FOOD TRUST: FOOD SECURITY USING BLOCKCHAIN

Dr. Surekha Mariam Varghese, Shilpa Sreedhar K, Shilpa K V, Vishnupriya M

Professor and HOD,
Department of Computer Science and Engineering

Mar Athanasius College of Engineering
Kothamangalam, Kerala, India

***Abstract:* In recent times food safety has drawn upsurge of academic and commercial concerns. In supply chain area, with the rapid growth of internet technologies, a lot of emerging technologies has been applied in traceability systems. However, to date, nearly all of these systems are centralized which are monopolistic, asymmetric and opaque that could result in the trust problem, such as fraud, corruption, tampering and information. Besides, centralized system is vulnerable to collapse, since a single point of breakdown will lead the whole system to be crashed. Today, a new technology called the blockchain which is a ground-breaking innovation in decentralized information technology presents a whole new approach. Here we will build a food supply chain traceability system for real-time food tracing based on blockchain. Using blockchain could usher in a new era of food traceability, and that it benefit areas beyond food safety, such as im- proving sustainability by reducing waste and lowering costs by eliminating food system sciences. Moreover, using blockchain could enable the capture of data beyond mere traceability attributes including those that promote greater transparency.**

***K*eywords: Food supply chain; traceability systems; decentralized systems; blockchain; food safety**

I.INTRODUCTION

People often talk about the food supply chain, but in reality it isn’t a chain at all. The food system today—that is, the way we get our food from farm to table— has evolved into a complex network that is interdependent on many entities. And while there is no question that today’s food system provides consumers with a more diverse, convenient, and economical source of food, it also presents new challenges. For example, in today’s food system, the output from one ingredient producer could end up in thousands of products on a grocery store shelf.

Today there is no widely adopted industry standard for how each segment of the food system (farmer, processor, distributor, retailer, etc.) tracks and records data for food traceability purposes. Many simply record their data on paper, and while some are using digital methods, these methods do not enable communication with other parties in the food system. Thus, the system is limited to traceability capabilities that are often described as “one step forward and one step back.” Piecing together traceability data by sifting through hundreds or even thousands of documents during a foodborne outbreak can be slow and complicated, and it all too often is not an effective way of identifying and informing action through lessons learned to prevent future outbreaks.

These inefficiencies and complexities are one of the many reasons we at ’Food Trust’ were looking for a technological solution to help us achieve enhanced food trace- ability and transparency.

Similarly, there is a very important issue has not been touched is that whether the information shared by food supply chain members in the traceability systems can be trusted. This kind of centralized organization could become so powerful by possession of this data that could result in information asymmetry between the organizations and individuals. It can become a vulnerable target for bribery, and if, for example, the administrator can be bribed, valuable information can be tampered with, and then the whole system can not be trusted anymore.

Another potential risk is that it has a single point of failure which leaves the whole system vulnerable to failure (e.g. hacking and corruption). The novel technology that could be the key to these issues is the blockchain, which can remove the reliance on a central entity. Instead of storing data in an opaque network sys- tem, with the blockchain, all the information of the food products can be stored in a shared and transparent system for all the members along the supply chain.

Blockchain is a technology that enables the creation of a decentralized, dis- tributed, and trusted digital ledger that can be used to record transactions from multiple entities across a complex network. A record on a blockchain cannot be altered retroactively without the alteration of all preceding blocks and the consensus of the network.

How to enhance food traceability and transparency for our customers is one challenge that has been working on. Blockchain is often associated with cryptocur- rency, but it is being looked at more and more as a solution to food-supply problems that will enhance trust and transparency. Using blockchain could usher in a new era of food traceability, and that it could benefit areas beyond food safety, such as improving sustainability by reducing waste and lowering costs by eliminating food system sciences.

Moreover, using blockchain could enable the capture of data be- yond mere traceability attributes (where and when), including those that promote greater transparency (How was food produced? Was it sustainably grown?).

It is time for a technology like blockchain to transform the food sector and usher in a new era of transparency. Because it can improve our ability to definitively link foodborne outbreaks to their causative food vehicle, which could result in fewer and smaller outbreaks and fewer people harmed. It could allow for more recent analysis to determine the root cause of an outbreak, which also would inform future prevention efforts. The U.S. Centers for Disease Control and Prevention estimates that 48 million consumers get sick from foodborne illnesses each year. The global estimates by the World Health Organization are even more concerning.

