future internet

Article

SeedChain: A Secure and Transparent Blockchain-Driven Framework to Revolutionize the Seed Supply Chain

Rohit Ahuja [1,†], Sahil Chugh [1,†] and Raman Singh [2,*,†]

[1] Department of Computer Science & Engineering, Thapar Institute of Engineering & Technology, Patiala 147004, India; rohit.ahuja@thapar.edu (R.A.); schugh_be19@thapar.edu (S.C.)

[2] School of Computing, Engineering and Physical Sciences, University of the West of Scotland, Blantyre, Glasgow G72 0LH, UK

[*] Correspondence: raman.singh@uws.ac.uk

[†] These authors contributed equally to this work.

Abstract: Farming is a major sector required for any nation to become self-sustainable. Quality seeds heavily influence the effectiveness of farming. Seeds cultivated by breeders pass through several entities in order to reach farmers. The existing seed supply chain is opaque and intractable, which not only hinders the growth of crops but also makes the life of a farmer miserable. Blockchain has been widely employed to enable fair and secure transactions between farmers and buyers, but concerns related to transparency and traceability in the seed supply chain, counterfeit seeds, middlemen involvement, and inefficient processes in the agricultural ecosystem have not received enough attention. To address these concerns, a blockchain-based solution is proposed that brings breeders, farmers, warehouse owners, transporters, and food corporations to a single platform to enhance transparency, traceability, and trust among trust-less parties. A smart contract updates the status of seeds from a breeder from *submitted* to *approved*. Then, a non-fungible token (NFT) corresponding to approved seeds is minted for the breeder, which records the date of cultivation and its owner (breeder). The NFT enables farmers to keep track of seeds right from the date of their cultivation and their owner, which helps them to make better decisions about picking seeds from the correct owner. Farmers directly interact with warehouses to purchase seeds, which removes the need for middlemen and improves the trust among trust-less entities. Furthermore, a tender for the transportation of seeds is auctioned on the basis of the priority location loc_p, *Score*, and *bid_amount* of every transporter, which provides a fair chance to every transporter to restrict the monopoly of a single transporter. The proposed system achieves immutability, decentralization, and efficiency inherently from the blockchain. We implemented the proposed scheme and deployed it on the Ethereum network. Smart contracts deployed over the Ethereum network interact with React-based web pages. The analysis and results of the proposed model indicate that it is viable and secure, as well as superior to the current seed supply chain system.

Keywords: seeds; blockchain; breeder; smart contract; agricultural supply chain; farmers; DApp

check for updates

Citation: 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. https://doi.org/10.3390/fi16040132

Academic Editor: Yuansong Qiao

Received: 4 March 2024
Revised: 31 March 2024
Accepted: 10 April 2024
Published: 15 April 2024

1. Introduction

In developing countries, the agricultural sector is a major sector for the livelihood of its citizens. For sustainable agriculture, seeds are the primary and most critical ingredients. The performance of all other farming inputs is largely reliant on the quality of the seeds. According to estimates, the direct contribution of high-quality seeds to overall production ranges from 15% to 20%, depending on the crop, and can reach up to 45% with the effective management of other inputs [1]. In past decades, there have been major advancements in the seed sector. Government bodies have executed a major re-structuring of the seed industry to empower the seed infrastructure. To survive in the competitive market and effectively contribute to the national effort to increase food production in order to achieve food and nutritional security, seed corporations must urgently transform themselves in line with the industry in terms of infrastructure, technologies, approaches, and management culture [2].

Breeders procure seeds and get them validated through a government entity such as a food corporation, which validates the seeds and stores them in their warehouses, which are provided to the farmers based on their demand [3]. The food supply chain is critical in terms of its impact on a country's economy and its relevance to sustaining the essential sector of any country. In this supply chain, the exchange of goods relies on complex and paper-thin settlement processes, and these processes are not very transparent, with a high risk to breeders and farmers during the exchange of value. Since transactions are prone to fraud, middlemen step in, increasing the total costs of remittances and making it difficult for the farmer to receive the right product overall.

Existing seed supply chain solutions in the agricultural sector focus on enhancing transparency between producers, i.e., farmers, and consumers, with an aim to minimize intermediaries between end-users and producers [4]. In addition, systems supporting the traceability of food products and the identification of the original sources of products [5,6] have been suggested. Furthermore, the agricultural system financially benefits from the identification of buyers ready to pay additional charges for a specific product [7,8]. For the optimization of food supply chain purchasers' trading portfolios, the Practical Byzantine Fault Tolerance (PBFT) algorithm was laid out and validated using a consortium blockchain [9,10]. However, major concerns in agriculture related to seed distribution have not received enough attention. There is a requirement of the seed distribution framework that allows farmers to keep track of seeds from breeders throughout the chain and to identify the sources of seeds. In addition, the supply chain framework allows transparent and fair bidding and tender mechanisms for logistics.

Blockchain is an immutable technology consisting of interconnected blocks of data, each containing a list of transactions and a unique reference to the previous blocks [2,11–13]. By assigning unique digital identifiers, blockchain enables the easy traceability of food products across the supply chain, incorporating essential information such as batch numbers and expiry dates [3,14]. This ensures transparency and facilitates the efficient tracking of food products from their origin to the end consumer. Implementing a food ledger and transaction register through blockchain technology has the potential to prevent fraud and enhance traceability, enabling the identification of the sources of foodborne illnesses [15].

Our Contribution: We propose a blockchain-based solution that not only significantly reduces corruption but also optimizes the transaction of seeds for farmers and government officials. The proposed approach is a "decentralized application" that keeps an immutable record of every transaction between farmers and the Food Corporation of India (FCI). It allows farmers to keep track of seeds throughout the supply chain across all stakeholders and to identify the original sources of seeds. In addition, the system grants non-fungible tokens corresponding to approved seeds that explicitly state their date of cultivation and their owner to make the system more transparent. Furthermore, it enables a fair auction-driven transportation system for logistics. The proposed solution is implemented and deployed in a P2P (peer-to-peer) network and is executed on a two-phase verification system that primarily comprises nodes (FCI, farmer, warehouse, transport) in the chain. Farmers looking to buy seeds and fertilizers can check prices and availability at various FCI warehouses within a pre-specified location. Our proposed solution offers an effective mechanism for farmers to conveniently purchase seed products from warehouses and carry out transactions using Ethers *Eth* on the Ethereum mainnet private blockchain.

The rest of this work is organized in the following manner. Section 2 describes the existing seed distribution system and its limitations. Section 3 describes the tool known as blockchain, along with its types and smart contracts. The proposed "SeedChain" framework is discussed in Section 4, while Section 5 discusses its implementation along with its features and security analysis. Finally, Section 6 discusses the conclusion and future work.

2. Existing Systems

The existing seed supply chain in agriculture employs minimum technology and is based upon the manual updating of records, which is tangible and prone to malpractices, such as the misrepresentation of product availability and the black marketing of important and in-demand seeds, as depicted in Figure 1. The government's role in the pricing, sale, and purchase of products creates significant opportunities for corruption [16]. In India, corruption at Food Corporation of India (FCI) warehouses is often reported, wherein officials input incorrect information into their government databases. For example, if a farmer purchases 50 kg of seeds, FCI officials would often record it as 100 kg sold, and the remaining 50 kg are back-channeled and sold later, creating an expensive market for the same. While such actions lead to increased corruption in the government, they also make it difficult for a poor farmer to access good-quality seeds and fertilizers, which is a huge problem in the initial stages of the food supply chain [17]. For agri-food, a detailed survey was conducted, and a framework corresponding to the Vietnamese cashew nut business [18] was discussed. To efficiently address concerns in Iraqi agriculture, blockchain technology has been incorporated so that it can benefit from growth-promoting solutions to enduring problems. It can increase productivity and competitiveness by improving data management, accountability, and intelligent contracts. Notwithstanding these challenges, blockchain's advantages, such as its efficiency and transparency, make it a wise investment for Iraq's agriculture industry [19]. The potential of blockchain technology in precision agriculture, food supply chains, crop insurance, and agricultural product transactions is examined in [20], taking into account both theoretical frameworks and real-world applications. It also tackles the difficulties in logging farm-owner transactions and creating an ecosystem powered by blockchain for the food and agriculture industries. A blockchain-based system, "AgriOnBlock", was designed to address issues in the agriculture industry to enhance transparency among various stakeholders, such as bankers, retailers, customers, farmers, wholesalers, etc. [21]. It intends to handle relevant issues within the industry and efficiently connect stakeholders by utilizing Ethereum smart contracts and Internet of Things (IoT) devices. A blockchain framework that is based on the IoT and incorporates an artificial intelligence system is intended to oversee and control smart water management [22]. An IoT-based smart water irrigation system is recommended to efficiently address the water crisis in the agriculture industry today, taking into consideration several factors, such as fertilizer quality. Most of the existing techniques primarily focus on food supply and food security, which should benefit all stakeholders by increasing transparency and trust among all of the stakeholders involved in the farming sector. However, seeds, which are the pioneering and fundamental elements in the farming sector, have not received enough attention.

