ISSN No:-2456-2165

Blockchain Technology-Based Agri-Food Supply Chain System

Vaishnavi Madhave,
Monali Tambe,
Sonal Kale,
Naina Kokate (Professor)
Department of Computer Engineering, Smt.Kashibai Navale College of Engineering, Pune, India
Department of Computer Engineering, Smt.Kashibai Navale College of Engineering, Pune, India
Assistant Professor, Department of Computer Engineering, Smt.Kashibai Navale College of Engineering, Pune, India

Abstract:- Supply chains are turning into automated and extremely complicated networks and are becoming a key source of potential benefits in the modern world. At the same time, people are becoming more interested in food product quality. However, it is tough to identify the provenance of data and preserve its traceability throughout the supply chain network. The old supply chains are centralized and they depend on a third party for transactions. These centralized systems lack transparency, accountability, and audibility. In our proposed solution, we have offered a complete solution for the block-chain based Agriculture and Food (Agri-Food) supply chain. It uses the key characteristics of blockchain and smart contracts, deployed on an Ethereum blockchain network. Although blockchain enables the immutability of data and records in the network, it still fails to solve certain major difficulties in supply chain management the trustworthiness of the involved entities, accountability of the trading process, and the traceability of the items. Therefore, there is a requirement for a dependable system that assures traceability, trust, and delivery mechanism in the Agri-Food supply chain. In the proposed system, all transactions are written to a blockchain which finally uploads the data to Interplanetary File Storage System (IPFS) (IPFS). The storage system returns a hash of the data which is kept on blockchain and ensures an efficient, safe, trustworthy solution. Our solution provides smart contracts together with accompanying algorithms to display the interaction of entities in the system. Furthermore, simulations and assessments of smart contracts together with the security and vulnerability studies are also included in this paper.

***Keywords*:-** *Accountability, Blockchain, Credibility, Reputation, Supply Chain, Traceability, Trust.*

I. INTRODUCTION

It is critical to food quality and safety management that food can be traced back to its origins. It is now an essential aspect of supply chain management to be able to track products and processes through the chain. At the same time, customers are more concerned than ever before with the quality of the food they consume.

A distributed database, a blockchain can be accessed by a network of computers. It is extremely difficult to remove a record from the chain after it has been added. A block is created from the data that the network accepts. There is a unique code in each block called a hash. The previous block's hash is also included in this block.

Transparency, trustlessness, and openness are the hallmarks of "blockchain technology," which refers to a publicly accessible ledger that uses public key encryption and proof of work mechanisms to securely transfer ownership of units of value.

The system relies on decentralized consensus to keep the network running smoothly, thus a bank, corporation, or government has no authority over it. To put it another way, the more the network expands and decentralizes, the more secure it is going to be.

One of the most important features of a blockchain is its ability to encrypt data and make it impossible for anyone to alter it without altering every subsequent block. Individuals and organizations use crowdsourcing to source their products, services, ideas, funds, and other resources from a vast, open, and often fast-growing online community. This strategy distributes work among participants to produce a cumulative outcome.

The term "blockchain technology" refers to the technology that serves as a distributed ledger in which digital transactions are recorded, verified, and validated throughout the network of nodes without the approval of a central authority. To ensure that no single resource dominates the entire system, decentralization is the most critical aspect. Eventually, the problem of a single point of failure can be dealt with and the latency reduced by using all of the resources available to participating nodes in the system. This system's robustness and scalability are ensured by its decentralized design.