One of the reasons unscrupulous suppliers are willing to commit food fraud is because they do not fear being caught, due to the anonymity of how food is produced and where it comes from. Having a digital, real-time ability to monitor and trace food as it flows from farm to store will be a strong deterrent for such fraudulent activities, as it will create a digital footprint that leads back to a fraudster's door.

Ultimately, blockchain-enabled traceability will create greater food transparency, which will lead to greater accountability and incentivize every stakeholder in the food system to do the right thing every time. Greater accountability will in turn encourage stakeholders to take greater responsibility for food safety, which will promote greater trust within the supply chain. Consumers are already demanding this, and it's up to the industry to step up to meet this challenge.

As an emerging technology, blockchain has its inherent shortcomings, and with the increasing application, scalability has become a primary and urgent concern. Here we will try to find a solution from the perspective of the blockchain and dis- tributed database. We hope that our system could make food traceability from "farm to fork" become a reality, and rebuild public confidence in the food supply chain.

II.EXISTING SYSTEM

Contamination in the context of food can be described as "the introduction or occurrence of an unwanted organism, taint or substance to packaging, food, or the food environment" . Food safety hazards have been defined as "a biological, chemical, or physical agent in, or condition of, food with the potential to cause an ad- verse health effect" . Codex Alimentarius defines a contaminant as: "any substance not intentionally added to food, which is present in such food as a result of the production (including operations carried out in crop husbandry, animal husbandry, and veterinary medicine), manufacture, processing, preparation, treatment, pack- ing, packaging, transport, or holding of such food or as a result of environmental contamination. The term does not include insect fragments, rodent hairs, and other extraneous matter".

Food defense is the collective term used to describe the activities associated with protecting the nation's food supply from deliberate or intentional acts of contamination or tampering. Food defense therefore encompasses intentional contamina- tion (perhaps better phrased as adulteration) of the food supply contrasting with the unintentional contamination that is the focus of established food safety measures. Further, food defense has been described as a process to ensure the security of food and drink and their supply chains from all forms of intentional malicious at- tack including ideologically motivated attack leading to contamination or supply failure . This definition suggests that the term food defense is not only used to de- fine national strategy toward intentional food adulteration, but also can be used at the supply chain and organizational level.

The HACCP which focused on risk management and prevention was considered to be synonymous with food safety.It can be easily linked to operational manage- ment and food chain safety assurance. In order to obtain high quality milk,Vilar et al. (2012)[1] implemented HACCP method on dairy supply chain, and they focus on the milk equipment and cooling tanks which could influence the milk quality by the hazards such as microbiological and chemical residues. They proved that imple- mentation of HACCP can be a feasible strategy for dairy supply chain safety. Based on a Pareto analysis, Fotopoulos et al. (2011)[2] examined the literature on the food safety assurance systems and recorded the vital critical factors which affect the implementation of HACCP. By using a case study, Herath Henson (2010)[3] pointed out four barriers to HACCP implementation, including perceptions which HAPPC is of "questionable appropriateness" to the company, the scale of change required to achieve implementation, low priority given to enhancement of food safety controls, and financial constraints.

With the rapid growth of internet of things, many researchers consider the appli- cation of relevant technologies for traceability systems in food supply chains. Foli- nas et al. (2006) pointed out that the efficiency of a traceability system depends on the ability to track and trace each individual product and logistics units, in a way that enables continuous monitoring from primary production until final disposal by the consumer. Shanahan et al. (2009) suggested a RFID based framework for beef traceability from farm to slaughter. By using RFID for the identification of individual cattle, this system proposed as a solution to the inaccessibility of trace- ability records and fraudulent activities. In order to build an automated system which integrates online traceability data and chill chain condition monitoring in- formation, Abad et al. (2010) tried to validate an RFID smart tag developed for real-time traceability and cold-chain monitoring of food under the case study of an intercontinental fresh fish logistics chain. Mattoli et al. (2010) developed a Flexible Tag Data-logger (FTD) which is attached to the bottles for collecting en- vironmental data, (like light, humidity, and temperature) in order to trace the wine bottles to a supermarket. The history data stored in the FTD can be read by smart phone or Personal Digital Assistant (PDA) with integrated infrared port to evaluate the safety status of wine bottles.

