humidity set by the user and the maximum humidity set by the user. It can be seen from Figure 12 that when the temperature is lower than the minimum humidity, the DeTea humidifier works. When the external humidity is between the minimum and maximum humidity, the humidifier device stops working.

The evaluation of IoT-based soil moisture control of DeTea is shown in Figure 13. The soil moisture content of DeTea is controlled between the lowest water content set by the user and the highest water content set by the user. It can be seen from Figure 13 that when the temperature is lower than the minimum moisture content, the DeTea irrigation device works. When the soil water content reaches the maximum water content set by the user, the irrigation device will stop working.

D. CHALLENGES OF APPLICATION

By effectively combining the advantages of blockchain and IoT technologies, the proposed blockchain-IoT-empowered DeTea platform can achieve full-process traceability and resource-saving automation for the tea PSC. The proposed solution is expected to be applied to agricultural traceability systems to ensure the safety, reliability, and efficiency of agricultural production. However, there are two challenges when applying to the real-world industry, including the algorithm level and market level. On the one hand, the blockchain algorithm is subject to $n \geq 3f + 1$, where n is the total number of nodes in the system and f is the number of nodes that are allowed to fail. Therefore, when more than $1/3$ of nodes (blockchain participants) are malicious, blockchain data security cannot be guaranteed. On the other hand, it needs the cooperation of multi-practitioner to achieve the maximum role of the system and standardize the market when applying to the real-world tea industry. It is difficult for a few companies or practitioners to push industry development. Moreover, the enterprise's consideration of cost in industrial upgrading is also a challenge.

VII. CONCLUSION

Traditional traceability systems may use IoT technology but generally lack traceability throughout the entire production process. Moreover, these traceability systems may have security risks when there are dishonest collaborators, which makes it hard to guarantee the authenticity of product data required for traceability from the source. In this work, blockchain technology is introduced to achieve full-process traceability of tea PSC by combining the advantages of blockchain and IoT technologies. We propose a blockchain-IoT-empowered platform DeTea with resource-saving automation and counterfeit detection for the tea PSC. DeTea automates the processes based on IoT technology to reduce human participation and guarantee data integrity from data collection to data exhibition. To reduce the resource cost and improve the tea product quality, an improved adaptive weighted data fusion algorithm and the automatic plantation environment adjustment via the optimal irrigation strategy are adopted. The dishonest behaviors in the tea PSC are all accountable to DeTea participants. Moreover, DeTea adopts an incentive scheme to attract more participants and incentive honest behavior. DeTea can reveal and publish dishonest behaviors, which provides trustworthy proof of tea counterfeit for tea customers and a better environment for the tea market.

Furthermore, we implement a DeTea prototype based on FISCO BCOS and the IoT-based system sandbox for automatic environment monitor and equipment control. We develop ten main smart contracts in Solidity for DeTea blockchain to achieve chain-wide traceability and decentralized supervision with incentives and deterrence. Hyperledger Calliper is utilized to access the performance of the latency and throughput of the DeTea blockchain. The sandbox result shows the good performance of the DeTea blockchain and the efficiency of automatic environment monitor and equipment control. Besides the tea PSC, the proposed solution is expected to extend to other agricultural products to ensure the safety, reliability, and efficiency of agricultural traceability systems.

REFERENCES

[1] N. J. Langford, "From global to local tea markets: The changing political economy of tea production within India's domestic value chain," *Develop. Change*, vol. 52, no. 6, pp. 1445–1472, Nov. 2021.

[2] Z. Mishra and B. Acharya, "High throughput novel architectures of TEA family for high speed IoT and RFID applications," *J. Inf. Secur. Appl.*, vol. 61, Sep. 2021, Art. no. 102906.

[3] S. Kaushal, P. Nayi, D. Rahadian, and H.-H. Chen, "Applications of electronic nose coupled with statistical and intelligent pattern recognition techniques for monitoring tea quality: A review," *Agriculture*, vol. 12, no. 9, p. 1359, Sep. 2022.

