# PROJECT REPORT

# Agriculture Docs Chain

|  |  |
| --- | --- |
| **Date** | **28 October 2023** |
| **Team ID** |  |
| **Project Name** | **Agriculture Docs Chain** |

**TEAM MEMBERS**

|  |  |
| --- | --- |
| **A.HARISH** | **814620114002** |
| **M.AYYAPPAN** | **814620114001** |
| **A.PRASANTH** | **814620114004** |
| **N.MERGIN** | **814620114314** |

# ABSTRACT 1. INTRODUCTION

* 1. Project Overview
  2. Purpose

# LITERATURE SURVEY

* 1. Existing problem
  2. References
  3. Problem Statement Definition

# IDEATION & PROPOSED SOLUTION

* 1. Empathy Map Canvas
  2. Ideation & Brainstorming

# REQIREMENT ANALYSIS

* 1. Functional Requirement
  2. Non-Functional Requirements

# PROJECT DESIGN

* 1. Data Flow Diagrams
  2. Solution Architecture

# PROJECT PLANNING & SCHEDULING

* 1. Technical Architecture
  2. Sprint Planning & Estimation
  3. Sprint Delivery Schedule

# CODING & SOLUTIONING

* 1. Feature 1
  2. Feature 2
  3. Database Schema

# PERFORMANCE TESTING

* 1. Performance Metrics

# RESULTS

* 1. Output Screenshots

# 10.ADVANTAGES & DISADVANTAGE

# 11.CONCLUSION

# 12.FUTURE SCOPE

**13.APPENDIX**

Source Code

GitHub & Project Demo Link

# ABSTRACT

Blockchain can be used to create a tamper-proof and traceable record of various agricultural documents and transactions, such as supply chain data, crop certifications, and more. This can help improve transparency, reduce fraud, and enhance trust in the agricultural industry. Blockchain technology has emerged as a game-changer in the agricultural sector, revolutionizing the way data is managed, shared, and secured. This abstract explores the application of blockchain in agriculture, highlighting its potential to enhance transparency, traceability, and trust within the food supply chain. We discuss the key benefits, challenges, and real-world use cases of blockchain in agriculture, shedding light on how this innovation is reshaping the industry and ensuring the safety and authenticity of agricultural products from farm to fork. This overview provides valuable insights into the pivotal role that blockchain plays in modernizing and securing the agricultural ecosystem. Discuss the advantages of using blockchain, such as data integrity, security, and decentralization.Explain how blockchain can enable real-time tracking of agricultural products, reducing the risk of contamination and fraud. Start by introducing the concept of blockchain technology and its relevance in the agricultural sector.Mention the increasing need for transparency and trust in the agricultural supply chain.

# Introduction

# An Agriculture Document Chain, often referred to as a "Farm-to-Fork" or "Seed-to-Table" document chain, is a comprehensive system that leverages blockchain technology and other digital tools to enhance transparency, traceability, and efficiency in the agricultural industry. This innovative approach brings together various stakeholders in the agricultural ecosystem, including farmers, suppliers, distributors, retailers, and consumers, to create a secure and transparent network of information and transactions. Here's an introduction to the concept of an Agriculture Document Chain. It is a critical industry that impacts food security, environmental sustainability, and the livelihoods of billions of people worldwide. However, it faces challenges such as food fraud, supply chain inefficiencies, and a lack of transparency. An Agriculture Document Chain seeks to address these issues by digitally documenting and verifying every step of the agricultural process.The core technology behind an Agriculture Document Chain is blockchain. Blockchain is a decentralized and immutable ledger that records transactions in a secure and transparent manner. It ensures that data cannot be altered or deleted, providing trust and accountability throughout the agricultural supply chain.

# Blockchain Technology in Agriculture:

# Decentralized Ledger:

# Blockchain is a distributed ledger that records transactions in a decentralized and secure manner. This ledger is maintained by a network of nodes (computers), which adds transparency and trust to the data.

# Immutable Records:

# Once data is recorded on the blockchain, it becomes virtually impossible to alter or delete, ensuring the integrity of the information.

