International Journal of Modern Developments in Engineering and Science
Volume 1, Issue 3, March 2022
https://www.ijmdes.com | ISSN (Online): 2583-3138

Agri Food Supply Chain Using Ethereum Smart Contract

Bawankar Chetan Daulatrao[1], Dheple Pravin Nandkumar[2], Jadhav Girish Atmaram[3], Pawar Yogesh Dattatray[4], Sonvane Saurabh Mohanrao[5*]

[1]*Professor, Department of Information Technology, Sanjivani College of Engineering, Kopargaon, India*
[2,3,4,5]*Student, Department of Information Technology, Sanjivani College of Engineering, Kopargaon, India*

***Abstract*: The supply chains of the contemporary world are changing to become automated and extremely complicated networks, gaining many advantages. Due to this, customers are more concerned about the quality of food products. It is not easy to ensure data integrity across the supply chain network, however, In contrast to decentralized supply networks, conventional ones are centred and rely on a third party for trade. As a result, there is a lack of transparency, accountability, and audibility in centralized systems. We have suggested a comprehensive solution for the Agri-Food supply chain using Ethereum. It brings together blockchain and smart contracts, which are both linked to Ethereum. However, the inherent immutability of blockchain still does not adequately address several supply chain management issues, such as the trustworthiness of the participating entities, accountability of the trade process, and product traceability. To fulfil these needs, a trusted system is required that guarantees traceability, trust, and delivery mechanism for the supply chain in the Agri-Food industry. The suggested system uses blockchain technology to keep track of all transactions, and after that, the data is uploaded to Interplanetary File Storage System (IPFS). A hash of the data is returned to the storage system, and it is made efficient, safe, and trustworthy via the use of blockchain. The interaction of entities is shown with the help of smart contracts and their algorithms in our system. The findings provided in this study also include simulations and evaluation of smart contracts along with the assessment of security and vulnerability.**

***Keywords*: Blockchain, Ethereum, IPFS, Smart contract, Supply chain, Traceability.**

1. Introduction

Management of supply chain is a group of processes, subprocesses and transactions implemented that turn crops into the finished product. Gaining trust of the end consumer is the primary intention to build supply chain over ethereum smart contracts. Supply chain is a network of business parties located at different Geographic locations. By considering the wide network of producers and consumers different phases have been created. Any process in the supply chain takes a long-time span of several months to complete [1]. As a result of which there is insecurity about the quality of food products. In the case of a centralized supply chain, it becomes difficult to determine this stage when tampering with products happens. It has been discovered many times that action taken in one part of the supply chain can have adverse or beneficial effects on the other parts. Data produced at every stage of the supply chain is very large in volume as a result it becomes difficult to manage the data in a centralized system [2]. Network becomes more complicated. As the volume of data increases, the problem of bottleneck also increases. There is risk of misrepresentation and inaccuracies in information stored at a centralized server. Due to the centralized architecture of the traditional supply chain, there is a lack of reliability in financial transactions. In the case of centralized architecture, a large number of users tries to access the data over the supply chain simultaneously which results in the creation of a bottleneck, which results in the degrading of performance. In case of centralized supply chain, the whole access of database lies with administrator so there are chances of data tampering at the administrator site.

To overcome this issue related to centralized architecture proposed architecture offers a distributed system. Distributed system has best fault tolerance, Sub current handling and scalability. Blockchain is the best ever solution for these problems in the supply chain, though there are issues of storage and throughput. Consensus algorithm is the backbone of blockchain which aims to maintain data integrity while allowing high storage capacities up to and improved [14]. In the case of agricultural supply chain effective tracking of agricultural products is necessary for the safety of products. Smart contract is an additional feature in ethereum blockchain that leverages secure business transactions between entities.

