Computers, Materials & Continua

Tech Science Press

DOI: 10.32604/cmc.2023.035074
Article

Scalable Blockchain Technology for Tracking the Provenance of the Agri-Food

B. Subashini* **and D. Hemavathi**

Department of Data Science and Business Systems, School of Computing, SRM IST, Kattankulathur, Tamilnadu, 603203, India
*Corresponding Author: B. Subashini. Email: sb8375@srmist.edu.in

Received: 06 August 2022; Accepted: 04 December 2022

Abstract: Due to an increase in agricultural mislabeling and careless handling of non-perishable foods in recent years, consumers have been calling for the food sector to be more transparent. Due to information dispersion between divisions and the propensity to record inaccurate data, current traceability solutions typically fail to provide reliable farm-to-fork histories of products. The three most enticing characteristics of blockchain technology are openness, integrity, and traceability, which make it a potentially crucial tool for guaranteeing the integrity and correctness of data. In this paper, we suggest a permissioned blockchain system run by organizations, such as regulatory bodies, to promote the origin-tracking of shelf-stable agricultural products. We propose a four-tiered architecture, parallel side chains, Zero-Knowledge Proofs (ZKPs), and Interplanetary File Systems (IPFS). These ensure that information about where an item came from is shared, those commercial competitors cannot get to it, those big storage problems are handled, and the system can be scaled to handle many transactions at once. The solution maintains the confidentiality of all transaction flows when provenance data is queried utilizing smart contracts and a consumer-grade reliance rate. Extensive simulation testing using Ethereum Rinkeby and Polygon demonstrates reduced execution time, latency, and throughput overheads.

Keywords: Blockchain; IPFS; sidechain; supply chain management; traceability

1 Introduction

Agriculture contributed to civilization. It began independently in many locations worldwide, depending on the climate and topography. Beyond what could be supported by hunting and gathering, the human population was able to increase significantly due to agriculture. Agriculture is essential to a country's economy [1]. Scientists and farmers are researching genome editing, blockchain technology, artificial intelligence, and other methods to increase agricultural yields, use less water, and lessen environmental impact.

Supply Chain Management (SCM) coordinates business contacts in the non-perishable agricultural sector. It manufactures and supplies farm-to-plate goods to meet customers' quantity, quality, and price expectations. The supply chain management for non-perishable agri-food is based on the flow of raw materials, finished goods, and customers [2]. War, pandemics, and natural disasters require non-perishable meals. Shelf-stable, non-perishable products are essential in these situations. Non-perishables aren't refrigerated. Beans, dried cereals, nut kinds of butter, dried fruit, peanut butter, plant-based crackers, and energy-protein-rich meals including bottled juice, sugar and powdered creamer, powdered juice or lemonade, tea or instant coffee, cookies, hard candies, sweetened cereals, bottled water, and other comfort foods. Making, processing, and storing non-perishable foods. The traceability of non-perishable agricultural foods is essential for food safety. Traceability evaluates food chain security. Every supply chain step must collect data to keep agriculture open and honest. Real-time traceability adapts to unexpected events. It helps, but it is not safer or better [3]. Blockchain improves food traceability, quality, safety, and agricultural profitability. Blockchain data can instantly identify dangerous goods, preventing outbreaks and saving lives [4].

The main contribution of this paper is to build a complete Non-Perishable Agri-food Supply Chain (NPAFSC) traceability system that provides excellent provision for demanding customers concerned about their health and the safety of the food they consume. The traceability system uses blockchain technology, which provides decentralization, an immutable ledger with privacy and improved scalability. It integrates blockchain technology for the traceability issues of non-perishable agricultural products to overcome heavy computing load, slow query speed, and privacy data protection.

2 Related Work

Traditional NPAFSC industries are complicated, ever-changing systems with many actors. Fig. 1 shows the traditional NPAFSC food procurement, manufacturing, distribution, and finally, how it reaches the customer through the retailer.

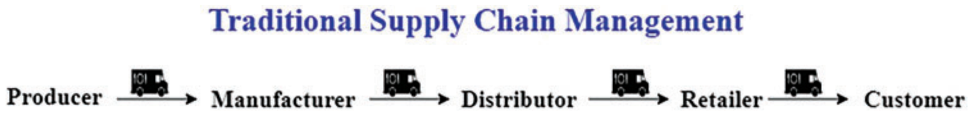

Figure 1: Traditional food supply chain management

Some challenges include Security and privacy, Credentials and Governing Compliance, Traceability, Lack of end-to-end visibility, Interoperability, Expiration, and Counterfeit Products, Stakeholders' Trust management, Conflict of interests, and Temperature-controlled Logistics. In NPAFSC with blockchain the global food distribution has agri-food safety. Before and after harvest, agri-foods may have safety risks. Fertilizers, pesticides, extra chemicals, and even scrap metal deposits from wastewater irrigation might damage agri-foods during and after harvest. Counterfeiting, falsely identifying a food's provenance, and mislabeling the manufacture and expiration dates can damage agri-foods throughout production [5]. The lack of an efficient monitoring or tracking system commonly results in these safety concerns, which pose a significant risk to human health [6]. Fig. 2 depicts blockchain-enabled information sharing among many partners throughout NPAFSC networks. Every stage of the value chain for a product can be tracked, from the point of manufacture to the point of end-user [7].

Peer-to-peer (P2P) network technology combines cryptography and timestamping technologies to develop an e-cash financial architecture [8]. It is transparent, tamper-proof, open, and accessible due to the blockchain's database schema, timestamp setting, and Merkle tree. When the predetermined circumstances are satisfied, a smart contract, written as code on blockchains, automatically executes itself without manual intervention. Smart contracts are the blockchain's most significant aid in removing financial industry limitations and integrating with other sectors [9]. This dependable data storage solution helps farmers. That includes independence, traceability, non-repudiation, compensation, and proprietary trading automation [10].

Public blockchains are readable, writable, and auditable. No one owns blockchain nodes, making changes impossible. Organizations manage private blockchain. Private blockchains are decentralized data storage. The first two blockchains create a consortium blockchain. A consortium blockchain seeks to foster industry cooperation. Blockchain improves efficiency, transparency, and accountability. 74% of organizations use blockchain, per Deloitte. Blockchains are advertised as business solutions [11]. Internet of Things (IoT), Artificial Intelligence (AI), and blockchain can increase efficiency, information traceability, smart farming, and logistics. Blockchain technology combined with IoT and machine learning may provide a complete picture of the agriculture business. By using IoT, the item/product will be well connected to supply chain resources and items [12].

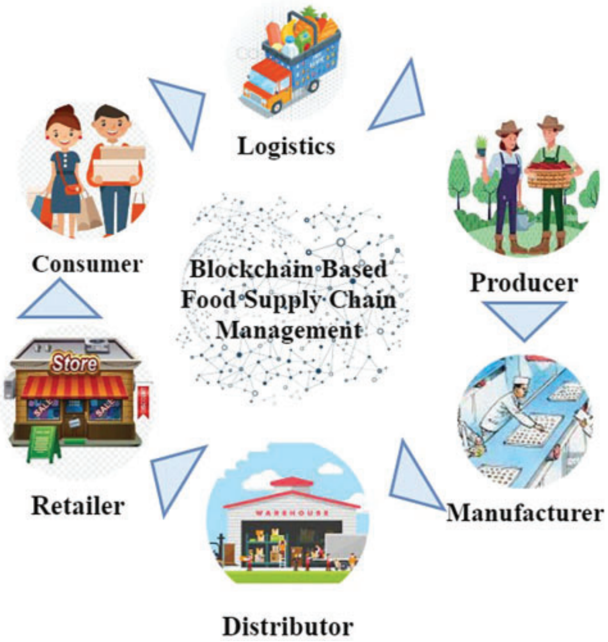

Figure 2: Blockchain-based food supply chain

The use of BigchainDB in the construction of the system enables it to meet the requirements of all participants in the agro-food supply chain. It is for availability, visibility, integrity, neutrality, and reliability. In [13], to incorporate the unique deployment of blockchain, IoT technology, and fuzzy logic into a total traceability shelf-life management system. These methods control perishable food, and a Blockchain-IoT-based Food Traceability System (BIFTS) is presented. Smart farming is made possible by IoT, Big Data, Global Positioning System (GPS), Cloud Services, and AI. To deploy production materials that are specifically targeted, agricultural production workers may monitor field data, weather conditions, pests, illnesses, and risk factors. To develop intelligent growing environment control, various execution equipment can be relocated to manage temperature, dimming, ventilation, and other activities. Time and money were saved by smart farming. It can help small and vulnerable farmers build extensive networks and intelligent transformation. Traditional agriculture can be "smartened" for mobile or computer platforms using sensors, gateways, cloud servers, etc. Smart agriculture includes e-commerce, food tracing, tourism, and information services.

