Optimizing the Trust Factor of Organic Agriculture Business

A dissertation submitted for the Degree of

Master of Computer Science

G. B. I. De Silva

University of Colombo School of Computing

2019

Declaration

The thesis is my original work and has not been submitted previously for a degree at this or any other university/institute. To the best of my knowledge it does not contain any material published or written by another person, except as acknowledged in the text.

Student Name	: G. Buddhi Iroshana De Silva
Registration Number	: 2016 /MCS/024
Index Number	: 16440246

Signature: _____ Date: _____

This is to certify that this thesis is based on the work of

Mr. G. Buddhi Iroshana De Silva

under my supervision. The thesis has been prepared according to the format stipulated and is of acceptable standard.

Certified by:

Supervisor Name: Dr. Kasun de Zoysa

Signature: _____ Date: _____

Contents

List of Figures

List of Tables

Acronyms and Abbreviations

DEFRA	Department for Agriculture and Rural Affairs
GMO	Genetically Modified Organisms
USD	United States Dollars
FiBL	The Research Institute of Organic Agriculture
IOT	Internet of Things
DAO	Autonomous Decentralized Organizations
URL	Unified Resource Location
MSP	Membership Service Provider
DAO	Decentralized Autonomous Organization
CRUD	Create, Read, Update and Delete operations in database context
DA	Device Agent
HL	Hyperledger Blockchain system
SDK	Software Development Kit
TLS	Transport Layer Security

Abstract

Organic food consumption among consumers is no longer considered as a luxury lifestyle behaviour. When looking at consumer market statistics, it is possible to see positive growth in organic agriculture business. It is also notable that organic foods tend to be sold at higher prices when compared with non-organic foods available in the market. This is mainly because additional effort which organic crop farmers need to put on organic products with compared to regular crops. Even though organic products are selling at higher prices than the usual, there is a significant tendency among consumers to buy organic products mainly due to their associated health and environment benefits. However, when looking at the current context or organic agriculture business, it is possible to say that consumers have to keep their trust on so-called organic certification authorities on their organic product certifications. In the present context, the process of verifying the organic food compliance parameters against crops are not transparent to the end users and it directly leads to improve distrust among end consumers about the products that they purchase. This study has been carried out to formulate a computer science approach to optimize the trust factor in organic agriculture ecosystem. In order to come up with an end solution, within this study, several candidate systems have been analyzed including blockchain systems. At the end, a computer science based model will be proposed to improve trust factors within the organic agriculture ecosystem.

Chapter 1

Introduction

1.1 Introduction to the Chapter

This chapter defines the problem which is addressed by this project. By doing so, it gives the background to the problem domain, problem analysis, scope definition and motivation.

1.2 Background to the Problem

1.2.1 Introduction to Organic Food Industry

1.2.1.1 Introduction to Organic Foods

Today, thanks to the industrialization and the advancement of science and agricultural domains, scientist/ researchers have been able to suggest various ways for farmers in worldwide to produce their crops and dietary products which we consume in daily basis without using any non–natural pesticides, weedicides and chemical fertilizers but only to use organic versions of them. Today, in agricultural context, such products are called as 'organic foods' [1].

By looking at the organic food industry, it is possible to say that there is no any exact definition to define organic foods, it mainly depends on the country or region in which they are being produced. According to the Department for Agriculture and Rural Affairs (DEFRA) – United Kingdom, organic foods are not only limited to usage of organic materials such as organic pesticides and weedicides but also they are not allowed to use any direct or indirect variations of Genetically Modified Organisms (GMO) [2] during the cultivation process. Even though in most of the definitions which relates to organic foods, it is said that usage of non-natural pesticides, weedicides and chemical fertilizers on organic crops during the production phase is prohibited but, in some definitions which belongs to specific countries, it is said that the usage of such non-natural chemicals on organic crops are acceptable up to some extent and those should be within the approved limits [3].

1.2.1.2 Benefits of Organic Foods

There are various benefits of harvesting and consuming organic foods. Some of them directly leads to health benefits of living beings and others are directly contributing to wellness of the environment. This can be considered as one of the major reason for consumers to buy organic products for higher price with compared to regular foods in today's market.