Moreover, in the Indian context, carrying huge amounts of cash is precarious, especially in Northern Indian Rural Areas, as thefts and burglaries lead to significant losses. This creates a need for a cashless system so that the need for physical money is eliminated when purchasing input materials for farming. Also, at times, a farmer has to travel to various FCI warehouses before finding products with the required availability and quality [23]. This leads to an enormous wastage of time as well. While we intend to solve these ground-level problems in rural areas and decrease the pitfalls for farmers, as well as simplify paperwork for the government, the broader vision of India 2030 is also fulfilled, as this development in the agricultural field will lead to an increase in digital literacy among farmers as well.

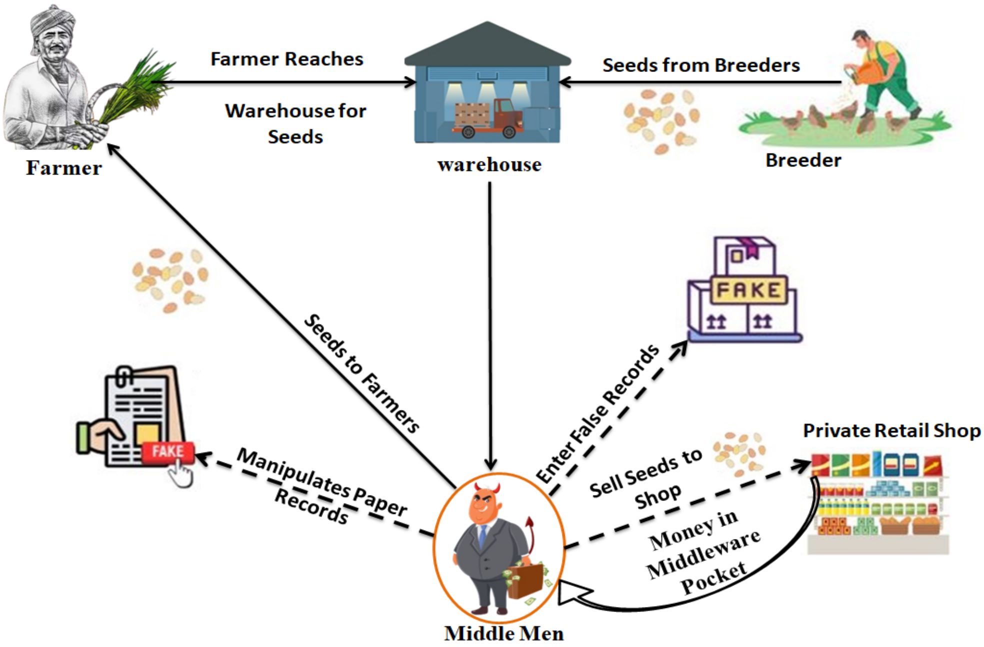


Figure 1. Existing seed-purchasing system.

Limitations of Existing Systems

1. Lack of digitization: Every monetary transaction and storage entry is recorded on paper. Piles of record registers take up a great amount of space in the form of filing cabinets. These are susceptible to manipulation, theft, fire, water, and bugs. Searching for a record would become a cumbersome task and would lead to a waste of time and labor.
2. Extensive corruption: The easy manipulation of records largely contributes to corruption. Authority figures might authorize a fake transit of goods, and the money would get transferred to a bogus account. The seeds are often hoarded so that a state of scarcity can be established and are then sold for a higher price.
3. Opaque operations: In the existing system, no operation is logged at any step of the supply chain. In case of any exigency, there would not be any chain of custody to identify the point where things went wrong. There is no transparency in operations, due to which it is easy to hide bogus transactions and shipments.
4. Inefficient and slow: There is no automation of any of the tasks, starting from breeder registration and ending with a farmer's purchase of a packet of seeds. Entering and searching paper records is extremely time-consuming, which becomes a burden to the entire system.
5. Security: Records are kept in a file cabinet in an unguarded room, which any intruder can visit and then view the details without any restrictions. This is conducive to data leaks, which could be catastrophic to farmers, as their account details and seed purchase routines could fall into the wrong hands.
6. Middleman: The present system comprises middlemen who take advantage of the manual system and sell seeds at a greater price than the maximum retail price by manipulating the taxes for their advantage. In addition, expired seeds are sold with normal seeds. The practice of hoarding and creating a fake demand allows middlemen to sell seeds at a higher price, which causes trouble for farmers.

3. Preliminaries

This section delves into blockchain technology, smart contracts, and various classifications of blockchain systems.

3.1. Blockchain Technology

The term blockchain was coined in 2008 and came into practice in the year 2009 as a core mechanism in Bitcoin [24]. Blockchain is analogous to a public ledger/database that is shared among peers in a network and stores records of every transaction made on a chain of blocks. Decentralization, traceability, and persistence are the key characteristics of blockchain technology.

Decentralization: Conventional systems require every transaction to be approved by a centrally trusted authority, which results in additional costs and poor efficiency. On the contrary, transactions that take place within a blockchain network can be executed directly between two users, obviating the necessity for intermediary supervision. Blockchain technology consequently reduces operational and development expenditures by a substantial amount.

Traceability: Each blockchain transaction is validated and subsequently documented with a timestamp. This feature grants users the ability to inspect and trace historical records from any node within the decentralized network, thereby augmenting the transparency and traceability of the data that are stored.

Persistence: In the blockchain network, each effectively completed transaction is confirmed and recorded in blocks, rendering falsification extremely difficult. Furthermore, prior to being disseminated, every block is validated by neighboring nodes, which guarantees the confirmation of transactions and simplifies the process of detecting tampering.

Blockchain comprises a series of blocks that contain records of all transactions that have been carried out across the network. The initial block in the blockchain sequence is referred to as the genesis block and lacks a preceding node, known as the parent node. Subsequent blocks reference the previous block by its hash value, establishing a sequential chain. Each block consists of a body and a block header, as depicted in Figure 2. Specifically, the block header includes the parent block hash of 256 bits and the sum of all block transactions, i.e., the Merkle tree root hash, as well as the block version, 4-bit Nonce, and timestamp expressed time in seconds.

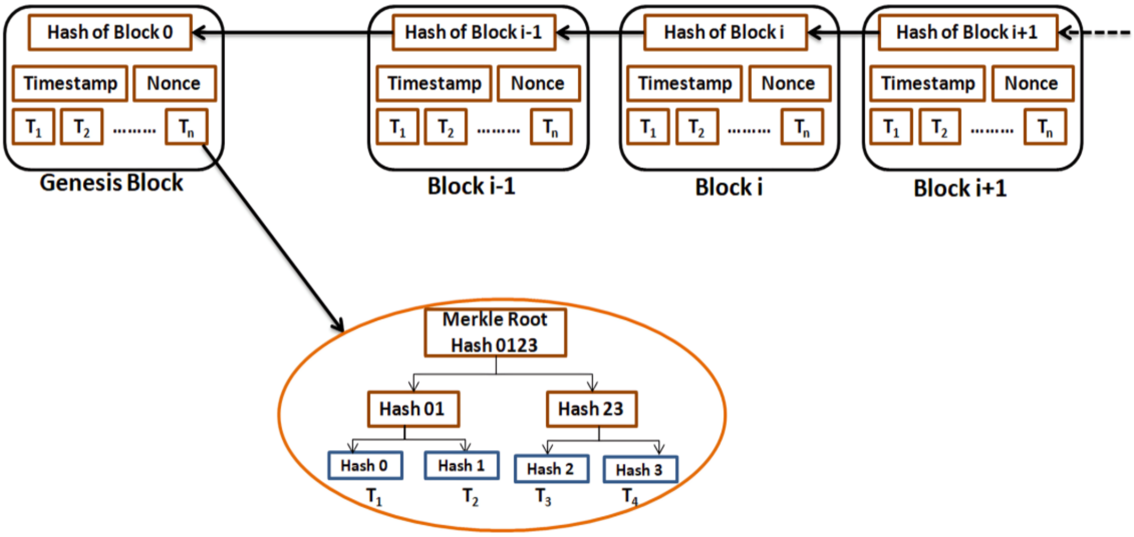


Figure 2. Blockchain.

3.2. Smart Contracts

These are contracts crafted using Solidity that are implemented between the deployer and the recipient and act as independent contracts binding the parties involved, as depicted in Figure 3. These contracts can be programmed to be deployed on the chain and can be triggered in the event of any action. Thus, they are automated, and once deployed on the chain, they cannot be altered, which implies that these programmable contracts are non-disputable and hence play an important role in establishing trust in a trust-less environment. If there exists a system where there is a lack of confidence in a deal between two parties who do not have complete faith in each other, a smart contract written to eliminate issues can be deployed on a blockchain, which is triggered in real time [25,26].