Lin et al. [14] developed AgriBlockIoT, a ledger traceability system for the agro-food supply chain. The system was built on the Hyperledger Sawtooth and Ethereum platforms. Costa et al. [15] reviewed Radio Frequency Identification (RFID) and agri-food supply chain traceability, which explains the benefits and challenges of using RFID in the food supply chain. Future work proposes a cloud-based farm traceability system. Since then, as blockchain technology has grown in data science, cloud traceability systems leveraging Digital Ledger Technology (DLT) have been submitted. Feng et al. [16] demonstrated an IoT and blockchain-based food traceability system. He asserts that integrating IoT systems to collect data and a consortium blockchain as the core network will enable traceability. Based on the Hazard Analysis Critical Control Point (HACCP) system, Zhang et al. [17] developed an intelligent traceability platform for waterless fish long-distance transportation to promote quality control and safety transparency using Electronic Product Code (EPC) traceability system. Demestichas et al. [18] discuss how blockchains will be used to support traceability in the agri-food supply chain before delving into some of the commercialized applications that are currently in use, detailing their drawbacks and potential long-term applications.

3 Proposed Architecture for NPAFSC

3.1 Network Model

For non-perishable agri-food products, we created a digital traceability system that tracks them from the source point to the point of consumption across the supply chain. Our design implements a transaction and distribution mechanism that enables secure trading amongst agricultural and food supply chain companies. Using the permissioned blockchain, we leverage privacy preservation and incentive enforcement techniques based on ZKPs [19] and commitment systems. ZKP intends to allow a prover to convince a verifier that they are aware of some secret information x without telling any of the secrets. In our proposed model, we require confidentiality and openness for traceability. In the blockchain, trading confidentiality refers to the secrecy of who trades with whom and for how much of a property. We designate the variables p(x), m(x), and r(x) as the stakeholder states in the permissioned blockchain, the contributions in the permissioned blockchain, and the productions in the permissioned blockchain, respectively.

Consider the "distribution ratios" as matrices L(x), M(x), and N(x). The terms "who swap goods with whom and for how much" is denoted by the variables p(x), L(x), M(x), and N(x). Despite m(x) and r(x) being publicly available, they are private. A hidden Markov model is how we express the relationship:

$$p\left(x+1\right)=p\left(x\right)L\left(x\right)+m\left(x\right)M\left(x\right) \tag{1}$$

$$r\left(x+1\right)=p\left(x\right)N\left(x\right) \tag{2}$$

We also bring up the privacy and security of trade. The private information l(x), M(x), N(x), and p must be concealed to guarantee privacy. We define trade privacy as being secure if no probabilistic polynomial-time algorithm can tell whether the internal state p(x), the distribution ratios L(x), M(x), and N(x) were encrypted with truthful plaintexts or just zeros (false plaintexts). This concept stands to reason because L(x), M(x), N(x), and p(x) must all be private pieces of information. Protection and disengagement make up openness.

Protection: All of the commodities on the blockchain, both input and output, are unchangeable.

That is,

$$\sum_{u=1}^{q} p_u (x+1) + \sum_{u=1}^{s} m_u (x+1) = \sum_{u=1}^{q} p_u (x) + \sum_{u=1}^{t} r_u (x) \tag{3}$$

With the understanding that,

$$\sum_{v=1}^{q_o} d_{uv} + \sum_{v=1}^{s_o} e_{uv} = 1 \text{ for u} = \{1, 2, \ldots, q_o\} \tag{4}$$

$$\sum_{v=1}^{q_o} d_{uv} = 1 \text{ for u} = \{1, 2, \ldots, t_o\} \tag{5}$$

Disengagement: Evidence can be shown to show that certain blockchain users were not involved in a string of transactions. In the case of a participant u,

$$d_{uv} = e_{uv} = 0 \, for \, all \, v \neq u, \tag{6}$$

$$d_{vu} = e_{vu} = 0 \, for \, all \, v \neq u, \tag{7}$$

$$g_{vu} = 0 \, for \, all \, v \tag{8}$$

All of the given equations are encrypt ted using Learning With Errors (LWE). The ciphertext of f(p) – m is a ciphertext of zero because f(p) = m remains in plaintext. We demonstrate with zero knowledge that every cryptographic function has a plaintext q = 0, using the blockchain system as a prover and the permissionless blockchain as a verifier.

The proposed model has four tiers and is built on the layered network design given in Fig. 3. The **physical layer**, for example, mediates interactions between active stakeholders and querying stakeholders in the NPAFSC. The NPAFSC supply chain's producer is the first party to use a smart contract and begin trading. The producer is responsible for producing a sizable quantity of non-perishable food and monitoring and assuring the food's characteristics from the beginning. He offers these components for sale to food processors. The manufacturer or the processor is in charge of removing superfluous elements and transforming the food into a finished good once it has been obtained from the producer. Wholesalers buy the completed product from the processor. Retailer and Distributor—According to the non-perishable products, a distributor maintains a warehouse with the ideal temperature. It is in charge of purchasing finished items from processors and selling them to retailers. Retailers buy finished, traceable products in larger quantities from wholesalers and then sell them to customers.

Data on provenance may be monitored using the distinctive identifiers on traceable products. The logistics firm ensures that the products are delivered from the relevant parties to the customers in a secure and auditable manner. Regulators, inspectors, and government personnel comprise the Food Safety Authority (FSA). Customers can learn about their food safety rights and obligations from these monitoring groups. The FSA can apply food benchmarks and conduct physical audits and inspections to ensure food safety. The customers are the end users. They are the query members regarding the products. When transactions are completed, active stakeholder nodes generally respond to block generation and feedback generation and keep track of transactions that pertain to them.