According to the literature [4] [5], some of major benefits of organic foods can be listed as follows,

- Increased antioxidant capabilities:
  Which eventually leads to produce free radicals within animal immune system and thereby leading to chain reactions that may damage the cells of organisms.
- Pesticides reduction:
  Most of the organic foods which are being manufactured are free from pesticides. By having chance to use pesticide free foods it directly lead to reduce the amount of unwanted and harmful materials to be produced within human body.
- Less genetically modified crops:
  Organic foods are said to be cultivated in natural way. Studies point out that by consuming genetically modified foods might lead to less responsive immune system.
- Support to keep plants and environment healthy:
  According to usual procedures mandated by organic cultivation process, plants which are used to harvest organic crops needs to be treated with organic materials and in natural ways – which will leads to increase healthier plants percentage on the globe.

1.2.2 Statistics on Organic Food Industry

According to the latest statistics collected on organic food industry by the research institute of organic agriculture (FiBL), at the end of year 2016, 178 countries were cultivating organic crops which covers 57.8 million hectares of total land worldwide – which is equivalent to the 1.2% of the total agricultural land area in worldwide [6]. Following figure 1.1 on the following page provides overview of how current organic cultivation lands have been spread across the world and table 1.1 provides overview of region wise distribution of organic lands.

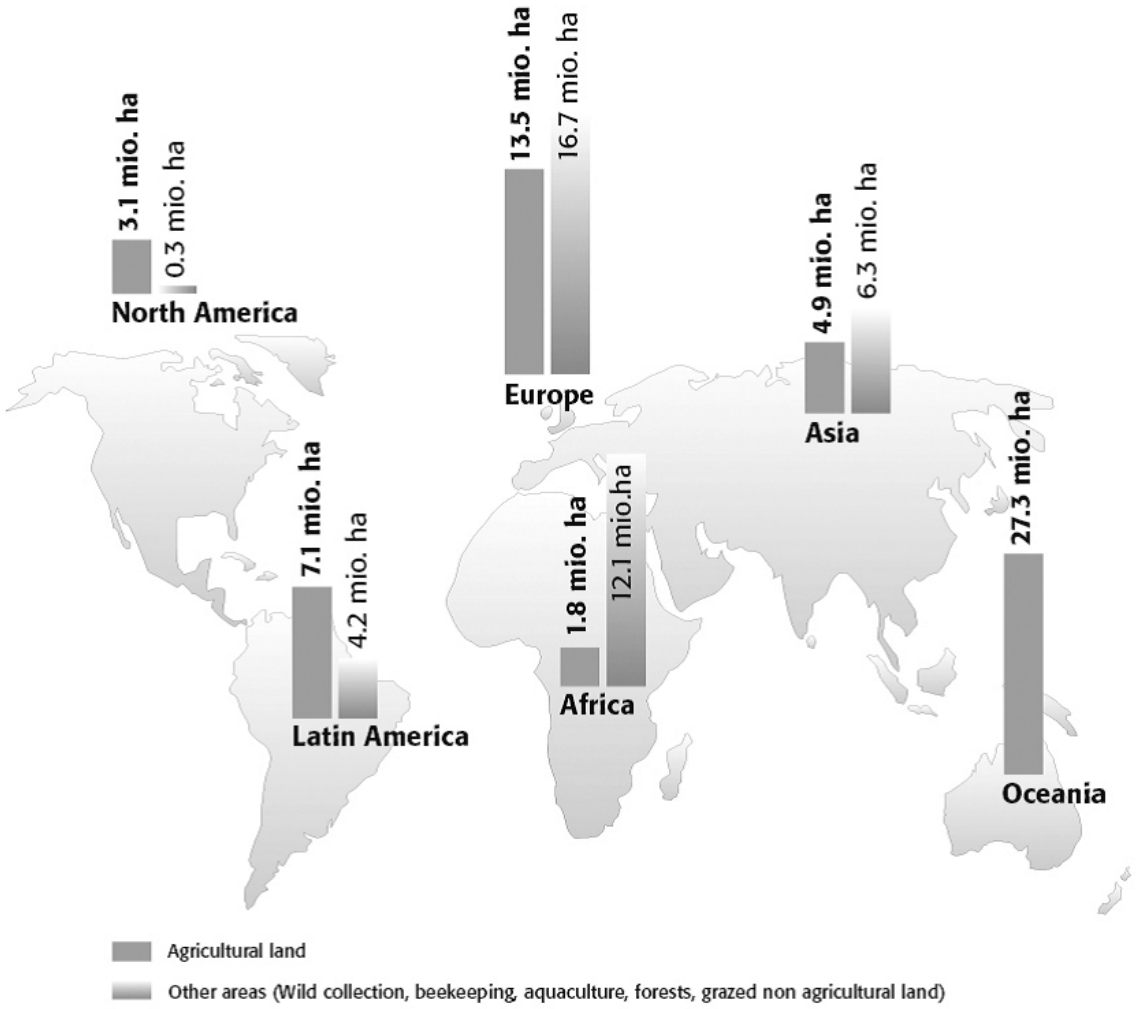


Figure 1.1: Worldwide Organic Land Distribution