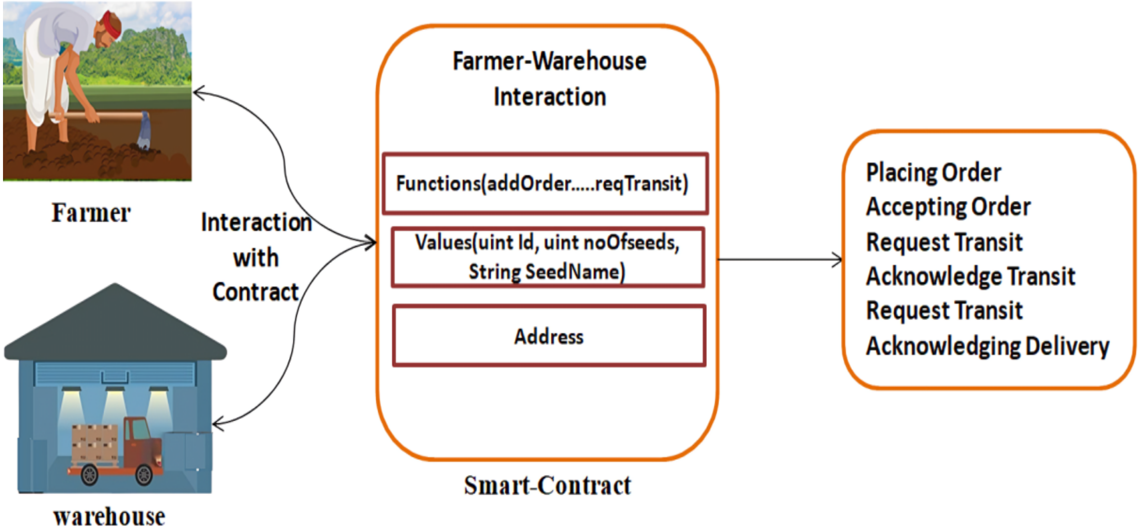

Farmer
warehouse
Interaction with Contract
Farmer-Warehouse Interaction
Functions(addOrder.....reqTransit)
Values(uint Id, uint noOfseeds, String SeedName)
Address
Smart-Contract
Placing Order
Accepting Order
Request Transit
Acknowledge Transit
Request Transit
Acknowledging Delivery

Figure 3. Smart contract.

For instance, a smart contract is deployed on the Ethereum blockchain, which will record a transaction between a farmer and a warehouse whenever one takes place. So, whenever an order is started, the contract is triggered, and it keeps updating the status of the order on-chain in an automated manner. Since this contract is already deployed and the logic cannot be altered, the status of the order cannot be manipulated by anyone, which helps us achieve a list of records that cannot be changed and are non-disputable. The contract is responsible for maintaining faith in the seed-purchasing process, and all the relevant parties have a limited scope of participation in the purchasing process [27].

3.3. Different Types of Solutions Based on Blockchain Technology

For efficient seed supply chain management, a decentralized application that makes use of blockchain and smart contract technologies may be a good option [28,29]. There are four main categories of blockchain systems available for use:

1. Public blockchain: Nodes in a public blockchain are arranged so that anyone can become a part of the blockchain and participate in mining future blocks of the chain. Such a chain that is accessible by the general public without any restrictions is termed a public blockchain, as depicted in Figure 4.
2. Private blockchain: A private blockchain refers to an arrangement of nodes for a restricted network rather than being open to everyone willing to contribute processing power. Such a chain is also referred to as a managed blockchain, as only the central authority permits a node to join the chain, as shown in Figure 5.
3. Hybrid blockchain: In a hybrid blockchain, as depicted in Figure 6, an organization can join a chain, which allows it to use the best of both public and private blockchains. They can create a permission-based system along with a permissionless system. In this manner, the administering organization can control who can access specific data and what data can be open to the public.
4. Consortium blockchain: Figure 7 depicts the consortium blockchain, as it shares similarities with the hybrid blockchain on the grounds of having both public and private features. The differentiating factor for this blockchain is that various organizations collaborate in a decentralized network, hence eliminating the risk of one entity's monopoly over the entire network.

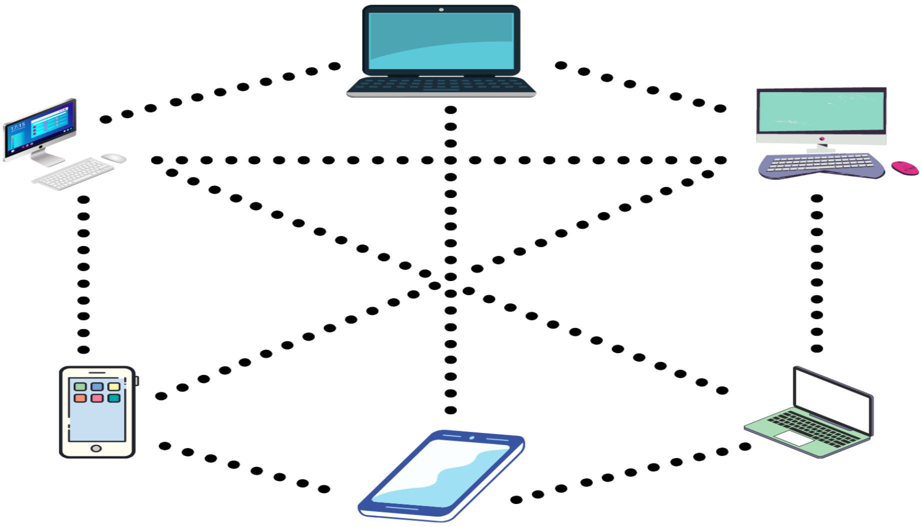


Figure 4. Public blockchain.

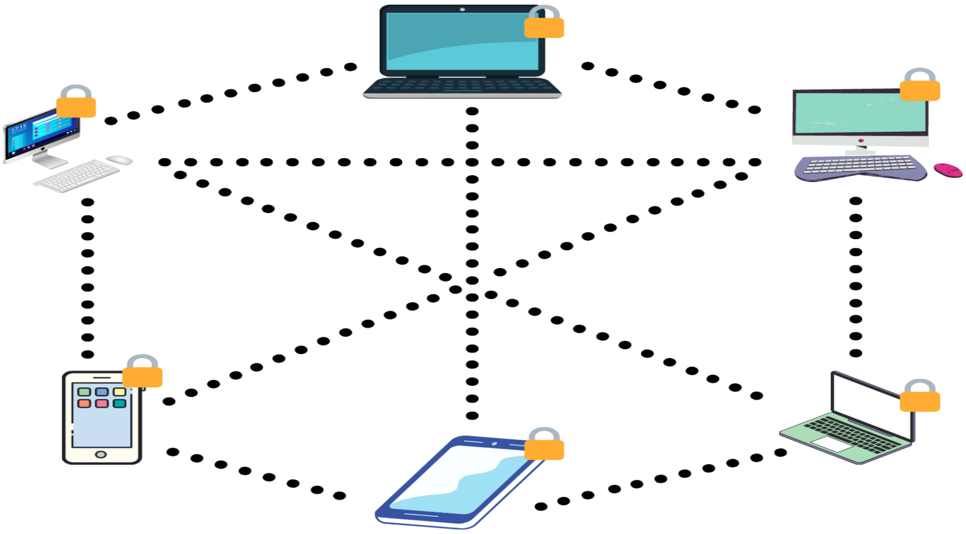


Figure 5. Private blockchain.

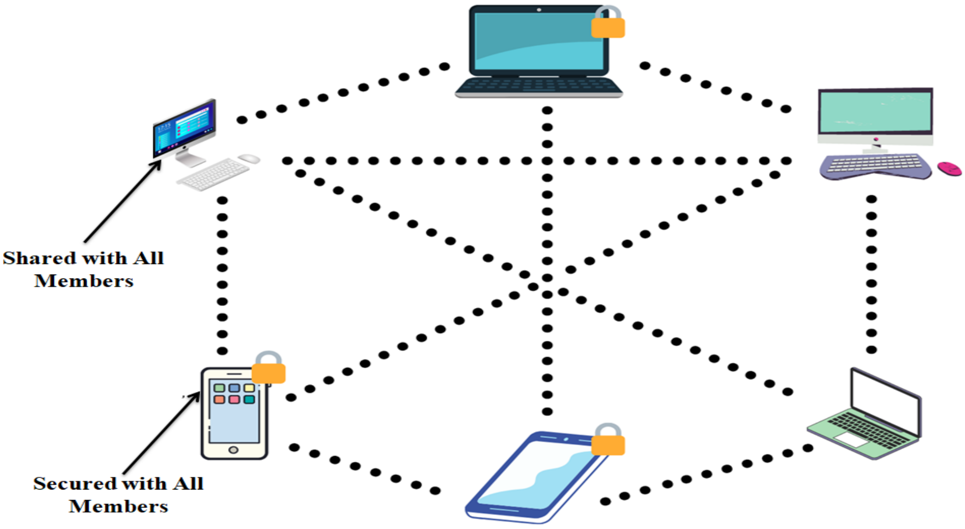


Figure 6. Hybrid blockchain.

