electronics

MDPI

Article

IoT-GChain: Internet of Things-Assisted Secure and Tractable Grain Supply Chain Framework Leveraging Blockchain

Karan Singh Thakur [1,†], Rohit Ahuja [1,†] and Raman Singh [2,*]

[1] Department of Computer Science & Engineering, Thapar Institute of Engineering & Technology, Patiala 147004, India; kthakur1_be20@thapar.edu (K.S.T.); rohit.ahuja@thapar.edu (R.A.)
[2] School of Computing, Engineering and Physical Sciences, University of the West of Scotland, Glasgow G72 0LH, UK
* Correspondence: raman.singh@uws.ac.uk
† These authors contributed equally to this work.

Abstract: The grain supply chain is crucial for any nation's self-sustainability due to its huge impact on food security, economic stability, and the livelihoods of several people. The path grain takes from farmers to consumers is opaque and complicated, due to which consumers cannot trust grain quality and its origin. Although blockchain is widely used for fair and secure transactions between farmers and buyers, issues related to transparency and traceability in the grain supply chain, such as counterfeiting and middlemen involvement, have not been adequately addressed. To tackle these issues, a blockchain-based solution is proposed that unites farmers, warehouses, government central and state agencies, transporters, and food corporations on a single platform to enhance transparency, traceability, and trust among all parties. This system involves minting a non-fungible token (NFT) corresponding to each lot of grain approved by government officials. The NFT comprises grain quality, type, temperature data from sensors, weight, and ownership information, which updates as the grain lot moves across the supply chain from central agencies to state agencies and so on. NFTs enable stakeholders to track the grain lot from cultivation to end-users, providing insights into grain conditions and quality. An Internet of Things-based circuit is designed using a Digital-output relative humidity & temperature (DHT22) sensor, which offers real-time temperature and humidity readings, and geolocation coordinates are gathered from the GPS module across the supply chain. Farmers can directly interact with warehouses to sell grains, eliminating the need for middlemen and fostering trust among all parties. The proposed four-tier framework is implemented and deployed on the Ethereum network, with smart contracts interacting with React-based web pages. Analysis and results of the proposed model illustrate that it is viable, secure, and superior to the existing grain supply chain system.

Keywords: blockchain; grain supply chain; Internet of Things; non-fungible tokens (NFTs)

check for updates

Citation: Thakur, K.S.; Ahuja, R.; Singh, R. IoT-GChain: Internet of Things-Assisted Secure and Tractable Grain Supply Chain Framework Leveraging Blockchain. *Electronics* **2024**, *13*, 3740. https://doi.org/10.3390/electronics13183740

Academic Editors: Tao Huang, Shihao Yan, Guanglin Zhang, Tsz Hon Yuen, YoHan Park, Jusak Jusak and Changhoon Lee

Received: 3 June 2024
Revised: 1 September 2024
Accepted: 4 September 2024
Published: 20 September 2024

Copyright: © 2024 by the authors. Licensee MDPI, Basel, Switzerland. This article is an open access article distributed under the terms and conditions of the Creative Commons Attribution (CC BY) license (https://creativecommons.org/licenses/by/4.0/).

1. Introduction

In developing countries, the agricultural sector is a primary source of livelihood for many citizens. For sustainable agriculture, high-quality grain is essential, as it significantly influences the effectiveness of other farming inputs. Estimates suggest that the direct contribution of high-quality grain to overall production ranges from 15% to 20%, depending on the crop, and can reach up to 45% with effective management of other inputs. In recent decades, the grain sector has seen substantial advancements [1]. Government bodies have restructured the grain industry to strengthen grain infrastructure. To remain competitive and contribute to national food and nutritional security, grain corporations need to transform their infrastructure, technologies, approach, and management culture in line with industry advancements. Producers procure grain and get it validated through government entities such as food corporations, which then store this grain in warehouses.

Farmers receive this grain based on demand. The food supply chain plays a crucial role in a country's economy and the sustainability of its agricultural sector. However, the exchange of goods within this supply chain is often marred by complex, opaque settlement processes, increasing the risk of fraud and the involvement of middlemen, which raises costs and complicates access to quality grain for farmers [2].

Existing grain supply chain solutions aim to enhance transparency between producers (farmers) and consumers. However, these solutions often overlook the specific challenges related to grain distribution, like grain condition across the chain, traceability of grains, continuous tracking, and accounting [3]. Furthermore, in existing grain chains, there is an intermediary who plays maliciously for illicit profit. Thus, there is a need for a grain distribution framework that enables farmers to track grain throughout the supply chain from producers and identify its sources.

Blockchain technology aims to revolutionize the existing public distribution system using a distributed and immutable ledger. Blockchain technology, along with non-fungible tokens (NFTs), enhances traceability, transparency, and accountability throughout the grain supply chain; the proposed scheme seeks to streamline operations, reduce fraud, and ensure the delivery of safe and high-quality grains to consumers. The primary objective is to create a decentralized and transparent grain supply chain system that addresses challenges such as counterfeiting, contamination, and lack of data sharing among stakeholders. The vision is to transform the current public distribution system into a technologically advanced ecosystem that ensures the availability of genuine and safe grains to every consumer. The proposed framework suggests a grain distribution system, i.e., with key entities, as discussed below:

1. Governing authority: As the central authority overseeing food distribution, it plays a pivotal role in the grain supply chain traceability system. It orchestrates the entire process by registering each level. It ensures adherence to regulations, assigns blockchain addresses, and manages permissions to ensure transparency and accountability in grain distribution.
2. Level 1 tier: This level collaborates closely with the governing authority to ensure effective implementation of the traceability process. It provides overarching guidance and regulatory framework and, through the governing authority, ensures that stakeholders are registered and operate within established protocols.
3. Level 2 tier: Level 2 works in tandem with the governing authority to ensure region-specific grain distribution. It facilitates the registration of level 2 and level 3 tiers within its jurisdictions, enhancing localized management and coordination.
4. Level 3 tier: Level 3, under the oversight of the governing authority, manages the distribution of grains within its respective sub-area. It is responsible for registering and supervising the level 4 tier, ensuring efficient and equitable access to essential commodities.
5. Level 4 tier: This level acts as the final point of contact with consumers. It provides grains to end-users, adhering to the regulations and maintaining grain quality and authenticity. Through the traceability system, the level 4 tier upholds the integrity of distributed grains.

Contributions of this article: The contributions of our proposed framework are discussed below:

- An Internet of Things-enabled circuit is designed to capture the real-time humidity and temperature of grain across the supply chain and continuously update it on blockchain so it can be monitored by all stakeholders.
- A non-fungible token-based system is created to verify grain quality and its ownership, which enhances the transparency of grains to consumers.
- We ensure grain traceability through each level using blockchain technology and an NFT-QR-based traceable mechanism for real-time monitoring and discrepancy detection.
- The proposed framework is implemented, Remix Ide is used for building smart contracts, and EtherScan is used for transaction monitoring.

- Security and threat analysis of smart contracts is conducted using the Solidity Scan tool.

2. Existing Systems

The existing grain supply chain in agriculture relies on minimal technology and predominantly manual record-keeping, making it susceptible to malpractices such as misrepresentation of product availability and black marketing of crucial and high-demand grains. This lack of transparency and traceability hinders the efficiency and integrity of the supply chain, ultimately impacting farmers, consumers, and the overall economy, as depicted in Figure 1. This situation allows for corruption in government-controlled product pricing, sales, and purchases due to the lack of transparency and efficient record-keeping [4,5]. In India, corruption at Food Corporation of India (FCI) warehouses is frequently reported. Officials often input incorrect information into government databases. For example, if a farmer purchases 150 kg of grain, FCI officials might record it as 225 kg sold. The remaining 75 kg is then back-channelled and sold later at inflated prices, creating an expensive market [6]. This corruption increases costs and makes it difficult for poor farmers to access good-quality grain, posing a significant issue at the initial stages of the food supply chain.

