Agri Food Traceability Using blockchain

AUTHORS:

DR. DEEPAK A. VIDHATE,
Prof and Head, Information Technology, Dr. Vithalrao Vikhe Patil College of Engineering, Ahmednagar

PROF. MRS.P.S. DOLARE,
Prof, Information Technology, Dr. Vithalrao Vikhe Patil College of Engineering, Ahmednagar

Janhavi Hire ,Prachi Patil, Saili Dhokchaule, Vaishnavi Thombal
Department of Engg, Information Technology, Dr. Vithalrao Vikhe Patil College of Engineering, Ahmednagar

Abstract— ***A secure Agri-Food Traceability System refers to a digital solution that enables the tracking and recording of the journey of agricultural products from farm to table. This system ensures transparency, accountability, and safety throughout the entire supply chain, offering consumers and stakeholders insight into the origin, production, processing, and distribution of food products. Implementing a secure traceability system in the agri-food industry has several benefits, including improving food safety, reducing fraud, enhancing supply chain efficiency, and fostering consumer trust.We propose to implement agri-food traceability system using microservices.***

Keywords:Technology :Java,Blockchain,SHA

I. INTRODUCTION

In the agri-food industry, traceability might be seen as a crucial component. Both laws and consumer advocacy groups call for better tracking and tracing without sacrificing data privacy. Traceability rules have been passed in a number of nations over the past few years:

In the EU, Regulation (EC) No 178/2002 of The European Parliament And of The Council of 28 January 2002 [2] establishes that food business operators shall be able to identify, for the competent authorities, any person who supplied them with alimentary commodities, and any business which takes food from the consumer.

The USA's "Farm Security and Rural Investment Act" mandates country of origin labeling for many types of food, including perishable agricultural commodities [1];

In today's Agriculture and Food (Agri-Food) supply chains, the great majority of traditional logistic information systems only track and store orders and deliveries without offering characteristics like transparency, traceability, and auditability.These characteristics are increasingly in demand from consumers since they would undoubtedly improve food quality and safety .

In order to enable remote monitoring of the conditions in food transportation scenarios and at a very fine granularity along the entire AgriFood supply chain, such as from production to consumption, several Research & Development communities are focusing their efforts on adopting some specific Internet of Things (IoT) technologies like RFIDs and Wireless Sensor Networks, or everyday-cheaper connected devices [2].

In the agri-food industry, it is crucial for the recorded records to be tamper-proof in order to maintain confidence and reliability along the whole supply chain. Ideally, each actor issuing transactions would be able to do so independently of any centralized third-party intermediary. The Blockchain technology, a peer-to-peer digital ledger that doesn't rely on centralized servers, may be able to allay these problems and worries. This distributed ledger is immutable by design and provides an auditable and transparent source of information because every record kept in a blockchain is based on a consensus reached at least by the absolute majority of peers of the network itself.Additionally, from an Internet of Things (IoT) standpoint, sensor networks in a blockchain-based traceability system would just need a solid connection to their nearby peer, as opposed to access to a central cloud. Blockchains thus reveal all the necessary characteristics for decentralizing food traceability systems and making traceable data accessible throughout the whole supply chain.

The proposed project will benefit women who travel alone, tourists who are unfamiliar with the area, and women who have late-night jobs feel safe with the application.

II. RELATED WORK

Numerous studies have been conducted on agri-food supply chains. For the agri-food supply chain, Li et al. (2006)[5] developed a dynamic planning system. This approach aims to maximize earnings for agri-food supply chain participants while minimizing losses of agri-food products.
According to Trienekens & Zuurbier (2008)[6], government agencies must take action to ensure the efficacy and security of agri-food products by establishing laws and guidelines. Many steps are also being done to ensure the quality and safety control through the transparency of the agrifood supply chain management in order to rebuild customer confidence in the wake of many scandals (Akkerman et al., 2010).[7]

Other academics take into account the use of cutting-edge technology, particularly RFTD technology, in supply chain management. Sari (2010)[8] created a simulation model for a supply chain company to determine the circumstances in which investing in RFTD technology is more advantageous for the company. The study's findings indicate that when supply chain members collaborate more closely, employing RFlD technology will be more beneficial. A rule-based decision support system was proposed by Wang et al. (2010)[9] to fulfill the real-time monitoring of agri-food items during their distribution process. This system determines the remaining value and shelf-life of agricultural and food products in transmission based on data supplied by sensor-RFID instruments from the refrigerated containers.