Typical hazard controls for the food supply chain includes

- **Safety risk from background environment**

The control measures that can be taken for the safety risks from background environment involves site assessment as part of assured scheme. Some assessments that can be made are the quality check on soil, water, air, sunlight, etc. This scheme needs regular monitoring for the smooth flow and functioning of the system. A routine reassessment is also highly advised for this kind of risk scenarios. The site classification can be reviewed for any faults in the system. It also requires reassess- ment of site designation which includes documentation of actions to be taken.

- **Safety risk from field practices**

The safety risk due to field practices in growing can be controlled by keeping and maintaining everything accordingly in the best manner. There is a need for good working conditions and practices in the field. The growing information also needs to be recorded properly. The facts that are to be recorded include variety, item number, producing area, growth conditions etc. Along with these planting time, plucking time and staff needs to be recorded in the right manner. The monitoring practice can be site documentation. As a corrective action against this type of hazard, the procedures need to be reviewed and revised. There is an urgent need for the reviews of the training provided to the workforce. All the actions and corrections are to be documented.

- **Excess residues of applied fertilizers and pesticides**

As a control measure to the excess use of fertilizers and pesticides, there needs strict measures to be taken to ensure the purchase of these from reputed suppliers. All the applied chemicals come under this measure. The situation in which these fertilizers and pesticides are applied is also recorded and monitored. The monitoring scenario can also expand to include the documentation from the supplier, and the documentation at the site. A regular approval check can be made mandatory for controlling this hazard. There should be corrective actions to review the status of the supplier for verification. The status of the producer also needs to be reviewed, along with review of the training given to the workforce. All the actions taken are carefully documented.

- **Safety risk associated with processing environment**

The working site should be under assessment as part of the scheme. Site assess- ment include checking and control activities such as temperature controlling, disin- fecting, equipment check etc. The monitoring task comprises of regulator approval and routine reassessment. The documentation at site is also a major factor in this. The corrective action to be enforced mainly is the review of the site classification. The site designations are reassessed and all the actions taken are documented.

- **Safety risk associated with processing step**

The processing step should follow all the required rules and regulations. It should be according to good working practices and professional ethics. The use of suitable process additives for their intended purposes are also recommended. The monitoring tasks typically include site documentation and documentation at the sup-plier end. This hazard lists a set of actions as corrective measures to be taken. The procedures and the training given to workforce should be reviewed. All the actions taken must be documented. The status from the supplier end should be reviewed and the necessary documentations need to be done as well.

- **Safety risk from site equipment**

The proper actions need to be done to ensure that there does not occur any safety risk from the equipment at site. All the equipment needs to be properly maintained. There should be facilities for cold storage, and additional temperature and humidity controlling systems. The monitoring tasks limits to records of the maintenance works that have happened. The corrective actions involve the review of the maintenance procedures, and a review of the workforce training. As with all the other hazard controls, all the taken actions need to be documented for future reference.

- **Safety risk from warehouse management**

The warehouse should be properly managed with all the good working practices as per the rules and guidelines issued. For example, the environment of cold storage needs to be recorded, along with the quality and storage time of products that are present in the warehouse. Monitoring involves site documentation. The procedures need to be reviewed. The workforce training needs to be reviewed. All these actions need to be documented as well.

- **Safety risk from site equipment**

There should be proper control measures to ensure that all the equipment are well maintained. An example includes facilities for a refrigerated truck. The monitoring tasks involve maintenance records of all the equipment. The procedures need to be reviewed. The workforce training needs to be reviewed. All these actions need to be documented.

- **Safety risk associated with retail management**

All the retail management practices should be according to good working prac- tices and this should be guaranteed. Examples include using the refrigeration; checking the lifetime; replacing expired products. Monitoring deals with site doc- umentation. The procedures need to be reviewed. The workforce training needs to be reviewed. All these actions need to be documented.