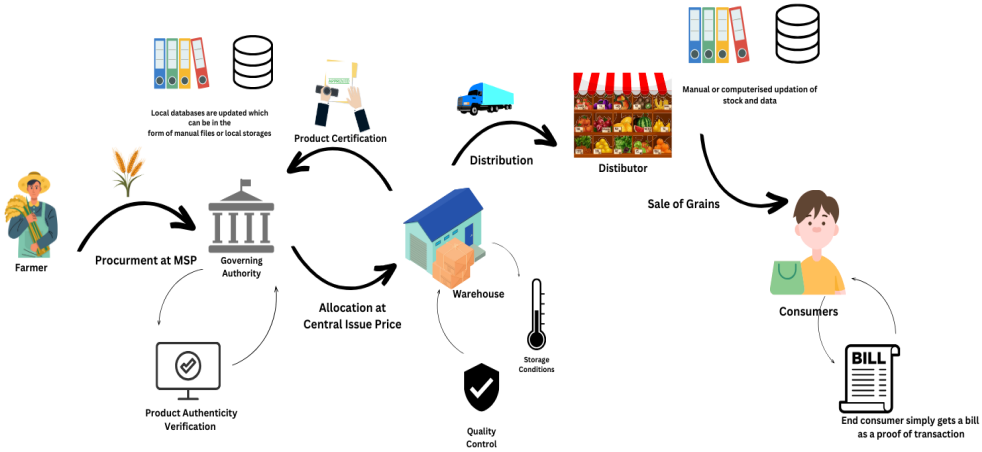

Figure 1. Existing grain distribution.

A detailed survey of the agri-food sector and a framework corresponding to the Vietnamese cashew nut business have been discussed to address such concerns [7–10]. In Iraqi agriculture, blockchain technology has been incorporated to tackle these issues by improving data management, accountability, and intelligent contracts, thus increasing productivity and competitiveness. Blockchain's efficiency and transparency make it a wise investment for Iraq's agricultural industry, with potential applications in precision agriculture, food supply chains, crop insurance, and agricultural product transactions.

A blockchain-based system called "AgriOnBlock" is designed to enhance transparency among various stakeholders, such as bankers, retailers, customers, farmers, and wholesalers [11]. It aims to handle industry-specific issues and connect stakeholders efficiently using Ethereum smart contracts and Internet of Things (IoT) devices. Additionally, a blockchain framework built on an IoT that incorporates artificial intelligence is intended to oversee and control smart water management. An IoT-based smart water irrigation system is recommended to address the water crisis efficiently, considering factors like fertilizer quality [12]. Most existing techniques focus primarily on food supply and food security, benefiting all stakeholders by increasing transparency and trust. However, grain, being a fundamental element in the farming sector, has not received sufficient attention, and its distribution suffers from the following issues:

1. Identification of beneficiaries: Governments or relevant authorities identify individuals or households eligible for subsidized food based on socio-economic indicators, income levels, or specific criteria.

2. Allocation of food resources: Governments allocate essential food resources, including grains like rice and wheat, to regions or states based on population size, socioeconomic factors, and nutritional needs. The quantity and types of allocated food resources may vary to align with regional preferences and dietary requirements.
3. Distribution points: Authorized distribution points, which may include government-operated stores, local markets, or community centers, facilitate the distribution of subsidized food items.
4. Distribution process: Beneficiaries visit designated distribution points to collect their allocated food resources. Transactions may involve manual or digital record-keeping, depending on the technological infrastructure of the region.
5. Monitoring and evaluation: Governments and relevant agencies monitor the distribution process to ensure fair and effective delivery of food resources to beneficiaries. Regular evaluations may be conducted to assess the performance of the distribution system and identify opportunities for improvement.

The existing public distribution system faces challenges such as leakages, corruption, and inefficiencies. There have been instances of grains not reaching the intended beneficiaries, leading to concerns about the system's effectiveness.

Limitations of Existing Systems

Before delving into the reasons for employing blockchain technology in grain supply chain management, it is essential to understand the limitations of previous systems. These traditional systems, which often rely on centralized databases and manual processes, are fraught with several challenges that hinder the effective management of grain distribution. Below are some generic limitations that transcend geographical boundaries and apply to grain supply chains worldwide:

1. Lack of traceability: Traditional systems often lack robust mechanisms for tracing the journey of grains from farm to fork. This absence of traceability makes it difficult to identify the origin of grains, track their movement through the supply chain, or ascertain their quality and safety status accurately.
2. Limited transparency: Centralized systems typically offer limited transparency regarding grain transactions and movement. Stakeholders may not have access to real-time information about inventory levels, pricing, or quality checks, leading to opacity in the supply chain and potential opportunities for fraud or malpractice.
3. Vulnerability to fraud and counterfeiting: Manual record-keeping and paper-based documentation systems are susceptible to errors, tampering, and fraudulent activities. Without robust authentication mechanisms, such as digital signatures or unique identifiers, there is a heightened risk of counterfeit products entering the supply chain, compromising food safety and integrity.
4. Inefficiencies in record-keeping: Paperwork-intensive processes are inherently inefficient and prone to delays, inaccuracies, and data discrepancies. Manual record-keeping not only consumes time and resources but also increases the likelihood of human errors, leading to inefficiencies in inventory management, order processing, and regulatory compliance.
5. Limited accountability and compliance: Traditional systems may lack mechanisms to hold stakeholders accountable for their actions or ensure compliance with regulatory standards and industry best practices. Without transparent audit trails or mechanisms for verifying the authenticity of data, it becomes challenging to enforce accountability or address non-compliance issues effectively.
6. Fragmented information silos: Grain supply chains often involve multiple stakeholders, including farmers, distributors, retailers, and regulatory authorities. In traditional systems, information may be siloed within individual organizations or departments, leading to fragmentation and duplication of efforts. This lack of data interoperability and collaboration impedes the seamless flow of information across the supply chain, hindering decision-making and coordination efforts.

7. Susceptibility to contamination and quality issues: Inadequate monitoring and oversight in traditional systems can exacerbate the risk of grain contamination or quality degradation during storage, handling, or transportation. Without real-time visibility into environmental conditions or quality control measures, it is challenging to prevent or mitigate contamination incidents effectively.
8. High operational costs: The manual nature of traditional systems often results in high operational costs associated with labor, paperwork, and administrative overheads. Moreover, inefficiencies in inventory management, order fulfilment, and compliance management can further inflate operational expenses, reducing profitability and competitiveness in the market.

Addressing these limitations requires a paradigm shift towards more transparent, efficient, and secure approaches to grain supply chain management. Blockchain technology offers a promising solution to overcome these challenges by providing a decentralized, transparent, and tamper-resistant platform for tracking and tracing grain transactions throughout the supply chain.

3. Preliminaries

This section discusses blockchain technology, smart contracts, and the various types of blockchain solutions, which are essential for grasping the effectiveness of the proposed scheme.

3.1. Blockchain

Traditional systems are primarily based on the client–server architecture and centralized database. Blockchain is a decentralised ledger with a peer-to-peer system of networks. It is a cryptographically secure, immutable, append-only ledger, which can replace the current system [13,14]. Blockchain comprises blocks that are append-only, and a particular block may store data such as a list of transactions, as depicted in Figure 2. Next, a block is attached to the pertaining block, forming a chain, giving it the name blockchain. Each block except the first block, called the genesis block, stores a hash of the previous and next block, which is a cryptographic code. The hash must match in order to form a link between blocks. If anything in the block is changed, the hash is updated to a new value, thus breaking the link and the chain. The blockchain is a decentralized network and works on a mutual consensus paradigm to make any change. The consensus algorithms verify and authenticate the transactions so the public ledgers remain in harmony and ensure only valid transactions are further added to the blockchain. Proof of work [15,16] is the most widespread consensus algorithm today, which requires the exertion of the computational power of a node to solve an arbitrary puzzle to validate transactions.

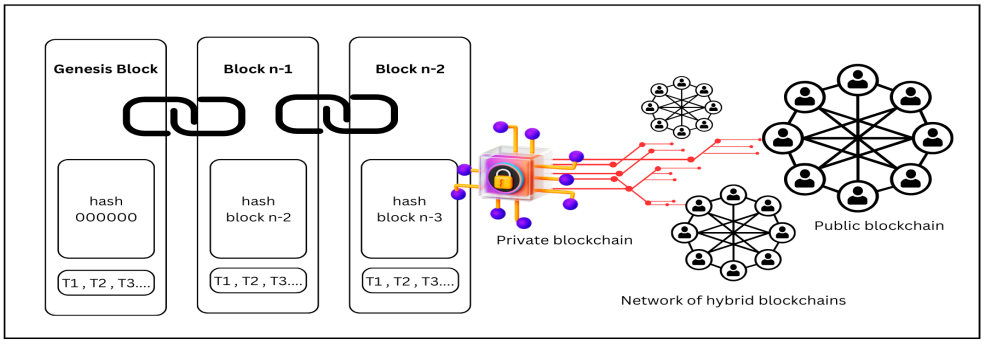

Figure 2. Blockchain.