[4] N. Deka and K. Goswami, "Economic sustainability of organic cultivation of Assam tea produced by small-scale growers," *Sustain. Prod. Consumption*, vol. 26, pp. 111–125, Apr. 2021.

[5] P. Sharma, "A study on the problems and prospects of small tea growers with special reference to Margherita area of Tinsukia district," *Ann. Romanian Soc. Cell Biol.*, vol. 25, no. 4, pp. 8920–8933, 2021.

[6] C. Hui-Chuan and L. Te-Tsai, "An innovative business model of Chinese herbal medicine in handmade tea beverage market in China," in *Proc. 8th Int. Conf. Entrepreneurship Bus. Manag. (ICEBM) UNTAR*, 2020, pp. 25–29.

[7] M. S. Hossain, R. Uddin, P. Barua, M. Yasin, M. S. Al Mamun, and M. M. Hoque, "Effects of plant age, topography and processing system on the biochemical traits and quality of tea," *Bangladesh J. Botany*, vol. 50, no. 3, pp. 633–639, 2021.

[8] J. Zhao, W. Liu, Y. Chen, X. Zhang, X. Wang, F. Wang, Y. Qian, and J. Qiu, "Identification of markers for tea authenticity assessment: Non-targeted metabolomics of highly similar oolong tea cultivars (Camellia sinensis var. sinensis)," *Food Control*, vol. 142, Dec. 2022, Art. no. 109223.

[9] L. Zhao, J. Ruan, and X. Shi, "Local industrial policies and development of agricultural clusters: A case study based on a tea cluster in China," *Int. Food Agribusiness Manage. Rev.*, vol. 24, no. 2, pp. 267–288, Mar. 2021.

[10] T. Paul, S. Mondal, N. Islam, and S. Rakshit, "The impact of blockchain technology on the tea supply chain and its sustainable performance," *Technol. Forecasting Social Change*, vol. 173, Dec. 2021, Art. no. 121163.

[11] X. Shen and Z. Su, "Expanded authenticity? Changing standards for identifying Longjing tea," *Asian J. Social Sci.*, vol. 50, no. 3, pp. 214–221, Sep. 2022.

[12] X. Xu, F. Rahman, B. Shakya, A. Vassilev, D. Forte, and M. Tehranipoor, "Electronics supply chain integrity enabled by blockchain," *ACM Trans. Design Autom. Electron. Syst.*, vol. 24, no. 3, pp. 1–25, May 2019.

[13] P. Fraga-Lamas and T. M. Fernández-Caramés, "A review on blockchain technologies for an advanced and cyber-resilient automotive industry," *IEEE Access*, vol. 7, pp. 17578–17598, 2019.

[14] J. Hu, M. Reed, N. Thomos, M. F. AI-Naday, and K. Yang, "Securing SDN-controlled IoT networks through edge blockchain," *IEEE Internet Things J.*, vol. 8, no. 4, pp. 2102–2115, Feb. 2021.

[15] K. R. K. Reddy, A. Gunasekaran, P. Kalpana, V. R. Sreedharan, and S. A. Kumar, "Developing a blockchain framework for the automotive supply chain: A systematic review," *Comput. Ind. Eng.*, vol. 157, Jul. 2021, Art. no. 107334.

[16] X. Li, P.-L. Lai, C.-C. Yang, and K. F. Yuen, "Determinants of blockchain adoption in the aviation industry: Empirical evidence from Korea," *J. Air Transp. Manage.*, vol. 97, Oct. 2021, Art. no. 102139.

[17] S. Cao, W. Powell, M. Foth, V. Natanelov, T. Miller, and U. Dulleck, "Strengthening consumer trust in beef supply chain traceability with a blockchain-based human-machine reconcile mechanism," *Comput. Electron. Agricult.*, vol. 180, Jan. 2021, Art. no. 105886.