Smart contracts ensure one entity to trust in another entity while making financial transactions. One of the benefits of introducing blockchain technology in the supply chain is that there is no need for a third party for trading, it is a peer-to-peer network. Also provides a platform for farmers to sell their crops directly to processor. In [9] the proposed architecture we have to use ipfs (interplanetary file storage system) to store actual data generated. Different encryption algorithms are used to encrypt the data and one hash value gets generated, data over ipfs can be easily accessed using this hash value. We have tried to build an ethereum smart contract-based agriculture food supply chain to overcome problems faced during the traditional supply chain.

*Corresponding author: sonvanesaurabh7@gmail.com

A. Blockchain

Blockchain was first introduced in 1979 by Chaum. In 1992, the concept of blockchain was improvised by Bayer by adding the merkle tree as one of the parts of block design [6]. The structure of a blockchain continuously expands itself by adding the blocks which are cryptographically connected to each other. Every block in the blockchain contains the information that is the hash value of the previous block. Also, it contains data, timestamps which are used for the transaction of data. Due to the complex design of a blockchain, blockchain strongly opposes the modification in the data. In 2008 the blockchain was used in developing cryptocurrency called Bitcoin by an anonymous person named Satoshi Nakamoto. Since then, the blockchain is widely used worldwide.

Blockchain is a distributed data system that has the timestamps which are in the form of the decentralized database in a peer-to-peer network [2]. Due to Bitcoin, the blockchain technology came into public awareness and got popular slowly-slowly. In the last few years the blockchain became the trending topic, though it is dependent on some of the technologies such as peer-to-peer protocol, encryption technology which have existed for a long period of time. Blockchain is one of the best combinations of timestamp technology, consensus algorithms, smart contracts and encryption technology which forms a distributed system where users can be unknown and data can be trustworthy. It gives advantages of privacy, immutability, decentralization of data, etc. It is generally used in the medical field, supply chain, education systems.

It is a public distributed database that holds the encrypted ledger, and therefore the transactions which take place in the process are strongly encrypted by cryptographic algorithm. Every new information or data is checked and validated before storing it on the system. Blockchain is a distributed ledger system whose aim is to provide the same information across a network without tampering.

There are three different types of blockchain as follows:

1) Public Blockchain

Public blockchains are publicly accessible blockchains. The public blockchain, anyone can access it and therefore it has no restrictions for users. In a public blockchain nobody has total control over the blockchain, due to this the data remains secure and no one can make changes in it. All the participants of public blockchain have equal power, therefore public blockchain is a totally distributed system. Bitcoin is an example of a public blockchain.

2) Private Blockchain

Private blockchain is accessible to only the members of the blockchain ecosystem. All the transactions which are carried out in the private blockchain are only visible to the members of the private blockchain. The private blockchain is more centralized as compared to public blockchain. As private blockchain is more centralized than public blockchain, hence it is easy to regulate and govern [15]. It can be manipulated according to the owner of the blockchain.

Private blockchain has an administrator to its network, who has responsibility to take care of any requirement of the user. In any case the user requires more authority to carry out its operation, so it is a duty of a network admin to provide authority to the user. It is mostly used in private organisations. Hyperledger is an example of private blockchain.

3) Consortium/Hybrid blockchain

Consortium blockchain has two different types, in which some nodes are private and some nodes are public [2]. Hybrid blockchain is a perfect balance between private blockchain and public blockchain. In hybrid blockchain we can access all the nodes but accessing the data depends on the level of Information and type of a node.

The hybrid blockchain has two different types of users, in which have total control on the blockchain and determine the security of a particular system but the other user has access to the blockchain only according to its function.

B. Ethereum

Ethereum was introduced in 2013 by Vitalik Buterin and in 2014 the work started on it and then Ethereum was released in 2015. Ethereum is a platform for decentralized programs, also called as decentralized applications [13]. Ethereum Blockchain works as an open-source platform. Ethereum is a network of independent computers which are connected to each other. These connected computers are also called nodes. These nodes by connecting to each other form a continuous chain of blocks, known as ethereum blockchain.

Ethereum is fully compatible with frameworks such as truffle, ganache, etc. It has programmed smart contracts which carry out transactions with some sort of conditions. Ethereum allows any user to deploy and run decentralized programs on it. Ether is a digital currency of Ethereum [17]. Ethers are used for transactions on ethereum.