The data stored in a blockchain are considered practically unalterable because if a single block needs to be altered, the whole network needs to consent to the change, and that would require computation power greater than the whole network combined. This renders the human intervention aspect of tampering entries moot and makes blockchain

a plus point over the centralized system where a hack may be possible and thus lead to tampered data [17].

3.2. Smart Contracts

A smart contract is a programme/script that is triggered to execute on a blockchain whenever a specified condition is met, as depicted in Figure 3. It uses blockchain technology to verify, validate, capture, and enforce agreed-upon terms between multiple parties. In addition, it allows transactions and agreements to be carried out among anonymous parties without the need for a central entity, external enforcement, or legal system. Smart contracts define rules as well as enforce them automatically [13]. The user interacts with the contract, and each interaction is a transaction, which incurs some transactional cost called gas fees to record the transaction on the blockchain. This enables the secure, instantaneous, and efficient transfer of land titles. This also ensures trust that the ownership is immune to external factors and is conclusive in nature.

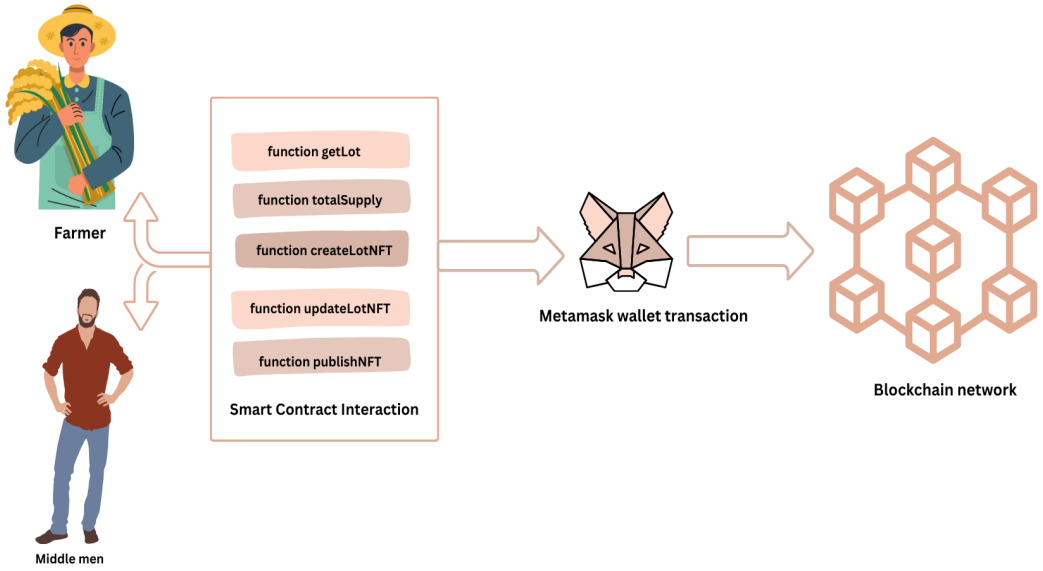

Figure 3. Smart contract.

3.3. Types of Blockchain-Based Solutions

A decentralized app that uses technologies like blockchain and smart contracts can be a viable solution for a new land registration system [14]. There are four primary types of blockchain solutions that can be employed:

1. Public blockchain: A public blockchain is an open network that allows anyone to set up a node for the blockchain. There is no restriction on joining the blockchain, and every transaction is visible on the ledger (the users are anonymous), thus making it transparent. It is decentralized and easy to set up [18]. An Ethereum blockchain is a commonly used public blockchain. Currently, the Ethereum blockchain is the most prevalent and established smart contract provider. It uses the Ether cryptocurrency *ETH* and works on the proof of stake consensus mechanism. Every time a transaction occurs, a reward (in terms of Ether) is given to the validator of the transaction. This provides an incentive for people to set up nodes and has greatly increased outreach. Public blockchains are easy to set up and open for all, due to which they are difficult to regulate and often slower.
2. Private blockchain: A private blockchain can be considered a blockchain network that is owned by a particular entity or authority and is directly managed by it. It can be considered a special type of private networking solution that is decentralized [14]. A private blockchain network requires an invitation and must be validated by either the network starter or by a set of rules by the network starter. It is not fully transparent,

as only the nodes on the network may view the transactions, and it is not open to everyone. The managing authority may perform relevant changes, albeit not that easily. This can be considered a partially decentralized system.
Several companies offer private blockchain solutions to make businesses more secure. Private blockchains usually require low costs to set up and are more efficient due to less network congestion. A private blockchain is easier to manage but may not necessarily be immutable, as the whole network may be updated, which may be possible depending on the size of the network and is an inescapable drawback to private blockchains. The issuing authority has to ensure trust; thus, it makes it similar to traditional centralized systems but with distributed nodes acting as servers.

3. Hybrid blockchain: This blockchain aims to combine both public and private blockchains by offering a solution that is open for all but reserves some permissions and activities for a selected group of nodes in the network. This is made possible by using a permission-based system within the permission-less system of a public blockchain. This may largely help to reduce fraud, as only verified users may be allowed to use the blockchain. This makes it a permissioned blockchain, which is also open to the public, ensuring better decentralization of the system.
4. Consortium blockchain: Consortium and hybrid blockchains are similar as they both have a public and private blockchain component. The difference lies in the structure of the organization's management of the permissioned part. For a consortium blockchain, multiple entities govern the platform. The entities also define the roles of nodes and the permissions granted to each.

4. The Proposed Framework

The proposed framework integrates various steps, utilizing blockchain technology, Firebase, and additional components to establish transparency and traceability within the public distribution system for grains [19–21]. The framework involves the collection of real-time sensor data, including temperature, humidity, and geolocation coordinates, which are stored in the Firebase real-time database for immediate accessibility. The Firebase integration acts as a dynamic link between sensor inputs and the web application, ensuring instantaneous reflection of any changes. The blockchain interaction encompasses the creation of non-fungible tokens (NFTs) for grain lots and updating and transferring ownership through transactions on the Sepolia blockchain. IPFS integration further contributes to the decentralized and tamper-resistant storage of NFT metadata. The web application serves as the user interface, featuring a dashboard with a QR code scanner, status log, location map, and quality log for stakeholders to retrieve detailed information about grain lots and enhance traceability. Quality verification involves a check on the grain's temperature against defined thresholds, with results displayed in the quality log. User interaction is facilitated through MetaMask integration, offering features like the connect button, notification icon, dark mode, and profile icon for a seamless and secure experience. Continuous monitoring ensures system health, detects anomalies, and plans regular updates based on user feedback, technological advancements, and industry standards. The procedural workflow, depicted in Figure 4, underscores the seamless integration of sensor data, blockchain technology, IPFS, and Firebase, contributing to the proposed scheme's overarching goals of improving traceability [22], accountability, and real-time monitoring in the grain supply chain.

The implementation of non-fungible tokens (NFTs) within the proposed scheme is designed to facilitate comprehensive traceability of grains, offering intricate insights into the origin, transportation, and handling of each grain lot. The decentralized nature of the blockchain technology employed ensures a transparent environment, granting stakeholders real-time access to critical information regarding the state, location, and condition of both grain lots and orders. The permanence of data recorded on the blockchain guarantees integrity, as it cannot be altered or deleted, thereby ensuring the accuracy and reliability of information across the entire supply chain. Leveraging NFTs and smart contracts, the

proposed scheme establishes a robust system of accountability by meticulously recording interactions and actions taken by each stakeholder. This not only encourages responsible behavior but also significantly reduces the potential for fraudulent activities. The incorporation of smart contracts introduces automation to streamline processes, eliminating manual paperwork and reducing administrative overhead, ultimately leading to enhanced operational efficiency. As a result, the optimized processes, coupled with the reduction in fraudulent activities, are anticipated to contribute substantially to cost savings within the grain supply chain.