III.PROPOSED SYSTEM

We have developed a blockchain project which will help to trace the entire journey of a food product.The solution provides authorized users with immediate access to actionable food supply chain data, from farm to store and ultimately the consumer. The complete history and current location of any food item along with its accompanying information .Food Trust solution assigns predefined roles that grant users Authorization to execute specific network tasks on behalf of their Organiza- tion. Assigning roles enables Account Administrators to easily control the level of access provided to each individual user in their Organization. Each member orga- nization owns its data on the blockchain network and maintains full control over who can access different data elements. All data is stored on blockchain ledgers, protected with the highest level of encryption, and is made accessible only as data owners grant permission to share relevant records. Data connector application pro- gramming interfaces allow enterprise IT teams to efficiently upload supply chain data from existing data stores to their Food Trust network for seamless integration of data from enterprise systems to a Food Trust solution network. Smaller organi- zations can on board data through an easy-to-use web experience. When it comes to food safety, speed is paramount in controlling food-borne contamination—so is the accuracy of the information that the investigating team acts on. To use the Food Trust solution to trace food products, data on food products needs to be uploaded to the network by participants. Once data is uploaded, the trace module allows an authorized user to search the provenance of a food product via product id. This module enables participant organizations to quickly and accurately determine the path that a given shipment has taken. Authorized participants can then determine the scope of the problem, block further contamination, and narrow the scope and impact of a recall.

IV. SYSTEM DESIGN

1. INPUT DESIGN

It is part of the overall system design. Internal control must be established for monitoring number of input and for ensuring that the data is coming from a registered user. The basic steps involved in the system design are:

- **Review input requirements**
- **Decide how the input data represents**
- **Design the source document**
- **Prototype online input screens**

The quality of the system input determines the quality of the system output. Input specification describes the manner in which data enter the system for pro- cessing. Input design features can ensure the reliability of the system and produce results from the accurate data, or they can result in production the input design also determines whether the user can interact efficiently with the system.

2. MODULAR DESIGN

The major modules in Food Trust are listed as follows.

- **User**

Users being the consumers of any product does not need to login or register. The user can know the entire journey of the product when specifying the product id of that particular product.

- **Data Acquisition and Processing**

The data entered by the organisation they are part of the network is used for building the history of products. The data is converted to encrypted form and used for further processing. Supply chain members can register themselves in the system as a user through the registrar, which can provide credentials and a unique identity to the members. After registration, a public and private cryptographic key pair will be generated for each user. The public key can be used to identify the identity of the user within the system and the private key can be used to authenticate the user when interacting with the system. This enables each product can be digitally addressed by the users when being updated, added, or exchanged to the next user in the downstream position of the supply chain.

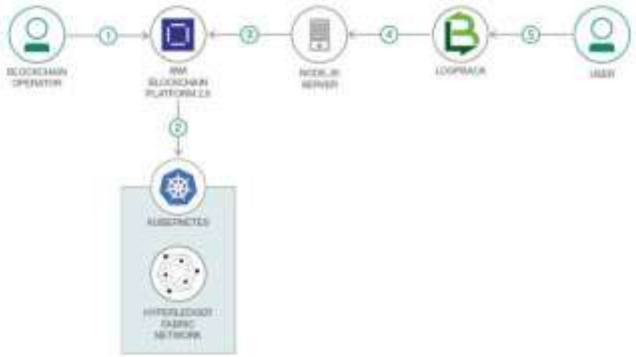
In food supply chains, when a user who is in a particular link receives a product, only this user can add new data into the profile of the product with its private key. In addition, when user transfers this product to the next user, both of them have to sign a digital contract to authenticate the exchange. Therefore, the details of the transaction will be added to the BigchainDB and the system will process and update the data in the product's profile automatically, which allows users in the system sharing the status of the products at anytime.

After receiving products, processing enterprise could read the product's profile by entering their product id in the html page.

3. OUTPUT DESIGN

It is the part of overall system design. The goal of the output design is to cap- ture the output and get the data into a format suitable for the computer. Data flow diagram identifies the data tone entered and the output to the system. Output is the information delivered to the users through an html page. Without quality output the entire system appears to be unnecessary that users will avoid using it. Users gener- ally merit the system solely by its output in order to create the most useful output possible. One works closely with the user through an interactive process until the result is considered to be satisfactory. The output of the system depends on data entered by the participating organisations.

4. DATA FLOW DIAGRAM



IMPLEMENTATION

Implementation comprises of detailed modular design of the system, how var- ious functions work, their core algorithm. Detailed design of a project deals with the entire functionality it handles. A well-defined detailed description includes ma- jor functional components in that application along with sub modules included and table handled. It shows actual data flow within the system and how each function handles the data. In computer science, an implementation is a realization of a techni- cal specification or algorithm as a program, software component, or other computer system through computer programming and deployment. Many implementations may exist for a given specification or standard. In an information technology con- text, software or hardware implementation encompasses all the post-sale processes involved in something operating properly in its environment, including analysing requirements, installation, configuration, customization, running, testing, systems integrations, user training, delivery and making necessary changes. The word "deployment" is sometimes used to mean the same thing.