# Smart Contracts:

# Smart contracts are self-executing agreements with the terms of the contract directly written into code. In agriculture, they can automate various processes, such as payment upon delivery, quality verification, and compliance with regulations.

# Transparency:

# Participants in the ADC network have access to the same data in real-time, enhancing transparency and trust throughout the supply chain.

# Digital Identity:

# Each participant, whether it's a farmer, distributor, or consumer, has a unique digital identity on the blockchain, which allows for the traceability of products and actions.

# Key Components:

# Smart Contracts:

# These self-executing contracts automate various processes in agriculture, such as payment, quality control, and compliance verification.

# Digital Identity:

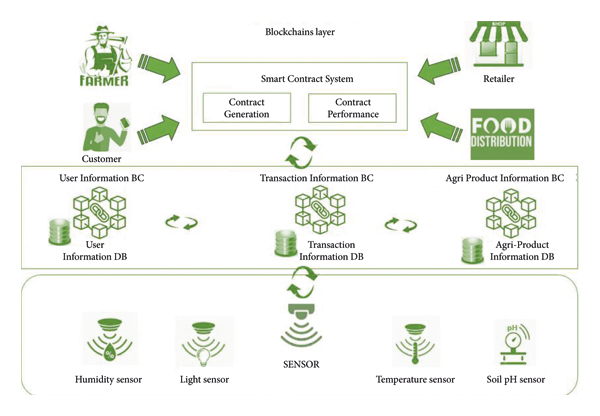
# Each participant in the chain has a unique digital identity, enabling the traceability of products and actions.

# Data Recording:

# Data about crops, farming practices, transportation, and more are recorded in a tamper-proof manner on the blockchain.

The future of Agriculture Document Chains looks promising, with the potential to revolutionize the agricultural industry. It can help address issues like food fraud, reduce waste, improve sustainability, and provide consumers with greater confidence in the safety and quality of the food they consume. Furthermore, it can contribute to the development of "smart agriculture" by enabling data-driven decision-making and automation in the field.In summary, Agriculture Document Chains are a specific application of blockchain technology tailored to the needs of the agriculture industry. They offer a transformative approach to increasing transparency, efficiency, and trust throughout the agricultural supply chain, benefiting all stakeholders from farmers to consumers.

The high-value data gathered by applying machine learning is stored in IPFS (Interplanetary File System), a distributed storage platform with addresses hashed and stored on the blockchain.The existing method of storing essential information in the centralized server has a risk of a single point of failure. However, with blockchain, the data is distributed across every node in the network. Hence, it prevents a central authority to control the system.The information captured in the blockchain will trigger smart contracts to process rules defined within them. Smart contracts facilitate the exchange of data stored on the blockchain with the specific stakeholders in the system. Since information will be visible to every agriculture market participant, it will become seamless to bring efficiency in crop or food production.



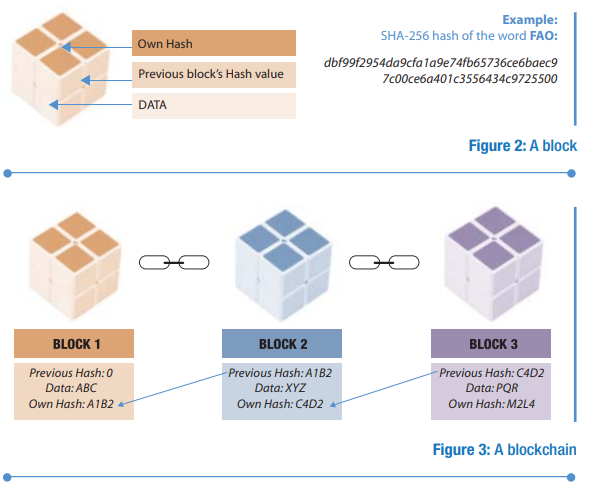
## Crop and Food Production

While improving profitability under unfavorable environmental conditions, the agriculture sector has many challenges to overcome, such as:

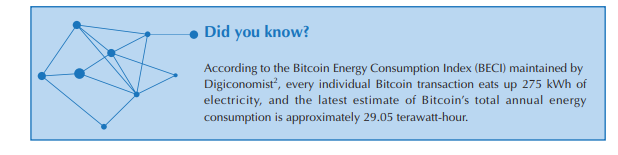
* catering to the needs of the increasing population by growing more food with minimal resources
* reducing environmental footprint
* maximizing customer satisfaction
* enabling transparency across the supply chain
* ensuring fair income to farmers
* handling weather fluctuations

**The blockchain basis :**

The blockchain basis In the simplest terms, a blockchain consists of a linked chain that stores auditable data in units called blocks. Many commentaries online start by explaining that a blockchain is similar to a Google document spreadsheet where multiple authors can contribute because of the mechanism of locking. Blockchain is a bit more complex than that example and has unique characteristics that make it an attractive technology for tagging, storing and tracking anything of value. Bitcoin was one of the first and most popular implementations of blockchain technology. To begin, a blockchain consists of blocks, each block containing the data (anything of value), its own hash value (a unique cryptographic value containing characters and numbers generated through a complex computational algorithm) and a pointer to the hash of the previous block. Figure 3: A blockchain E



The consensus algorithm forms one of the key mechanisms in the creation of new blocks and appending them to the blockchain. The most discussed algorithms are proof-of-work (PoW), proof-of-stake (PoS), and proof-of-authority (PoA). Blockchain uses a PoW consensus model, in which a node gets the right to publish the next block by solving a computationally intensive puzzle. The result of the computation is easy to verify and thus helps other nodes to validate and update the blockchain easily. The node that solves the computational puzzle wins the “reward” and this process is called “mining”. Because this is time and energy intensive, other alternative methods of verifying a block, such as proof-of-stake, have been developed and implemented in subsequent spin-offs. Unlike in proof-of-work, the proof-of-stake takes away the energy and computational overheads and replaces it with a stake. The chances of a node to be the creator of the next block depends on the stake that the node is willing to lock up for a certain amount of time. However, the drawback of the PoS model is that “rich” nodes can easily put more digital assets at stake thereby earning themselves the right to create the next node and earning more assets. Delegated PoS (DPoS), built on the PoS model takes a slightly different approach in that the nodes vote to elect delegates to do the validation on their behalf. Each algorithm has its own characteristics regarding incentive/reward, requirements as well as energy cost.



**Smart contracts**

Smart contracts Smart contracts are self-executing agreements that are triggered on the basis of predefined and agreed events (for example rainfall of more than 200 mm, market price of commodity more than USD 100). The “smart” in a smart contract comes from the fact that the clauses in the contract are evaluated and the appropriate code executed without human intervention. Settlements in smart contracts are automatically triggered if the pre-agreed conditions coded into the contract are met. Imagine something along the lines of the automatic debit used by merchants to take payment from your bank account, based on pre-agreed conditions (full payment, part payment, minimum amount etc.) on a pre-agreed day or date (first Wednesday of the month, every 10 May etc.). A key link between the physical world and blockchain is an oracle. This is a trusted intermediary and an integral part of the smart contract ecosystem and facilitates data feeds to the blockchain ecosystem. By design, a blockchain cannot access data from outside its system and thus data to make the blockchain is supplied through a predefined entity called an oracle. An oracle can be hardware-based, software-based, or consensus-based. Examples of hardware oracles are sensors, IoT and weather stations. Examples of software oracles are a New York Stock Exchange index, expiration date, output of some computation, etc. A consensus-based oracle works on the basis of consensus from a group of predefined nodes on a particular question. A consensus-based oracle can also source data from several other oracles to trigger an event in a smart contract. Moreover, inbound oracles pass external data to smart contracts and outbound oracles communicate smart contract-based data to the outside world. Ethereum is the first blockchain. Ethereum is the first blockchain platform that focuses on providing a Turing-complete3 smart contracts-based system and decentralized applications. Hyperledger Fabric and R3 Corda are some of the other DLTs that are used to create smart contracts.