II. RELATED WORK

“ New directions in cryptography ” Two kinds of contemporary developments in cryptography are examined. Widening operations of teleprocessing have given rise to a need for new types of cryptographic systems, which minimize the need for secure crucial distribution channels and supply the fellow of a written hand. This paper suggests ways to break these presently open problems. It also discusses how the propositions of communication and calculation are beginning to give the tools to break cryptographic problems of long standing. “ An effective protocol for authenticated crucial agreement ” This paper proposes an effective two- pass protocol for authenticated crucial agreement in the asymmetric(public- key) setting. The protocol is grounded on the Diffie- Hellman crucial agreement and can be modified to work in an arbitrary finite group and, in particular, elliptic wind groups. Two variations of this protocol are also presented a one- pass authenticated crucial agreement protocol suitable for surroundings where only one reality is online, and a three-pass protocol in which crucial evidence is also handed. Variants of these protocols have been formalized in IEEE P1363(17), ANSI X9.42(2), ANSI X9.63(4), ISO 15496-3, and are presently under consideration for standardization and by the U.S. government's National Institute for norms and Technology. “ Identity- grounded fault-tolerant conference key agreement ” Lots of conference key agreement protocols have been suggested to secure computer network conferences. utmost of them operate only when all conferees are honest but don't work when some conferees are vicious and attempt to delay or destruct the conference. lately, Tzeng proposed a conference key agreement protocol with fault forbearance in terms that a common secret conference key among honest conferees can be established indeed if vicious conferees live. In the case where a conferee can broadcast different dispatches in different subnetworks, Tzeng’s protocol is vulnerable to a “ different crucial attack ” from vicious conferees. In addition, Tzeng’s protocol requires each conferee to broadcast to the rest of the group and admit n 1 communication in a single round(where n stands for the number of conferees). also, it has to handle n contemporaneous broadcasts in one round. In this paper, we propose a new fault-tolerant conference key agreement protocol, in which each conferee only needs to shoot one communication to a “semi-trusted" conference ground and admit one broadcast communication. Our protocol is an identity- grounded crucial agreement, erected on elliptic wind cryptography. It's resistant to the different crucial attacks from vicious conferees and needs lower communication cost than Tzeng’s protocol. " Identity-grounded crucial agreement protocol employing a symmetric balanced deficient block design" crucial agreement protocol is a abecedarian protocol in cryptography whereby two or further actors can agree on a common conference key to communicate securely among themselves. In this situation, the actors can securely shoot and admit dispatches with each other. An adversary not having access to the conference key won't be suitable to decipher the dispatches. In this paper, we propose a new identity- grounded authenticatedmulti-user crucial agreement protocol employing a symmetric balanced deficient block design. Our protocol is erected on elliptic wind cryptography and takes advantage of a kind of bilinear chart called Weil pairing. The protocol presented can give an identification(ID)- grounded authentication service and repel different crucial attacks. likewise, our protocol is effective and needs only two rounds for generating a common conference key. It's worth noting that the communication cost for generating a conference key in our protocol is only O(n √ n) and the calculation cost is only O nm2, where n implies the number of actors and m denotes the extension degree of the finite field Fpm. In addition, to repel the different crucial attacks from vicious actors, our protocol can be further extended to give fault-tolerant property.

III. EXISTING SYSTEM

- *The agriculture sector employs nearly half of the pool in the country. still, it contributes to17.5 of the GDP(at current prices in 2015- 16).*
- *Over the once many decades, the manufacturing and services sectors have decreasingly contributed to the growth of the frugality, while the husbandry sector’s donation has dropped from further than 50 of GDP in the 1950s to15.4 in 2015- 16(at constant prices).*
- *Agriculture and the food assiduity are snappily entering the period of platform economics. The rapid-fire development of digital interfaces isn't simply a matter of matching force and demand. cooperative platforms have surfaced alongside commerce, some devoted to finance, others to change services. Professionals are reinventing and rediscovering aged forms of solidarity. Eventually, private individualities are also getting into the game, radically catching everyday practices and rewriting canons.*
- *Cooperative spots, whether marketable or not, form a alternate order of the platform, which puts emphasizes sharing and exchange and in which both druggies and providers are professionals.*