For an implementation process to be successful, many tasks between different departments need to be accomplished in sequence. Companies strive to use proven methodologies and enlist professional help to guide them through the implementa- tion of a system but the failure of many implementation processes often stems from the lack of accurate planning in the beginning stages of the project due to inadequate resources or unforeseen problems that arise. Software/hardware implementations should always be designed with the end user in mind and the implementation pro-cess usually benefits from user involvement and support from managers and other top executives in the company. If users participate in the design and implementation of the system, ideally it will serve their business objectives more accurately and re- flect their priorities and the ways in which they prefer to work. Software/hardware implementations should always be designed with the end user in mind and the implementation process usually benefits from user involvement. Their involvement in the process also makes them more receptive to changes that need to be implemented because they have first hand experience of what the system comprises.

A. A FAIR TRADE SUPPLY NETWORK WITH HYPERLEDGER FABRIC 1.4

Since this is a big network, we can not complete the entire system on a project. So, we imply a chain of coffee . Here we will create a blockchain app that in- creases visibility and efficiency in the supply chain of a coffee retailer using IBM Blockchain Platform V2 Beta. We will use different transactions to show differ- ent possible actions for the different participants in the supply chain. This sample application will record all transactions on the IBM Blockchain Platform V2 Beta, and enable a coffee retailer to ensure the customer that their coffee is organic and fair-trade.

IBM Blockchain Platform V2 Beta, IBM Cloud Kubernetes Service and IBM Blockchain Platform Extension for VS Code are the included components in the project. IBM Blockchain Platform V2 Beta gives you total control of your blockchain network with a user interface that can simplify and accelerate your journey to deploy and manage blockchain components on the IBM Cloud Kubernetes Service. IBM Cloud Kubernetes Service creates a cluster of compute hosts and deploys highly available containers. A Kubernetes cluster lets you securely manage the resources that you need to quickly deploy, update, and scale applications. IBM Blockchain Platform Extension for VS Code is designed to assist users in developing, testing, and deploying smart contracts – including connecting to Hyperledger Fabric envi- ronments. Featured technologies included are Hyperledger Fabric v1.4 , Node.js and Loopback 4. Hyperledger Fabric v1.4 is a platform for distributed ledger so- lutions, underpinned by a modular architecture that delivers high degrees of con- fidentiality, resiliency, flexibility, and scalability. Node.js is an open source, cross- platform JavaScript run-time environment that executes server-side JavaScript code. Loopback 4 LoopBack is a highly-extensible, open-source Node.js framework that enables you to: Create dynamic end-to-end REST APIs with little or no coding. Access data from major relational databases, MongoDB, SOAP and REST APIs. Incorporate model relationships and access controls for complex APIs.

B. START WITH VISUAL STUDIO CODE

Clone the repo onto our computer in the destination of our choice, then go into the web-app folder and install dependencies. Next, we have to package the smart contract and then run our smart contract on the cloud.

C. CREATE IBM CLOUD SERVICES

So for this the first thing we'll need to do is actually create a free cluster so if we go into Kubernetes. If we just go to IBM cloud we can do so. We can go into the cube or in Eddie's and then we'll just want to create this light plan that's free .

Once we've created our cloud service then we can see that we are greeted with our blockchain platform home page. Go ahead and the first thing we want to do is create a certificate authority. Because before we can actually install the smart contract on the peer and interact with the smart contract , we can actually update the ledger and send transactions to the orderer and then cut blocks and then up- date the ledger. we have to create identifiers and we have to make sure that the certificate authority knows who is transacting on the network and that they are all approved by the certificate authority . We will build a network as provided by the IBM Blockchain Platform documentation. This will include creating a channel with a single peer organization with its own MSP and CA (Certificate Authority), and an orderer organization with its own MSP and CA. We will create the respective iden- tities to deploy peers and operate nodes. So we'll go ahead and add certificate. Inorder to create your peer organization CA, Click Add Certificate Authority. Select IBM Cloud under Create Certificate Authority and Next. Give it a Display name of Org1 CA. Specify an Admin ID of admin and Admin Secret of adminpw.