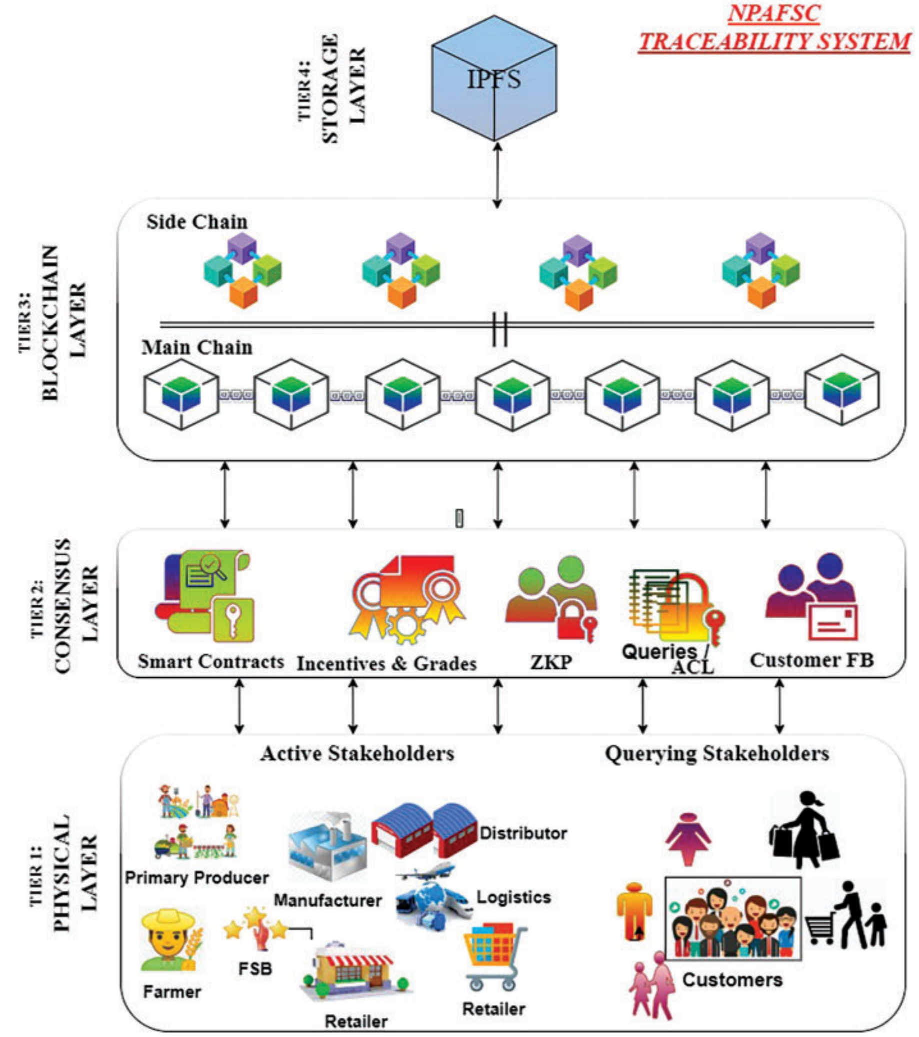

Figure 3: Layered architecture

These contacts may include product exchanges and delivery confirmations. The **second tier** is the consensus layer, which manages transactional data and the process and distribution method. In addition, its ledger keeps track of the credentials using Zero-Knowledge proofs, the reputation of the system's stakeholders, and consumer feedback. The **third tier** is the blockchain layer, which aids in network scaling. The blockchain layer retains hashes of data in order to improve storage capacity. A side-chain solution is utilized to boost scalability. Side chains aim to offload part of the work that the main blockchain must perform; The **fourth tier**, the storage layer, is where the actual data is saved. The blockchain layer uses robust access control methods to stop illegitimate readings and writing to the storage layer. To reduce the data explosion in the blocks that happens due to the tracing and tracking of products from origin until delivery, we opt for InterPlanetary File Storage (IPFS). IPFS is a decentralized method of storing data that gives maximum throughput, reduced latency, and scalability.

3.2 Traceability Authorization Centre Ledger (TACL)

At frequent intervals, the TACL monitors and supervises active stakeholders and FSA in the food supply chain. They keep detailed records of all stakeholders, customers, and FSA, as well as transaction and feedback evaluation data. They have access to and control over all stakeholder data in a blockchain. The NPAFSC traceability system should clarify who provides the data and who is responsible for its accuracy and timeliness. As a result, the authentication mechanism must be added, which is the responsibility of the TACL. The ledger is only in charge of user registration and does not process any data related to product traceability. The TACL receives the user's registration application and then authenticates the user's identity either online or offline, depending on which method the user chooses.

After the user has successfully authenticated themselves, the asymmetric encryption process is used to generate a pair of keys. The user is responsible for keeping the private key a secret. The company's public key is then submitted to the TACL and connected with the account of the business, which is explained in detail in Section 3.4. After that, the user's registration is finished being processed.

3.3 Traceability Data Ledger (TDL)

A supply chain trader acquires trader credentials after completing an onboarding process on TACL. The permissioned blockchain, the Traceability Data Ledger (TDL), only allows registered SC companies to participate. Using Zero Knowledge Proofs (ZKPs), the shopper joins TDL by validating his identification obtained on TACL. Stakeholders can use ZKP to establish their credentials for TDL without revealing them. The TDL administrator is in charge of new entity registration. Traceability-related transactions can only be recorded on TDL by traders with verifiable TACL credentials. TDL admin has a public credentialed identity on TACL and processes TACL entity join requests to TDL. TDL admin requires evidence of trading credentials as part of this process. TDL enables the trader to sign up for TDL using any of his publicly accessible digital identities. A vendor needs to submit verification of its credentials while registering, not private certificates.

Using public digital identification, credentials, and ZKP, Algorithm 1 outlines the steps in registering a trader with TDL. Through ZKP, the trader can demonstrate his trading qualifications without disclosing them completely. A ZKP allows an entity (the Prover) to confirm a personal value, *V*, to another entity (the Verifier). In our scenario, TDL's administrator serves as both a credential prover and a credential validator. The seller has an identity, *I*, on his digital identity, *V*, which states a good, *G*, about *V*, which is made up of attributes a_1, a2… an. Assume a supply chain authority (SCA) has confirmed Prover's identity *V* for a commodity *G*. It delivers (*G, I*) to the Verifier, who can authenticate that *I* issued by the issuer. Setup, proof generation, and proof verification are the three primary processes in the ZKP process.

Algorithm 1: Credentials Registry and Traceable Data Entry.

```
Input: Trace data entry permission commences.
Output: Permission Provided with ZKP.
    for each stakeholder $\acute{S} \in$ TDCL do,
    Initiate permission request with $\acute{R}$.
    $\acute{R}$ creates $ID_P^{\acute{R}\text{-}\acute{S}}$, Stakeholder saves in wallet.
    $\acute{R}$ records $ID_P^{\acute{R}\text{-}\acute{S}}$ creation + $V_k^{\acute{R}}$ in TDCL.
```

(Continued)

Algorithm 1: Continued

```
5.  Ŕ sends joining call, $J_C = [ID_P{}^{\acute{R}\text{-}\acute{S}} \| V_k{}^{\acute{R}\text{-}\acute{S}} \| N] \rightarrow \acute{S}$,
                            where N stands for nonce.
6.  Ś receives $J_C$ with wallet (w) creation.
7.  Ś generate $J_{Res} = [ID_P{}^{\acute{S}\text{-}\acute{R}} \| V_k{}^{\acute{S}\text{-}\acute{R}} \|N]$
8.  Ś directs Encryption $(J_{Res}, V_k{}^{\acute{R}\text{-}\acute{S})} \rightarrow \acute{R}$.
9.  Ŕ Decrypts $J_{Res}$.
10. Ŕ records $[ID_P{}^{\acute{S}\text{-}\acute{R}} + V_k{}^{\acute{S}\text{-}\acute{R}}] \rightarrow$ TDCL.
11. End for.
12. For each stakeholder $\acute{S} \in$ TDCL do, // For entering traceable data.
13. Include public parameter (Pu) → ZKP.
14. Create a random prime number p and number n, such that $\gamma = pn+1 \rightarrow$ prime and p does not
    divide by n.
15. Construct random $r < \theta$, where $r^n \neq 1 (\bmod \theta) \|$ compute $r' = r^b \neq 1$.
16. Construct random $y < p \|$ compute $h = r'^y$, where $\theta$, p, r′, $h \in Pu$.
17. keyG $(1^k, S) \rightarrow$ (ProveK, VerifyK), where k is the secret parameter in S.
18. ProofG (ProveK, i, L) $\rightarrow \alpha$, where i is the input secret that$\rightarrow \alpha$.
19. VerifyG (VerifyK, $\alpha$, i) $\rightarrow$ {1,0}, where {1 →Provide Trace Permission
                                          0 →No Permission}
20. End for
```

3.4 Traceability System Workflow

We propose organizing a consortium of businesses and NPAFSC members who will agree on permissioned Blockchain accessibility rules. The formation of a consortium aims to reduce the impact of individual NPAFSC businesses on judgment while also giving participating NPAFSC businesses a platform to work together on a common objective and consumer expectation goal. The consortium members will collaborate to determine the access rules for writing to and reading from the blockchain.