1) Ganache

Ganache is a local blockchain simulator for rapid decentralized application development using ethereum. This allows you to develop, deploy and test decentralized applications or smart contracts. There are two versions of ganache-Ganache CLI and Ganache GUI.

2) Truffle

Truffle is a free JavaScript framework for developing solidity smart contracts. It runs on node.js. It used to create, manage and test smart contracts. It is considered as the most popular blockchain based application development tool.

3) Remix IDE

Is an online IDE for the solidity programming language It is written in JavaScript, it supports running in local and desktop versions as well as in your browser. It is also used for developing, testing, deploying smart contracts without need of actual ethers. It provides different testing environments such as javascript vm, injected web3.

4) Metamask

Metamask is a wallet to store cryptocurrency and helps to interact with ethereum blockchain. This will allow users to access ethereum wallets through browser extensions or mobile apps and interact with decentralized applications.

5) Solidity

Solidity is the main programming language for writing smart contracts on Ethereum blockchain. It is contract oriented

language, which runs on an ethereum virtual machine. It is similar to JavaScript and very easier to write.

6) Smart contract

A smart contract is a small computer program that is stored inside a blockchain. Smart contracts resemble real life contracts but smart contracts are in the digital form. Smart contracts are immutable. Immutability of smart contracts means that once they are created cannot be changed, even by the owner of the contract. Smart contract Solidity is the programming language used to write smart contracts.

2. Related Work

Now-a-days food safety has become a most important concern in agri food industries. Many of these supply chains are centralised, due to the series issues such as manipulation and fraud. That's why we have introduced some traceability and security which is based on blockchain into the supply chain system [4]. In addition to its advantages, blockchain also has some drawbacks. In other words, when the amount of data rises to some level it lacks scalability. In this concern BigchainDB is used to fill the gap in providing a scalable solution. The given solution is applied to the given case to show key efficiency and transparency so it can help with hazard analysis and key control points regulations [5]. In [3] the given system is not providing any information regarding the ownership of the product, tracking the origin of a product in the Supply Chain needs to be adaptable, transparent and tamper proof to the changing world. That's why we develop the main chain using public blockchain and private blockchain. Hash value of the data is stored on the main supply chain and the files and data of the ethereum smart contract is stored on the off-chain storage like IPFS, with food security in mind solution which is based on IOT and blockchain for agri food supply chain and information security has been proposed. They created farm to table product traceability use cases and matches this result by using a different execution platform which is hyperledger and Ethereum [7]. In traditional storage systems data was stored in a centralized way and after introducing blockchain this decentralised way of storing data comes into picture there is a beneficial storage system for agriculture food product tracking. Using the IPFS with another database for traceability, an interplanetary file storage system is nothing but a network for sharing data and storing data in a distributed file storage system. To read the data from an interplanetary file storage system, access the hash key from another database. Problems of a centralized system are minimised by the proposed solution and to remove the need for trusted third parties, maintenance reliability, higher security and integrity [8]. This document aims to overcome the demerits or leakage of important data and single point of failure of the centralized storage system. In [9] the proposed work file is encrypted using an algorithm before storing data in the interplanetary file store system. The interplanetary file store system provides a hash of the stored file [16]. The given solution keeps the rating of the product anonymous and provides the security analysis [10]. However, it does not provide the performance analysis needed to guarantee the efficiency of token generation. It is also vulnerable to malicious users because there is no correlation between reviews and transactions. All online trading platforms have a question of truth between sellers and buyers. This is because they do not meet in person to make a transaction. Therefore, we need a rating system that matches the sellers rating with profile and helps the buyer pre-assess the seller and product. In [19] conclusion from the above author, use of blockchain technology in agriculture food supply chain systems is increasing rapidly. It is used to improve food safety issues, traceability issues in current agriculture and food supply chain systems. So, based on the above author we have suggested the system of blockchain based solution to maintain verifiability, reliability of agricultural food supply chain.