Region	Organic agricultural land [hectares]	Regions' shares of the global organic agricultural land
Africa	1'801'699	3%
Asia	4'897'837	8%
Europe	13'509'146	23%
Latin America	7'135'155	12%
North America	3'130'332	5%

Table 1.1: Region-wise Distribution of Organic Lands

When considering about the organic food producers, there are 2.7 million organic food producers exists in worldwide [6]. Following figure 1.2 illustrate how organic producers have spread across the globe.

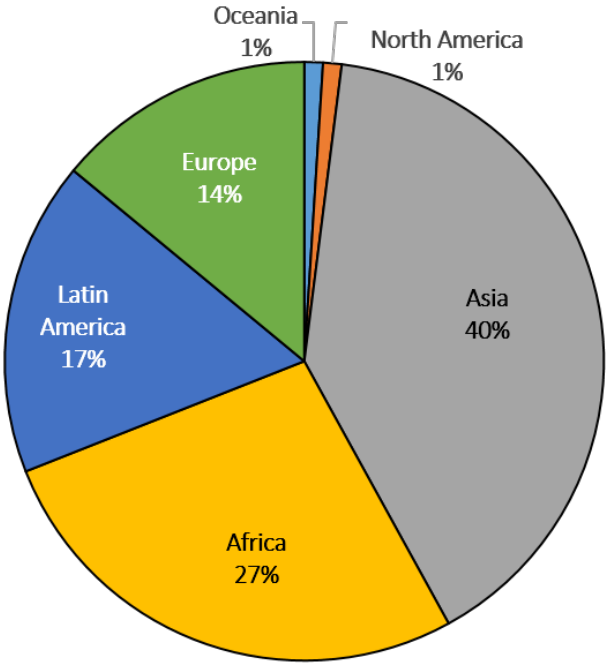


Figure 1.2: Distribution of Organic Lands - Worldwide

When looking at the present context of food industry, it is obvious to mention that there is a huge trend towards consuming/ purchasing organic foods among regular consumers (due to factors provided in above section) in the market. Some studies suggest that there can be more than 16% growth with compared to today in organic food industry by the year of 2020 [7]. The usage of organic food is not considered as a part of modern luxury lifestyle limited to developed countries because some studies shows that there are tendencies in consuming organic foods in rural areas in some developing countries as well [8].

By comparing organic cultivation statistics and buying patterns of organic foods in last few years, a positive trend for organic food cultivation and consumption can be observed. If considered in more precise manner, organic farmland increased by 7.5 million hectares or nearly 14% in year 2016 with compared to year 2015. Not only that but there has been an increment in the number of organic producers of 300 000, or over 13% in year 2016 compared with year 2015. Following figure 1.3 illustrates how trend for organic food has been progressing over time and table 1.2 shows how organic food producers have evolved over time [6].