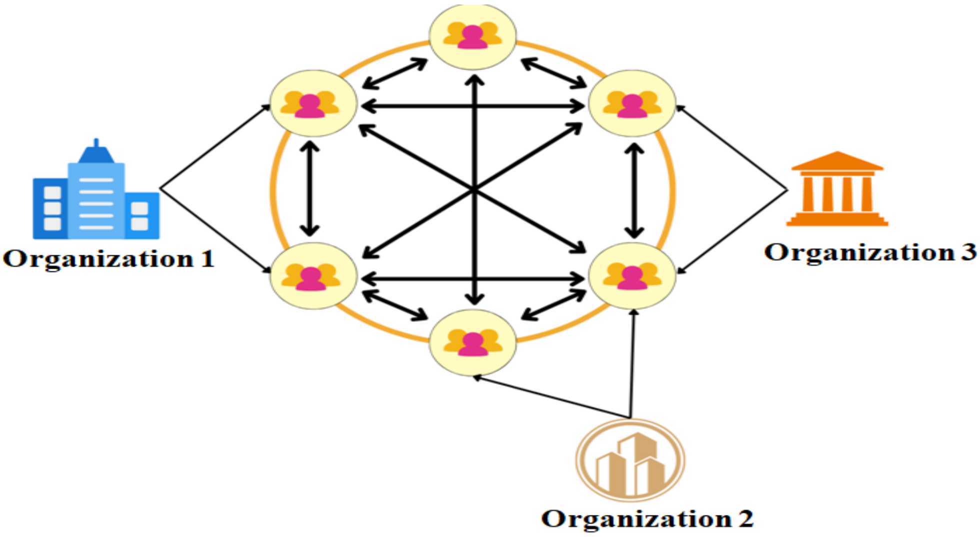


Figure 7. Consortium blockchain.

4. The Proposed Framework

Our proposed solution involves establishing a sense of trust among trust-less parties, i.e., farmers who are willing to purchase raw materials and warehouses where all quality seeds can be found. The introduction of blockchain technology also improves relationships with third-party logistics and FCI while efficiently managing the approval of new seeds from various breeders within the framework.

A total of five entities play a vital role in this ecosystem, as depicted in Figure 8, i.e., breeders, government agencies (*in our case, the Food Corporation of India (FCI)*), farmers, warehouses, and a third-party logistics company. The entire supply chain, right from the cultivation of seeds, will be digitally recorded to ensure that all the necessary transactions that take place, ranging from approving a particular seed quality to capturing the purchasing history of a farmer, are available in a non-disputable fashion. Entities such as breeders and third-party logistics companies are in a direct relationship with FCI, and their respective roles are highlighted, showing the shift of these manual processes to on-chain recorded processes in a blockchain environment. The proposed algorithms are discussed below.

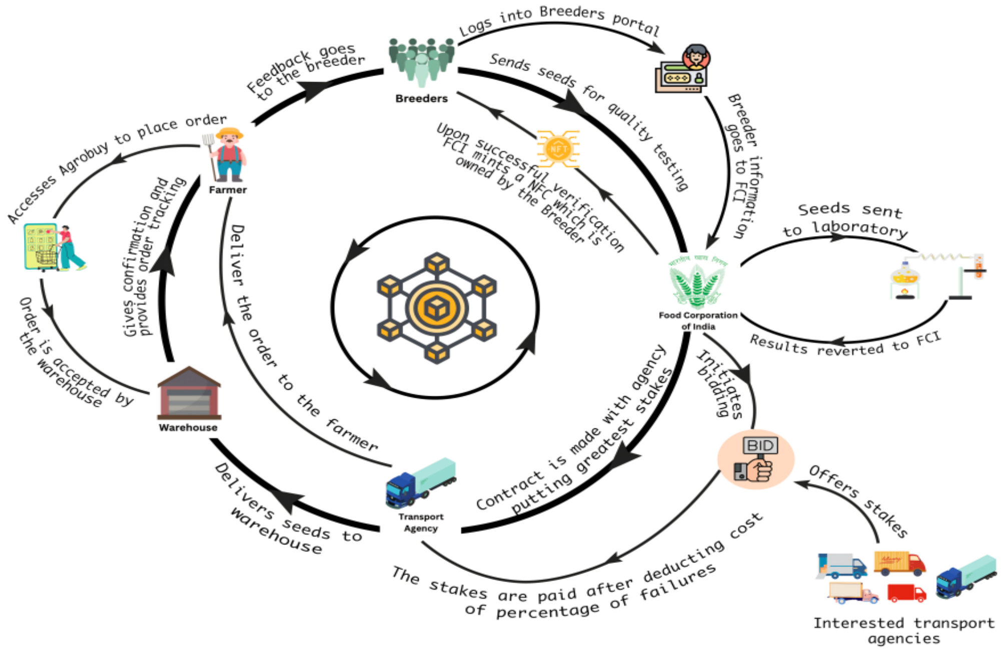

Logs into Breeders portal
Feedback goes to the breeder
Breeders
Sends seeds for quality testing
Breeder information goes to FCI
Upon successful verification FCI mints a NFC which is owned by the Breeder
NFT
Accesses Agrobuy to place order
Farmer
Gives confirmation and provides order tracking
Deliver the order to the farmer
Order is accepted by the warehouse
Warehouse
Seeds sent to laboratory
Food Corporation of India
Results reverted to FCI
Initiates bidding
BID
Offers stakes
Contract is made with agency putting greatest stakes
Transport Agency
Delivers seeds to warehouse
The stakes are paid after deducting cost of percentage of failures
Interested transport agencies

Figure 8. Proposed blockchain-based breeder–farmer system.

Farmer Registration: Prior to purchasing any seeds, firstly, the farmer calls Algorithm 1 to register him- or herself. Every farmer F_N is expected to provide his or her phone no. F_P, email F_E, and unique id F_{Id}.

Algorithm 1 FrmReg: Farmer Registration.

Input: Takes F_N, F_P, F_E, and F_{Id} as input.
Output: Farmer Registered Successfully.

```
$Frm_{Portal} \xleftarrow{Input} [\xi]\ Farmer : \xi = \left(F_N, F_P, F_E, F_{Id}\right)$
$F_E \xleftarrow{\tau} Frm_{Portal}$ : $\tau$ = One-Time Password
if ($verify(\tau) = 1$) then
    Farmer details verified
else
    Incorrect $\tau$ entered
end if
$Frm_{Portal} \xleftarrow[Input]{User_{Name}, pswd} Farmer$
if ($Unique(User_{Name}) == 1$) then
    if ($Criteria(Pswd) == 1$) then
        Farmer Registered Successfully
    else
        Password criteria mismatch
    end if
else
    Username exist
end if
```

Breeder Registration: The breeder calls Algorithm 2 to register him- or herself and then sell/verify seeds. Every breeder B_N is expected to provide his or her phone no. B_P, email B_E, and unique id B_{Id}.

Algorithm 2 BrdReg: Breeder Registration.

Input: Takes B_N, B_P, B_E, and B_{Id} as input.
Output: Breeder Registered Successfully.

```
$Brd_{Portal} \xleftarrow{Input} [\xi]\ Farmer : \xi = \left(B_N, B_P, B_E, B_{Id}\right)$
$B_E \xleftarrow{\tau} Brd_{Portal}$ : $\tau$ = One-Time Password
if ($verify(\tau) = 1$) then
    Breeder Authenticated
else
    Incorrect $\tau$ entered
end if
$Brd_{Portal} \xleftarrow[Input]{Breeder_{Name}} Breeder$
if ($Unique(Breeder_{Name}) == 1$) then
    $Brd_{Portal} \xleftarrow[Input]{Password} Breeder$
    if ($Criteria(Password) == 1$) then
        Breeder Registered
    else
        Password criteria mismatch
    end if
else
    Breeder exists/Choose different name to sign up
end if
```

Transporter Registration: Before participating in the bidding, every transporter needs to register him- or herself on the portal using Algorithm 3. Every transporter T_N is expected to provide his or her phone no. T_P, email T_E, and unique id T_{Id}. In addition, every transporter enters three preferred locations $Loc_{i:i \in \{1,2,3\}}$ based on his or her preference for operating services, with Loc_1 and Loc_3 as the highest and lowest priorities, respectively.

Algorithm 3 TransReg: Transporter Registration.

```
Input: Takes $T_N$, $T_P$, $B_E$, $T_{Id}$, and $Loc_{i:i \in \{1,2,3\}}$ as input.
Output: Transporter Registered Successfully.
$Trp_{Portal} \xleftarrow{Input} [\xi]\ Farmer : \xi = (T_N, T_P, T_E, T_{Id}, )$
$T_E \xleftarrow{\tau} Trp_{Portal}$: $\tau$ = One-Time Password
if ($verify(\tau) = 1$) then
    Transporter Authenticated
else
    Incorrect $\tau$ entered
end if
$Trp_{Portal} \xleftarrow[Input]{Transporter_{Name}} Transporter$
if ($Unique(Transporter_{Name}) == 1$) then
    $Trp_{Portal} \xleftarrow[Input]{password} Transporter$
    if ($Criteria(Password) == 1$) then
        Registration Completed
    else
        Password criteria mismatch
    end if
else
    Transporter exists/Choose different name to sign up
end if
```

Approve Seeds: Breeders submit seeds along with their meta-data S_M, i.e., the seed name S_N and location S_{loc}, where the seeds are harvested S_{harv}, and their quantity S_Q, to FCI, which calls Algorithm 4 to check the quality of seeds and, based on that, mints an NFT as a certificate, as shown in Figure 9, to approve the seeds or otherwise rejects the seeds. The flowchart for approving seeds is depicted in Figure 10.