# The Research

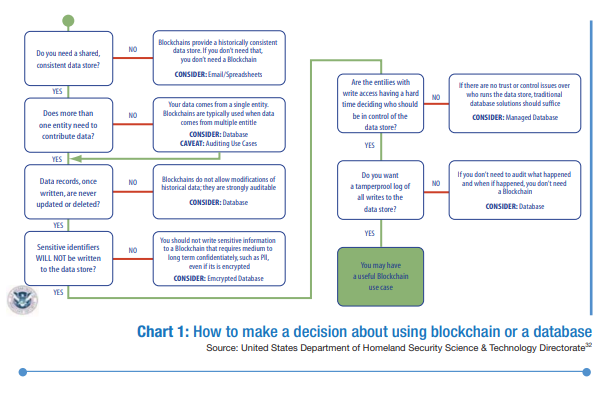
All old concepts are in service of the suggested theoretical architecture (see Figure [2).](file:///C:\Users\win%2010\Downloads\Project%20Report.docx#_bookmark1) It is a multi-layer design, which is the cause why it will be easier to control. The Internet of Things (IoT) layer is the ﬁrst. It consists of essential sensors like humidity, temperature, pressure, acceleration, and other variables connected to ARDUINO boards. Bluetooth or a wireless network is used to communicate between the de- vices. The Arduino features will provide us with data, which will be exploited in the subsequent layers. The ﬁrst layer can supply us with reliable environmental data.The blockchain layer contains three particular block- chains, and the agri-product information blockchain is the ﬁrst. The user information blockchain is the second one. It has all the information about the network participants.

The transaction information blockchain is the last one on the list. It holds a wealth of information, including user personal information, intermediate information, transac- tions, logistics, and agricultural product data. Smart con- tracts are used in this paradigm. Those automated contracts use the highest level of data encryption currently available in the security industry. As a result, it will conﬁrm the quality of the decision and guarantee clarity and eﬀective communi- cation between entities [.](file:///C:\\Users\\win%2010\\Downloads\\Project%20Report.docx" \l "_bookmark37)

Many sides will attempt to check the average transaction fees because the whole system comprises a multi-blockchain system. But let us see the other meaning of the blockchain model. The suggested architecture concurrently distributes secure data to all network participants. It is regarded as signiﬁcant advantage that can increase the eﬃcacy agri- cultural system.

The block will be full of transactions containing recorded data, and we will get multiple veriﬁed transactions at once. Combining numerous transactions into a single block each period is cost and space-eﬃcient. So, batching allows for reducing per-transaction fees by aggregating various transactions into one. Following this protocol beneﬁts you and keeps the fees low across the board for everyone. We can use cryptocurrencies for frequent transfers across platforms if we want to add crypto money to our model. Their transaction fees are virtually nothing, for example, Ripple orLitecoin, because generally, cryptocurrencies are con- structed for lowering or eliminating fees.

A careful analysis of the requirements is highly recommended before selecting blockchain as a technology of choice. If high performance is necessary for your application, a relational database, not blockchain, may be the better choice. A way to balance performance issues while leveraging the benefits of blockchain is not to store the full data records in the blockchain but simply to store a cryptographic hash of the record. This will serve to determine with a high level of confidence whether data have been compromised and can resolve any dispute issue. This approach is used, for example, in the case of electronic health records. Failing to make a sound decision might lead to the risk of making an unnecessary high-cost investment. Cost savings from disintermediation, that is by having the network as the trusted party might not balance out the costs to support and maintain a blockchain-based application. A number of flowcharts are available that are used to make this decision. For example, the United States Department of Homeland Security (DHS) uses a flowchart as provided in Chart 1 below.