[18] M. Thakur, G. M. Tveit, G. Vevle, and T. Yurt, "A framework for traceability of hides for improved supply chain coordination," *Comput. Electron. Agricult.*, vol. 174, Jul. 2020, Art. no. 105478.

[19] K. Biswas, V. Muthukkumarasamy, and W. L. Tan, "Blockchain based wine supply chain traceability system," in *Proc. Future Technol. Conf. (FTC)*. Queens, NY, USA: The Science and Information Organization, 2017, pp. 56–62.

[20] Y. Cao, F. Jia, and G. Manogaran, "Efficient traceability systems of steel products using blockchain-based industrial Internet of Things," *IEEE Trans. Ind. Informat.*, vol. 16, no. 9, pp. 6004–6012, Sep. 2020.

[21] Y.-S. Tsai, R.-S. Chen, Y.-C. Chen, and C.-P. Yeh, "An RFID-based manufacture process control and supply chain management in the semiconductor industry," *Int. J. Inf. Technol. Manage.*, vol. 12, nos. 1–2, pp. 85–105, Jan. 2013.

[22] M. K. Lim, Y. Li, C. Wang, and M.-L. Tseng, "A literature review of blockchain technology applications in supply chains: A comprehensive analysis of themes, methodologies and industries," *Comput. Ind. Eng.*, vol. 154, Apr. 2021, Art. no. 107133.

[23] S. Bouraga, "A taxonomy of blockchain consensus protocols: A survey and classification framework," *Expert Syst. Appl.*, vol. 168, Apr. 2021, Art. no. 114384.

[24] S. N. Khan, F. Loukil, C. Ghedira-Guegan, E. Benkhelifa, and A. Bani-Hani, "Blockchain smart contracts: Applications, challenges, and future trends," *Peer-to-Peer Netw. Appl.*, vol. 14, no. 5, pp. 2901–2925, Sep. 2021.

[25] J. Zarrin, H. Wen Phang, L. Babu Saheer, and B. Zarrin, "Blockchain for decentralization of Internet: Prospects, trends, and challenges," *Cluster Comput.*, vol. 24, no. 4, pp. 2841–2866, Dec. 2021.

[26] D. Khan, L. T. Jung, and M. A. Hashmani, "Systematic literature review of challenges in blockchain scalability," *Appl. Sci.*, vol. 11, no. 20, p. 9372, Oct. 2021.

[27] A. I. Sanka and R. C. C. Cheung, "A systematic review of blockchain scalability: Issues, solutions, analysis and future research," *J. Netw. Comput. Appl.*, vol. 195, Dec. 2021, Art. no. 103232.

[28] M. N. A. Latif, N. A. A. Aziz, N. S. N. Hussin, and Z. A. Aziz, "Cyber security in supply chain management: A systematic review," *Logforum*, vol. 17, no. 1, pp. 49–57, Mar. 2021.

[29] A. Raja Santhi and P. Muthuswamy, "Influence of blockchain technology in manufacturing supply chain and logistics," *Logistics*, vol. 6, no. 1, p. 15, Feb. 2022.

[30] R. Kumar and R. Tripathi, "Traceability of counterfeit medicine supply chain through blockchain," in *Proc. 11th Int. Conf. Commun. Syst. Netw. (COMSNETS)*, Jan. 2019, pp. 568–570.

[31] L. Lao, Z. Li, S. Hou, B. Xiao, S. Guo, and Y. Yang, "A survey of IoT applications in blockchain systems: Architecture, consensus, and traffic modeling," *ACM Comput. Surv.*, vol. 53, no. 1, pp. 1–32, Feb. 2020.

[32] H. Li, L. Pei, D. Liao, X. Wang, D. Xu, and J. Sun, "BDDT: Use blockchain to facilitate IoT data transactions," *Cluster Comput.*, vol. 24, no. 1, pp. 459–473, Mar. 2021.