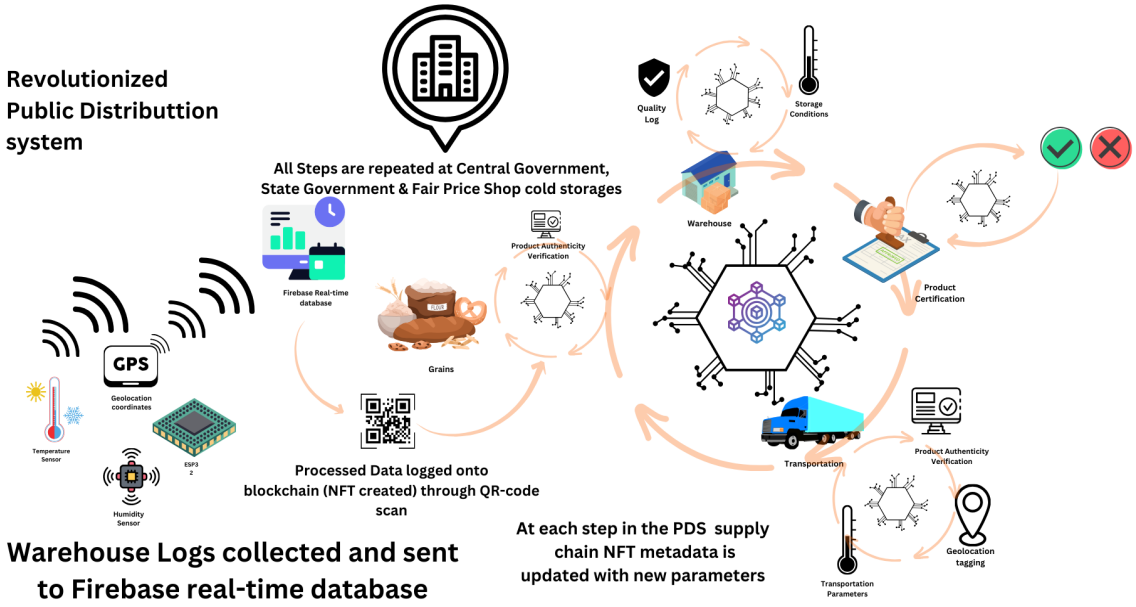

Figure 4. Proposed framework.

Farmer registration and verification: To register and verify a farmer based on their public Ethereum address, Algorithm 1 is employed.

Algorithm 1 Farmer registration and verification

Input: Farmer's Ethereum address F_{Addr}.
Output: Farmer successfully registered and verified.

$F_{Addr} \xleftarrow{Input} (Farmer)$
if $(\exists F_{Addr} == 0)$ **then**
  $F_{Details} \xleftarrow{Extract} getDetailsFromBlockchain(F_{Addr})$
  $F_{Verified} \xleftarrow{Verify} verifyDetails(F_{Details})$
  if $(F_{Verified} == 1)$ **then**
    $F_{Reg} \leftarrow registerFarmer(F_{Details})$
    if $(F_{Reg} == 1)$ **then**
      return Farmer successfully registered and verified
    else
      return Farmer registration failed
    end if
  else
    return Farmer details verification failed
  end if
else
  return Farmer already registered
end if

Mint NFT for grain sack: To mint an NFT corresponding to a grain sack, Algorithm 2 is employed. The grain type is taken as input, i.e., G_{type} and G_Q grain quality, the weight of the grain sack G_{w_S}, its location $G_{S_loc} : (G_{S_latitute}, G_{S_longitude})$, the grain sack temperature, and its humidity G_{S_teamp} and G_{S_humid}.

Algorithm 2 Mint NFT of grain sack G_{Sack}

Input: G_{type}, G_Q, G_{w_S}, G_{S_loc}, G_{S_temp}, G_{S_humid}
Output: NFT $\mathbb{N}$ for G_{Sack}

$FCI \xleftarrow[Submitted]{G_{type}, G_Q, G_{w_S}, G_{S_loc}, G_{S_temp}, G_{S_humid}} G_{Sack}$
if $(G_{Sack}(Source) == 1)$ **then**
  $G_{Sack} \cdot append(Id) \leftarrow tokenIdCounter$
  $G_{Sack} \cdot append(Manuf) \leftarrow msg.sender$
  $G_{Sack} \cdot append(Ts) \leftarrow timestamp$
  $G_{Sack} \cdot append(state) \xleftarrow{Input} State : State \in \{Central, District, Retail\}$
  $\mathbb{N} \xleftarrow[mint()]{G_{type}, G_Q, G_{w_S}, G_{S_loc}, G_{S_temp}, G_{S_humid}, G_{Sack.Id}, G_{Sack.Manu}, G_{Sack.Ts}, G_{Sack.state}} G_{Sack}$
  $\mathbb{N}$ created successfully
  $tokenCounter++$
else $\mathbb{N}$ creation aborted
end if

Grain sack NFT update: To update G_{Sack} NFT, Algorithm 3 is employed. This algorithm updates the information associated with G_{Sack}, including the grain description $G^{new}_{S_loc}$, $G^{new}_{W_S}$, $G^{new}_{S_temp}$, $G^{new}_{S_humid}$, and grain quality $G^{new}_{S_Q}$.

Algorithm 3 Grain sack NFT update

Input: $G_{Sack.Id}$, $G^{new}_{S_Q}$, $G^{new}_{S_loc}$, $G^{new}_{S_temp}$, $G^{new}_{S_humid}$, $G^{new}_{S_Q}$
Output: Returns true if update is successful.

$G_{Sack}[] \leftarrow G_{Sack.Id} : \forall Id \in \{1, ..., n\}$
for i $\in G_{Sack}[]$ **do**
  $W_{prev} \leftarrow G_{Sack}[i].weight$
  $G_Q \leftarrow G_{Sack}[i].Quality$
  $G_{Sack}\left(\text{push}\left(G^{new}_{S_loc}, G^{new}_{W_S}, G^{new}_{S_temp}, G^{new}_{S_humid}, G^{new}_{S_Q}\right)\right)$
  $\triangle \text{T} = \left(G^{new}_{S_temp} - G_{S_temp}[i]\right)$
  if $\left(\triangle T <= \delta\right)$ **then** ▷ $\triangle$T is change in temperature, δ is threshold
    if $(W_{prev} == G^{new}_{W_S}[i])$ **then**
      $\mathbb{N}$ updated successfully
    end if
  end if
end for
Generate signal for G_{Sack} tampering

Buying grains: Algorithm 4 is employed to buy grains. This algorithm handles updating all necessary data structures and ensures the proper handling of transactions, as depicted in Figure 5.

Algorithm 4 Buying grains

Input: Grain Sack Id $G_{Sack.Id}$ and buyer address B_{Addr}.
Output: Grain purchased successfully.

$G_{Sack}[] \leftarrow G_{Sack.Id} : \forall Id \in \{1, \ldots, p\}$
for i $\in G_{Sack}[]$ **do**
  if $(\exists\ G_{Sack}[i])$ **then**
    if (Authenticate(Buyer)==1) **then** ▷ Change State and Ownership Status
      $G_{Sack}\Big(\text{push}\Big(\ G_{Sack_Id}\ \cdot\ (State = Sold), G_{Sack_Id} \cdot (Ownership = B_{Addr})\Big)\Big)$
      Transaction T_{Id} ▷ Update Weight Changes
      Emit event for a successful purchase
      $G_{Sack_Id}\Big(\text{push}\Big(G_{W_S_Id} = G_{W_S_Id} - G_{Sack_Id} \cdot (\text{W}(\text{B}_{Addr}))\Big)\Big)$
    else
      Authentication fails
    end if
  else
    $G_{Sack}[i]$ is sold
  end if
  Required grain does not exist
end for

The proposed system is depicted in Figure 4, and the flow between all the discussed algorithms is depicted in Figure 6.