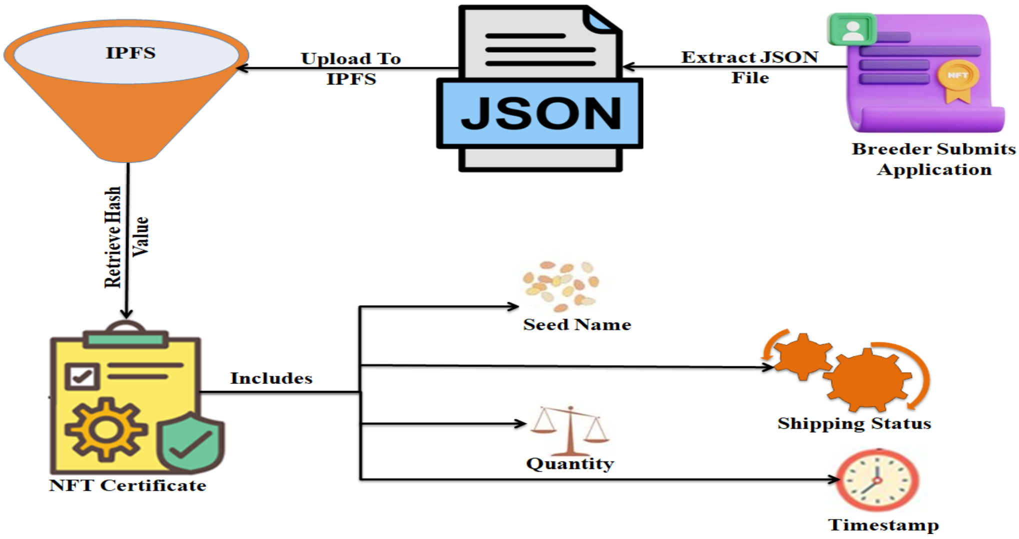


Figure 9. NFT minting.

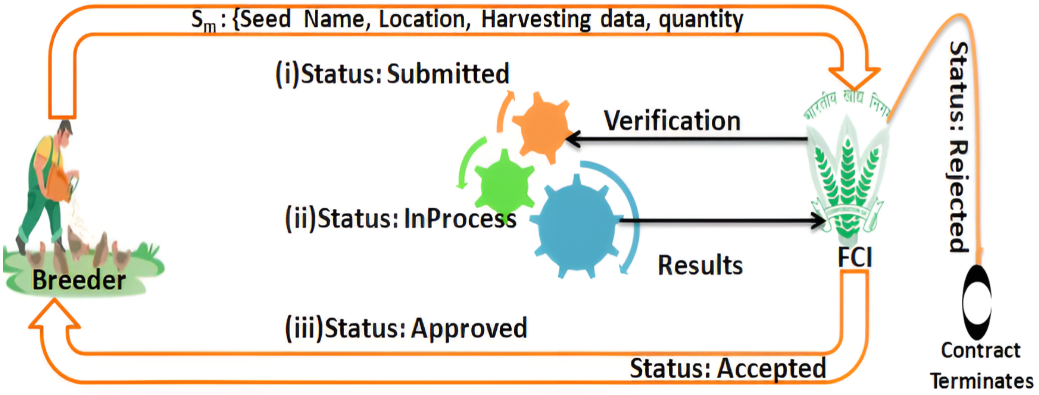


Figure 10. Flowchart for approving seeds.

Algorithm 4 ApprvSeed: For approving seeds.

```
  Input: Order $S_M = \{S_N, S_{loc}, S_{harv}, S_Q\}$.
  Output: Seeds Approved/Rejected.
$FCI \xleftarrow[S_M:Submitted]{S_N,S_{loc},S_{harv},S_Q} Breeder.$
$S_M : In\_Process$
if $(Check(S_M) == 1)$ then
    $S_M : Verified$
    if $(Verify(S_M) == 1)$ then
        $Breeder \xleftarrow[S_M:NFT]{} FCI$
    end if
else
    $S_M : Rejected$
end if
```

Order Seed: Every farmer creates an order $O_F = \{S_N, S_Q, F_N, F_Q\}$, where S_N and S_Q are the name and quantity of seeds, respectively, while F_N and F_Q are the name and quantity of fertilizer. To place an order for seeds, the farmer calls Algorithm 5. The flowchart for ordering seeds/fertilizers is depicted in Figure 11.

Algorithm 5 OrdSeed: For ordering seeds.

```
  Input: Order $O_F = \{S_N, S_Q, F_N, F_Q\}$.
  Output: $O_F$ completed successfully.
$W_H \xleftarrow[S_O:Initiated]{S_N,S_Q,F_N,F_Q} F_k.$
$S_{Contract} \xleftarrow{\delta_{Eth}} F_k$, where $\delta_{Eth}$=Order value + gas fees.
$F_k \xleftarrow{S_O:Accepted} W_H$
$T \xleftarrow{S_O:Transit\_Request} W_H$
$W_H \xleftarrow{S_o:Transit\_Acknoweldge} T$
if $(AckTrans(S_O) == 1)$ then
    $F_k \xleftarrow{S_O:Request\_Delievery} T$
    $T \xleftarrow{S_O:Delievery\_Acknoweldge} F_k$
    if $(AckDel(S_O) == 1)$ then
        $W_{Metamask} \xleftarrow{\delta Eth} S_{Contract}$
    end if
end if
```

Bidding: To select a transporter to successfully complete the bid B_i, FCI calls Algorithm 6.

Algorithm 6 Bid: To select transporter T for bid B_i.

Input: N bids $Bid[i][i][i] = \{B_i, loc_i, Price_i\}_{i,\ldots,N}$ and k transporters $Trans[K][k] = ([T_{id1}, T_{id2}, \ldots, T_{idK}][Amt_1, Amt_2, \ldots, Amt_k])$.
Output: Bid_i is allocated to transporter T_j.

```
for $i$ in $Bid$ do
    for $j$ in $Trans$ do
        if $Bid[0][0][i] > Trans[0][j]$ then
            $T.add(Trans([T_{idj}]))$
        end if
    end for
    for $j$ in $T$ do
        if $T_{idj.loc_1} == loc_i$ then
            $T^{'}.add(T_{idj})$
            $B_{Vj}.add(T_{idj.Amt} + 0.2 * T_{idj.Amt} + C)$
        end if
    end for
    if $(X < len(T^{'}))$ then
        for $j$ in $T$ do
            if $(T_{idj.loc_2} == loc_i)$ then
                $T^{'}.add(T_{idj})$
                $B_{Vj}.add(T_{idj.Amt} + 0.1 * T_{idj.Amt} + C)$
            end if
        end for
    end if
    if $(X < len(T^{'}))$ then
        for $j$ in $T$ do
            if $(T_{idj.loc_3} == loc_i)$ then
                $T^{'}.add(T_{idj})$
                $B_{Vj}.add(T_{idj.Amt} + 0.05 * T_{idj.Amt} + C)$
            end if
            if $(X < len(T^{'}))$ then
                $B_i$ bid canceled
            end if
        end for
    end if
    $T_j \xleftarrow[B_i]{Bid} max(B_{vj})$
end for
```