[33] D. Han, Y. Zhu, D. Li, W. Liang, A. Souri, and K. Li, "A blockchain-based auditable access control system for private data in service-centric IoT environments," *IEEE Trans. Ind. Informat.*, vol. 18, no. 5, pp. 3530–3540, May 2022.

[34] Y. Feng, W. Zhang, X. Luo, and B. Zhang, "A consortium blockchain-based access control framework with dynamic orderer node selection for 5G-enabled industrial IoT," *IEEE Trans. Ind. Informat.*, vol. 18, no. 4, pp. 2840–2848, Apr. 2022.

[35] Y. Li, W. Susilo, G. Yang, Y. Yu, D. Liu, X. Du, and M. Guizani, "A blockchain-based self-tallying voting protocol in decentralized IoT," *IEEE Trans. Dependable Secure Comput.*, vol. 19, no. 1, pp. 119–130, Jan. 2022.

[36] S. K. Mangla, Y. Kazançoğlu, A. Yıldızbaşı, C. Öztürk, and A. Çalık, "A conceptual framework for blockchain-based sustainable supply chain and evaluating implementation barriers: A case of the tea supply chain," *Bus. Strategy Environ.*, vol. 31, no. 8, pp. 3693–3716, Mar. 2022.

[37] Y. Wu, X. Jin, H. Yang, L. Tu, Y. Ye, and S. Li, "Blockchain-based Internet of Things: Machine learning tea sensing trusted traceability system," *J. Sensors*, vol. 2022, pp. 1–16, Feb. 2022.

[38] T. Paul, N. Islam, S. Mondal, and S. Rakshit, "RFID-integrated blockchain-driven circular supply chain management: A system architecture for B2B tea industry," *Ind. Marketing Manage.*, vol. 101, pp. 238–257, Feb. 2022.

[39] D. Kumar and R. K. Dwivedi, "Blockchain and IoT based smart agriculture and food supply chain system," in *Proc. Int. Conf. Intell. Innov. Technol. Comput., Electr. Electron. (IITCEE)*, Jan. 2023, pp. 755–761.

[40] W. J. Shuttleworth, "Towards one-step estimation of crop water requirements," *Trans. ASABE*, vol. 49, no. 4, pp. 925–935, Jul. 2006.

[41] R. D. Jackson, W. P. Kustas, and B. J. Choudhury, "A reexamination of the crop water stress index," *Irrigation Sci.*, vol. 9, no. 4, pp. 309–317, Oct. 1988.

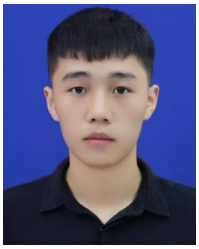
XIAOFENG XU (Member, IEEE) received the B.S. and Ph.D. degrees in computer science and technology from the Nanjing University of Science and Technology, China, in 2014 and 2020, respectively.

He is currently a Lecturer at the School of Computer and Information, Anhui Polytechnic University, China. His research interests include digital image processing, machine learning, deep learning, computer vision, and information security.

XIANGLIN BAO received the B.S. degree in information security from Anhui University, China, in 2017, and the M.S. degree in computer application technology from the University of Science and Technology, China, in 2020.

She is currently a Lecturer at the School of Computer and Information, Anhui Polytechnic University, China. Her research interests include machine learning, blockchain technology, and information security.

HAODONG YI received the B.S. degree in computer science and technology from Anhui Polytechnic University, China, in 2022. He is currently pursuing the M.S. degree in computer science and technology with the School of Computer Science and Engineering, South China University of Technology, China. His research interests include machine learning, blockchain technology, and the Internet of Things.



JUN WU is currently pursuing the B.S. degree in Internet of Things engineering with the School of Computer and Information, Anhui Polytechnic University, China.

His research interests include the Internet of Things and blockchain technology.

JINGLEI HAN is currently pursuing the B.S. degree in Internet of Things engineering with the School of Computer and Information, Anhui Polytechnic University, China.

Her research interests include the Internet of Things and blockchain technology.