Use the CA to register identities. For that Select the Org 1 CA Certificate Au- thority that we created. First, we will register an admin for our organization "org1". Click on the Register User button. Give an Enroll ID of org1admin, and Enroll Se- cret of org1adminpw. Click Next. Set the Type for this identity as client and select org1 from the affiliated organizations drop-down list. We will leave the Maximum enrollments and Add Attributes fields blank. We will repeat the process to create an identity of the peer. Click on the Register User button. Give an Enroll ID of peer1, and Enroll Secret of peer1pw. Click Next. Set the Type for this identity as peer and select org1 from the affiliated organizations drop-down list. We will leave the Maximum enrollments and Add Attributes fields blank.

Now create the peer organization MSP definition. Navigate to the Organizations tab in the left navigation and click Create MSP definition. Enter the MSP Display name as Org1 MSP and an MSP ID of org1msp. Under Root Certificate Authority details, specify the peer CA that we created Org1 CA as the root CA for the organi-zation. Give the Enroll ID and Enroll secret for your organization admin, org1admin and org1adminpw. Then, give the Identity name, Org1 Admin. Click the Generate button to enroll this identity as the admin of your organization and export the iden- tity to the wallet. Click Export to export the admin certificates to your file system. Finally click Create MSP definition.

Next step is to create a peer. On the Nodes page, click Add peer. Click IBM Cloud under Create a new peer and Next. Give your peer a Display name of Peer Org1. On the next screen, select Org1 CA as your Certificate Authority. Then, give the Enroll ID and

Enroll secret for the peer identity that you created for your peer, peer1, and peer1pw. Then, select the Administrator Certificate (from MSP), Org1 MSP, from the drop-down list and click Next. Give the TLS Enroll ID, admin, and TLS Enroll secret, adminpw, the same values are the Enroll ID and Enroll secret that you gave when creating the CA. Leave the TLS CSR hostname blank. The last side panel will ask you to Associate an identity and make it the admin of your peers. Select your peer admin identity Org1 Admin. Review the summary and click Submit.

Create the node that orders transactions. Create your orderer organization CA. Click Add Certificate Authority. Click IBM Cloud under Create Certificate Author- ity and Next. Give it a unique Display name of Orderer CA. Specify an Admin ID of admin and Admin Secret of adminpw. Use your CA to register orderer and orderer admin identities In the Nodes tab, select the Orderer CA Certificate Author- ity that we created. First, we will register an admin for our organization. Click on the Register User button. Give an Enroll ID of ordereradmin, and Enroll Secret of ordereradminpw. Click Next. Set the Type for this identity as client and select org1 from the affiliated organizations drop-down list. We will leave the Maximum enrollments and Add Attributes fields blank. We will repeat the process to create an identity of the orderer. Click on the Register User button. Give an Enroll ID of orderer1, and Enroll Secret of orderer1pw. Click Next. Set the Type for this identity as peer and select org1 from the affiliated organizations drop-down list. We will leave the Maximum enrollments and Add Attributes fields blank.

Create the orderer organization MSP definition. Navigate to the Organizations tab in the left navigation and click Create MSP definition. Enter the MSP Display name as Orderer MSP and an MSP ID of orderermsp. Under Root Certificate Au- thority details, specify the peer CA that we created Orderer CA as the root CA for the organization. Give the Enroll ID and Enroll secret for your organization admin, ordereradmin and ordereradminpw. Then, give the Identity name, Orderer Admin. Click the Generate button to enroll this identity as the admin of your organization and export the identity to the wallet. Click Export to export the admin certificates to your file system. Finally click Create MSP definition.

Now create an orderer. On the Nodes page, click Add orderer. Click IBM Cloud and proceed with Next. Give your peer a Display name of Orderer. On the next screen, select Orderer CA as your Certificate Authority. Then, give the Enroll ID and Enroll secret for the peer identity that you created for your orderer, orderer1, and orderer1pw. Then, select the Administrator Certificate (from MSP), Orderer MSP, from the drop-down list and click Next. Give the TLS Enroll ID, admin, and TLS Enroll secret, adminpw, the same values are the Enroll ID and Enroll secret that you gave when creating the CA. Leave the TLS CSR hostname blank. The last side panel will ask to Associate an identity and make it the admin of your peer. Select your peer admin identity Orderer Admin. Review the summary and click Submit.

Add organization as Consortium Member on the orderer to transact. Navigate to the Nodes tab, and click on the Orderer that we created. Under Consortium Members, click Add organization. From the drop-down list, select Org1 MSP, as this is the MSP that represents the peer's organization org1. Click Submit.