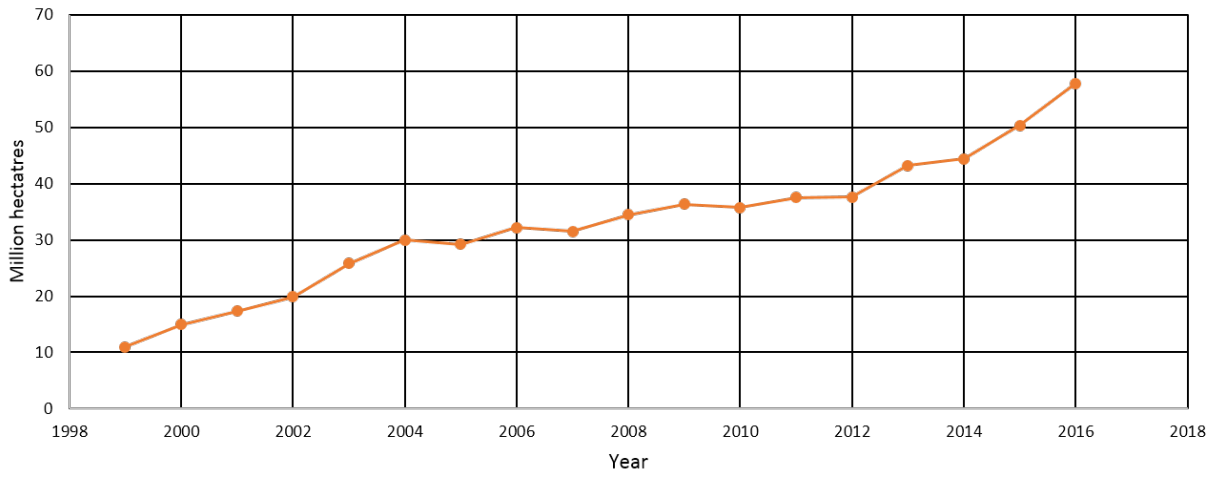


Figure 1.3: Growth of Organic Agricultural Land

Region	Total producers - 2015	Total producers - 2016
Africa	719710	741367
Asia	851016	1108040
Europe	348986	373240
Latin America	456806	458532
North America	19356	18422
Oceania	22009	27366

Table 1.2: Worldwide Organic Food Producers

Apart from factors which can be derived from organic cultivation land growth to prove positive tendency for organic food industry, the overall monitory value in today's organic food industry can also be considered. According to latest statistics provided by FiBL, the total organic market share is worth about 89.7 billion US Dollars (USD). When looking at how organic market share distributed across the globe and the usage of organic foods by consumers worldwide, it is obvious to say that there was a significant market/ industry growth in organic food industry in recent years. Following table 1.3 lists down how overall retail sales distributed worldwide and per capita spending in each region in year 2016.

Region	Retail Sales(Million USD)	Per Capita Consumption (USD)
Asia	8330.0	1.93
Europe	38036.12	46.29
Latin America	918.97	1.47
North America	47580.89	132.0
Oceania	1208.0	30.0

Table 1.3: Organic Food Market Share and Per Capita Spending

1.2.3 Current Procedure

If we consider about the current process of how these organic foods are being manufactured and assured their quality, it is obvious to say that most of the farmers are using smart farm solutions (in large scale farms in developed countries) where they can continuously monitor their crops' status in a centralized location and act upon them. For the assurance of quality of their cultivated crops, in some countries there are governing bodies in which each of these organic farms must register themselves in order to evaluate their products against authority's governing rules [9].

According to the FiBL survey on organic rules and regulations, 87 countries have implemented organic governing standards by the year of 2017. However, some countries have no organic legislation but have national production standards. Such standards eventually leads to a national definition of organic products and can be considered as a reference point for certification activities in future [6].

In present context, consumers are tend to buy organic products which are being certified by a certification authority. Usually, such certification authorities issue logos (to producers) as given in following figure1.4 to use when they market their products. Consumers are simply trusting those labels and purchase organic products because most of them are backed by government organizations.

Figure 1.4: Organic Certification Logos

1.3 Introduction to the Problem

In present context, even though we have enough brands and variations of organic foods in regular food groceries, the only way for end users to validate the quality of each of these products is either by keeping their trust on logos/ badges provided by organic food governing authorities or keeping the trust on company brand names of which those are being produced. This leads consumers to believe what governing authorities and food production companies are saying about quality of their products without analysing any transparent process which is being presented to the end consumers by the manufacturers. According to some studies conducted [8], consumers are not willing to keep their trust on governing authorities and other respective companies due to some recent events occurred which involved in using heavy non-organic based fertilizers and pesticides on so-called organic products [10].

In most cases, even though modern farms are using complex and sophisticated Internet of Things (IOT) based solutions to capture data and process them, anyone who is having higher system privileges in those respective systems can perform fraudulent activities on collected data to forge end results. Therefore, it is not possible to conclude that by simply having a computer based system to manage organic food cultivation process will resolve trust issues exist within the current process.