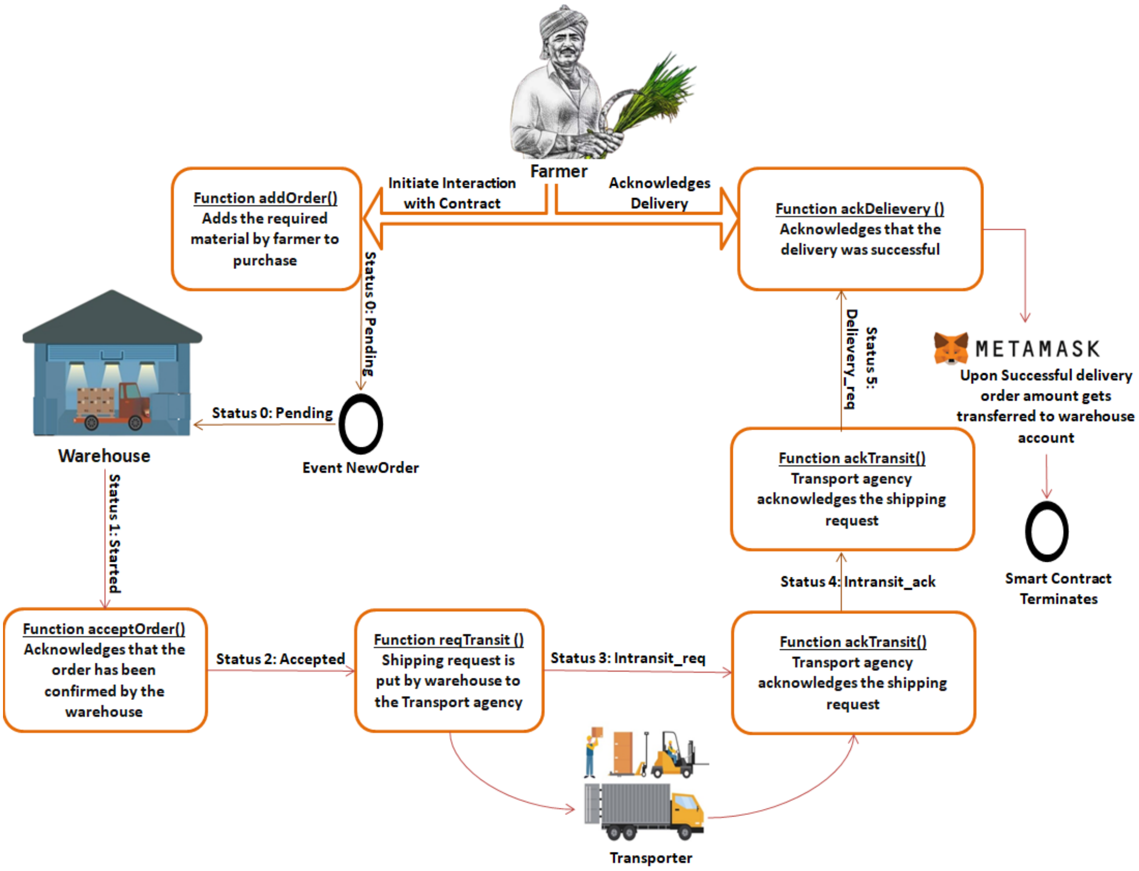

Farmer
Initiate Interaction with Contract
Acknowledges Delivery
Function addOrder()
Adds the required material by farmer to purchase
Function ackDelievery ()
Acknowledges that the delivery was successful
Status 0: Pending
Status 5: Delievery_req
METAMASK
Upon Successful delivery order amount gets transferred to warehouse account
Warehouse
Status 0: Pending
Event NewOrder
Function ackTransit()
Transport agency acknowledges the shipping request
Smart Contract Terminates
Status 1: Started
Status 4: Intransit_ack
Function acceptOrder()
Acknowledges that the order has been confirmed by the warehouse
Status 2: Accepted
Function reqTransit ()
Shipping request is put by warehouse to the Transport agency
Status 3: Intransit_req
Function ackTransit()
Transport agency acknowledges the shipping request
Transporter

Figure 11. Flowchart for ordering seeds.

5. Implementation

To implement the proposed system, a decentralized application is built to encompass the basic functionalities of the proposed system. The application is a JavaScript-based web application consisting of the basic logic defined by a smart contract residing on the Ethereum blockchain [30]. This DApp provides functionalities like adding and verifying users and their properties, provided they can offer the necessary title deeds. The users can view their properties and further sell or lease them to a buyer for the price they set.

5.1. Technology Stack Used

This subsection describes the technology utilized in the implementation of our proposed system.

1. Ethereum and Solidity: It is an open-source blockchain-based platform employed to create and share business, financial services, and entertainment applications. These contracts are written for various points in the supply chain, especially for interactions between two adjacent entities, such as breeders and FCI, farmers and warehouses, etc. These smart contracts help implement features provided by blockchain, such as storing immutable records of purchases by farmers from the government or documenting the quality of seeds approved by FCI.
2. Web3 JS Library: Web3 is a collection of libraries of the World Wide Web that incorporates and facilitates blockchain applications. We have used web3.js, which is an Ethereum JavaScript API that helps in connecting the smart contracts deployed on the chain at the back end to the front end, which is the portal for breeders and FCI and the website available to farmers for purchasing seeds. Therefore, while the purchase of seeds is initiated at the front end by the farmer, the recording of the purchase and the transfer of the order value from the farmer's wallet to the warehouse address are executed by the contract and are synced with the help of web3.js.

3. Ganache and Truffle: Ganache and Truffle are essential for testing the smart contracts and assist in creating a virtual environment to understand the behavior of the deployed contracts in different scenarios. Thus, with the help of these tools, we were able to develop test cases and expand the scope of the contract so that the contract does not fail or produce unexpected results in case of exigency.
4. React JS: The React JavaScript library is the open-source library used to develop the front-end user interface and add functionalities to different portals, such as navigation between different pages and registration and the login of different entities. Thus, the web pages displayed to the users and the interaction of users with the portals are made possible with the help of this library.
5. Inter Planetary File System (IPFS): IPFS is a *p*2*p* method of efficiently storing data and sharing data in a distributed file system. It is designed to hold data in a manner such that no single entity in a network holds the entire table of data. We have utilized IPFS to store data from seed applications and will employ the details in the future with the help of the generated hash.
6. Metamask: This wallet is used to assist in the transfer of Ethers among different parties and between parties and smart contracts in instances where the smart contracts store Ethers until an event has been successfully concluded.
7. MongoDB: Since every single detail, like user login details, for entities such as breeders, farmers, and logistics companies cannot be stored on-chain, we have used MongoDB services to create a back-end environment and store these details, and it is integrated with the user interface.

5.2. The Architecture of the Proposed System

Due to Ethereum's significant smart contract support, the system, which is largely a peer-to-peer network, was used to develop the blockchain-based seed supply chain. The proposed system's architecture is shown in Figure 12.

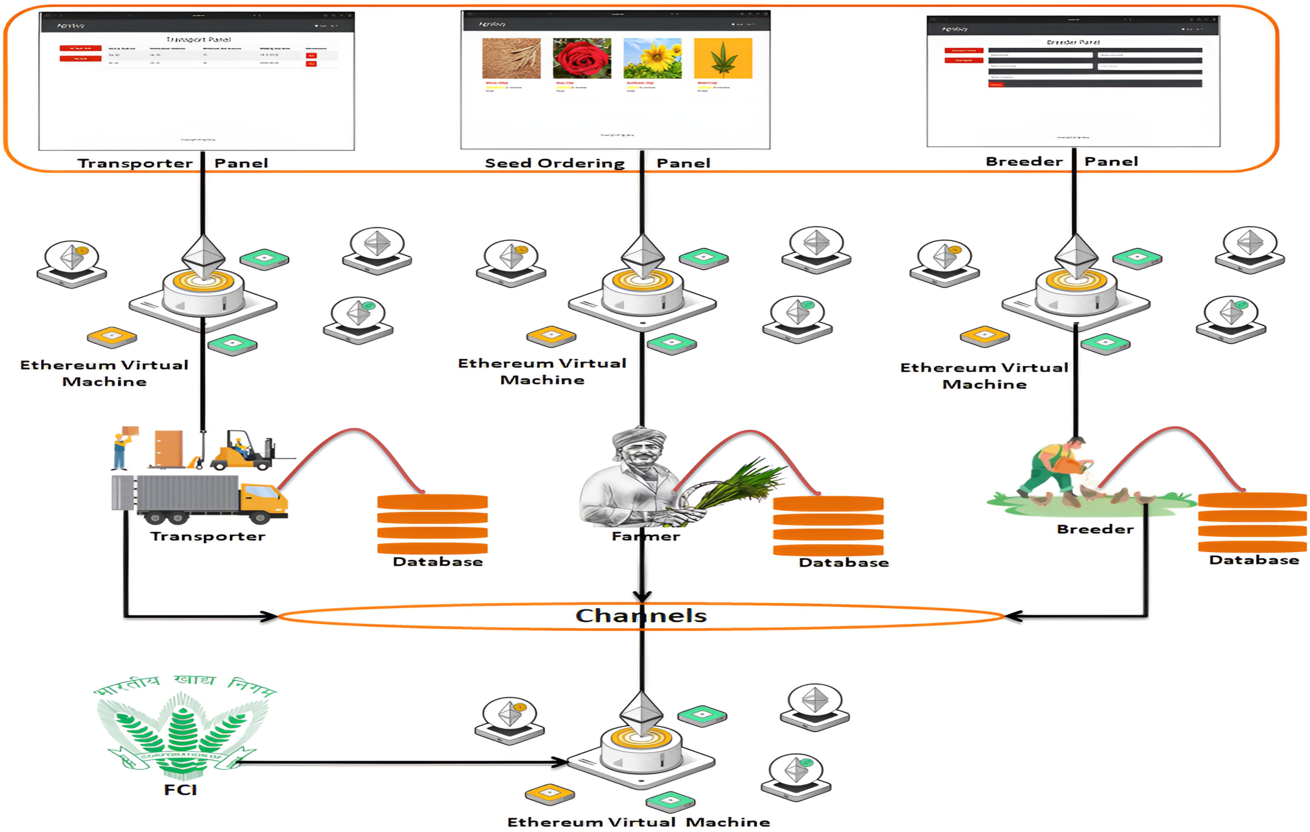


Figure 12. Architecture of the proposed framework.

Several entities (computers) connected as nodes on the internet make up a peer-to-peer network. Without a central authority, transactions are passed from one peer to another. A blockchain, which is a type of public distributed ledger, houses all of the network's transactions. To compare it with other peer nodes, peers also have a synchronized copy of this public ledger. Additionally, any node (peer) that tries to interfere with the network will be immediately removed from it. The Ethereum Virtual Machine powers every node in the Ethereum network (EVM). In Ethereum, a block takes an average of 15 s to mine. An ETH block reward will be given to the successful miner. The user committing each transaction pays the whole gas cost incurred by the block's transaction execution, and the gas cost incurred is credited to the miner's account.