Its now time to create and join channel. Inorder to create the channel first of all navigate to the Channels tab in the left navigation. Click Create channel. Give the channel a name, mychannel. Select the orderer you created, Orderer from the orderers drop-down list. Select the MSP identifying the organization of the channel creator from the drop-down list. This should be Org1 MSP (org1msp). Associate available identity as Org1 Admin. Click Add next to your organization. Make your organization an Operator. Click Create. Inorder to join your peer to the channel, Click Join channel to launch the side panels. Select your Orderer and click Next. Enter the name of the channel you just created. mychannel and click Next. Select which peers you want to join the channel, click Peer Org1 . Click Submit.

D. DEPLOY SMART CONTRACT OF COFFEE ON THE NETWORK

The first step for this is to install a smart contract. Click the Smart contracts tab to install the smart contract. Click Install smart contract to upload the blockchainbean smart contract package file, which you packaged earlier using the Visual Studio code extension.

Click on the Add file and find your packaged smart contract. Once the contract is uploaded, click Install. Then instantiate smart contract. On the smart contracts tab, find the smart contract from the list installed on your peers and click Instantiate from the overflow menu on the right side of the row. On the side panel that opens, select the channel, mychannel to instantiate the smart contract on. Click Next. Select the organization members to be included in the policy, org1msp. Click Next. Give Function name of init and leave Arguments blank. Click Instantiate

E. CONNECT APPLICATION TO THE NETWORK

For that connect with sdk through connection profile. Under the Instantiated Smart Contract, click on Connect with SDK from the overflow menu on the right side of the row. Choose from the dropdown for MSP for connection, org1msp. Choose from Certificate Authority dropdown, Org1 CA. Download the connection profile by scrolling down and clicking Download Connection Profile. This will download the connection json which we will use soon to establish connection. You can click Close once the download completes.

Create an application admin Go to the Nodes tab on the left bar, and under Certificate Authorities, choose your organization CA, Org1 CA. Click on Register user. Give an Enroll ID and Enroll Secret to administer your application users, app-admin and app-adminpw. Choose client as Type and any organization for affiliation. We can pick org1 to be consistent. You can leave the Maximum enrollments blank. Under Attributes, click on the Add attribute. Give attribute as hf.Registrar.Roles = *. This will allow this identity to act as registrar and issues identities for our app. Click Add-attribute. Click Register. Now update application connection. Copy the connection profile you downloaded into server folder Name the connection profile you downloaded ibpConnection.json.

Update the config.json file with: The connection json file name you downloaded. The enroll id and enroll secret for your app admin, which we earlier provided as app-admin and app-adminpw. The orgMSP ID, which we provided as org1msp. The caName, which can be found in your connection json file under ”organization” -¿ ”org1msp” -¿ certificateAuthorities”. This would be like an IP address and a port. This is circled in red above. The username you would like to register. Update gateway discovery to enabled: true, asLocalhost: false to connect to IBP.

F. RUN THE APPLICATION

First, navigate to the server directory, and install the node dependencies. Run the enrollAdmin.js script. Now Register User by running the registerUser.js script. Start the web client. We are now able to access the loopback application.

To get started submitting our first transaction on the network, we can update the ledger with some of our suppliers info, such as their address, their uniqueId, and their organization. To do this, first click on GrowerController. You should see the Controller expand with the GET/POST methods. Click on the green POST/Grower button and then Try it out to the right of the POST/Grower button. This will enable you to write in a request body. Go ahead and write the code for the transaction and execute. If all went well, you can now go into your blockchain network, click on the channel, and then you should see the block height increased, and if you click on the last block, you should see the latest JSON that we input being written to the blockchain. We have made our first update to the ledger.

Similar way add the trader, shipper, retailer and the regulator. Add coffee and supply chain data to the network. Note that here we are getting all data that is associated with our batchId. I.e. on our ledger, we keep updating our key with more and more data. So that the value of our key keeps expanding with more supply chain data. At the end of our app, we can then query and parse the important data.

VI. RESULT

While starting with food traceability, the ultimate goal was greater food trans- parency, which will benefit all food system stakeholders. In case there is any attempt to alter a food item anywhere within the supply chain, blockchain technology would immediately identify it and notify the producer before the item reaches a retailer. Blockchain supported retailers by identifying the altered items that may somehow reach the shelves. This eliminated the practice of batch recalls which are extremely costly for the producer of the item.