When considering about some of the trust factors which lead to improve the distrust among end consumers about organic foods that they are purchasing, following can be identified.

- Not being able to verify the validity of environment conditions in which crops have been cultivated in: this typically includes the monitoring of required humidity levels, soil moisture levels, lighting conditions and other measurable factors (which are typically collected from sensors deployed in cultivation fields) that are available during the cultivation process.
- Not being able to verify whether the authenticity and accuracy of data which is being collected from cultivation fields have been tempered or not.
- Not being able to see collected data on crops cultivation in a simplified manner by the end users.

1.4 Motivation

Since majority of consumers are purchasing organic foods for a considerably high price (with compared to non-organic foods) because of the health benefits associated with them, a trend has emerged in organic food industry to verify the accuracy and authenticity of details about organic foods which are being produced to the end consumers at the end of production chain. Basically, the end consumers are in the need of having a mechanism to trust the quality of

their purchasing organic products in a simple manner rather than having to keep their trust on centralized non-transparent regulation bodies and companies (who claim to be providing a guarantee on organic food quality and their standards).

1.5 Significance of the Project

Both consumers and organic food producers will be beneficial by having a solution to improve the transparency of organic food manufacturing process. This is possible because from consumers' perspective, they will have a better, trustful and transparent way of getting to know about foods that they are purchasing – which eventually leads to improve trust within consumers on organic products as well as increased purchase patterns. From organic food producers' perspective, they will be beneficial by increased sales of their crops due to increased trust about their products among consumers.

By having an ability to provide a computer science based solution to improve trust factors within the organic agriculture business will provide more confidence to end consumers rather than providing a solution through some other means. This is because in modern computer science domain, systems which includes concepts such as autonomous decentralized organizations (DAO) and integrated Blockchain with smart contracts concepts are capable of providing full transparent and cryptographically proven solutions for these kind of scenarios.

Hence, it is possible to conclude that there will be a huge significance to organic agriculture business domain by providing a solution to optimize its trust factors through computer science approach.

1.6 Scope of the Project

Following points will only be considered when developing this project.

- This project will only consider about enforcing transparency of organic vegetables/ fruits production in agriculture business.
- This project will only address how to securely capture information about organic farm fields and present them to end consumers in a transparent manner.
- This project will consider starting point as the organic vegetable/ fruit cultivation fields and end point as the cultivated items being sent out to outbound logistic chain from the cultivation fields – which means this project will not consider about ensuring the validity of any organic items such as fertilizers used in the cultivation fields and out bound logistic validity afterwards.

1.7 Goals and Objectives

1.7.1 Goals

By successfully achieving this project, it is assumed that following goals can be reached.

- Increase well-being of organic food consumers by providing a mechanism to verify the products which they purchase are meeting minimum required parameters during the cultivation process.
- Increase the production growth of organic foods through improving trust among consumers about product they purchase.
- Improve animal and environmental welfare through promoting organic agriculture.

1.7.2 Objectives

To achieve above specified goals, following objectives will be used,

- Provide a computer science approach to make organic food manufacturing process more transparent to end consumers.
- Reduce fraudulent activities through a computer science approach which can occur in regular certification systems.

1.8 Conclusion of the Chapter

In this chapter, current literature and trends with respect to organic agriculture business have been analysed. With the results of analysis it is clear that consumers are in the need of better trust framework to verify the quality of organic foods which they are purchasing in present market due to various trust issues exists in current organic food manufacturing and verification process.

Chapter 2

Literature Review

2.1 Introduction to the Chapter

In this section, existing literature related to organic agriculture business and its applications will be discussed. In order to maintain a proper flow and simplicity, literature will be studied under several sections. Finally a discussion and a conclusion based on performed literature will be presented.

2.2 Analysis on Current Organic Certification Process

According to literature [11], leading organic certifiers in the world such as USDA, Canadian Organic Production Systems and European organic certification authorities are still relying on manual inspection procedures of crop fields when issuing organic certifications to their clients. As for the Organic Certifier's manual [11] and other materials [12] [13] following steps need to be satisfied in order to receive organic certifications from certification authority by the organic food manufactures.