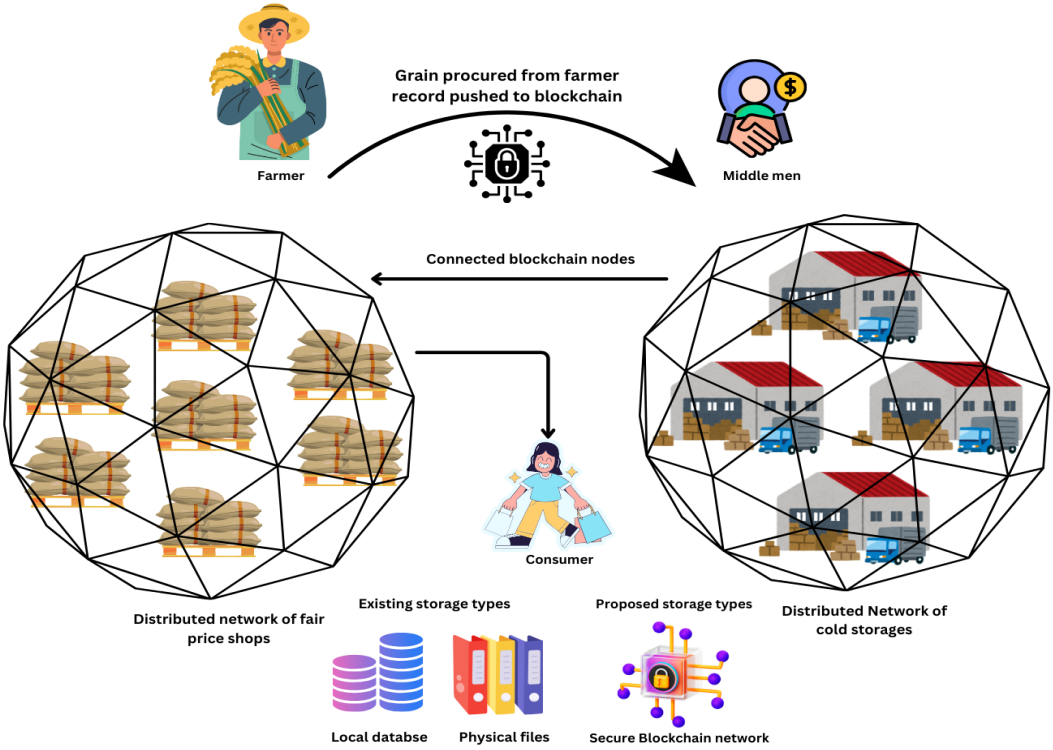

Figure 5. Blockchain nodes interaction.

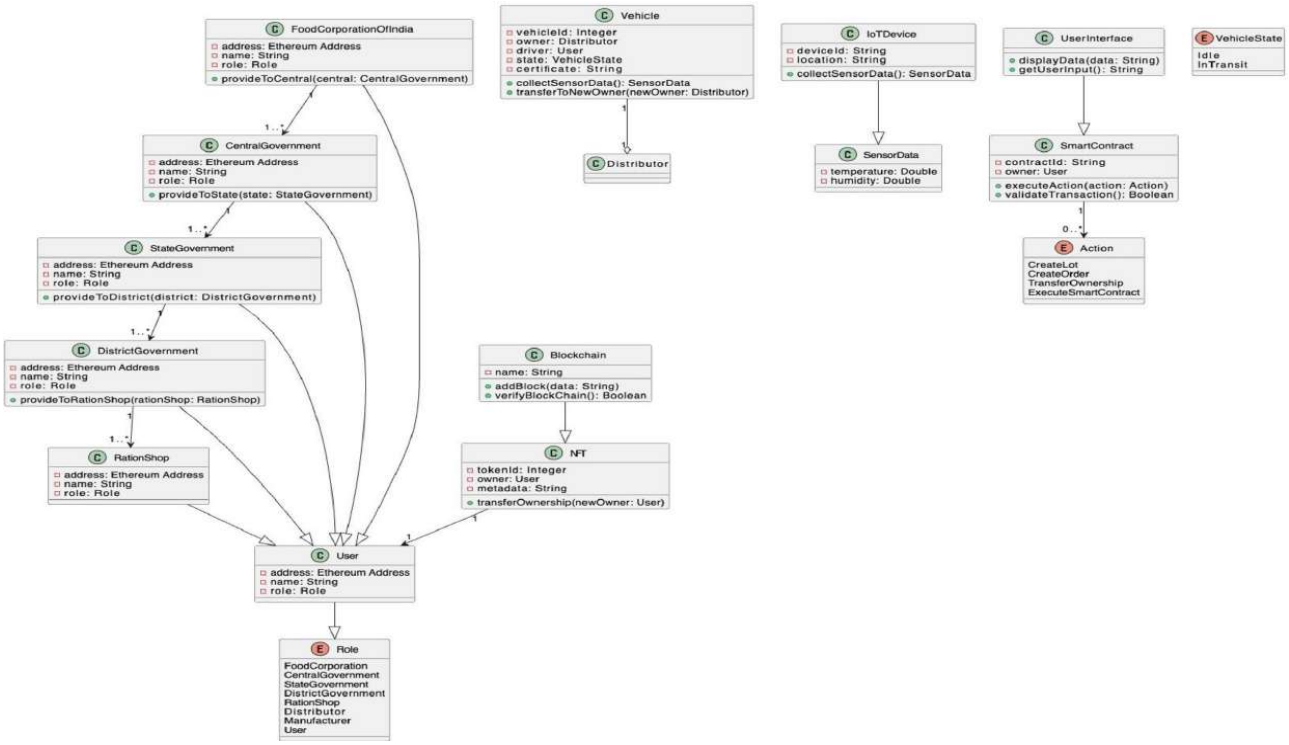

Figure 6. Algorithm flow.

5. Implementation

This section discusses the experimental setup, architecture, and smart contract design employed in the proposed scheme, as well as the integration and feature analysis utilized.

5.1. Experimental Setup

This subsection describes the tools and technology utilized in the implementation of our proposed architecture.

5.1.1. InterPlanetary File System (IPFS)

IPFS will be used to securely store sensitive data off-chain. It provides decentralized, distributed, and verifiable storage, with only the hash values stored on the blockchain.

5.1.2. Remix IDE

The development and initial testing of the smart contract were conducted using Remix IDE, a powerful web-based integrated development environment tailored toward Solidity smart contracts. Remix IDE offers a range of features that streamline the process of writing, debugging, and deploying smart contracts.

5.1.3. EtherScan for Transaction Monitoring

EtherScan is employed to monitor and verify transactions of smart contract "GrainChain". EtherScan is a widely used block explorer for the Ethereum blockchain, providing detailed information on transactions, blocks, addresses, and smart contracts. Monitoring through EtherScan comprises of the following steps:

1. Contract deployment: After deploying the 'GrainChain' smart contract to the Ethereum testnet, the contract address is obtained and entered into EtherScan.
2. Transaction tracking: EtherScan is used to monitor all transactions related to the smart contract, including NFT creation, state updates, and event emissions.

3. Verification: The details of each transaction are verified on EtherScan to ensure that the contract functions behaves as expected and that state changes are accurately recorded on the blockchain.
4. Event logs: EtherScan provides access to event logs, which are crucial for tracking the 'NFTCreated' event and other significant state changes within the contract.

5.1.4. SolidityScan

SolidityScan is employed to ensure the security and reliability of the 'GrainChain' smart contract, which is a cloud-based smart contract vulnerability scanner [23]. SolidityScan is designed to uncover potential vulnerabilities and anti-patterns in smart contract code. It integrates seamlessly into the development pipeline, scanning the contract's code and flagging known vulnerabilities. SolidityScan generates a detailed audit report that highlights which parts of the code might pose security risks. The process of SolidityScan is defined below:

1. Code upload: The 'GrainChain' smart contract code is uploaded to SolidityScan's cloud-based platform.
2. Automated scanning: SolidityScan performs a comprehensive scan of the code, using both automated detection methods and predefined rules for identifying vulnerabilities.
3. Report generation: The scanner generates a detailed audit report outlining the identified issues, their severities, and recommendations for remediation.

Here, the SolidityScan tool provided a security score of 84.56 and a threat score of 87.50, based on the lines of code and the severity of detected issues.

5.2. Architecture of the Proposed Scheme

Figure 7 depicts the architecture of the proposed system. A blockchain-based grain chain management solution can be designed using a layered architecture that incorporates various components to ensure transparency, security, and efficiency [24]. The following is an overview of the architecture for a blockchain-based grain chain solution:

1. Data collection: Information on grain transactions can be held at this state, i.e., warehouse logs, a description of the grain, data from its sensors, temperature and humidity from the DHT22 sensor, geolocation coordinates from the GPS module, grain lot, among others, as depicted in Figure 8. This phase uses distributed ledger technology to safeguard information in a decentralized manner, thus ensuring transparency and security.
2. Smart contract: Next, intelligent contracts are used to facilitate the various transactions in the grain chain. Smart contracts refer to self-executing contracts in which the agreement terms between two parties are directly written into the software. For example, in the grain chain, smart contracts are used to automate the transfer of ownership of a grain lot from the level 1 to level 2 tier.
3. Consensus mechanism: Afterwards, a consensus mechanism between the nodes of the network is employed. Consensus is vital to ensure all network nodes agree on the state of the blockchain. This layer might be materialized with a consensus algorithm, such as proof-of-work or proof-of-stake.
4. User interaction: The Farmer/retailer/agency interacts with the blockchain environment at this stage, along with the user interface. For instance, the applications could be a create lot portal, a transfer lot portal, an update lot portal, and a sell portal. It uses RESTful APIs to interact with the blockchain.