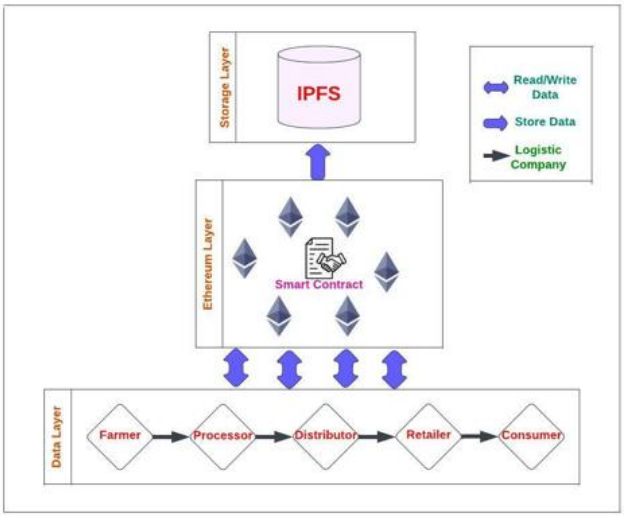

Fig. 1. System architecture for agri food supply chain using ethereum smart contract

3. System Overview

Supply chain in any field focuses mainly on the tamper less transportation, good traceability and tracking systems. It connects two ends (producer and consumer) of any business. Supply chain in the agricultural field involves raw to edible production and logistic activities. This supply chain includes all the entities from farmer as a producer to end consumer of edible food products. Supply chains include complex functions which makes tracking of products very efficient. Transaction and delivery mechanisms between parties are the key factors in the supply chain. System proposed by us concentrates mainly on these factors. Considering these conditions and constraints of food supply we have followed three layered architectures. First layer of this architecture is the data layer which focuses on the interaction of entities in the supply chain. Blockchain layer is the second layer which handles the data related to transactions and this data is uploaded to ipfs (interplanetary file storage system). By considering the volume of data, the second layer stores hashes of data and actual data gets uploaded to the third layer which is the storage layer.

Entities in the supply chain are,

1) Farmer

Farmers are at the origin stage of the supply chain. Farmer is the first party which is going to access smart contracts. Crops

produced by farmers need to be monitored using sensors for assurance of quality product. Sensors are used to monitor basic details of air quality, soil type, amount of sunlight in the period of Crop growth[11]. Crop details are stored over ipfs in image format so that any node in the network can analyse data easily by visualization. It is up to the farmers to whom they want to sell their crop.

2) Processor

Processes are the deciding factor of good quality food products. Processing methods on the crop post harvesting decides the quality of the product. Processing involves the process of removing non edible material and converting the crop into finished product. For monitoring this process of manufacture edible product there is need of quality assurance team. The reports generated by quality assurance team is stored at ipfs, only hash of that data is stored at blockchain layer.

3) Distributor

Distributor buys the product from the processor after checking basic details. There might be another network of distributors working under wholesaler, so this creates another network of distributors. Responsibilities of product safety and warehousing lies with distributors. Data integrity related to processing company, price, dates of processing achieved by matching hash values.

4) Retailer

Retailers order the product according to the needs of the consumer. There are chances that retailer can stock product for a long time, so retailers also upload their details related to price, current stock available to ipfs.

5) Consumer

It is a final entity who purchases and consumes the final product (agricultural food) from retailers and obtains the full transaction history of the product by using barcode QR codes on the package [8].