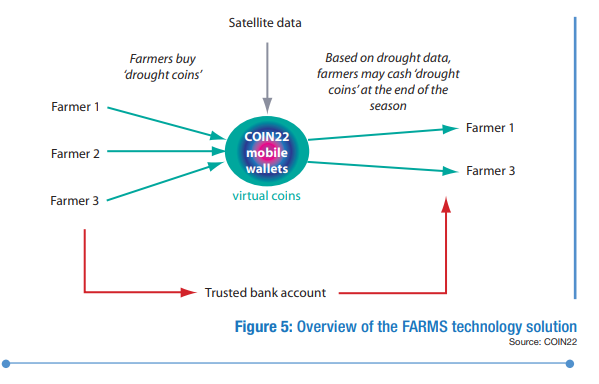


Identity and security:

Public blockchains carry out transactions based on the public and private key of the individual and do not keep the mapping of the identity with the key. This raises security constraints for the law enforcers and applications where identity is important. In contrast, there are privacy concerns in disclosing identity on permissionless blockchains that require data to be public facing and transaction histories to be disclosed. Most DLTs use encryption algorithms that are hard to break by normal non-quantum computers. Going forward, where quantum computing (relying on cubits rather than bits) gains momentum and enhances computing powers, these encryptions are not secure enough. There have been a large number of successful attacks on DLTs and there are security risks associated with DLTs (e.g. blockchain attacks, phishing, malware, cryptojacking, endpoint miners, implementation vulnerabilities, wallet theft, technology attacks, legacy attacks which have been modernized, dictionary attacks, quantum computing-based attacks).

**3.Testing and Analysis**

Since 2016, AgriDigital has pioneered, non-commercially so far, the use of blockchain across agricultural supply chains. Conducting the world’s first proof-of-concept (PoC) algorithm with leading agricultural businesses, AgriDigital has deep domain expertise in blockchain technology and applies blockchain and related technologies to solve the embedded agri-supply chain challenges. The company operates primarily along grains supply chains. As its founders have over 80 years combined experience in the Australian grains industry, this was the natural first market. AgriDigital is expanding rapidly into the global grains industry, and across commodities with initial trials underway in the rice and cotton industries. AgriDigital has a cloud-based commodity management solution in marketing for the global grains industry. It connects grain farmers, buyers, site operators and financiers through a single platform, allowing them to contract, deliver and make payments securely and in real time. Although the AgriDigital platform is cloud based, it is also blockchain enabled, meaning it acts as a user interface with the blockchain protocol layer. With the launch of a commercial blockchain protocol for agriculture, the AgriDigital platform will operate as the primary application layer for users to interact with the blockchain. The company has developed a library of smart contracts operating on the blockchain protocol, allowing users to trade, finance and trace agri-commodities. At the core of AgriDigital’s solution is the creation of digital assets. Using digital assets, AgriDigital brings together the trade, finance and data flows that are often disparate in traditional, paper based agri-supply chains. This provides users with a more informed and robust view of their assets and the supply chain, and improves liquidity, transparency and security for all supply chain participants including farmers, traders, producers, financiers and consumers. The company is dedicated to building a robust digital infrastructure that connects the physical commodity to the digital representation at every stage along the supply chain. In doing so, AgriDigital uses the Internet of things, sensors and integrations with machinery such as weighbridges wherever possible. AgriDigital is an Australian company based in Sydney. The company’s blockchain solution has been trialed at a number of locations across Australia including Dubbo in New South Wales and Bordertown in South Australia. The customers are grain farmers, buyers, site operators and financiers. The initial target market for the company’s commodity management solution is the global grains industry. However, the blockchain solution is designed to operate for a full range of commodities and the company works across grain, rice, cotton and livestock. 26 The company has worked closely with a number of major participants in Australian agriculture to test the blockchain protocol and the smart contract library. These include: Fletchers International Exports; CBH Group, Australia’s largest exporter of grain; and Rabobank, the largest global agri-bank. AgriDigital’s award-winning SaaS34 platform has a network of 1,300 active grain supply chain users with a broader network of over 4 500 total users. To date, over 1.6 million metric tons of grain have been transacted by these participants on the AgriDigital platform (since November 2016). These users will be transitioned to using the blockchain protocol once it is launched commercially. AgriDigital was founded in 2015 with a vision to solve three key challenges across agri-supply chains: 1. farmers are not paid for the commodities they produce when they deliver them; 2. buyers don’t have access to flexible supply chain finance to pay farmers, as financiers lack visibility and control when financing commodities; and 3. consumers don’t really know where their food and fibres come from thus restricting their ability to make informed purchasing abilities. Buyers and sellers along agri-supply chains cannot operate with confidence, knowing that they will be paid and can access the finance necessary for business stability and growth. This finance is often limited to highly reputable borrowers with bricks and mortar security, and is often only accessible for commodities where the risk price can be hedged. This results in settlement latency, with title transferring months before payment is made. This introduces enormous counterparty risk that most often falls on the producer at the start of the supply chain. Supply chain participants are vulnerable to fraud, with global food fraud costing USD 40 billion annually and global trade in fake goods accounting for a staggering USD 500 billion annually. Without verifiable and data rich assets, counterfeit goods move in large quantities across supply chains. The real cost of this to the end consumer is abundantly evident, with food security a growing issue. Indeed a number of high profile food contamination cases have had global impacts. AgriDigital is addressing these challenges by providing a digital infrastructure that brings trust and transparency to supply chain participants. The company started with the first transaction along many supply chains, with the sale from the farmer to the buyer. Blockchain technology was immediately identified as a tool for building creative and innovative solutions to solve these problems. However, blockchain is only a piece of a larger digital infrastructure, one that allows users to easily access the protocol layer and that ensures the information that is recorded truly represents the state of the physical commodity in the real world.