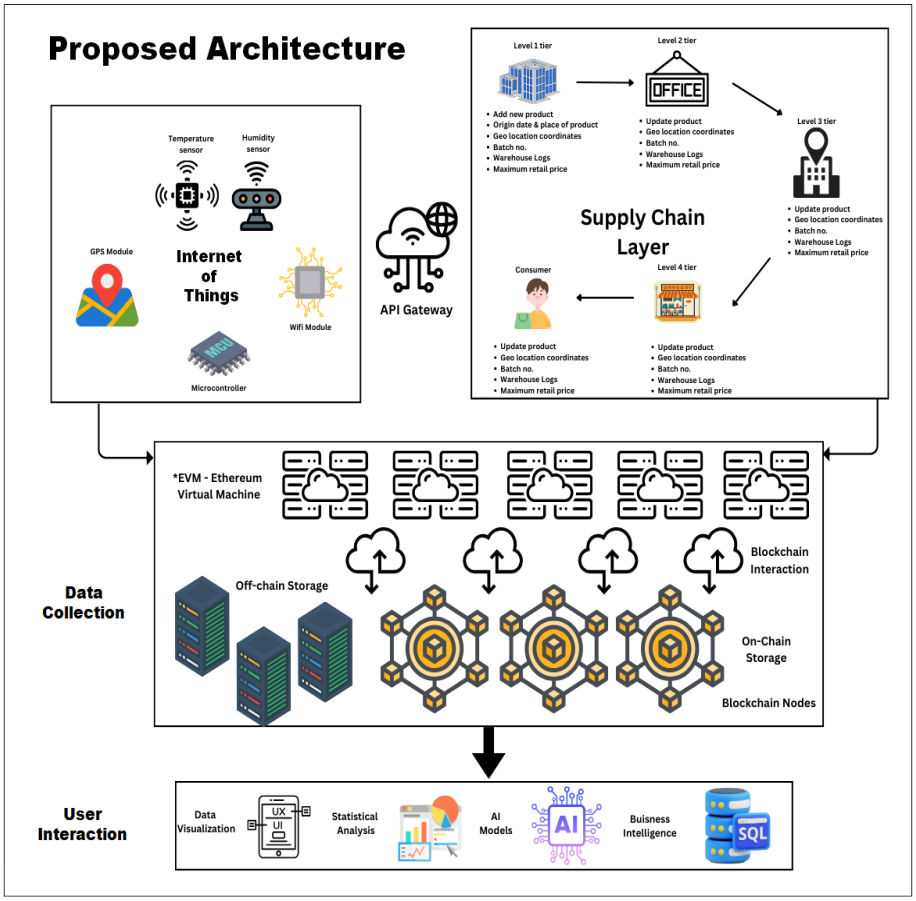

Figure 7. Proposed architecture.

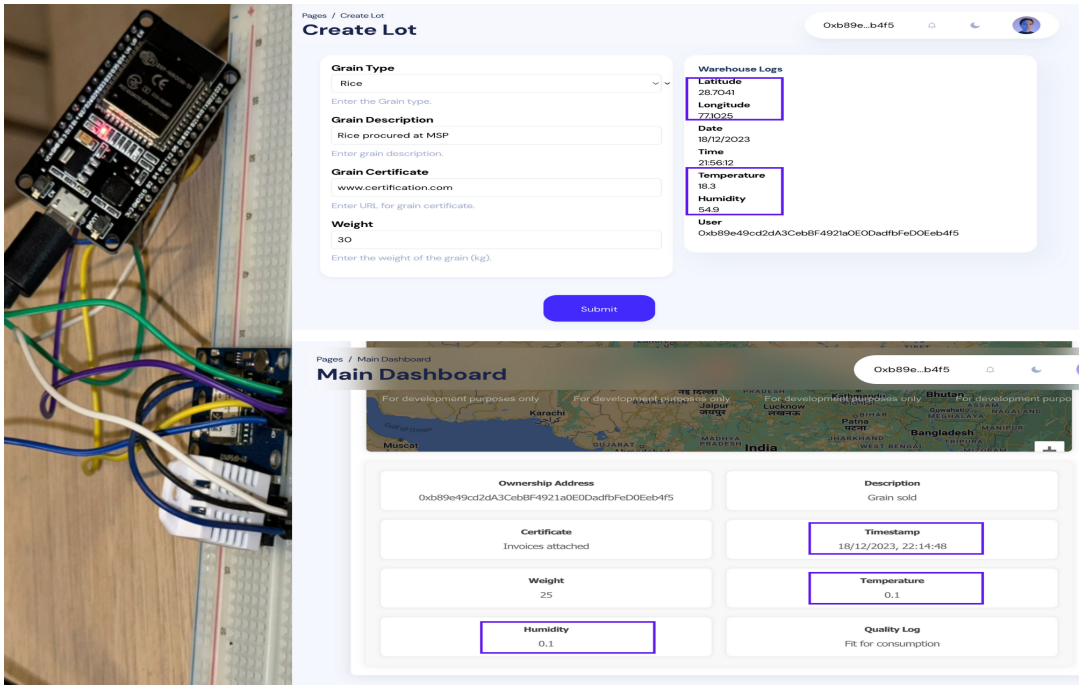

Figure 8. Temperature monitoring using sensors.

5.3. Designing the Smart Contract

The smart contract provided outlines the functionality of a decentralized grain supply chain tracking system using blockchain and non-fungible tokens (NFTs). Let us delve into the design aspects of this contract:

1. Inheritance and Imports
   - The contract is inherited from ERC-721 URIStorage, which is part of the OpenZeppelin library for ERC-721 token standards [18]
   - It also implements the ERC-721 Supply interface, indicating that it adheres to the ERC-721 token standard with additional supply-related functions.
2. State Variables
   - 'tokenIdCounter' tracks the unique identifier for each NFT token.
   - 'allLots' uses mapping to store information about each grain lot, indexed by their token IDs.
   - 'ownerOfToken' uses mapping to track the owner of each token.
3. Structs
   - Locate represents the geographical location with latitude and longitude coordinates.
   - State defines the state of a grain lot, including ownership, description, timestamp, weight, certificate URL, temperature, humidity, location, and exceeded temperature.
4. Constructor
   - The initializes the contract with the name "GrainNFT" and symbol "GNFT" upon deployment.
5. Functions:
   - 'getLot' retrieves information about a specific grain lot based on its token ID.
   - 'totalSupply' returns the total number of NFT tokens minted.
   - 'createLotNFT' creates a new grain lot NFT, mints it to the caller, and stores relevant information about the lot.
   - 'updateLotNFT' updates information about an existing grain lot based on its token ID.
   - 'publishNFT' sets the token URI for a specific NFT, essentially linking it to off-chain metadata such as descriptions or images.
6. Helper Function
   - 'uintToString' converts a uint256 value to its string representation.
7. Design Considerations
   - Efficiency: The contract design appears efficient, with minimal gas usage for common operations like creating and updating grain lots.
   - Security: The contract should be audited for potential vulnerabilities, especially regarding access control and input validation to prevent unauthorized operations or data manipulation.
   - Scalability: While the current design can handle a moderate number of grain lots, considerations for scaling, such as gas optimization and data storage efficiency, should be taken into account for large-scale adoption.
   - Interoperability: The contract should conform to relevant standards like ERC721 to ensure compatibility with existing NFT marketplaces and infrastructure.
   - User Experience: User interaction with the contract should be intuitive and well-documented to facilitate adoption by stakeholders in the grain supply chain.

By addressing these design considerations, the smart contract can serve as a robust foundation for implementing a decentralized grain supply chain tracking system, leveraging blockchain and NFTs to enhance transparency, traceability, and efficiency in grain distribution.