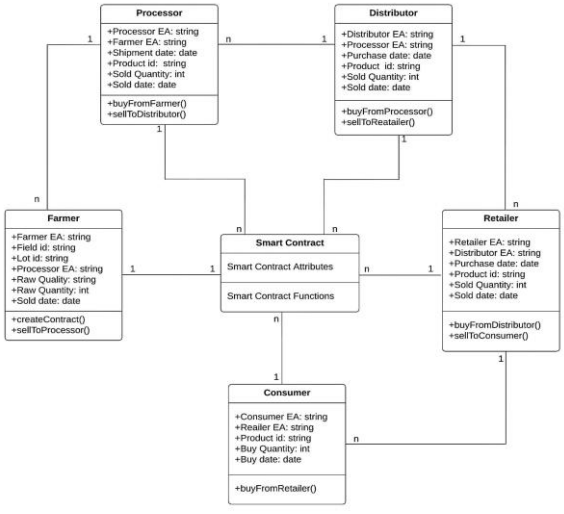

Fig. 2. Entity Relationship diagram

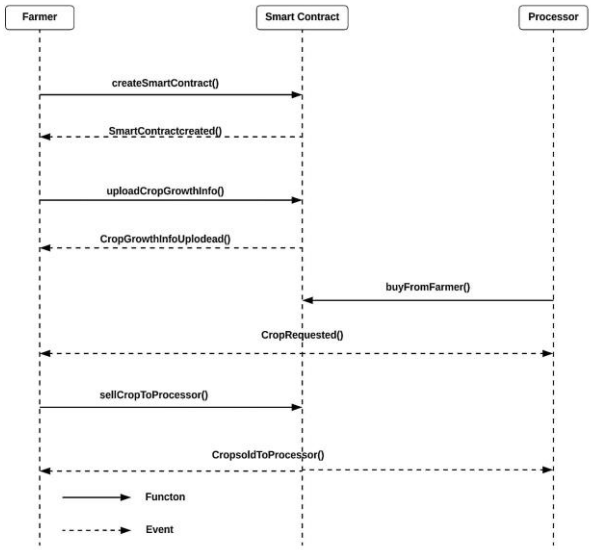

Fig. 3. Sequence diagram between farmer and processor

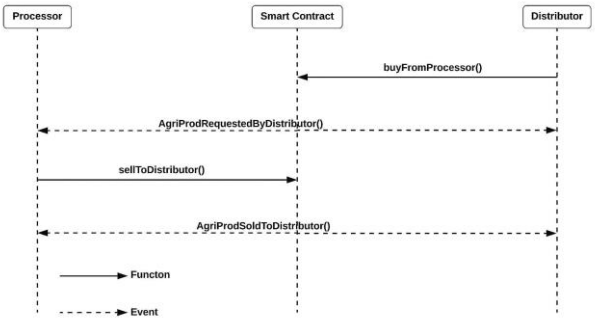

Fig. 4. Sequence diagram between processor and distributor

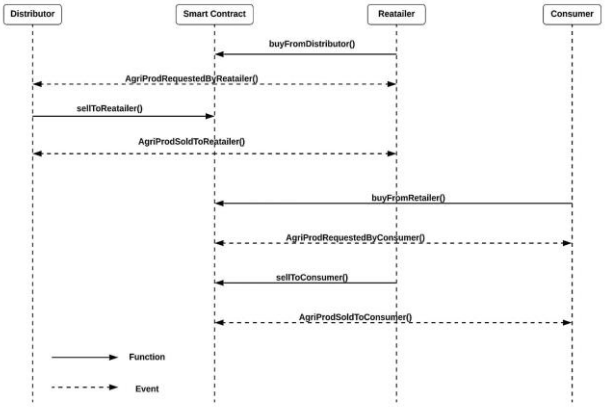

Fig. 5. Sequence diagram between distributor, retailer and consumer

Figure 2 entity relationship diagram shows relationship between smart contract and entity. Each entity consists of smart contract attributes and smart contract functions. Smart contract attributes are parameters that are passed to smart contract function. Every entity in the supply chain performs tasks by calling functions in a smart contract. In figure 3, it shows interaction between farmer and processor via smart contract. Farmer regularly upload the crop growth information by calling

function uploadCropGrowthInfo().Crop information and images are stored in ipfs and ipfs hash stored in ethereum layer.