Entities actively engaged in the food supply chain process are "**active stakeholder**s." "**Querying Stakeholder**s" are entities that are not naturally a part of the NPAFSC and do not provide any information to the blockchain. However, these entities can query the blockchain for traceability information and offer feedback suggestions.

The **Food Safety Authority** (FSA) determines who has the power to update the Access Control List and creates access controls for NPAFSC objects in the form of an Access Control List. The food control board includes representatives from food regulatory agencies, food inspection boards, and government entities. These monitoring bodies can also educate customers and NPAFSC members about their food safety rights and obligations. The FSA can enforce rules like food safety regulations and perform physical reviews and audits of pertinent facilities to ensure that food safety criteria are satisfied. They can, for example, ensure that frozen foods are kept cold and non-perishable foods are correctly wrapped.

TACL and TAL are the important ledgers of the blockchain layer. Data relating to distributed stakeholder identifications and the Food Safety Authority (FSA) is managed using the public permissioned blockchain known as TACL, which is based on Sovereign Identity Design (FSA) [20]. Distributed identities include forms, wallets, and smart contracts as destinations. To get their permits, a supply chain trader and an FSA must complete the registration process on TACL. TDL is a public blockchain where participation is restricted to authorized supply chain companies. Active stakeholders can ask to upload traceability data into TDL by establishing their legitimacy in TACL through Zero Knowledge Proofs (ZKPs). The ZKP lets stakeholders show the TDL admin their credentials without revealing them. After proving their validity, a stakeholder can record trade-associated transactions on TDL. Since the bulk of traceability data is present, which leads to the data explosion, we move the TDL data to the side chain. Dealing with scalability is a significant problem when implementing a collective solution. Transaction load in non-perishable food supply chains increases in response to activity in the supply chain and anticipation of the future expansion of supply chain players in the network. The latency and throughput of the block chain are limited to a few hundred nodes [21]. We use the side chain concept to solve the scalability issue [22]. It is built on parallel processing, in which numerous nodes simultaneously work on the same task. There is a "local TDL" for each side chain, which is synced with the global TDL and contains all transactions connected to a single end product. Since the global supply chain, we organize the side chain per diverse places. In the supply chain, a Validator (V) is a computer server dedicated to gathering all the transactions, confirming them, and adding them to the blockchain.

As the number of side chains grows, a side chain's role in the network's scalability is enhanced. Once again, the blockchain and the side chain store lots of transactional records, which is cumbersome. We turn to the **InterPlanetary File System (IPFS) to overcome that situation.** IPFS is a file-sharing and data-access system that is distributed. We do not need to keep whole files on a blockchain if we use IPFS storage. We merely save the IPFS hash, which is far less expensive [23]. The CID, or hash in blockchain, can be used to get files from IPFS. A smart contract is a condition that must be met for all the events in the workflow shown in Fig. 4 to take place. With meeting the ZK proof requirements, action is started from the active stakeholders towards TACL and TDL as specified in Subdivisions 3.2 and 3.3. Smart contracts send out the requested relevant data, which includes instances of the trigger condition when the trigger condition is satisfied. This system of transaction processing modules and state operations implements smart contracts in response to the parties' needs rather than generating or updating them. The action sequences of the querying stakeholders begin when traceability details are recorded. The execution of smart contracts is done by thousands of nodes in the traceability network. Customers may monitor, track, and provide feedback using smart contracts since they gather events and deploy them as function calls.

3.5 Traceable Data-Transaction Generation

All stakeholders will be able to record details about their product once their details are acknowledged by the network using Zero Knowledge Proof. Table 1 details the descriptions of various notations used in this work. After the ZKP has cleared the network, the stakeholders are free to enter the commodities' traceable-related data. The digital signature's public and private keys will be available to stakeholders. To begin with, take a producer like a farmer as an example. The product movement starts with them. The relevant smart contracts will initiate each transaction in this scenario. Starting with a primary producer's transaction, TS_i authenticates a new commodity's formation and describes its quality smart contract, a register containing data about each commodity produced. A quality contract specifies valuation procedures, temperature limitations, rating criteria, etc. A product can be traded amongst the numerous organizations that make up the supply chain once it has been produced by its primary producer and is on its way to the marketing rack. Verification that the product was genuinely transferred from the seller to the buyer is provided by the conclusion of the trade transaction, TS_P.

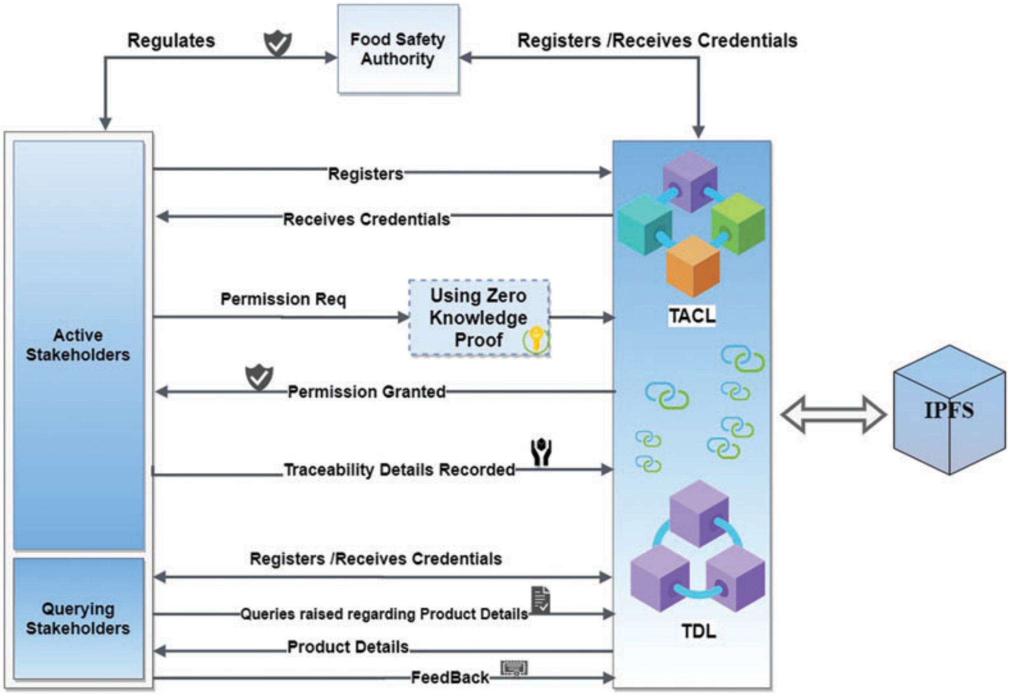

Figure 4: Trace system workflow

Table 1: Descriptions of various notations

Notations	Descriptions	Notations	Descriptions
TS	Transaction	QC_{Sco} (NPP)	Quality check score of the commodity
SH	Producer (P), Manufacturer (M), Distributor (D), Retailer (R), Logistics (L), Customer (C).	DS_{Sh}	Digital signature of stakeholders
SH_{ID}	Stakeholders identity	Pu_{Sh}	The public key of stakeholders
TS_i	Transaction initiate	Piv_{Sh}	The private key of stakeholders
TS_{Sh}	Stakeholders' transactions	C_{FB}	Customer feedback
TS_{IoT}	Transactions related to IoT	Gn	Gateway node
TS_{FSA}	Transaction by food safety authority	GR_{SH} (NPP)	Stakeholders give a grade to the NPP
TS_E	Transaction ends	GR_{FSA} (SH)	FSA gives a grade to the stakeholders
NPP_{Id}	Non-Perishable product ID	GR_{FSA} (NPP)	FSA gives a grade to the NPP
H (NPP)	Hash of non-perishable product details	GR_{IoT} (NPP)	IoT gives a grade to the NPP
O_{Sh}	Stakeholders ownership	RR	Reliance rate

Also, the ownership of the product that was O_P in TS_i would be changed to O_M in TS_P. Since the commodity is registered using TS_i, IoT devices that track a commodity's temperature through different logistics can record temperature-related data using IoT transactions, TS_{IoT}, on the Blockchain. Because IoT sensors have restricted computing ability, gateway nodes (Gn) perform these transactions. The transaction's production rate is different from the commodity's trading rate. Before a trade event, this ensures the product is routinely monitored in storage.