5.4. Integration

Integrating the smart contract with a MetaMask wallet and deploying it on the Ethereum Sepolia test chain enables users to interact with the grain supply chain tracking system in a decentralized manner. Here is how the integration process would typically unfold, along with minting procedures:

1. Setting up MetaMask
    - Users install the MetaMask browser extension or mobile app and create or import their Ethereum wallet.
    - They connect MetaMask to the Sepolia test network to interact with smart contracts deployed on this test chain.
2. Deploying the Smart Contract
    - The developer compiles the smart contract code using a Solidity compiler like Remix or Truffle.
    - Using MetaMask version 11.0.0 the developer selects the Sepolia test network and deploys the compiled contract to this network.
    - Upon deployment, MetaMask prompts the developer to confirm the transaction and pay the gas fee using test Ether (ETH) from their MetaMask wallet.
3. Interacting with the Contract
    - After deployment, users can interact with the smart contract through a decentralized application (dApp) interface connected to MetaMask.
    - They can view existing grain lots, create new grain lots, update information about existing lots, and perform other permitted actions defined by the contract's functions.
4. Minting Procedures
    - To mint a new grain lot NFT, users initiate the minting process through the dApp interface.
    - They specify details such as grain type, description, weight, certificate URL, location coordinates, temperature, humidity, and any other relevant information required by the contract.
    - Upon confirmation, MetaMask prompts the user to sign the transaction and pay the gas fee for minting the NFT.
    - Once the transaction is confirmed and included in a block on the Sepolia test chain, the new grain lot NFT is minted, and its details are recorded on the blockchain.
5. Transaction Confirmation
    - Users can monitor the status of their transactions on MetaMask, which provides real-time updates on transaction confirmations, gas fees, and network activity.
    - Once the transaction is confirmed, users can view the newly minted grain lot NFT in their MetaMask wallet or explore its details through the dApp interface.
6. Testing and Debugging
    - Developers and users can test the functionality of the smart contract on the Sepolia test chain without incurring any actual Ether transactions or gas fees.
    - They can simulate various scenarios, such as creating multiple grain lots, updating information, and transferring ownership, to ensure the contract behaves as expected.

By integrating the smart contract with the MetaMask wallet and deploying it on the Ethereum Sepolia test chain, users can seamlessly interact with the grain supply chain tracking system, mint new grain lot NFTs, and contribute to the development and testing of decentralized applications for enhancing transparency and traceability in grain distribution. Figure 9 depicts the gas fees used for our implementation.

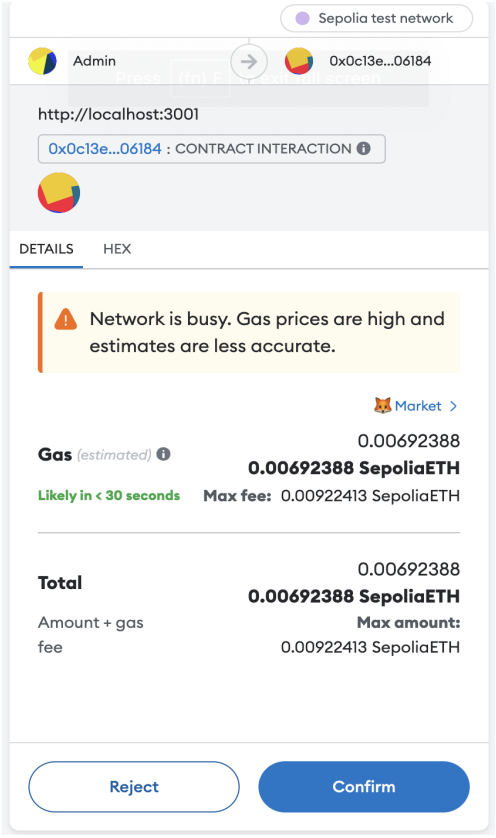

Figure 9. Example of gas fees paid.

5.5. Feature Analysis

1. Decentralization: We have created a system that significantly enhances transparency and decentralization compared to conventional practices. This decentralization not only provides clarity for end-users but also streamlines processing tasks during the product's production life cycle.
2. Reliable metadata handling: The proposed scheme has effectively published NFT metadata on IPFS and retrieved grain status information, showcasing its robust integration into the InterPlanetary File System (IPFS). The system's ability to store and retrieve decentralized and tamper-resistant metadata on IPFS has been validated.
3. Accurate real-time data handling: The logging and real-time exchange of sensor data with Firebase have been thoroughly tested and proven accurate. This ensures that the system precisely captures sensor inputs and updates the Firebase real-time database, establishing a reliable mechanism for data collection. This is critical for maintaining transparency and traceability in the grain distribution process.
4. Efficient grain status retrieval: The get lot function, designed to retrieve grain status information based on the grain ID, has successfully returned the expected grain info object. This functionality demonstrates the system's precision in retrieving and presenting detailed information about specific grain lots, contributing significantly to transparency and traceability.
5. User-friendly transaction facilitation: The generation of QR-CODEs during lot NFT creation has passed testing, highlighting the user-friendly nature of the system. The successful generation of QR codes is crucial for facilitating seamless transactions and interactions within the platform, ultimately enhancing the overall user experience.

5.6. Security and Threat Analysis

The "GrainChain" smart contract is designed to create and manage NFTs representing lots of grain. Each lot tracks various states, including ownership, description, timestamp,

weight, certificate, temperature, humidity, location, and exceeded temperature. This subsection presents an in-depth analysis of the security aspects of the contract, highlighting identified issues, explaining the security and threat scores, and recommending improvements as depicted in Figure 10.

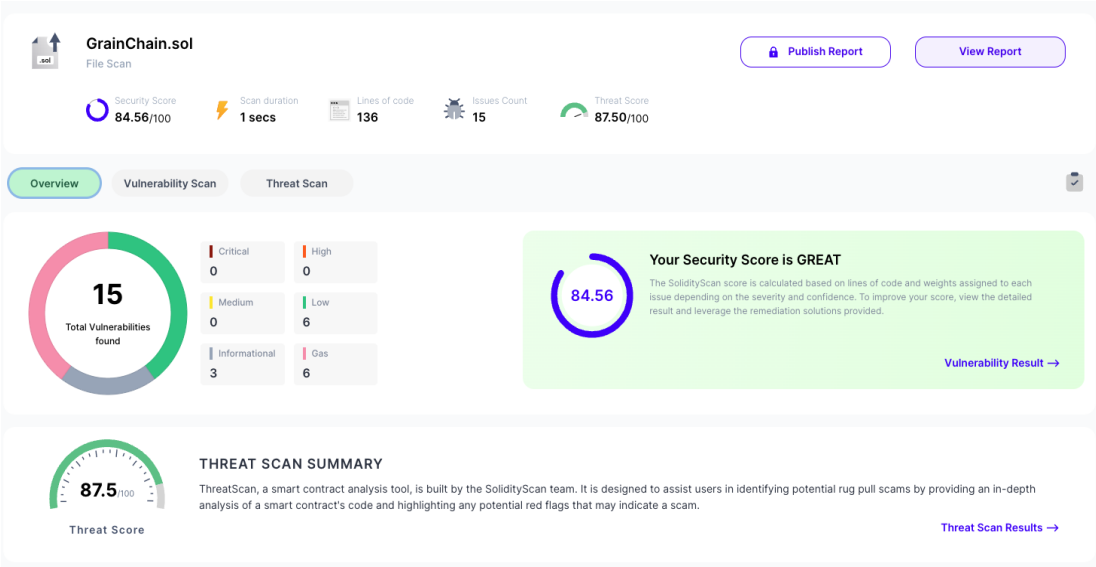

Figure 10. SolidityScan security analysis.

5.6.1. Security and Threat Scores Explanation

The security score is calculated based on the lines of code and the weights assigned to each issue depending on the severity and confidence of detection. The score reflects the overall security posture of the contract, with a higher score indicating fewer and less severe issues. In this case, a score of 84.56 suggests that the contract is generally secure but has some areas for improvement.

1. Lines of code (136): A relatively moderate codebase size, which typically helps in maintaining readability and manageability.
2. Issues count (15): The number of identified issues impacts the score, with each issue's severity contributing to the overall reduction of the score.
3. Severity and confidence: Issues with higher severity and detection confidence weigh more heavily against the security score.