1. First, farm owners should request for organic certification from respective organic certifiers.

2. Then respective inspectors from organic certification authorities will evaluate the applicant's operations through observations, collection and testing of samples, taking of photographs, and review documents and records of the operation process.

3. After carefully inspecting for the required minimum standards needed for organic certification, respective organic certifiers will issue them the certification.

4. In order to maintain the validity of organic certifications, random visits to farm without any prior notices are conducted time to time.

5. If organic certifiers found that they have been using non organic materials or other mean of non-organic products during the inspection phase that respective authority might take legal action against them in order to maintain the quality of certified organic products and seeds.

According to above organic food certification process, it is obvious that organic certification authorities are not using any real time crop monitoring system to monitor crop fields' status in real time. It is possible that fraudulent information or activities can be produced/ performed upon investigators visits to the fields.

Apart from manual procedures, there is one more loop hole in this process, which is consumers have to keep their trust on respective certification authorities for maintaining accurate and up to date information about organic food manufactures (simply, consumers are in the assumption that these authorities are regularly inspecting organic food manufactures for their expected quality). Therefore, consumers have to believe in organic certification authorities' procedures and assume that they are not performing any fraudulent activities when issuing / renewing organic certifications to manufactures.

This current organic certification process has formulated a centralized governing mechanism for today's organic food industry. Therefore, it is required to proceed with more decentralized and transparent way of issuing organic certifications if required to improve trust among consumers regarding organic foods that they purchase.

2.3 Analysis on Existing Information Systems for Real-Time Monitoring of Crops

There exists several off the shelf software products and applied research grade applications which can be used to track real time status of crop cultivations. Some of them can be listed as follows,

1. A Crop Monitoring System Based on Wireless Sensor Network [14]:
   This paper proposed one of the agricultural applications of wireless sensor networks. This research project was deployed in Beijing, China to capture cultivation farms' real time status using wireless sensor networks. This system collects two types of information parameters – one is the real-time pictures (not video streams, but still images) of the cultivation fields which will be used to monitor the crop growth over time and the other parameter type is environmental conditions such as environmental temperature, humidity, wind, air flow, rainfall, and soil pH level. This paper suggests that agricultural information network which can be built up by using wireless sensor networks has its practical significance as a large-scale application of agriculture IOT. The solution

proposed by this research internally uses two major protocols for data collection and distribution. Collection tree protocol is used to collect data from distributed sensor nodes to root nodes and dissemination protocol is used to distribute data among nodes [15].
However, in this paper it is not clearly mention that what kind of data security and authentication mechanisms are used to validate basic cryptographic concerns such as data integrity and non-repudiation.

2. OnFarm [16]:
OnFarm is a smart farming solution produced in USA which has the capability of collecting soil moisture levels, reading data from various irrigation equipment, acting as weather stations and producing timely crop protection levels. This solution also provide big data analytics capabilities with collected data.
Mainly this system facilitates centralized and one-stop features to manage entire farm with few clicks. This system lacks of sharing farm's crop details to outside such as sharing cultivation parameters with purchasers to improve the transparency etc. According to this system's web site, there is no indication of how data is being securely captured from field deployed sensors and distribute them to centralized location for storage and processing. Simply this system seems to good solution for internally managing farm's aspects rather than exposing its functionality and data to outside for better transparency because, when thinking about optimizing trust factor among consumers it is required to have easy way of viewing the origin of foods and their authenticity. Therefore, if a system is not compatible with sharing data with outside then that system might not be suitable to use for trust factor optimization.

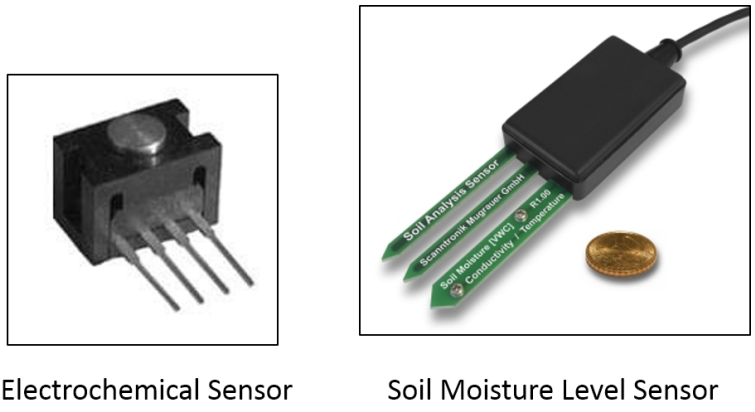
2.4 Analysis on Capturing Environmental Factors for Monitoring

In order to securely monitor factors, it is required to capture environmental factors such as temperature, humidity, rainfall and other necessary nutrition levels which includes Nitrogen (N), Phosphorus (P), Potassium (K) and Calcium (Ca) etc [17]. from farm fields. When looking at how currently those parameters are being captured it is possible to list down following mechanisms.