Blockchain facilitates trustworthy and real-time information sharing. The blocks are contained in this immutable chain in the order that they occurred. This paper [1] provides a framework that aids in managing the supply chain for pharmaceuticals. It includes various smart contracts for supply management, stock purchases, raw material purchases, etc. While the medications are being exchanged between two entities, the quality is confirmed using quality checking contracts. Through the use of pseudo identities, this framework achieves user privacy, transparency of the drug supplied because all users have access to the data stored in the blockchain, tracking of drugs through the use of pseudo identities, consistent and high-quality service, and demand supply management by obtaining demand data from distributors.

the Vickrey-Clarkegrove (Vickrey auction) method and takes into account the second-highest bid for determining payouts. It aids in the trading that is encouraged between farmers and consumers.
A model with a central authority, a producer, a distributor, a wholesaler, a retailer, and a consumer is suggested in paper [3]. Three smart contracts—Provenance, Bidding, and Tracking—have been used to implement this paradigm on the Ethereum platform. The Provenance contract aids the nodes in obtaining producer and product information. The terms that are verified before choosing the winning bidder are listed in the bidding contract. The features are included in the tracking contract includes features for tracking the item received with a serial number.

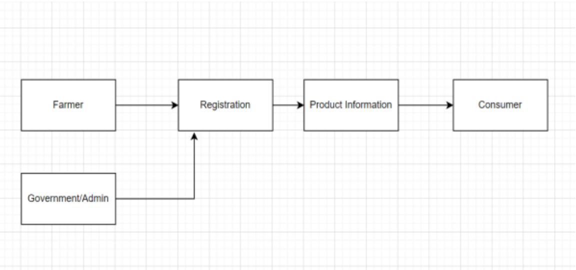
The design of [4] connects many platforms for supply chain information service. Nodes for the administrator, producer, processor, logistics, and distributor are present in the system. The system is divided into four parts. They are the Application Layer, which includes a Web user interface and Internet of Things devices, the Service Layer, which includes Node.js, the Contract Layer, which includes smart contracts, the Data Layer, which includes data from the Ethereum Blockchain, and the MySQL Database. It explains timestamp reliance, reputation management, and the tracing procedure.

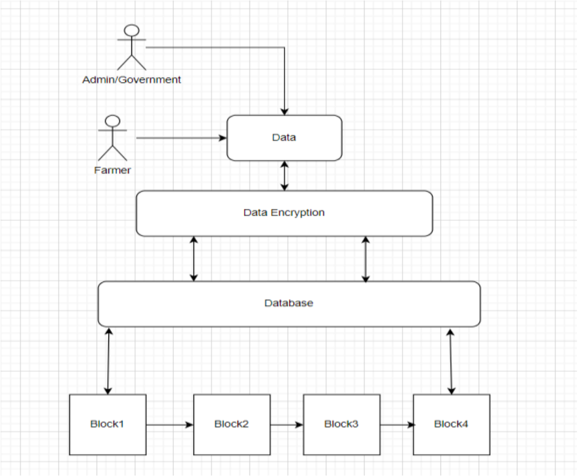
This [5] examines the viability of a Business-to-Consumer (B2C) business model using the Ethereum blockchain to enable online supply chain systems. They suggest the Consumer Ordering Consensus Protocol (COCP) for B2C online retailers to process orders safely and quickly. They contrast three distinct systems: a physical retail store, an online retailer, and an online retailer based on smart contracts for order requests. To showcase smart contracts in the B2C Supply Chain system, they have created an application. When conducting order transactions, from placing an order to receiving a shipment, they talk about the function of smart contracts.

The different options available to developers when creating an app on the Ethereum blockchain technology are discussed in [6]. It covers how to set up several software programs that are useful while setting up a blockchain system. That includes Visual Studio code, Truffle, Ganache, Node Package Manager, and Node Package Manager. It provides the potential tool set needed to create applications on Ethereum quickly. [7] provides a comparison of the network's various blockchain technologies. It provides a detailed explanation of the blockchain's recording and transaction processes. It is mentioned how blockchain is being used in numerous areas. It is suggested to use the fundamental framework of Item, Store, Carrier, Insurance, Importer, Wholesaler, and Retailer, Customer. Blockchain enables businesses to advance their internal processes, which fosters organization growth.