****

# 4.Performance Evaluation

The ﬁrst issue users have represented in transaction latency is the delay between initiating a transaction or payment and receiving conﬁrmation that it is valid. You would anticipate a ﬂattening of the throughput once all users have logged in, begun to work, and sent requests. In our case, however, we have not added cryptocurrency-based ﬁnancial transactions yet, and the project’s goal is to simultaneously receive data from sensors and send it to the blockchain network. Hence, the automated system of smart contracts helps data arrive in any case and in good time for analyses. With minimal competition, throughput varies by simply adjusting the load while latency remains constant. The reason is that whatever comes in comes out directly since there is a reasonable minimum cost to complete a transaction, and the queuing time is zero at low congestion.Every newly formed block has a timestamp. The blockchain system uses timestamps to count the number of blocks added and produced during speciﬁc time intervals, such as per hour. The transaction latency metric can be calculated by looking up each transaction’s timing and comparing the time it got completed to the time it was approved and saved. This measure can also reveal the speed at which consensus methods got used. The outcomes of these tests provide evaluations of the blockchain system’s func- tionality and scalability.

A 3.5 GHz CPU device with 32 GB RAM and a 3 TB hard drive will execute the model (Ethereum blockchain network—8 nodes) with a margin of 100–120 seconds for latency and a margin of 235–260 transactions per second (TPS) for throughput. Data must wait to get transferred when the local network’s capacity gets exceeded by traﬃc. Naturally, there will be more delay as a result. The latency will increase as the network becomes more crowded and we have many activities simultaneously. However, solid wireless signals make it possible for data to be transported from the source to the destination within a short period and decrease latency. Adding more controllers or validators who conﬁrm blockchain transactions may boost performance.

The analyzers must measure a large-scale distributed system to identify obstacles or blockages and predict ex- pected behavior under pressure.

*4.1. Security Analysis.* Now we will go on to the security analysis part, where we will list all of the model’s compo- nents and discuss how they can provide security services and how they operate together to secure our data and deliver accurate information to all network members.

Smart contracts, apps, and the blockchain environment are vulnerable to attacks if the model gets weakly built. Let us start with the blockchain-based system, a public ledger of data kept on all nodes, with all participants receiving the same version of information and updates in real time as data changes. Furthermore, users authenticate using public-key cryptography, and validators check the data for accuracy before storing them in blocks; thus, all data transactions ought to have acceptance from all nodes in the network. Finally, once transactions get preserved in blocks, no one or entity may edit or alter the block’s content.