1. Solutions Exists for Small Scale Farms
There are various low priced to high priced sensory devices which can be used to capture above mentioned properties from atmosphere and soil. The common property of these devices is that, those are just sensory devices and they lack of computational power – which means, for them to transfer data to remote location or do any sort of edge processing, they need to be connected to some sort of small computer such as smart

Sensor Name / Type	Description / Purpose
Location Sensors	Use signals from GPS satellites to determine latitude, longitude, and altitude to with approximations [18]. These sensors typically used within other sensors / devices to capture their current location.
Electrochemical Sensors	This sensor type is capable of providing key information required in precision agriculture such as pH and soil nutrient levels. Sensor electrodes work by detecting specific ions in the soil [18]. Figure 2.1 shows a picture of typical Electrochemical sensor.
Dielectric Soil Moisture Sensors	Assess moisture levels by measuring the dielectric constant (an electrical property that changes depending on the amount of moisture present) in the soil [18]. Figure 2.1 illustrates a typical soil moisture sensor.

Table 2.1: Different Sensor Types for Environment Factors Detection



Electrochemical Sensor Soil Moisture Level Sensor

Figure 2.1: Different Sensor Types

phone, Arduino board or Raspberry Pi etc. Some of these devices which are used in agricultural fields can be summarized as follows,

2. Solutions Exists for Medium and Large Scale Farms

   When there is large area to be covered manufacturing sensor components (assembling sensors together and connecting them into computation devices) in large scale will not be a feasible solution. In this kind of scenarios it is possible to find following type of devices (given in Table 2.2) which are provided by third party organizations (Figure 2.2 shows images of each of following devices).

Device	Description
Arable	An integrated analytics platform which capable of capturing environmental precipitation, evapotranspiration and weather etc [19].
Observant	A cloud based integrated platform which can be used in align with already existing devices. This device is capable of monitoring environmental conditions such as temperature, soil health, humidity etc [20].
Pycno	A device capable of collecting data on Solar radiation, air temperature and humidity, soil temperature and soil moisture [21].

Table 2.2: Various Device Types

Figure 2.2: Large Scale Farm Devices

2.5 Attempts Taken to Optimize Trust Factors in Agriculture Business

There are number of studies which conducted various types of research studies on how to improve efficiency of agriculture food business but, since recently there were not much of research found for improvement of trust factor within agriculture business. This is because in most cases, people tend to use advanced techniques to model systems and improve their effectiveness and efficiency with different technologies / concepts but, it was impossible to create fully open and transparent mechanism to capture every piece of transaction happening

within a given system and still make it unhackable until unveil of Blockchain after the original Bitcoin paper [22].

Several research attempts can be summarized as follows which were done to improve trust factors within agriculture business.

1. Case study alimentary supply chain: How Blockchain improves the supply chain [23].
   This case study points out the disadvantages of traditional and already existing supply chain systems which involved in different domains (this case study was conducted on a hypothetical agriculture domain related supply chain). According to this study, the main disadvantage of traditional supply chain is the lack of information for the consumer about the origin of the product.
   This study has proposed to use a Blockchain integration with supply chains so that the entire system would work only through a trusted peers. In an abstract view, in this study, they have stored all supply chain transaction data in Blockchain and introduce smart contracts to manage entire supply chain process more efficiently. Hence, entire supply chain would become more efficient due to less processing required during entire transaction cycle. It is also pointing out that if any of the parties involved in supply chain process such as consumers, suppliers etc. is not fulfilling the established conditions defined by smart contract, a penalty is imposed and the agents keep respective monitory value in the control entity until the conditions agreed upon are met.