The FSA regulates people's food safety rights and responsibilities. In addition to food safety rules, the FSA can conduct physical audits and inspections. The FSA assigns a rating for the seller, GR_{FSA} (SH), and a rating for the commodity, GR_{FSA} (NPP), by the smart contract that TS_{FSA} provides following a physical inspection of a storage facility, recognition from the customer's C_{FB}, and other safety details. Thus, for an NPP to move from a producer (TS_P) to a manufacturer (TS_M), the different transactions triggered by the smart contracts carry unlimited data and undergo various quality checkpoints given in Table 2. Similar transactions take place from manufacturer until it reaches the customer.

Table 2: Transaction details from producer to manufacturer

1. The producer (Farmer) rolls to TACL and creates a wallet.
2. The producer is provided with Pu_P, Piv_P, DS_P.
3. The producer registers to TDL through ZKP and acquires permission to enter the traceable data.
4. The producer initiates transaction,
   $TS_i \rightarrow NPP_{Id} \,\|\, H\ (NPP) \,\|\, O_P \,\|\, QC_{Sco}\ (NPP) \,\|\, DS_P \,\|Pu_P$
5. Product handover transaction,
   $TS_P \rightarrow NPP_{Id} \,\|\, H\ (NPP) \,\|\, O_M \,\|\, DS_P \,\|\, Pu_P\| \, DS_M \,\|\, Pu_M$
6. Transaction by IoT sensors during transportation from Producer to Manufacturer,
   $TS_{IoT} \rightarrow NPP_{Id} \,\|\, H\ (IoT\ Data) \,\|DS_{Gn}$
7. FSA Audit and Inspection details at the Producer end,
   $TS_{FSA} \rightarrow P_{ID}\| \, H\ (Inspection\ Details) \,\|\, NPP_{ID}$
8. The transaction ends with the summation of 4 to 7 transactions and is given as,
   $TS_E \rightarrow NPP_{ID} \,\|\, DS_M \,\|\, Pu_M$
9. Steps 4 to 8 repeat through the active SH until it reaches Querying SH.
10. Finally, customer receives the product, traces the provenance, and gives the feedback, C_{FB}.

3.5.1 Transaction Validation and Verification

In order to maintain the visibility of trade flows, a transaction is not announced to all NPAFSC participants; instead, it is revealed just to the validators. Verifying nodes on third-tier side chains, selected randomly based on the Quality Check smart contract, commit a new block. The NPAFSC transactions are kept locally after they have been verified. Because the parallel side chain will employ the identity validation process, we restrict the explanation of transaction validation to just one side chain. Many validators can be added to each side chain to spread out the strain of transaction verification and prevent bottlenecks and single points of failure.

Reputation details for transaction validation and verification will be calculated in two phases. First, the details to be provided from the trader's side; The co-stakeholders' honest opinion regarding the product. For example, the manufacturer is to provide the product status they received from the vendor (Producer) at the time (t). It is given as $GR_{purchaser}(t)$. The condition is to specify how it reaches them. The grade (GR) of the purchaser to the vendor can be given as good, average, or bad with a score of 1, 0.5, and 0, respectively. The product will be in very good condition; sometimes, it can be from average to bad. Accordingly, the ratings can be given. Secondly, Food Safety Authority (FSA) suggestions regarding the product FSA can openly give an opinion regarding the NPP's health-related information, exact details about the ingredients, nutritional values, price, and expiry details.

So, on the whole, it provides the inspection details, GR_{FSA} (NPP), and the grade (healthy or junk) of the item to be purchased. Also, FSA provides the grade for the stakeholders, GR_{FSA}(SH), audits them. Finally, the results of the IoT sensors at various checkpoints regarding the optimum temperature to be maintained during transport. It is given as GR_{IoT} (NPP), whose value can be either 0 or 1. Grade 1 is necessary for the product to reach the customer, and 0 for recall. The second phase includes the details provided by the end customer based on the product status they received. A customer must rate the product based on its quality and how much they are satisfied with its provenance. It is given as C_{FB}.

The grade scores for the present and prior supply chain events GR_{vendor} (t_0), GR_{vendor} (t_1) ..., GR_{vendor} (t_n) are taken into account to determine the total GR (t_n) for a trader at time t_n as in Eq. (9).

$$GR(t_n) = \sum_{t=t_0}^{t=t_n} GR_{vendor}(t) \times \delta(t_n - t) \tag{9}$$

Where, GR_{vendor} (t_0) and GR_{vendor} (t) are the vendor's grade at the start time and any specific "t" time, respectively, also, any specified "t" time will have a neglected parallel element, $\delta(t_n - t)$. Subsequently, the impact of the new occasions on store network rules has happened before in time. GR (t_n) is a trader's overall grade for trading a single product. Commodity-specific grades are produced for each product type and saved on the vendor's side to give a count for the trader. Periodically, a trader's grade can be measured. For a transaction involving a purchaser and a vendor that occurs at time t, the GR $_{vendor}$ (NPP) is calculated based on the value of $GR_{purchaser}$ (t), GR_{FSA} (NPP), GR_{FSA} (SH), GR (NPP), GR_{IoT} (NPP), and lastly, the C_{FB}. Each factor may or may not have an incremental element, i = 1, 2 . . . α, that can be multiplied by the supply chain features. Furthermore, the equation is given in Eq. (10).

$$GR_{vendor} = \sum GR_{purchaser}(t) + GR_{FSA}(NPP) + GR_{FSA}(SH) + GR(NPP) + GR_{IoT(NPP)} + C_{FB} \tag{10}$$

Thus, we can calculate a stakeholder's reliance rate, RR_{SH} (t_n), using the total grade score GR (t_n) and a few different estimation scores e1, e2 . . . e_N, as given in Eq. (11).

$$RR_{Vendor}(t_n) = \sum_{\partial=\mathbf{1}}^{\partial=n} \partial \times GR(t_n) \tag{11}$$

These quality check details in the form of smart contracts help choose the validator. This validator can be any stakeholder who validates and provides consensus for adding the transactions to the blockchain. On the whole, GR (t_n) and RR_{SH} (t_n) at the time 't', together provide QC_{Sco} (NPP), Quality Check Score of the product. These values and ratings will be published on the network to incentivize the stakeholders.

3.5.2 Block Validation and Addition

We traded the transaction TS between the producer (SH_P) and the manufacturer (SH_M). To validate the transaction TS, the validation algorithm below chooses the prime validator (PV) out of all the validator nodes V to validate the transaction TS. It then distributes that information to the side chain producer (SH_P). The assumed procedure guarantees that each group member is familiar with PV, the Prime Validator. For transaction validation, the initiator node, SH_P, submits the identical transaction TS to the primary validator node, PV.

Algorithm 2

```
    Requirement $GR_{SH}$ and $RR_{SH}$ at time 't'
1:  If $GR_{SH} \geq Max \| RR_{SH} = Good$ then
    $SH \overset{becomes}{\rightarrow} V$
    Else "Not a Validator"
    If SH >1, choose SH >max (Incentives)
    $SH \overset{becomes}{\rightarrow} PV$
    End if
    End if
2:  $SH_P \rightarrow H(TS \| TS_{ID} \| ID_{SH}) = X$
3:  $SH_P \rightarrow PV_{Pu} Ency(DS(TS)) = Y$
4:  $SH_P \overset{Publicly\ sends}{\Longrightarrow} (X, Y, TS_{ID}, ID_{SH})$ to PV
5:  $PV_{Pi}Decy(Y)$ and validates TS
6:  $H(TS \| TS_{ID} \| ID_{SH}) = Z$
7:  If $X = Z$,
    PV creates "New Block", B
    Else "validation is not successful"
    End If
8:  Block $\rightarrow$ Broadcasted by PV
9:  Other Validator(V) respond with {0/1},
    Where 1 $\rightarrow$ B accepted, 0 $\rightarrow$ B not accepted
```

The new block B is generated by the prime validator node (PV), which then delivers the encrypted block B to the other validator nodes for block validation. The additional validator nodes confirm B and send a 0 or 1 response message to the main validator node in return. We assume that a value of 0 indicates a negative response, which means that the other validator nodes have not correctly validated B. A value of 1 indicates a positive reply, which means that the other validator nodes have correctly verified B. According to Algorithm 2, if more validator nodes successfully verify B, B is accepted by PV. After PV has verified B, it is added to the blockchain network as part of a side-chain transaction or a transaction based on the main blockchain network. Moreover, the data is stored in the IPFS, and the hash value is stored in the blocks. The remaining network entities for the most recent iteration of the blockchain synchronize with the PV.