The level of security in the blockchain scheme is in- triguing, but let us now discuss smart contract security, which is more than simply a software program that gets run automatically. It is a part of the system. In our example, it can receive, transmit, and store data about the environment, such as temperature, humidity, light, and soil pH. It can also track down the merchandise and determine which company owns it. We must not forget that smart contracts specify the extent of an agreement between business parties by deﬁning criteria that function as a trigger event in the contractual terms. The code gets performed, and the results get displayed on all of the network’s nodes. Smart contracts get written conditionally, using if-then expressions, and thus neglect many of the problems caused by regular agreements, such as fraud. The use of blockchain to establish these types of arrangements eliminates the need for an intermediary. As a result, the total expenditures of the company get reduced. To prevent losses, professionals make timely code optimiza- tions, conduct frequent code audits, and monitor the ab- errant behavior of implemented deals.

Unless you install protection, IoT devices might be the

weakest link in terms of security. For example, the IoT confronts fake cell tower assaults and threats such as man- in-the-middle attacks and SMS attempts such as phishing. Blockchain technology has been a remarkable example of providing safety in transactions and information transfer. It oﬀers a unique data structure in addition to integrated se- curity measures. Consensus, decentralization, and cryp- tography—which ensure the trust of transactions—are the

foundations of the blockchain.

However, poor technical implementation has led to several security vulnerabilities with blockchain. Although blockchain has signiﬁcant security ﬂaws, cyber security experts with special analytical and technical skills may take some steps to minimize these problems and implement blockchain in the safest possible way. Although the sug- gested approach may not stop these attempts, it makes it diﬃcult for hackers to carry them out.

A 51% assault happens when one person or group of hackers gather more than half of the hash rate and takes over the entire system, which may be fatal for blockchains that handle ﬁnancial transactions. In this case, hackers can alter transactions and stop the veriﬁcation process. In sequence, the entire model will not add the transactions to the blocks. The attackers can even undo already ﬁnished transactions, which leads to double-spending. Thankfully, by increasing the hash rate and reducing the usage of proof-of-work techniques, we can avoid 51% assaults. The results conclude that this particular threat does not beneﬁt the attacker itself because the main goal of the suggested agricultural model is to organize farm environmental data, distribute it to all network participants, and provide a layer of security and conﬁdentiality to these data.

Phishing attacks are seriously impacting blockchain

networks. The purpose of a phishing attack is for the hacker to obtain the user’s login information. To the owner of the wallet key, they may send emails that appear to be honest. The user must enter their login information into a false hyperlink that is connected. A user’s passwords and other sensitive information may be compromised, which may cause harm to both the individual and the blockchain network. If blockchain network members get an e-mail asking for login information, they must conﬁrm with the partner (other members, for example). Additionally, in- stalling malicious link detection software might aid in defending against this threat. We can point out that con- necting to the blockchain through public Wi-Fi could be risky.

Routing attacks, for example, are attacks when a hacker

uses the anonymity of a user account to intercept data as they get sent to Internet service providers. Data transfer and activities continue as usual in the case of a routing attack, so the participants are typically oblivious to the threat. How- ever, establishing a secure routing protocol will solve this issue. The users of the network must use strong passwords and update them often. In practice, some farms are pretty likely to adopt this architecture, and there is a critical need to notify every blockchain participant of the risks related to data security.

Users connect with the blockchain using electronic devices like computers and smartphones, which are the endpoints of the blockchain network. Hackers can target devices and monitor user activity to obtain the user’s key. The participants should not save blockchain keys on com- puters as text ﬁles by network users. Identifying dangers and securing the device include installing antivirus software.

Hackers could consider creating plenty of phony net- work nodes (Sybil attack). They can gain majority consensus and stop the chain’s transactions using this technique. Massive Sybil strikes implied a 51% attack.

# 5.Conclusion and Future Work

# In conclusion An Agriculture Document Chain has the potential to revolutionize the agricultural industry, making it more sustainable, accountable, and responsive to consumer needs. It can also contribute to the development of "smart agriculture" by enabling data-driven decision-making. An Agriculture Document Chain is a forward-thinking approach to transform the agricultural sector into a more transparent, efficient, and trustworthy ecosystem through the application of blockchain technology and digital tools. This innovation has the power to benefit all stakeholders, from farmers to consumers, by ensuring the integrity and quality of agricultural products from the source to the table.

# Data Availability

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

# Conflicts of Interest

The authors declare that they have no conﬂicts of interest.

# References

**Demo link :**

**Github link :**