Smart contracts are designed in Solidity, while Reactjs is utilized to develop user interfaces. Users can engage with the Ethereum blockchain through interfaces and with the blockchain's smart contracts using DApps. DApps thus provide a user interface for the back-end smart contract that updates the blockchain with data. The transactions are signed and carried out using the Metamask wallet plugin. The Truffle framework will be used to test and deploy the DApp on regional test networks using Ganache, the open test network Rinkeby, and finally, the main Ethereum network.

5.3. Designing the Smart Contract

As shown in Table 1, smart contracts are designed to carry out tasks associated with seed ordering, enable interactions between FCI and transporters and between farmers and warehouses, perform seed approval, and create matching NFTs for accepted seeds. A smart contract uses logic to satisfy all requirements and consists of four fundamental functionalities. Because it requires funds to store documents like files or photos, we store them on IPFS, which gives us a hash that is kept on the blockchain.

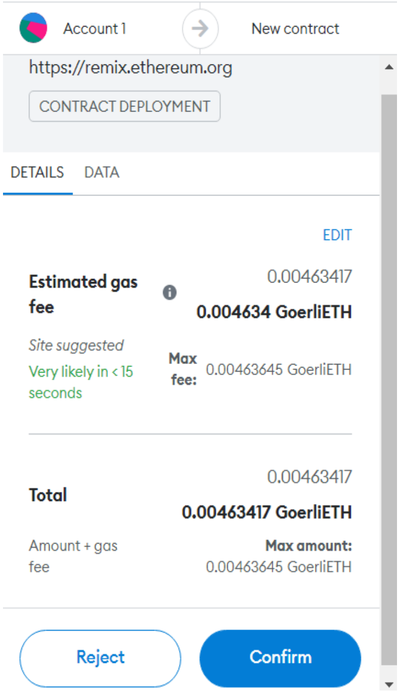
Table 1. Methods employed for smart contracts.

Method	Function Used	Explanation
Ordering Seeds	addOrder()	This is called to store the order placed by a farmer.
	acceptOrder()	Authorized warehouses call this to accept the placed order.
	reqTransit()	This is called to request the transit of the order shipment, and as a result, the status of the order shifts to "REQ-TRANSIT".
	ackTransit()	An authorized logistic company calls this function and updates the status to "TRANSIT ACKNOWLEDGED".
	reqDelievery()	Transit calls this method to request admission of delivery and simultaneously change the status to "REQUESTING DELIVERY".
	ackDelievery()	Once the status is changed to "DELIVERYACKNOWLEDGED", this is the final payable method that can only be called by the farmer.
Seeds Approval	addSubmission()	This adds a new submission for the breeder to the chain and updates the status of the process to "SUBMITTED".
	acceptSubmission()	FCI calls this to accept the submission, which updates the status to the "ACCEPTED" state.
	approveSubmission()	FCI calls this to mint an NFT for seeds with the seed name, timestamp, and approved quality standards.
Warehouse	addWarehouse()	FCI calls this to add a new warehouse to the list of approved warehouses.
	remWarehouse()	FCI calls this to remove a warehouse from the list of approved warehouses.

5.4. Integration

The Remix IDE (remix.ethereum.org accessed on 3 March 2024) was used to develop this contract, and the Ropsten test network, which is a test blockchain network, was used for deployment. An Application Binary Interface (ABI) and a contract address are formed following the smart contract's successful compilation, and they are copied and used. The contract is then initialized in the NodeJS code using the ABI and contract address, making it possible to call the subsequent methods that were explained. The project as a whole is tested on a local network before the smart contract is released to the Ropsten test network. Users connect to Metamask using the front end of a web browser like Chrome, and whenever a transaction needs to be made that will modify the blockchain or a user-end method needs to be called that will modify the blockchain, a Metamask popup will appear to request permission and display the gas price that will be used to execute the transaction. Accessing data stored on the blockchain is free, but gas fees are incurred only when altering data. Each time that any user changes the state of the blockchain, a gas fee in Ether has to be paid. The time taken by the transaction is inversely proportional to the gas price entered by the user. Sometimes, the transaction can be canceled, too. When the DApp loads, a contract instance is created and gets stored in the state of that particular React class component, which gets passed to its child components, and the contract methods can be used from there.

The successful execution of our blockchain-based seed supply chain proved to be an effective strategy for reducing the need for middlemen in the seed distribution process. The gas fees paid for transactions are significantly less than the charges in the current system and may be further optimized by using better smart contracts. The implementation successfully provides the proof of concept that a decentralized solution can be used for seed distribution. The proposed system is faster and provides traceability and immutability at a reasonable cost. Every action on the blockchain that involves adding new data requires a transaction and comes with a small transaction cost called a gas fee, and it is imperative when considering the running costs for the widespread and prolonged functionality of a fundamental system like the proposed one. Figure 13 depicts the gas fees used for our implementation.



https://remix.ethereum.org

CONTRACT DEPLOYMENT

Estimated gas fee 0.00463417
0.004634 GoerliETH

Site suggested
Very likely in < 15 seconds
Max fee: 0.00463645 GoerliETH

Total 0.00463417
0.00463417 GoerliETH

Amount + gas fee
Max amount: 0.00463645 GoerliETH

Figure 13. Example of the gas fees paid.

5.5. Feature Analysis

This section delves into the characteristics of the proposed system. Table 2 highlights the distinctions between the proposed approach and the existing framework.

1. Decentralization: The proposed workflow transforms the functionality of each entity involved in the supply chain, as there is no single authority that holds data centrally and can manipulate them to an extent that harms anyone in the chain. Blockchain embedding in the existing procedure enables a decentralized procedure for storing relevant data on the chain, such as FCI-approved seeds in the form of a minted token, and the transaction records of the purchases carried out by the farmer.

2. Accountability: The notion of updating the status in real time by triggering an appropriate function in a smart contract enables us to identify the responsible entity in the supply chain as accountable and hence figure out where the process is halted in order to optimize the operations of the chain in the near future.
3. Transparency: After ordering seeds, a farmer can track his or her order in real time, which ensures that no foul play is possible and that the farmer does not have to worry about his or her order getting misplaced, as the responsible entity can be tagged very easily.
4. Immutability: All data written to a blockchain are permanent, and hence, even a minor modification to the data can drastically change the hash of the next block, which will disrupt the entire chain. Since a purchase transaction between a government entity, i.e., the warehouse, and the farmer is recorded onto the chain in a similar fashion, it ensures that the record of the transaction is non-disputable and can be considered legally binding by both parties.
5. Security: Modifiers in smart contracts like "onlyFCI" ensure restricted access to calling functions, which enhances security, and most of the payable functions can only be called via the owner address, which means that the contract cannot be modified; unauthorized access is only possible if a person steals the Metamask wallet of the government entity that deploys the contract, i.e., the Food Corporation of India. Further, the blockchain provides the contents of all transactions in an encrypted format, due to which the personal data submitted are anonymous.
6. No middlemen: Middlemen are largely responsible for causing corruption in the supply chain, as they have the capability of modifying transactions to create a shortage of products in the warehouse. Corruption is eliminated because all of the processes are automated and the transactions are recorded, due to which modification is restricted.
7. Trust-less: Since the existing system comprises multiple parties, to ensure a convenient system where everyone can work, smart contracts are deployed, establishing mutual trust among all entities by ensuring that different entities interact with each other without the need to trust each other.
8. Auction-driven Transportation Tenders: Tenders for the transportation of seeds are auctioned, and transporters are granted tenders on the basis of their priorities for the location loc where they operate, their $CIBIL$ score, and the $price$ they code. Thus, the monopoly of transporters in the system is prohibited, and the proposed system provides equal opportunity for each transporter to participate in tendering.

Table 2. Comparison between existing and proposed techniques: "-" denotes absence of feature, and "✓" denotes presence of feature.

Features	**Existing**	**Proposed**
Decentralization	-	✓
Accountability	Low	High
Transparency	Low	High
Immutability	-	High
Security	Low	High
Middlemen	Yes	No
Trust-less	Low	High
Fair Tenders	Low	High
NFT-Driven Seed Approval	-	✓

5.6. Security Analysis

Blockchains are open to the 51% attack. If, somehow, an individual or entity gains control over 50% of the computational power of the blockchain, the attacker can prevent new transactions or cause double-spending issues when in control of the network. Although previous transactions remain immutable, changing anything will lead to a mismatched hash and the disruption of the whole blockchain.

Decentralized systems like blockchain require extensive computational resources and are usually accompanied by huge power draws. As we move toward a more energy-conscious future, unless there is an advancement in clean energy generation and transfer, this will remain a limitation of this proposal. Also, there are huge setup and development costs, but these may be justified by the system's minimal fraud and secure transfers.

A highly technical system that also encompasses a paradigm shift may be challenging to general users, and as most of India is just coming online, it may be prudent to expect all of the people to be technically inclined enough to understand the workings of systems like this. This means that the existing system may be required to remain functional for a long time, which introduces financial constraints.