3.6 Querying Stakeholders-Access Tokens for Tracking Data

Customers, in this case, who are referred to as stakeholders in querying, would prefer various types of questions [24]. Here, feedback on the goods and traceable information on the purchased item are required. Accordingly, the query parameters used to access the TDL are made with a smart contract based on the Access Control List (ACL), which means they can only be changed when the smart contract is updated. Due to anonymity, it might also be up to the stakeholders to decide whether to give customers all the information they require or just what they need. Therefore, no generic ACL parameters that smart contracts could use for customer queries are allowed. It changes accordingly to time and conditions. The requester will use an offline method to retrieve access tokens. Query Contract (QC) must generate the decryption request to ensure that decryption can only take place there and that SH's identities are not accessible to validators of the blockchain system outside of QC, even though the trader selects the cryptographic policy based on the parameters and the function of the requester, namely validator, consumer, stakeholder, and FSA.

Fig. 5 illustrates the steps involved in working on the QC. Step A gives the request token to the admin by querying SH. The TACL admin confirms the registration and issues the customer with a token. The customer submits the query request to the validator in step C, who approves the transaction in step D and initiates the QC in step E. The ACL-based smart contract gathers data from the ledgers and consolidates it appropriately in steps F and G. Finally, the customer receives the outcome through the validator in stages H and I. The end user acknowledges it by providing feedback.

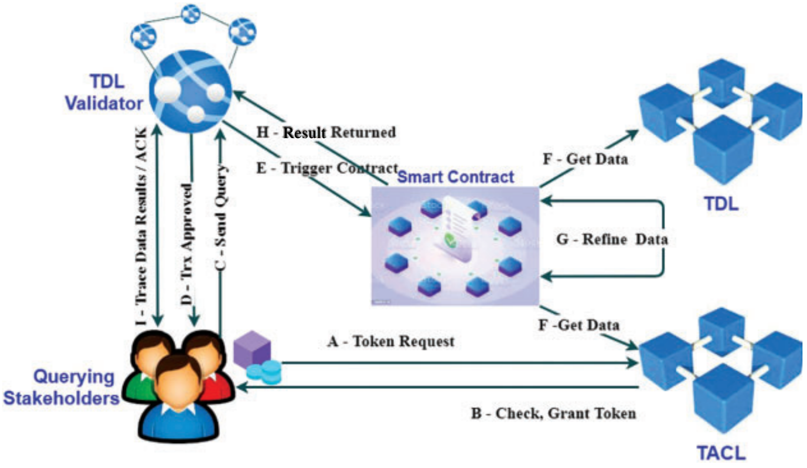

Figure 5: Querying trace data

Positive feedback increases success, while obstructive feedback decreases it. A lack of interactions between the two also causes experience to deteriorate. The present success value S_v, the feedback value α, and the volume of transactions all influence the rate at which success increases or decreases. Success value can be given in a mathematical difference equation. Positive feedback indicates that when α is normalized to the interval of (0,1), $\alpha > \beta_{\text{positive}}$.

A linear differential equation is used to model the rising trend and goes as follows:

$$S_{v+1} = S_v + \alpha_v \times \Delta S_{v+1} \tag{12}$$

$$\Delta S_{v+1} = \delta \times \left(1 - \frac{S_v}{Max_S}\right) \tag{13}$$

where, S_t is the current success rate at time t, init_S is the starting success rate, max_S represents the highest possible success rate, t represents the current good feedback score, and δ is the is the current maximum increase at time t.

The decrease due to negative feedback means, $\alpha < \beta_{\text{negative}}$ and modelled as,

$$S_{v+1} = Max\,(Min_s, S_v - (1 - \alpha_v) \times \gamma \times \Delta S_{v+1}) \tag{14}$$

where, ΔS_{t+1} is got by calculation (13). α_v, $\gamma > 1$, Min_S determines negative feedback values at period t, reduction rate and lowest success rate correspondingly.

4 Evaluation and Analysis

An open-source platform for blockchain, Ethereum, and Polygon is utilised for the simulations. We write and test smart contracts using the Remix Integrated Development Environment (IDE), Ganache, Truffle, and Metamask. The Ethereum Ropsten and Polygon test networks are where the smart contracts are executed and tested. Polygon runs on the summit of the Ethereum Virtual Machine (EVM). Ethereum uses blockchain technology to create decentralized applications. The script is coded using Solidity language to analyze the suggested smart contracts for the blockchain-based NPAFSC system. Solidity version 0.8.7 and Remix IDE use an Intel(R) Xeon(R) CPU E5-2630 v4 @ 2.20 GHz, 24.0 GB of RAM, Win10 Pro, 64-bit OS, x64-based processor, and IPFS version 0.8.0. is used here.

4.1 Cost of Transaction and Cost of Execution

Functions in the suggested smart contracts have a gas value. Every smart contract function's gas cost is being tracked. Execution and transaction costs apply to all functions. The execution cost is what it costs to carry out the computational operations, and the transaction cost is the cost of transmitting the code to the blockchain. The cost when the smart contract changes from one state to the next and transaction costs are higher than the execution cost is shown in Fig. 6. The price calculated by Remix IDE is expressed in Ethereum gas. This unit represents the processing required to carry out smart contract functions. Our blockchain-based technology offers many advantages. Every transaction on Ethereum is encrypted. Attackers cannot alter the transaction because the private key is required for signing it. The transaction would not be recorded in the miner's block. Complete and uninterrupted supply chain communication is maintained.

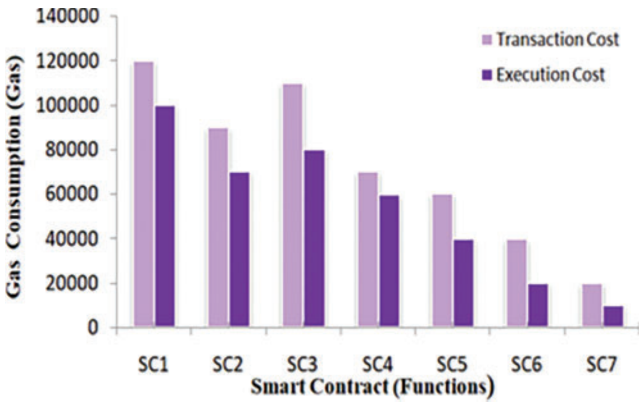

Figure 6: Transaction cost & execution cost

4.2 Performance Validation

The three-performance metrics used to track and evaluate the blockchain platform's performance are throughput, latency, and scalability. We test our implementation's latency and throughput on

Ethereum and Polygon. In this part, we examine how transaction rates affect blockchain network efficiency. 50, 100, 150, 200, 250, and 300 transactions per second were tested. Changing the number of transactions in a blockchain helped study their impact. Both regular operations and query transactions were tested. Total transactions were adjusted to understand better how they affect blockchain throughput and delay. All blockchain transactions' throughput and latencies have been measured. Figs. 7 and 8 show latency and throughput statistics on different platforms at different times.