III. Proposed Method

A. System Design





B. Implementation

A) Farmer:Is the producer who produce quality products.
provider: providers of raw materials, such as seeds and nutrients, but also pesticides, chemicals, etc; B) producer: usually the farmer e.g., the responsible of the actions from seeding/planting to harvesting; C) processor: this actor may perform various actions, from simple packaging to more complex processes (e.g., pressing of the olives); D) distributor: this actor is responsible of moving the output of the processor (e.g., the product) from processor’s site to retailers; E) retailer: this actor is responsible of selling the products, representing it either small local stores or big supermarkets; F) consumer: the final element of the chain.
Step 1. The alert can be activated by the IOT module when it senses a fall detection, or fall or rise in blood pressure, pulse rate, temperature or humidity above or below a specified optimal value.

Step 2. When an alert is triggered, a request is sent to the server, which retrieves the information and sends an emergency message to the registered emergency contacts as well as other health measurements that are updated at certain intervals.

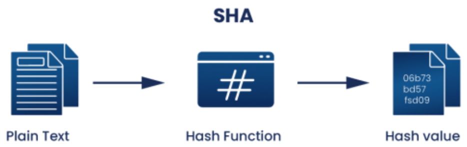
Step 3: The server will simultaneously have access to the whereabouts of any nearby users who have registered for the app. In order to get help or rescue for the victim as soon as possible, the server will transmit the same message to everyone within 500 meters of the victim.

Step 4 The identical request is also sent to the admin panel so that it can be forwarded to the police station, hospital, etc. The website also has a section on laws pertaining to women, child protection, and punishments, among other things.In order to enhance the functionality of the app, there is also a feedback section.

V. Algorithm

SHA

SHA stands for secure hashing algorithm. SHA is a modified version of MD5 and used for hashing data and certificates. A hashing algorithm shortens the input data into a smaller form that cannot be understood by using bitwise operations, modular additions, and compression functions. You may be wondering, can hashing be cracked or decrypted? Hashing is similar to encryption, the only difference between hashing and encryption is that hashing is one-way, meaning once the data is hashed, the resulting hash digest cannot be cracked, unless a brute force attack is used. See the image below for the working of SHA algorithm. SHA works in such a way even if a single character of the message changed, then it will generate a different hash. For example, hashing of two similar, but different messages i.e., Heaven and heaven is different. However, there is only a difference of a capital and small letter.



The initial message is hashed with SHA-1, resulting in the hash digest “06b73bd57b3b9”. If the second, similar, message is hashed with SHA-1, the hash digest will look like “66da9f3b8d9d8”. This is referred to as the avalanche effect. This effect is important in cryptography, as it means even the slightest change in the input message completely changes the output. This will stop attackers from being able to understand what the hash digest originally said and telling the receiver of the message whether or not the message has been changed while in transit.

SHAs also assist in revealing if an original message was changed in any way. By referencing the original hash digest, a user can tell if even a single letter has been changed, as the hash digests will be completely different. One of the most important parts of SHAs are that they are deterministic. This means that as long as the hash function used is known, any computer or user can recreate the hash digest. The determinism of SHAs is one of reasons every SSL certificate on the Internet is required to have been hashed with a SHA**.**

Different SHA Forms

When learning about SHA forms, several different types of SHA are referenced. Examples of SHA names used are SHA-1, SHA-2, SHA-256, SHA-512, SHA-224, and SHA-384, but in actuality there are only two types: SHA-1 and SHA-2. The other larger numbers, like SHA-256, are just versions of SHA-2 that note the bit lengths of the SHA-2. SHA-1 was the original secure hashing algorithm, returning a 160-bit hash digest after hashing. Someone may wonder, can SHA-2 be cracked like SHA-1? The answer is yes. Due to the short length of the hash digest, SHA-1 is more easily brute forced than SHA-2, but SHA-2 can still be brute forced. Another issue of SHA-1 is that it can give the same hash digest to two different values, as the number of combinations that can be created with 160 bits is so small. SHA-2 on the other hand gives every digest a unique value, which is why all certificates are required to use SHA-2.