The output of the application shows that each cup has a history based on which batch of coffee was used to make the cup. Additionally, you can see other details such as who poured the cup, at what time the cup was poured, which type of beans were used, etc. on the the cup page.

As far as consumers go, Food Trust takes care that they eat right! It ensured that a food item is exactly what the label on it says it is. The right information on a food item reaches the hands of a consumer, using the potential of a blockchain. Con- sumers can get to see a log of the journey of that food product from “farm to fork” by simply querying food product identifiers. Blockchain recorded and assigned a digital certificate for each interaction with a food item. This reduced the risk of adulteration and thus the foodborne outbreaks.

By getting rid of the anonymity that exists in the current food system, blockchain technology shined a light along every step of the way in the life of the food products and helped to help a safer, smarter, and more sustainable food system so that the customers can save money and live better.

VII. CONCLUSION

Food from across the world is available to consumers today, regardless of the season, location, or environment. However, the greater options and accessibility are accompanied by increasing complexity in the food supply chain.With growing data and lengthening ecosystems within the industry, the importance of trust weighs heavier than ever before. From the farmer, processor, retailer, to the consumer, Food Trust uses trust to build transparency. The blockchain solution is working to ensure that transparency enables the expanding food system. The solution provides authorized users with immediate access to actionable food supply chain data - from farm to store and ultimately the consumer. The complete history and current location of any food item along with its accompanying information (i.e. certifications, test data, temperature data) can be readily available in seconds. Food

Trust solution users can quickly locate items from the supply chain, in real time, by querying food product identifiers . To use the Food Trust solution to trace food products, data on food products needs to be uploaded to the network by participants. Once data is uploaded, the trace module allows an authorized user to search the provenance of a food product (via GTIN, product name, or Purchase Order) and can narrow down by a specific date.Authorized participants can then determine the scope of the problem, block further contamination, and narrow the scope and impact of a recall.

REFERENCES

[1] Vilar, M.J., Rodriguez-Otero, J.L., Sanju a´n, M.L., Die´gueza, F.J., Varelac, M., Yusa, E., Implementation of HACCP to control the influence of milking equip- ment and cooling tank on the milk quality. Trends in Food Science Technol- ogy. 2012, 23(1), 4-12.

[2] Fotopoulos, C., Kafetzopoulos, D., Critical factors for effective implemen- tation of the HACCP system: a Pareto analysis. British Food Journal. 2011, 113(5), 578-597

[3] Herath, D., Henson, S., Barriers to HACCP implementation: evidence from the food processing sector in Ontario, Canada. Agribusiness. 2010, 26(2), 265- 279

[4] Folinas, D., Manikas, I., Manos, B., Traceability data management for food chains. British Food Journal. 2006, 108(8), 622-633

[5] Shanahan, C., Kernan, B., Ayalew, G., McDonnell, K., Butler, F., Ward, S., A framework for beef traceability from farm to slaughter using global standards: an Irish perspective. Computer and Electronics in Agriculture. 2009. 66(1), 62-69

[6] Abad, E., et al., RFID smart tag for traceability and cold chain monitoring of food: demonstration in an intercontinental fresh fish logistic chain. Journal of Food Engineering. 2009, 93(4), 394-399

[7] Mattoli, V., Mazzolai, B., Mondini, A., Zampolli, S., Dario, P., Flexible tag datalogger for food logistics. Sensors and Actuators A: Physical. 2010, 162(2), 316-323.

[8]A Supply Chain Traceability System for Food Safety Based on HACCP, Blockchain Internet of Things Feng Tian Department of Information Systems and Operations Vienna University of Economics and Business Vienna, Austria.

[9] A new era of food transparency powered by blockchain Frank Yiannas Etiket: System for tracking the contents of packaged food products O¨ zlem Durmaz ˙Incel ; Mustafa Incel 2018 26th Signal Processing and Communica- tions Applications Conference (SIU)

[10] From farm to fork [Technology Food] Dominic Lenton Engineering Technol- ogy Year: 2010 , Volume: 5

[11] Food Supply Chain Management under Conditions of Food Safety Dianhua Wang ; Douxuan Huang 2010 International Conference on Management and Service Science Year: 2010

[12] Agri-Food Traceability Management using a RFID System with Privacy Pro- tection P. Bernardi ; C. Demartini ; F. Gandino ;
B. Montrucchio ; M. Rebau- dengo ; E.R. Sanchez 21st International Conference on Advanced Information Networking and Applications (AINA ’07) Year: 2007