Trade between farmers and processors begins after the harvesting of crops by farmers. Firstly, the processor executes the function buyFromFarmer() and passes parameters to activate smart contract which notifies farmers about crop requests by executing cropRequested(). Farmer calls the function sellCroptoProcessor() and passes parameters. After satisfying the conditions in smart contract executes acknowledgment function CropsoldToProcessor().It also other entities in the supply chain that the crop from the farmer is sold to processor and all the corresponding parameters are recorded. The next trade is between processor and distributor as shown in figure 4. First function in the contract is executed by distributor buyFromProcessor(),it results in the triggering of the function AgriProdRequestedByDistributor().If the certain processor is ready with the product demanded by distributor then processor calls the function sellToDistributor() by passing parameters. After that the trade is completed between processor and distributor,all the data about this transaction(price,mfg date,purchase date)are recorded .Figure 5 shows the interaction between retailer and distributor. Retailer executes the function buyFromDistributor() request product from the distributor. If certain distributor is available with the stock of requested product then distributor executes the function sellToRetailer() which trigger the event AgriProdSoldtoRetailer() to notify other entities about the transaction. At the last consumer and retailer executes buyfromRetailer() and sellToConsumer() function simultaneously.

Algorithm 1: Processor Buys Crop from Farmer

Input: 'pl' list of registered processor
Processor's ethereum address
Farmer's ethereum address
crop_price,crop_quantity
1 Contract state is BuyCrop
2 State of processor RequestCrop
3 State of farmer ReadytoSell
4 Access is restricted.Only p ϵ pl allowed
5 if processor =registered and crop_price=paid then
6 State of contract changes to CropRequestAgreed
7 New state of farmer AgreetoSellCrop
8 New state of processor WaitingforCrop
9 Notification of crop sell agreement send to processor
10 end
11 else
12 State of contract changes CropSellRequestDenied
13 New state of farmer DenyCropSellRequest
14 New state of processor FailedBuyCrop
15 Notification of crop sell request denied send to processor
16 end

Algorithm 2: Distributor Buys Food Product from Processor

Input: 'dl' list of registered distributor
distributors's ethereum address
Processor's ethereum address
price, purchase_date,mfg_date
1 Contract state is BuyProcessedAgriFood
2 State of processor CropReceivedFromFarmer
3 State of distributor ReadytoBuy
4 Access is restricted.Only d ϵ dl allowed
5 if distributor =registered and price=paid then
6 State of contract changes to SellRequestAccepted
7 New state of processor AgriFoodSold
8 New state of distributor WaitingforProductDelivery
9 success notification send to distributor
10 end
11 else
12 State of contract changes RequestDenied
13 New state of processor NotReadytoSell
14 New state of distributor FailedtoBuyProduct
15 failure notification send to distributor
16 end

Algorithm 3: Retailer Buys Food Product from Distributor

Input: 'rl' list of registered retailers
distributors's ethereum address
Retailer's ethereum address
purchase_date,FoodProductID
1 Contract state is ProcessedFoodSoldtoDistributor
2 State of retailer ReadytoBuyProduct
3 State of distributor ReadytoDistribute
4 Access is restricted.Only r ϵ rl allowed
5 if retailer=registered and payment=successful then
6 State of contract changes to SellRequestAccepted
7 New state of retailer ProductReceived
8 New state of distributor SellProducttoRetailer
9 success notification send to retailer
10 end
11 else
12 State of contract changes Sell RequestDenied
13 New state of retailer FailedtoPurchase
14 New state of distributor ProductSellCancelled
15 failure notification send to retailer
16 end

4. Conclusion

Using blockchain, the industry of supply chain has increased, moved towards decentralization and gained a trustworthy ecosystem for the processes. While having a trustworthy environment and dependable nature of a blockchain it is not easy to maintain trust between buyer and seller of the goods. This thing happens due to fraud and malicious actions of a company which brings doubts in the mind of the buyer about the authenticity of the product. Also, with this, the supply chain contains various processes and their sub processes that should be run in a decentralized way to gain accountability, traceability and security of the system.

We have proposed a system for tracking and executing transactions in smart contracts using ethereum blockchain. This

system is proposed by us to maintain authenticity of the agri food supply chain. Where it keeps track of the information of the agri food supply chain which must be secret and not be tampered by anyone. It maintains the privacy and integrity of transactions. This paper explains about the importance of food safety and its traceability.