SHA-2 can produce a variety of bit-lengths, from 256 to 512 bit, allowing it to assign completely unique values to every hash digest created. Collisions occur when two values have the same hash digest. SHA-1 can easily create collisions, making it easier for attackers to get two matching digests and recreate the original plaintext Compared to SHA-1, SHA-2 is much more secure and has been required in all digital signatures and certificates since 2016. Common attacks like brute force attacks can take years or even decades to crack the hash digest, so SHA-2 is considered the most secure hash algorithm.

Browser	Minimum Browser Version
Chrome	26+
Firefox	1.5+
Internet Explorer	6+ (With XP SP3+)
Netscape	7.1+
Safari	3+ (Ships with OS X 10.5)
Mozilla	1.4+

What SHA is used for and Why?

As previously mentioned, Secure Hashing Algorithms are required in all digital signatures and certificates relating to SSL/TLS connections, but there are more uses to SHAs as well. Applications such as SSH, S-MIME (Secure / Multipurpose Internet Mail Extensions), and IPSec utilize SHAs as well. SHAs are also used to hash passwords so that the server only needs to remember hashes rather than passwords. In this way, if an attacker steals the database containing all the hashes, they would not have direct access to all of the plaintext passwords, they would also need to find a way to crack the hashes to be able to use the passwords. SHAs can also work as indicators of a file's integrity. If a file has been changed in transit, the resulting hash digest created from the hash function will not match the hash digest originally created and sent by the file's owner.

We have now learned what SHAs are used for, but why use a Secure Hashing Algorithm in the first place? A common reason is their ability to stop attackers. Though some methods, like brute force attacks, can reveal the plaintext of the hash digests, these tactics are made extremely difficult by SHAs. A password hashed by a SHA-2 can take years, even decades to break, thus wasting resources and time on a simple password, which may turn many attackers away. Another reason to use SHAs is the uniqueness of all the hash digests. If SHA-2 is used, there will likely be few to no collisions, meaning a simple change of one word in a message would completely change the hash digest. Since there are few or no collisions, a pattern cannot be found to make breaking the Secure Hashing Algorithm easier for the attacker. These are just a few reasons why SHA is used so often.

SHA 2 Limitations

Browser support

Server Support

Operating System	SSL Certificate Minimum OS Version	Client Certificate Minimum OS Version
Android	2.3+	2.3+
iOS	3.0+	3.0+
ChromeOS	YES	YES
Mac OS X	10.5+	10.5+
Windows XP	SP3+ XP	SP3+ (partial)
Windows Server	2003 SP2 +Hotfixes (Partial)	2003 SP2 +Hotfixes (Partial)
Windows Phone	7+	7+
Blackberry	5.0+	5.0+

OS Support

The Future of Hashing

At this point in time, SHA-2 is the industry standard for hashing algorithms, though SHA-3 may eclipse this in the future. SHA-3 was released by the NIST, which also created SHA-1 and SHA-2, in 2015 but was not made the industry standard for many reasons. During the release of SHA-3, most companies were in the middle of migrating from SHA-1 to SHA-2, so switching right on to SHA-3 while SHA-2 was still very secure did not make sense. Along with this, SHA-3 was seen as slower than SHA-2, although this is not exactly the case. SHA-3 is slower on the software side, but it is much faster than SHA-1 and SHA-2 on the hardware side, and is getting faster every year. For these reasons, we will likely see the move to SHA-3 later on down the line, once SHA-2 becomes unsafe or deprecated.

Server	Minimum Server Version
AWS (Amazon Web Services)	YES
Apache	2.0.63+ w/ OpenSSL 0.9.8o+
Cisco ASA 5500	8.2.3.9+ for AnyConnect VPN Sessions; 8.4(2)+ for other functionalities
Java based products	Java 1.4.2+
IBM Domino Server	9.0+ (Bundled with HTTP 8.5+)
IBM HTTP Server	8.5+ (Bundled with Domino 9+)
IBM z/OS	v1r10+
OpenSSL based products	OpenSSL 0.9.8o+
Oracle Wallet Manager	11.2.0.1+
Oracle Weblogic	10.3.1+
Web Sphere MQ	7.0.1.4+

V. Conclusion

This paper promotes the idea to build a system that can trace the agriculture product from farmer to consumer securely. This application will present a highly secure, reliable, understated, and practical solution.