IV. PROPOSED APPROACHES

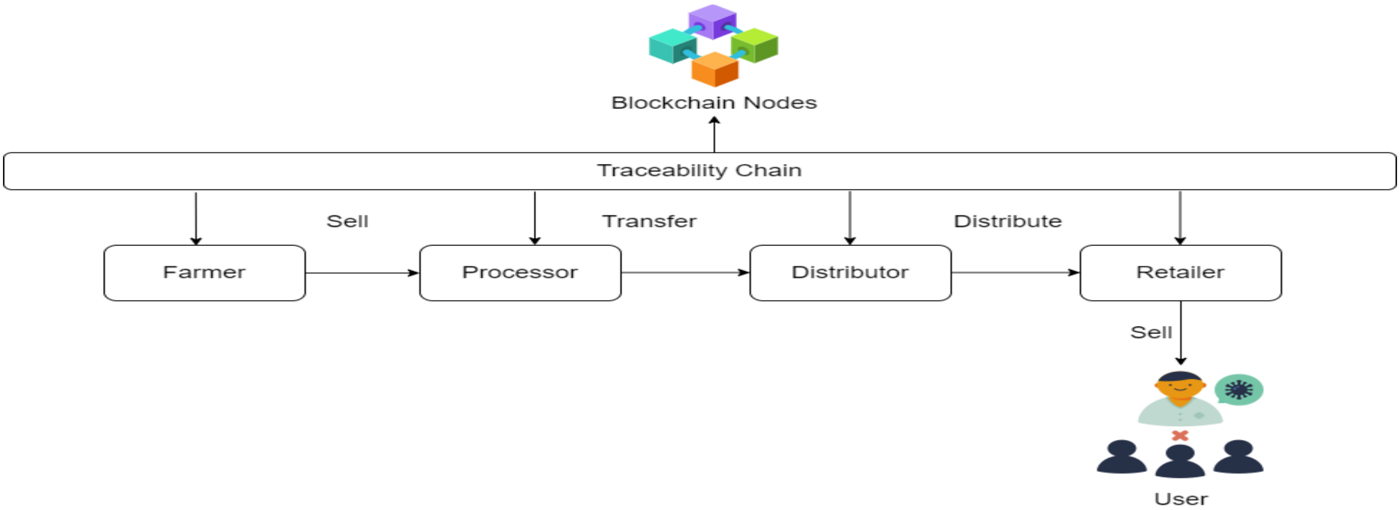


Fig 1 System Architecture

- *Farmer A planter is the first reality in the Agri- Food force chain and is the first one to bring smart contracts for trading. The Farmer produces a large number of crops and takes the responsibility for assuring and covering the crops' growth details. He sells these crops to the processors.*
- *Processor A processor buys the crops from growers. He's responsible for removing redundant accoutrements from the crops and converting them into the final product. The Processor sells this perfected product to distributors*
- *Distributor The distributor buys the final products from the processor and maintains the storehouse and is responsible for dealing them to retailers.*
- *Retailer A retailer buys the finished traceable products from distributors and sells them to guests in lower amounts. Traceable product refers to specific identifiers of the goods that allow tracking the provenance data.*
- *Consumer A consumer is an end stoner who buys and consumes products from retailers. Before copping the products, the client verifies the credibility of the dealer through the character system.*
- *The finance ministry is drawing up a plan to facilitate direct selling platforms for fruit and vegetable farmers' produce. a move aimed at cutting out middlemen and containing food inflation, which faces the risk of a re-emergence if the monsoon falters.*
- *Which governs the marketing of agricultural produce, to allow farmers to sell directly to consumers that will save high intermediation costs?*
- *SDG(Sustainable Development Goal) Targets halving per capita global food waste at the retail and consumer levels and reducing food loss along production and supply chains (including post-harvest losses)*