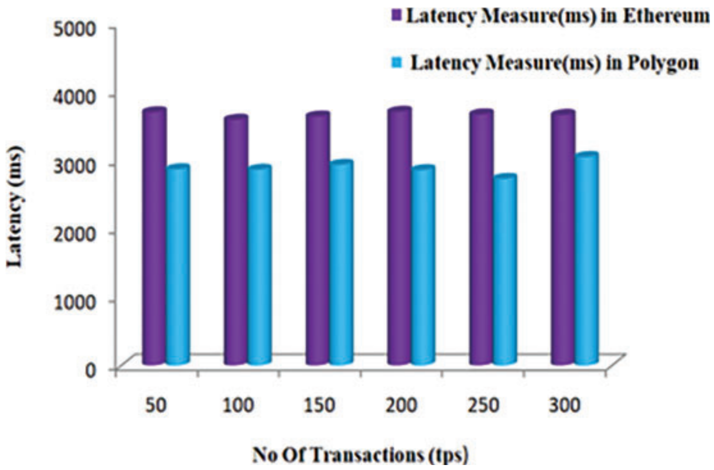

Figure 7: Latency measure of transactions in different networks

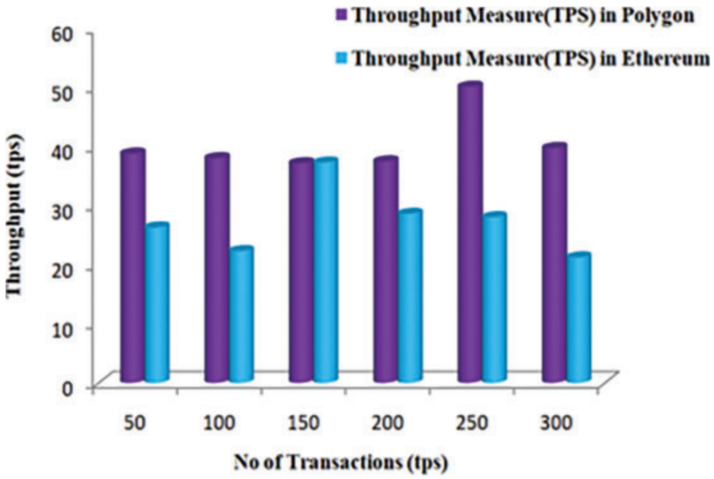

Figure 8: Throughput measure of transactions in different networks

The query time, also known as how long it takes to retrieve the whole product history, is one of the most crucial evaluation data points for traceability systems. When a query is run on TDL, the term "query time" means the amount of time it takes to find the transactions involving significant items. It is essential to remember that the query time may increase if a transaction comprises more than one key component because, at this point, the traceability to the initial transaction will be branched. We estimate the query time based on the number of side chains and IPFS while assuming there is just one essential component. Figs. 9 and 10 provide the delay and performance measures on different platforms.

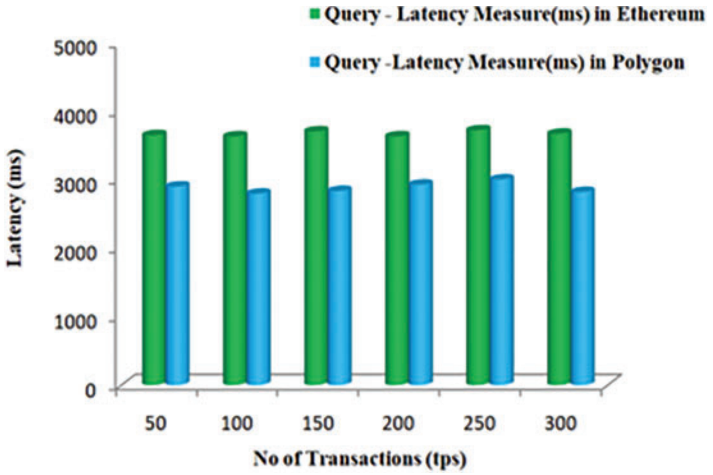

Figure 9: Latency measure of query transactions in different networks

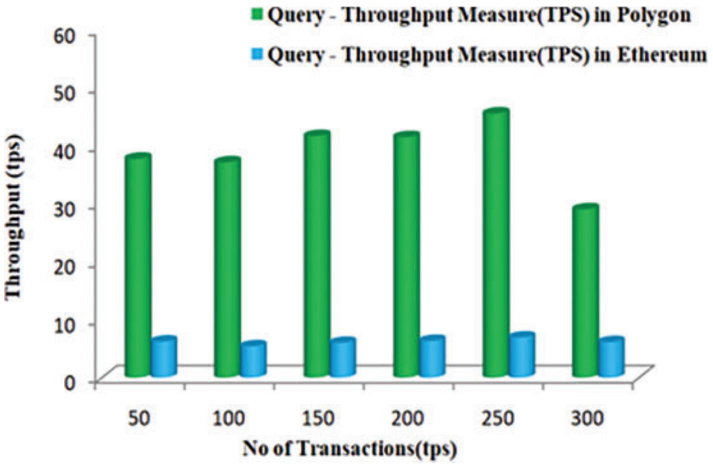

Figure 10: Throughput measure of query transactions in different networks

4.3 Scalability Comparison

Based on the test results conducted on the different test networks, namely Ethereum Rinkeby and Polygon test network, average latency and average throughput are calculated. The calculations are made for various transactions involving registration, trace data recording, approvals, recalls querying, etc. We calculate the latency and throughput for all transactions in general and query transactions alone. The result in Table 3 shows that the average latency of the Polygon test network is less compared to the Ethereum test network. Similarly, the throughput observed in the Polygon test network is higher than in the Ethereum test network.

Therefore, the proposed method with the polygon test network allows for more transactions to be added to the chain simultaneously. This situation makes it possible to offer services to a more significant number of users, which in turn improves the scalability of the system as a whole, as shown in Fig. 11. Additionally, the use of IPFS requires minimal load, which contributes to an increase in the overall scalability of the system. Also, we evaluated how well our system performed compared to other traceability solutions. The comparative results shown in Table 4 can confidently infer that our approach performs exceptionally well compared to other blockchain-based and centralized traceability systems. All systems are capable of completing the fundamental task of information traceability. However, our solution is more tamper-proof than centralized systems and other methods. This technique lessens the data explosion issue on the blockchain as compared to the standard blockchain system.

Table 3: Scalability comparison

	Ethereum (Rinkeby)	Polygon

Average latency	OT = 3653.45 ms
	QT = 3665.9 ms
		OT = 2874.71 ms
		QT = 2877.5 ms

Average throughput	OT = 27.3 tps
	QT = 6.1 tps
		OT = 40.2 tps
		QT = 38.72 tps

Note: OT-Other transactions QT–Querying Transactions.

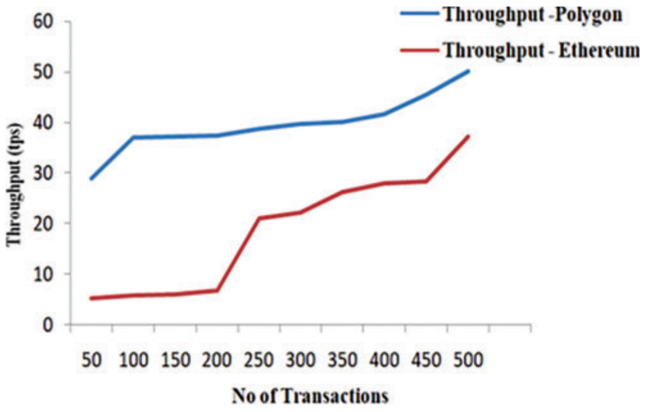

Figure 11: Scalability comparison

Table 4: Comparative results

Features	[25]	[26]	[27]	[28]	[29]	[30]	Our work
Traceability	Yes	No	No	No	No	No	Yes
Accountability	Yes	No	No	No	No	No	Yes
Reliability	No	No	Yes	No	No	No	Yes
Authenticity	No	No	No	No	No	No	Yes
Reliance rate	No	No	Yes	Yes	Yes	Yes	Yes
Scalability	No	No	No	No	No	No	Yes

5 Conclusion Notes and Future Work

Based on our research findings, we propose a blockchain-powered system that could be used to trace the origin of products purchased through a supply chain. A complete strategy is required by design, which may benefit customers, regulatory compliance bodies, and supply chain stakeholders.