References

[1] Affaf Shahid, Ahmad Almogren, Nadeem Javaid, Fahad Al-Zahrani, Mansour Zuair, Masoom Alam. "Blockchain-Based Agri-Food Supply Chain: A Complete Solution", April 2020.

[2] Lu Wang, Longqin Xu, Zhiying Zheng, Shuangyin Liu, Xiangtong Li, Liang Cao, Jingbin Li, and Chuanheng Sun. "Smart Contract-Based Agricultural Food Supply Chain Traceability", Jan. 2021.

[3] Huilin Chen, Zheyi Chen, Feiting Lin, and Peifen Zhuang. "Effective Management for Blockchain-Based Agri-Food Supply Chains Using Deep Reinforcement Learning", Feb. 2021.

[4] Inting Yang, Mengqi Li, Huajing Yu, Mingting Wang, Daming Xu, and Chuanheng Sun. "A Trusted Blockchain-Based Traceability System for Fruit and Vegetable Agricultural Products", March 2021.

[5] Luisanna Cocco, Katiuscia Mannaro, Roberto Tonelli, Lorena Mariani, Matteo B. Lodi, Andrea Melis, Marco Simone, and Alessandro Fanti. "A Blockchain-Based Traceability System in Agri-Food SME: Case Study of a Traditional Bakery", April 2021.

[6] Quang Nhat Tran, Benjamin P. Turnbull, Hao-Tian Wu, A. J. S. De Silva, Katerina Kormusheva, and Jiankun Hu. "A Survey on Privacy-Preserving Blockchain Systems (PPBS) and a Novel PPBS-Based Framework for Smart Agriculture", Jan. 2021.

[7] Mohamed Amine Ferrag, Lei Shu, Xing Yang, Abdelouahid Derhab, and Leandros Maglaras. "Security and Privacy for Green IoT-Based Agriculture: Review, Blockchain Solutions, and Challenges", Feb. 2020.

[8] K. Salah, N. Nizamuddin, R. Jayaraman, and M. Omar. "Blockchain-based Soybean Traceability in Agricultural Supply Chain", 2019.

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

[10] M. P. Caro, M. S. Ali, M. Vecchio, and R. Giaffreda, "Blockchain based traceability in agri-food supply chain management: A practical implementation," in Proc. IoT Vertical Topical Summit Agricult Tuscany (IOT Tuscany), May 2018, pp. 1–4.

[11] F. Tian, "A supply chain traceability system for food safety based on HACCP, blockchain & Internet of Things," in Proc. Int. Conf. Service Syst. Service Manage., 2017, pp. 1–6.

[12] A. M. Turri, R. J. Smith, and S. W. Kopp, "Privacy and RFID technology: A review of regulatory efforts," J. Consum. Affairs, vol. 51, no. 2, pp. 329–354, Jul. 2017.

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

[14] S. Wang, D. Li, Y. Zhang, and J. Chen, "Smart contract-based product traceability system in the supply chain scenario," IEEE Access, vol. 7, pp. 115122–115133, 2019.

[15] M. Yang, T. Zhu, K. Liang, W. Zhou, and R. H. Deng, "A blockchain-based location privacy-preserving crowdsensing system," Future Gener. Comput. Syst., vol. 94, pp. 408–418, May 2019.

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

[17] I. A. Omar, R. Jayaraman, K. Salah, M. Debe, and M. Omar, "Enhancing vendor managed inventory supply chain operations using blockchain smart contracts," IEEE Access, vol. 8, pp. 182704–182719, 2020.

[18] S. Xuan, L. Zheng, I. Chung, W. Wang, D. Man, X. Du, W. Yang, and M. Guizani, "An incentive mechanism for data sharing based on blockchain with smart contracts," Comput. Electr. Eng., vol. 83, May 2020, Art. No. 106587.

[19] Hobbs, J. (2006). Liability and traceability in agri-food supply chains. Quantifying the agri-food supply chain, 87-102.