- *Deployment Diagram*

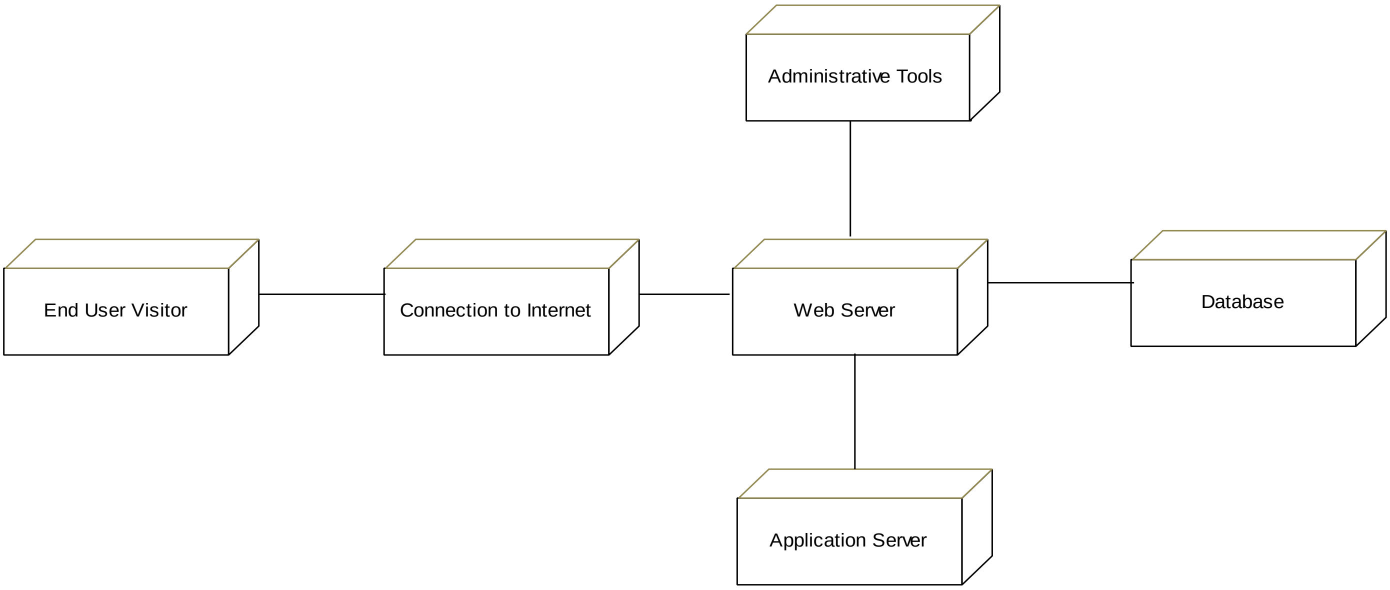


Fig 2 Deployment Diagram