5.6.2. Threat Score

The threat score is a measure of the potential risk posed by the identified issues. A higher threat score indicates a greater risk, taking into account the likelihood and impact of potential vulnerabilities being exploited. The score of 87.50 suggests a significant level of risk, warranting attention to the highlighted issues to mitigate potential threats.

6. Conclusions and Future Work

In conclusion, the proposed scheme demonstrates the transformational potential of integrating blockchain technology with IoT sensors to revolutionize grain supply chain operations. Milestones have presented significant improvements toward attaining more transparency, traceability, and security of the grain supply chain. The evidence of the scheme's viability can create additional value for stakeholders regarding the state of grain; the proposed solution will not only motivate but emphasize an essential contribution of such solutions in industry problem-solving areas. Thus, a blockchain-based grain chain management solution is envisaged with an architectural style that uses a layered approach that includes data storage, execution of smart contracts, consensus algorithms, development of user interface, and integration of the system. The architecture can ensure

transparency, security, and efficiency in supply chain transactions. Such conclusive evidence places solutions based on blockchain in the category of a viable and impactful approach towards grain supply chain management with an enhancement of its overall effectiveness and reliability. The results add to this knowledge bank as it pertains to supporting the adoption of innovative technologies in a fluid and increasingly complex grain supply chain landscape.

Author Contributions: Conceptualization, R.A., K.S.T. and R.S.; methodology, K.S.T.; software, R.A.; validation, R.A. and R.S.; formal analysis, R.A., K.S.T. and R.S.; investigation, R.A.; resources, R.A.; data curation, K.S.T. and R.A.; writing—original draft preparation, K.S.T.; writing—review and editing, R.A. and R.S.; visualization, K.S.T.; supervision, R.A.; project administration, R.A. All authors have read and agreed to the published version of the manuscript.

Funding: This research received no external funding.

Data Availability Statement: The data can be shared up on request.

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

References

1. Zhang, X.; Sun, P.; Xu, J.; Wang, X.; Yu, J.; Zhao, Z.; Dong, Y. Blockchain-based safety management system for the grain supply chain. *IEEE Access* **2020**, *8*, 36398–36410. [CrossRef]
2. Zhang, X.; Li, Y.; Peng, X.; Zhao, Z.; Han, J.; Xu, J. Information traceability model for the grain and oil food supply chain based on trusted identification and trusted blockchain. *Int. J. Environ. Res. Public Health* **2022**, *19*, 6594. [CrossRef] [PubMed]
3. Lucena, P.; Binotto, A.P.; Momo, F.D.S.; Kim, H. A case study for grain quality assurance tracking based on a Blockchain business network. *arXiv* **2018**, arXiv:1803.07877.
4. Zhang, Y.; Wu, X.; Ge, H.; Jiang, Y.; Sun, Z.; Ji, X.; Jia, Z.; Cui, G. A blockchain-based traceability model for grain and oil food supply chain. *Foods* **2023**, *12*, 3235. [CrossRef] [PubMed]
5. Thakur, K.S.; Ahuja, R. Empowering Fast-Moving Consumer Goods Supply Chain Leveraging Blockchain. In *International Conference on Recent Trends in Machine Learning, IOT, Smart Cities & Applications*; Springer Nature Singapore: Singapore, 2023; pp. 729–740.
6. Albaaji, G.F.; Chandra, S.V. Blockchain technology in agriculture: Digitizing the Iraqi agricultural environment. *Environ. Dev. Sustain.* **2024**, 1–12. [CrossRef]
7. Farooq, M.S.; Ansari, Z.K.; Alvi, A.; Rustam, F.; Díez, I.D.L.T.; Mazón, J.L.V.; Rodríguez, C.L.; Ashraf, I. Blockchain based transparent and reliable framework for wheat crop supply chain. *PLoS ONE* **2024**, *19*, e0295036. [CrossRef] [PubMed]
8. Balamurugan, S.; Ayyasamy, A.; Joseph, K.S. IoT-Blockchain driven traceability techniques for improved safety measures in food supply chain. *Int. J. Inf. Technol.* **2022**, *14*, 1087–1098. [CrossRef]
9. Caro, M.P.; Ali, M.S.; Vecchio, M.; Giaffreda, R. Blockchain-based traceability in Agri-Food supply chain management: A practical implementation. In Proceedings of the 2018 IoT Vertical and Topical Summit on Agriculture-Tuscany (IOT Tuscany), Tuscany, Italy, 8–9 May 2018; pp. 1–4.
10. Chang, A.; El-Rayes, N.; Shi, J. Blockchain Technology for Supply Chain Management: A Comprehensive Review. *J. Supply Chain Manag.* **2022**, *1*, 191–205. [CrossRef]
11. Patel, H.; Shrimali, B. AgriOnBlock: Secured data harvesting for agriculture sector using blockchain technology. *ICT Express* **2023**, *9*, 150–159. [CrossRef]
12. Zeng, H.; Dhiman, G.; Sharma, A.; Sharma, A.; Tselykh, A. An IoT and Blockchain-based approach for the smart water management system in agriculture. *Expert Syst.* **2023**, *40*, e12892. [CrossRef]
13. Ahuja, R.; Chugh, S.; Singh, R. SeedChain: A secure and transparent blockchain-driven framework to revolutionize the seed supply chain. *Future Internet* **2024**, *16*, 132. [CrossRef]
14. Devrani, S.; Ahuja, R.; Goel, A.; Kharbanda, S.S. A blockchain-driven framework for issuance of NFT-based warranty to customers on E-commerce. In *International Conference on Multi-Disciplinary Trends in Artificial Intelligence*; Springer Nature Switzerland: Cham, Switzerland, 2023; pp. 265–276.
15. Gervais, A.; Karame, G.O.; Wüst, K.; Glykantzis, V.; Ritzdorf, H.; Capkun, S. On the security and performance of proof of work blockchains. In Proceedings of the 2016 ACM SIGSAC Conference on Computer and Communications Security, Vienna, Austria, 24–28 October 2016; pp. 3–16.
16. Lim, M.K.; Li, Y.; Wang, C.; Tseng, M.L. A literature review of blockchain technology applications in supply chains: A comprehensive analysis of themes, methodologies and industries. *Comput. Ind. Eng.* **2021**, *154*, 107133. [CrossRef]
17. Yan, Z.; Gan, G.; Riad, K. BC-PDS: Protecting Privacy and Self-Sovereignty through BlockChains for OpenPDS. In Proceedings of the 2017 IEEE Symposium on Service-Oriented System Engineering (SOSE), San Francisco, CA, USA, 6–9 April 2017; pp. 138–144.
18. Lai, R.; Chuen, D.L.K. Blockchain–from public to private. In *Handbook of Blockchain, Digital Finance, and Inclusion*; Academic Press: Cambridge, MA, USA, 2018; Volume 2, pp. 145–177.

19. Patidar, A.; Sharma, M.; Agrawal, R.; Sangwan, K.S. A Smart Contracts and Tokenization Enabled Permissioned Blockchain Framework for the Food Supply Chain. In *IFIP International Conference on Advances in Production Management Systems*; Springer International Publishing: Cham, Switzerland, 2021; pp. 228–235.
20. Mishra, H.; Maheshwari, P. Blockchain in Indian Public Distribution System: A conceptual framework to prevent leakage of the supplies and its enablers and disablers. *J. Glob. Oper. Strateg. Sourc.* **2021**, *14*, 312–335. [CrossRef]
21. Menon, S.; Jain, K. Blockchain Technology for Transparency in Agri-Food Supply Chain: Use Cases, Limitations, and Future Directions. *J. Distrib. Ledger Traceability Transpar.* **2024**, *71*, 106–120. [CrossRef]
22. Ellahi, R.M.; Wood, L.C.; Bekhit, A.E.-D.A. Blockchain-Based Frameworks for Food Traceability: A Systematic Review. *Foods* **2023**, *12*, 3026. [CrossRef] [PubMed]
23. Mekkouri, M.; Hennebert, C. Practices for Assessing the Security Level of Solidity Smart Contracts. In *International Symposium on Foundations and Practice of Security*; Springer Nature Switzerland: Cham, Switzerland, 2023; pp. 71–86.
24. Bhat, S.A.; Huang, N.-F.; Sofi, I.B.; Sultan, M. Agriculture-Food Supply Chain Management Based on Blockchain and IoT: A Narrative on Enterprise Blockchain Interoperability. *Agriculture* **2022**, *12*, 40. [CrossRef]

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