VI. Reference

[1] Aarina Aarnisalo, Kaarle Jaakkola, Laura Raaska, Seppo Heiskanen, and Eva Landor. Traceability of foods and foodborne hazards. VTT Tiedotteita - Valtion Teknillinen Tutkimuskeskus, (2395):1 - 46, 2007.

[2] E. Abad, F. Palacio, M. Nuin, A. G. Zarate, A. Juarros, J. M. Gomez, and S. Marco. Rfid smart tag for traceability and cold chain monitoring of foods: Demonstration in an intercontinental fresh fish logistic chain. Journal of Food Engineering, 93(4):394-399, 2009.

[3] Mustafa Alani, Widad Ismail, and Js Mandeep. Active rfid system and applications. Electronics World, 115 (1877):22-24, 2009.

[4] Jose A. Alfaro and Luis A. Rabade. Traceability as a strategic tool to improve inventory management: A case study in the food industry. International Journal of Production Economics, 118(1):104 - 110, 2009.

[5] Cecilia Amador, Jean-Pierre Emond, and Maria Cecilia do Nascimento Nunes. Application of rfid technologies in the temperature mapping of the pineapple supply chain. Sensing and Instrumentation for Food Quality and Safety, 3(1):26-33, 2009. [6] Anonymous. The aloha tracker. Industrial Engineer, pages 50-52, 2008.

[6] Sandip Jangir, Alok Jaiswal, Sheetal Chandel, "A Novel Framework for Pharmaceutical Supply Chain Management using Distributed Ledger and Smart Contracts", 2019 10th International Conference on Computing, Communication and Networking Technologies (ICCCNT), Kanpur, India, 2019, pp. 1-7, doi: 10.1109/ICCCNT45670.2019.8944829.

[7] Alok Jaiswal, Sheetal Chandel, Ajit Muzumdar, Madhu G M, Chirag Modi, C. Vyjayanthi, "A Conceptual Framework for Trustworthy and Incentivized Trading of Food Grains using Distributed Ledger and Smart Contracts ", 2019 IEEE 16th India Council International Conference (INDICON), Rajkot, India, 2019, pp. 1-4, doi: 10.1109/INDICON47234.2019.9030290

[8] Ravi Chandra Koirala, Keshav Dahal, Santiago Matalonga, "Supply Chain using Smart Contract: A Blockchain enabled model with Traceability and Ownership Management ", 9th International Conference on Cloud Computing, Data Science & Engineering (Confluece 2019)

[9] Zhijun Xu, Yichen Liu, Jun Zhang, Zhaoxiong Song, Jun Li, Jihua Zhou, "Manufacturing Industry Supply Chain Management Based on the Ethereum Blockchain", 2019 IEEE International Conferences on Ubiquitous Computing & Communications (IUCC) and Data Science and Computational Intelligence (DSCI) and Smart Computing, Networking and Services (SmartCNS), Shenyang, China, 2019, pp. 592-596, doi: 10.1109/IUCC/DSCI/SmartCNS.2019.00124.

[10] Feiyang Qu1, Hisham Haddad1, Hossain Shahriar2, "Smart Contract-based Secured Business-to-Consumer Supply Chain Systems", 2019 IEEE International Conference on Blockchain (Blockchain), Atlanta, GA, USA, 2019, pp. 580-585, doi: 10.1109/Blockchain.2019.00084 [11] RuhiTaş, ÖmerÖzgürTanrıöver, "Building A Decentralized Application on the Ethereum Blockchain ", 2019 3rd International Symposium on Multidisciplinary Studies and Innovative Technologies (ISMSIT), Ankara, Turkey, 2019, pp. 1-4, doi: 10.1109/ISMSIT.2019.8932806 [12] Rana M. Amir Latif, Samar Iqbal, Osama Rizwan, Syed Umair Aslam Shah, Muhammad Farhan, Farah Ijaz "Blockchain

transforms the Retail Level by using a supply chain Rules and Regulation", 2019 2nd International Conference on Communication, Computing and Digital systems (C-CODE), Islamabad,