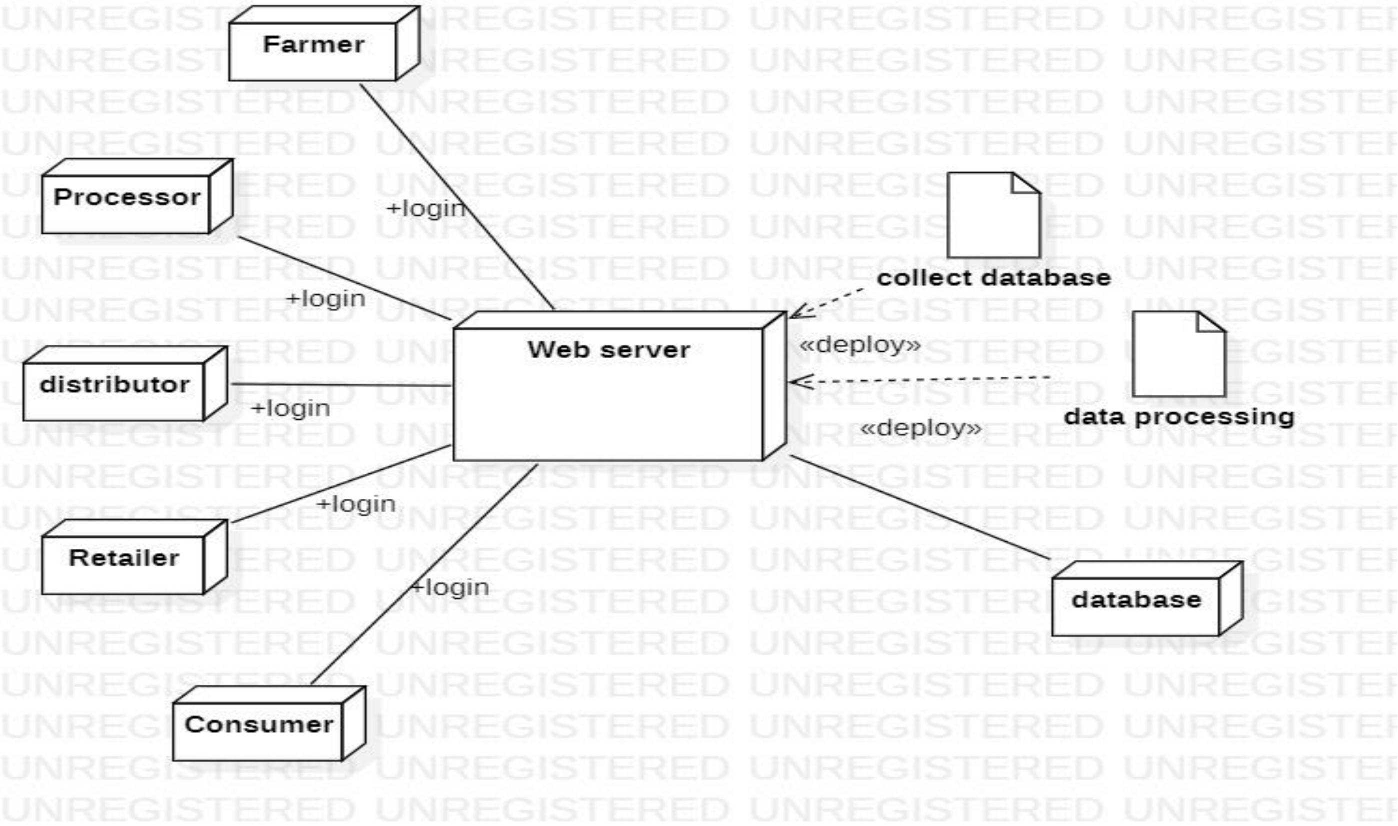
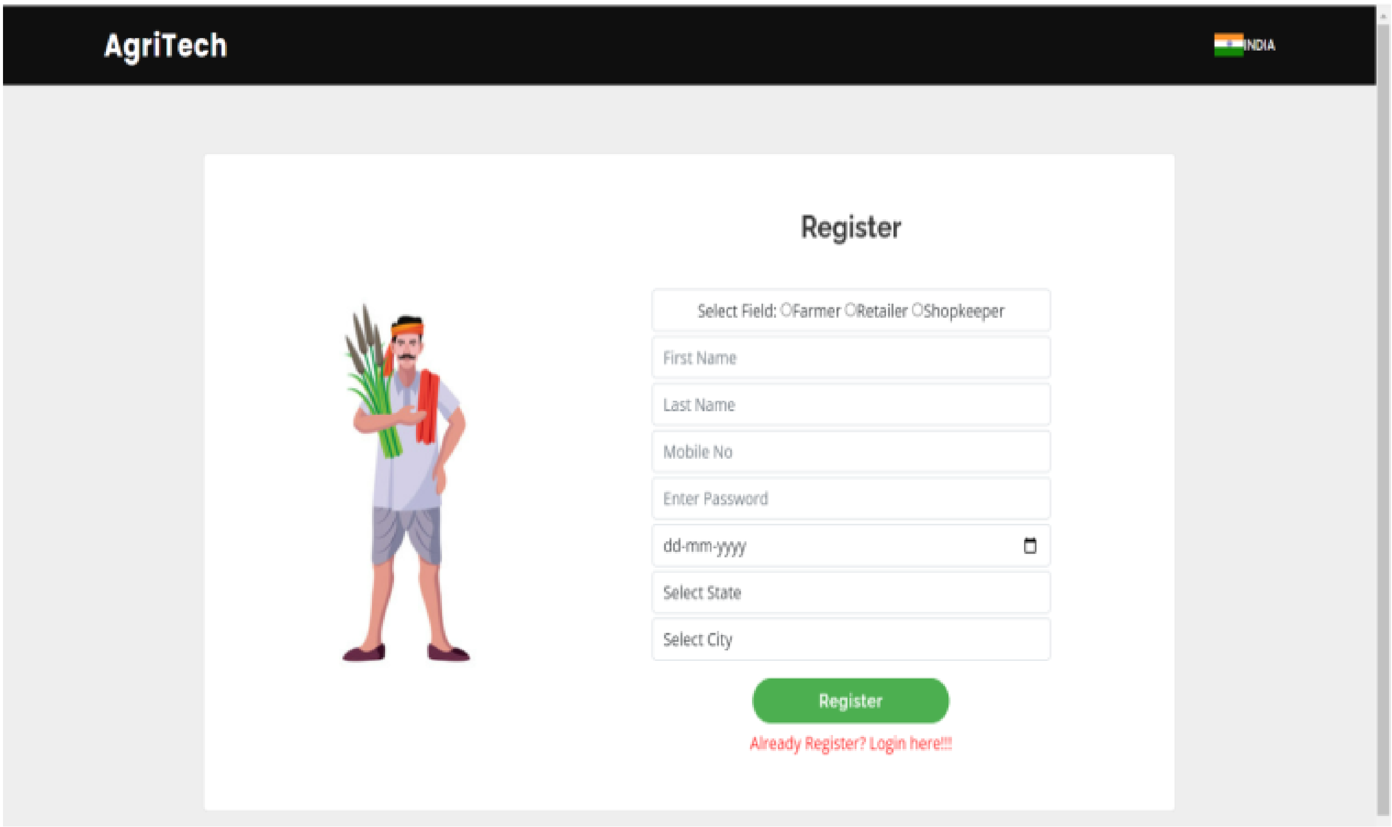