In addition, the framework provides a transaction that can be quickly traced back to a particular element; access control that ensures no single member has authority over the blockchain; and a layered system architecture that addresses scalability concerns. A security analysis demonstrates that our proposed method can withstand many client-and network-based attacks without being compromised. The simulation results show that the query time for the commodities record is sufficient for the application's needs. It was the subject of our research, and we conducted an in-depth investigation to determine its design defects.

A sensor linked to every blockchain transaction could help with traceability and inspection control if supply chain members misrepresent their intentions, offer erroneous information, or experience a quality reduction. The existing approach could be updated to support better-unconnected product ledgers, in which the production of a product account may be unsatisfactory without an intermediate transaction.

Acknowledgement: Authors are grateful to all who supported us in producing this article and for those who contributed to this study.

Funding Statement: The authors received no specific funding for this study.

Conflicts of Interest: The authors declare that they have no conflicts of interest to report regarding the present study.

References

[1] G. Sujatha, K. Sornalakshmi, S. Sindh and D. Hemavathi, "An architectural framework of a Decision Support System (DSS) to increase the returns of small scale farmers in Kanchipuram District, India," *EAI Endorsed Transactions on Energy Web*, vol. 7, no. 29, pp. e2, 2020.

[2] S. Kumar and A. Nigmatullin, "A system dynamics analysis of food supply chains-case study with non-perishable products," *Simulation Modelling Practice and Theory*, vol. 19, no. 10, pp. 2151–2168, 2011.

[3] L. Zhu, "Economic analysis of a traceability system for a two-level perishable food supply chain," *Sustainability*, vol. 9, no. 5, pp. 682, 2017.

[4] H. M. Kim and M. Laskowski, "Agriculture on the blockchain: Sustainable solutions for food, farmers, and financing," 2017. [Online]. Available: https://ssrn.com/abstract=3028164

[5] T. K. Dasaklis, F. Casino and C. Patsakis, "Defining granularity levels for supply chain traceability based on IoT and blockchain," in *Proc. of the Int. Conf. on Omni-Layer Intelligent Systems*, Crete Greece, pp. 184–190, 2019.

[6] J. Xu, S. Guo, D. Xie and Y. Yan, "Blockchain: A new safeguard for agri-foods," *Artificial Intelligence in Agriculture*, vol. 4, no. 1, pp. 153–161, 2020.

[7] H. Xiong, T. Dalhaus, P. Wang and J. Huang, "Blockchain technology for agriculture: Applications and rationale," *Frontiers in Blockchain*, vol. 3, pp. 7, 2020.

[8] S. Nakamoto, "Bitcoin: A peer-to-peer electronic cash system," 2008. [Online]. Available: https://bitcoin.org/bitcoin.pdf

[9] Z. Shahbazi and Y. C. Byun, "Blockchain and machine learning for intelligent multiple factor-based ride-hailing services," *Computers, Materials & Continua*, vol. 70, no. 3, pp. 4429–4446, 2022.

[10] L. B. Krithika, "Survey on the applications of blockchain in agriculture," *Agriculture*, vol. 12, no. 9, pp. 1333, 2022.

[11] P. Shanthi and K. Venkatesh, "An analysis of various techniques in blockchain applications," in *IEEE 6th Int. Conf. on Intelligent Computing and Control Systems (ICICCS)*, Madurai, India, pp. 857–860, 2022.

[12] P. Singh and N. Singh, "Blockchain with IoT and AI: A review of agriculture and healthcare," *International Journal of Applied Evolutionary Computation (IJAEC)*, vol. 11, no. 4, pp. 13–27, 2020.

[13] Y. P. Tsang, K. L. Choy, C. H. Wu, G. T. S. Ho and H. Y. Lam, "Blockchain-driven IoT for food traceability with an integrated consensus mechanism," *IEEE Access*, vol. 7, pp. 129000–129017, 2019.

[14] J. Lin, Z. Shen, A. Zhang and Y. Chai, "Blockchain and IoT based food traceability for smart agriculture," in *Proc. of the 3rd Int. Conf. on Crowd Science and Engineering*, Singapore, no. 3, pp. 1–6, 2018.

[15] C. Costa, F. Antonucci, F. Pallottino and J. Aguzzi, "A review on agri-food supply chain traceability by means of RFID technology," *Food and Bioprocess Technology*, vol. 6, no. 2, pp. 353–366, 2013.

[16] H. Feng, X. Wang, Y. Duan, J. Zhang and X. Zhang, "Applying blockchain technology to improve agri-food traceability: A review of development methods, benefits and challenges," *Journal of Cleaner Production*, vol. 260, no. 1, pp. 121031, 2020.

[17] Y. Zhang, W. Wang, L. Yan, B. Glamuzina and X. Zhang, "Development and evaluation of an intelligent traceability system for waterless live fish transportation," *Food control*, vol. 95, pp. 283–297, 2019.

[18] K. Demestichas, N. Peppes and T. Alexakis, "Blockchain in agriculture traceability systems: A review," *Applied Sciences*, vol. 10, no. 12, pp. 4113, 2020.

[19] O. Goldreich and Y. Oren, "Definitions and properties of zero-knowledge proof systems," *Journal of Cryptology*, vol. 7, no. 1, pp. 1–32, 1994.

[20] G. Kondova and J. Erbguth, "Self-sovereign identity on public blockchains and the GDPR," in *Proc. of the 35th Annual ACM Symp. on Applied Computing*, Brno, Czech Republic, pp. 342–345, 2020.

[21] M. Cash and M. Bassiouni, "Two-tier permission-ed and permission-less blockchain for secure data sharing," in *2018 IEEE Int. Conf. on Smart Cloud (Smart Cloud)*, New York, USA, pp. 138–144, 2018.

[22] W. Li, A. S. Forzin, S. Fedorov and G. O. Karame, "Towards scalable and private industrial blockchains," in *Proc. of the ACM Workshop on Blockchain, Cryptocurrencies and Contracts*, Abu Dhabi, United Arab Emirates, pp. 9–14, 2017.

[23] J. Hao, Y. Sun and H. Luo, "A safe and efficient storage scheme based on blockchain and IPFS for agricultural products tracking," *Journal of Computers*, vol. 29, no. 6, pp. 158–167, 2018.

[24] A. Stathopoulou and G. Balabanis, "The effects of loyalty programs on customer satisfaction, trust, and loyalty toward high-and low-end fashion retailers," *Journal of Business Research*, vol. 69, no. 12, pp. 5801–5808, 2016.

[25] J. Hao, Y. Sun and H. Luo, "A safe and efficient storage scheme based on blockchain and IPFS for agricultural products tracking," *Journal of Computers*, vol. 29, no. 6, pp. 158–167, 2018.

[26] S. Wang, X. Tang, Y. Zhang and J. Chen, "Auditable protocols for fair payment and physical asset delivery based on smart contracts," *IEEE Access*, vol. 7, pp. 109439–109453, 2019.

[27] S. Wang, Y. Zhang and Y. Zhang, "A blockchain-based framework for data sharing with fine-grained access control in decentralized storage systems," *IEEE Access*, vol. 6, pp. 38437–38450, 2018.

[28] Y. P. Tsang, K. L. Choy, C. H. Wu, G. T. S. Ho and H. Y. Lam, "Blockchain-driven IoT for food traceability with an integrated consensus mechanism," *IEEE Access*, vol. 7, pp. 129000–129017, 2019.

[29] K. Behnke and M. Janssen, "Boundary conditions for traceability in food supply chains using blockchain technology," *International Journal of Information Management*, vol. 52, no. 9, pp. 101969, 2020.

[30] Q. Lin, H. Wang, X. Pei and J. Wang, "Food safety traceability system based on blockchain and EPCIS," *IEEE Access*, vol. 7, pp. 20698–20707, 2019.