The digitization of the existing seed supply chain plays a very crucial role in the agriculture system. Without the digitalization of entire records corresponding to seeds, farmers, and transporters, it may be difficult to reap the actual benefits of this system. This also brings more responsibility to system administrators for digital verification, which does not bode well with the current systems and the powers they enjoy. There is no leeway for fraud in cryptographically safe digital signatures, but there is a chance that these officers might abuse their power even further, which will need to be checked. The quality of the records uploaded to the blockchain needs to be high to ensure proper functioning. There may be some initial hesitancy to move over to a digital ownership paradigm, too.

Cryptocurrencies and decentralized payment systems do not offer a stable currency like a fiat currency, at least not yet. The adoption of crypto has been quite nimble in recent times but is still questionable for future aspects. There are no regulatory decisions regarding this, which also makes it a little uncertain.

6. Conclusions and Future Work

In this article, we propose a blockchain-based seed supply chain system using the Ethereum blockchain, with the goal of achieving a transparent and fair bidding mechanism for transporters. In addition, the proposed system is immutable and removes the need for middlemen. The proposed system was implemented using Solidity and deployed on the Ethereum mainnet, while the front end was designed by leveraging React. In addition, our proposed system employs non-fungible tokens for breeders corresponding to their approved seeds, which enables the traceability of seeds by farmers. Thus, the scheme is best suited for a practical seed supply chain system.

Future research can explore opportunities to enhance the system's interoperability with other blockchain networks or traditional systems used in the seed supply chain industry. This could involve developing standards or protocols for data exchange and communication between different blockchain platforms or integrating with existing industry standards and protocols.

Author Contributions: Conceptualization, R.A., S.C. and R.S.; methodology, S.C.; software, R.A.; validation, R.A. and R.S.; formal analysis, R.A., S.C. and R.S.; investigation, R.A.; resources, R.A.; data curation, S.C. and R.A.; writing—original draft preparation, S.C.; writing—review and editing, R.A. and R.S.; visualization, S.C.; 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. GOI. Indian Seed Sector. 2022. Available online: https://seednet.gov.in/material/IndianSeedSector.htm (accessed on 11 December 2022).
2. 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.
3. Tribis, Y.; El Bouchti, A.; Bouayad, H. Supply chain management based on blockchain: A systematic mapping study. In *MATEC Web of Conferences, Proceedings of the International Workshop on Transportation and Supply Chain Engineering (IWTSCE'18), Morocco, 8–9 May 2018*; EDP Sciences: Paris, France, 2018; Volume 200, p. 00020.
4. Maslove, D.M.; Klein, J.; Brohman, K.; Martin, P. Using blockchain technology to manage clinical trials data: A proof-of-concept study. *JMIR Med. Inform.* **2018**, *6*, e11949. [CrossRef] [PubMed]
5. Iansiti, M.; Lakhani, K.R. The truth about blockchain. *Harv. Bus. Rev.* **2017**, *95*, 118–127.
6. Manski, S. Building the blockchain world: Technological commonwealth or just more of the same? *Strateg. Chang.* **2017**, *26*, 511–522. [CrossRef]
7. Dayana, D.; Kalpana, G. Survey on agri-food supply chain using blockchain. In Proceedings of the 2021 Fifth International Conference on I-SMAC (IoT in Social, Mobile, Analytics and Cloud) (I-SMAC), Palladam, India, 11–13 November 2021; pp. 1619–1626.
8. Vukolić, M. The quest for scalable blockchain fabric: Proof-of-work vs. BFT replication. In Proceedings of the Open Problems in Network Security: IFIP WG 11.4 International Workshop, iNetSec 2015, Zurich, Switzerland, 29 October 2015; Revised Selected Papers; Springer: Berlin/Heidelberg, Germany, 2016; pp. 112–125.
9. Kaijun, L.; Ya, B.; Linbo, J.; Han-Chi, F.; Van Nieuwenhuyse, I. Research on agricultural supply chain system with double chain architecture based on blockchain technology. *Future Gener. Comput. Syst.* **2018**, *86*, 641–649.
10. Dayana, D.; Kalpana, G. Augmented system for food crops production in agricultural supply chain using blockchain technology. *Int. J. Adv. Comput. Sci. Appl.* **2022**, *13*, 579–589. [CrossRef]
11. Chang, Y.; Iakovou, E.; Shi, W. Blockchain in global supply chains and cross border trade: A critical synthesis of the state-of-the-art, challenges and opportunities. *Int. J. Prod. Res.* **2020**, *58*, 2082–2099. [CrossRef]
12. Yadav, V.S.; Singh, A.R.; Raut, R.D.; Govindarajan, U.H. Blockchain technology adoption barriers in the Indian agricultural supply chain: An integrated approach. *Resour. Conserv. Recycl.* **2020**, *161*, 104877. [CrossRef]
13. Sharma, S.K.; Singh, V. Digitization of the food industry enabled by Internet of Things, blockchain, and artificial intelligence. In *Current Developments in Biotechnology and Bioengineering*; Elsevier: Amsterdam, The Netherlands, 2022; pp. 421–445.
14. Sanka, A.I.; Irfan, M.; Huang, I.; Cheung, R.C. A survey of breakthrough in blockchain technology: Adoptions, applications, challenges and future research. *Comput. Commun.* **2021**, *169*, 179–201. [CrossRef]
15. Kawaguchi, N. Application of blockchain to supply chain: Flexible blockchain technology. *Procedia Comput. Sci.* **2019**, *164*, 143–148. [CrossRef]
16. Morris, M.L.; Bellon, M.R. Participatory plant breeding research: Opportunities and challenges for the international crop improvement system. *Euphytica* **2004**, *136*, 21–35. [CrossRef]
17. Chiurugwi, T.; Kemp, S.; Powell, W.; Hickey, L.T. Speed breeding orphan crops. *Theor. Appl. Genet.* **2019**, *132*, 607–616. [CrossRef] [PubMed]
18. Vertical coordination in agri-food supply chain and blockchain: A proposed framework solution for Vietnamese cashew nut business. *Reg. Sci. Policy Pract.* **2024**, *16*, 12576.
19. Albaaji, G.F.; Chandra, S. Blockchain technology in agriculture: Digitizing the Iraqi agricultural environment. *Environ. Dev. Sustain.* **2024**, 1–12. [CrossRef]
20. Bansal, A.; Tewari, A.; Sharma, A.; Bansal, A. Implementations and Rationale for Blockchain Technique in Agriculture. In *Applications of Computer Vision and Drone Technology in Agriculture 4.0*; Springer: Berlin/Heidelberg, Germany, 2024; pp. 83–92.
21. Patel, H.; Shrimali, B. AgriOnBlock: Secured data harvesting for agriculture sector using blockchain technology. *ICT Express* **2023**, *9*, 150–159. [CrossRef]
22. 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]
23. van Ginkel, M.; Ortiz, R. Cross the best with the best, and select the best: HELP in breeding selfing crops. *Crop. Sci.* **2018**, *58*, 17–30. [CrossRef]
24. Nakamoto, S. Bitcoin: A Peer-to-Peer Electronic Cash System. 2009. Available online: https://metzdowd.com (accessed on 3 March 2024).
25. Khan, S.; Loukil, F.; Ghedira, C.; Benkhelifa, E.; Bani-Hani, A. Blockchain Smart Contracts: Applications, Challenges, and Future Trends. *Peer-Peer Netw. Appl.* **2021**, *14*, 2901–2925. [CrossRef] [PubMed]
26. 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 Proceedings of the 16th International Conference, MIWAI 2023, Hyderabad, India, 21–22 July 2023; Springer: Berlin/Heidelberg, Germany, 2023; pp. 265–276.
27. Rehal, M.; Ahuja, R.; Gandhi, D.; Sharma, A. A Blockchain-Based Custom Clearance Solution for International Trade Using IPFS and Non-fungible Tokens. In Proceedings of the International Conference on Data Analytics & Management, London, UK, 23–24 June 2023; Springer: Berlin/Heidelberg, Germany, 2023; pp. 551–564.

28. Singh, P. Role of Blockchain Technology in Digitization of Land Records in Indian Scenario. *IOP Conf. Ser. Earth Environ. Sci.* **2020**, *614*, 012055. [CrossRef]
29. Thakur, K.S.; Ahuja, R. Safeguarding Justice Employing Blockchain-Enabled Secure Chain of Custody Framework for Digital Evidence. In *International Conference on Electrical and Electronics Engineering, Proceedings of the The 4th International Conference on Electrical and Electronics Engineering (ICEEE), Chitkara University, Himachal Pradesh, India, 19–20 August 2023*; Springer: Berlin/Heidelberg, Germany, 2023; pp. 1–11.
30. Khan, R.; Ansari, S.; Sachdeva, S.; Jain, S. Blockchain based land registry system using Ethereum Blockchain. *Xi'An Jianzhu Keji Daxue Xuebao/J. Xi'An Univ. Archit. Technol.* **2020**, *12*, 3640–3648.

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.