Fig 3 Deployment Diagram

V. RESULT

➢ *Registration Form*



Register

Select Field: ○Farmer ○Retailer ○Shopkeeper

First Name

Last Name

Mobile No

Enter Password

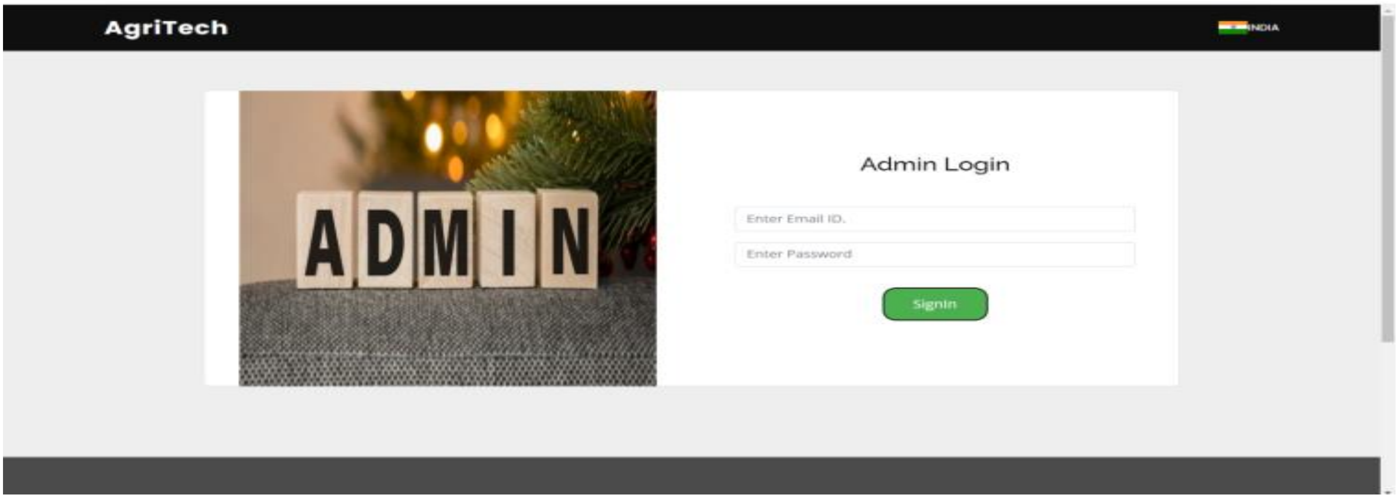
dd-mm-yyyy

Select State

Select City

Fig 4 Registration form

- *Admin Login*



Admin Login

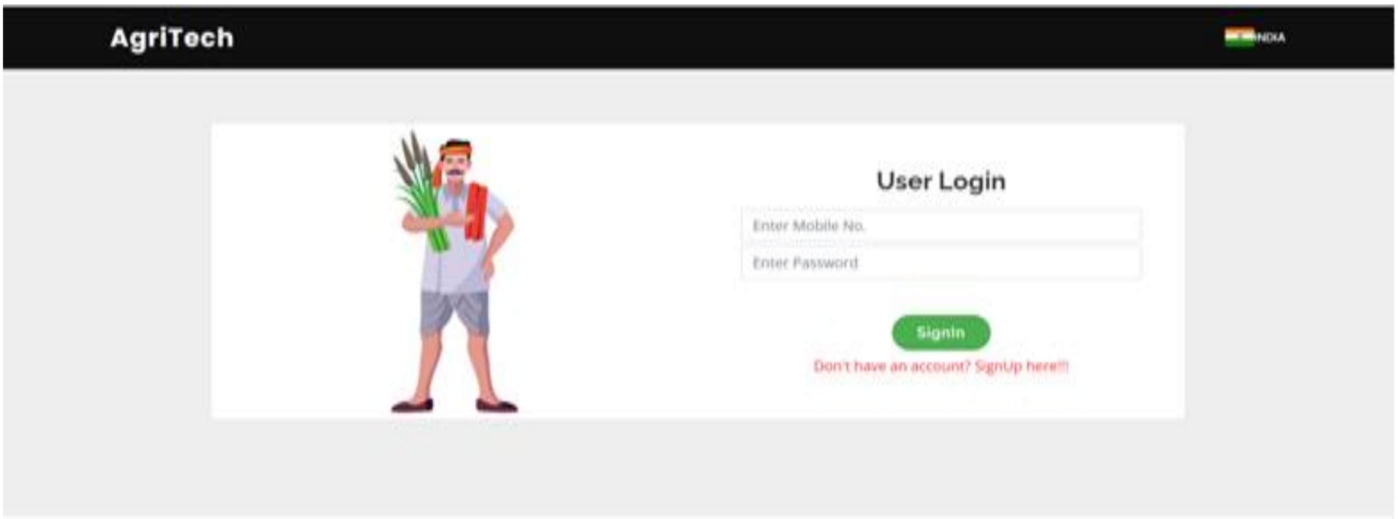
Enter Email ID.

Enter Password

Signin

Fig 5 Admin Login

- *UserLogin*



User Login

Enter Mobile No.

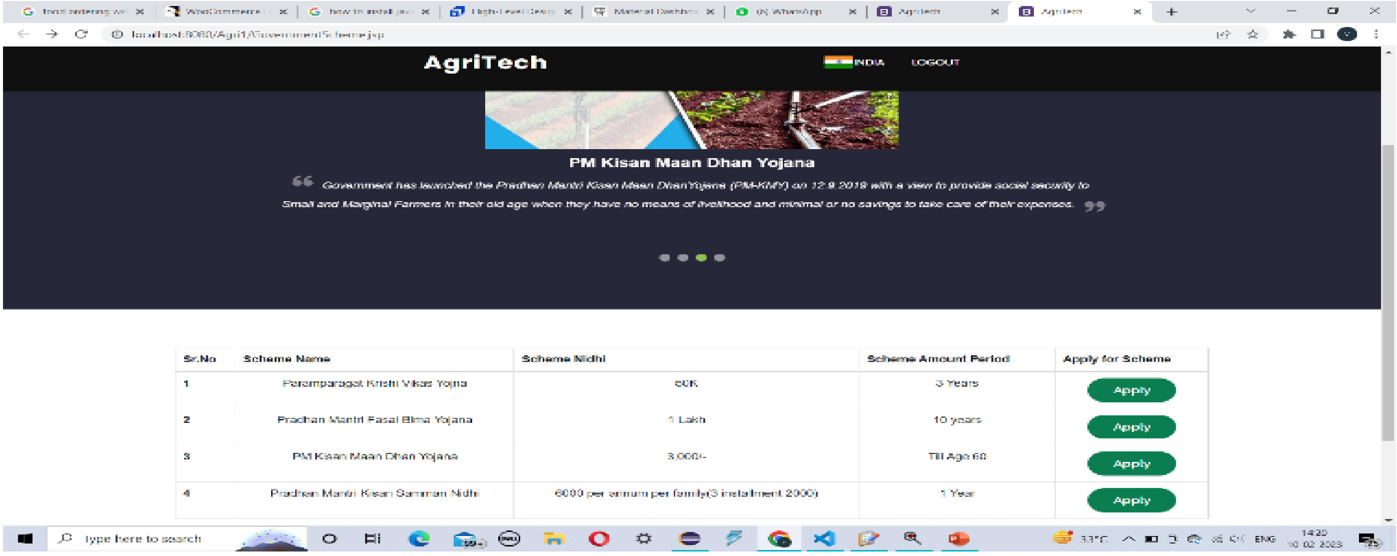
Enter Password

Signin

Don't have an account? SignUp here!!

Fig 6 User Login

- *Government Scheme*



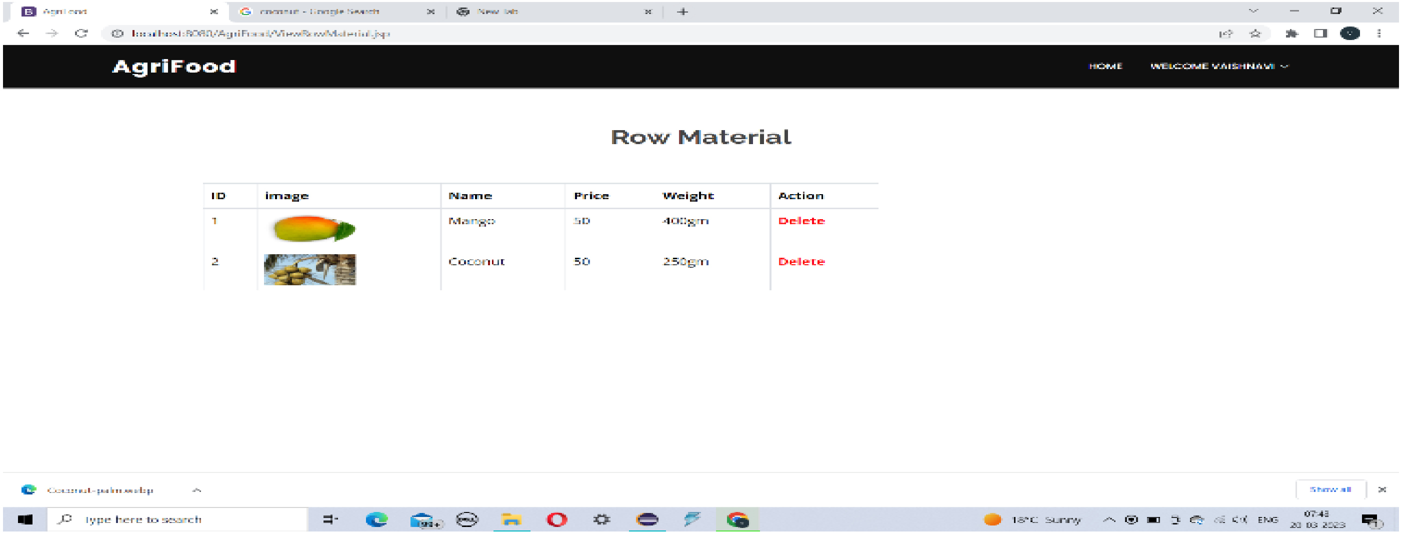
PM Kisan Maan Dhan Yojana

" Government has launched the Pradhan Mantri Kisan Maan Dhan Yojana (PM-KMY) on 12.9.2019 with a view to provide social security to Small and Marginal Farmers in their old age when they have no means of livelihood and minimal or no savings to take care of their expenses. "

Sr.No	Scheme Name	Scheme Nidhi	Scheme Amount Period	Apply for Scheme
1	Paramparagat Krishi Vikas Yojna	50K	3 Years	Apply
2	Pradhan Mantri Fasal Bima Yojana	1 Lakh	10 years	Apply
3	PM Kisan Maan Dhan Yojana	3,000/-	Till Age 60	Apply
4	Pradhan Mantri Kisan Samman Nidhi	6000 per annum per family(3 installment 2000)	1 Year	Apply

Fig 7 Government Scheme

- *Raw Material*



Row Material

ID	image	Name	Price	Weight	Action
1		Mango	50	400gm	Delete
2		Coconut	50	250gm	Delete

Fig 8 Raw Material

VI. MANAGERIAL IMPLICATIONS

The practical perpetration of our proposed block-chain- grounded Agri- Food force chain system will strengthen the traceability information of both agrarian and food products. All the important aspects of a secure and effective force chain system are taken into consideration which are developed in the following subsections

- *Responsibility:*

By enforcing blockchain in the proposed scheme, complete decentralization is achieved. It ensures the responsibility of all conduct by assaying the logs. In this regard, the proposed result allows judges to come a part of the system and dissect the logs in case of controversies. The controllers have access to the blockchain data and can recoup the required information to give evidence of responsibility. also, vicious bumps can not succeed in performing a vicious act as the bumps are defended with a standard hand scheme and it's insolvable for the bumps to deny their conduct.

- *Credibility :*

The Credibility of the system is anatomized grounded on of position of trust among the realities of the system. The proposed result; thus, contains a character system that's responsible for maintaining trust between realities like product possessors, purchasers, LC, etc. also, using the essential parcels of blockchain, the proposed result is proven to be believable and secure. Hackers can not hack the proposed system as long as they enthrall further than 51 of all bumps.

- *Auditability:*

The complete system is auditable by any licit use of the system. It provides traceable smart contracts to track the deals and events that passed. Blockchain provides the benefits like translucency, invariability, and traceability. It ensures that the deals are unforgeable.

- *Autonomy:*

All deals and data exchanges in the proposed result take place using smart contracts and help any kind of external hindrance. Hence, it ensures autonomy and security in a trusting terrain. also, agreement- grounded verification of blocks is also viewed as an independent property of blockchain- grounded results.

- *Authenticity:*

All the realities in the proposed result are authenticated before performing the sale. The authentication process ensures that certain functions are executed by authorized realities of the system only. Accordingly, it also ensures resistance to man- in- the- middle attacks.

VII. CONCLUSION

The supply chain industry has reaped various benefits from the implementation of blockchain, including increased growth and development, decentralization, and the creation of a trustless environment for all processes. Despite blockchain's lack of trustworthiness, it is difficult to retain complete confidence between the product's supplier and consumer. This is due to the possibility of harmful behavior on the part of the entities, and the buyer's uncertainty about their trustworthiness. Traceability, accountability, and security are all dependent on the decentralized nature of the supply chain, which is why it is so important. In this paper, we present a complete solution for the Agri-Food supply chain based on the blockchain. Traceability, trade, delivery, and reputation are all areas in which we've offered specifics about our approach. to verify that the offered solution is effective and stable, we've examined and studied the performance of smart contracts. Keeping the Agri-Food supply chain and product quality ratings credible is the goal of the reputation system. In addition, because the transactions are built on blockchain, they remain unaltered and uncorrupted.

REFERENCES

[1] Base Paper: Blockchain-Based Agri-Food Supply Chain: A Complete Solution. (IEEE)

[2] A. Jøsang, R. Ismail, and C. Boyd, ``A survey of trust and reputation systems for online service provision,'' Decis. Support Syst., vol. 43, no. 2, pp. 618644, Mar. 2007.

[3] Y. Chen, H. Li, K. Li, and J. Zhang, ``An improved P2P le system scheme based on IPFS and blockchain,'' in Proc. IEEE Int. Conf. Big Data (Big Data), Dec. 2017, pp. 26522657.

[4] Trufe Suite. Ganache: Ganache Quickstart: Documentation. Accessed: Dec. 6, 2019. [Online]. Available: https://www.trufesuite.com/docs/ganache/quickstart

[5] Y. Lu, ``The blockchain: State-of-the-art and research challenges,'' J. Ind. Inf. Integr., vol. 15, pp. 8090, Sep. 2019.

[6] K. Behnke and M. F. W. H. A. Janssen, ``Boundary conditions for traceability in food supply chains using blockchain technology,'' Int. J. Inf. Manage., vol. 52, Jun. 2020, Art. no. 101969.

[7] K. Salah, N. Nizamuddin, R. Jayaraman, and M. Omar, ``Blockchain-based soybean traceability in the agricultural supply chain,'' IEEE Access, vol. 7, pp. 7329573305, 2019.

[8] Y.-P. Lin, J. Petway, J. Anthony, H. Mukhtar, S.-W. Liao, C.-F. Chou, and Y.-F. Ho, ``Blockchain: The evolutionary next step for ICT E-agriculture,'' Environments, vol. 4, no. 3, p. 50, 2017.

[9] Y. P. Tsang, K. L. Choy, C. H. Wu, G. T. S. Ho, and H. Y. Lam, ``Blockchain-driven IoT for food traceability with an integrated consensus mechanism,'' IEEE Access, vol. 7, pp. 129000129017, 2019.

[10] K. Toyoda, P. T. Mathiopoulos, I. Sasase, and T. Ohtsuki, ``A novel blockchain-based product ownership management system (POMS) for anti-counterfeits in the post supply chain,'' IEEE Access, vol. 5, pp. 1746517477, 2017.