2. A Case Study for Grain Quality Assurance Tracking based on a Blockchain Business Network [24]
   This case study was conducted to improve the tractability of supply chain which involves in soybean manufacturing – agriculture domain. The main objective of this study was to highlight the gains obtained during the Blockchain implementation for agricultural domain supply chains. According to this study, the main advantages of using Blockchain, in spite of other software development platforms, is that all the members of the network can now share the same business rules and transaction data in their nodes which leads to reduce disputes among business partners, information asymmetries and consequently improving governance throughout the system. It is also mentioned that the transactions transparency provided by Blockchain requires that the companies involved in the supply chain to collaborate effectively defining common rules that can be expressed in smart contracts.
   During the system implementation of this study, they have mentioned that they have come across a controversial situation with Blockchain architecture. That is with respect to the signatures used to sign transactions. This is because, in order for government to legalize digitally signed documents, those has to be signed with legally accepted signatures. However, this solution has overcame this situation by introducing one such signature to their Blockchain system.

3. Blockchain ready manufacturing supply chain using distributed ledger [25]
   One research study has been carried out in Loughborough University, United Kingdom which showcases the usage of Blockchain and Smart-contracts to improve the transparency of supply chain system by considering the hypothetical scenario. This study emphasized on the business gain of which organization can achieve by using such solutions. This study suggests a solution to improve the supply chain transparency by introducing a QR code which carries a digital token (cryptographic signature) for each physical product within the supply chain and tracking the respective asset's state changes such as movements through Blockchain enabled supply chain system. At the end this solution illustrates how to view all transaction details of this particular product such as production date and state changed dates etc. through a Blockchain enabled supply chain.

4. WAVE: A Decentralized authorization system for IOT via Blockchain smart contracts [26]
   This is a solution provided by set of researchers at university of California at Berkeley. This study emphasizes on providing an authorization system for IOT devices without depending on any centralized trusted third party - instead this leverages the characteristics of Blockchain based smart contracts with combined delegation of trust mechanism to maintain the secrecy of resources. This study provides a powerful means of federating networks of embedded networks and supporting the life cycles of devices, services, smart environments, infrastructures, and individuals.

5. Blockchains and smart contracts for the Internet of Things [27]
   A publication in IEEE produced by North Carolina State University – USA points out how usage of Blockchain technology can improve the quality of logistics process in most of manufacturing organizations. This study also points out the usage of two different variations of Blockchain deployments which are public and private Blockchain modes and their importance. Moreover, it provides introduction to the state of the art concept of "Decentralized Autonomous Organization (DAO)" which heavily dependent on Blockchain's smart contracts which can be used to verify whether the captured parameters are within acceptable thresholds.

2.6 Analysis on Available Technologies

By looking at above findings it is obvious that Blockchain releted technologies such as Smart Contracts are bing widely used for implementations of trustful systems. This is mainly due to the nature of Blockchain architecture. Therefore, under this section more focus will be given for Blockchain releted concepts.

By the time of writing of this section, two major Blockchain platforms have been studied.

Those are Ethereum and Hyperledger. Both of these platforms have their advantages and disadvantages. By simply looking at these two platforms it is possible to say that Hyperledger platform is more popular among Blockchain community due to varios reasons. Some of them can be identified as follows,

- Hyperledger is being hosted and promoted by Linux foundation
- Hyperledger supports Javascripts as the smart contract writing language.
- Better comminity support

Some architectural aspects of Hyperledger

Hyperledger is an open source enterprise-grade permissioned distributed ledger technology (DLT) platform [28]. Hyperledger provides underlying architecture for different kind of Blockchain frameworks to be integrated and to work with it to achieve different Blockchain requirements. Hyperledger architecture encourages to use common building blocks via its modular architecture. Hyperledger project currently promotes several major implementations such as: Hyperledger Fabric, Hyperledger Iroha and Hyperledger Sawtooth etc. [29].

The Hyperledger work group lists down major components for their implementation. Those are: consensus layer, smart contract layer, communication layer, data store abstraction, crypto abstraction, identity service, policy service, APIs and interoperations [28]. Among those, consensus layer and communication layer are responsible for dealing with consensus and data replication among Hyperledger nodes.

Since the Hyperledger provides module architecture for consensus layer, different frameworks such as Hyperledger Fabric and Hyperledger Iroha can use different types of consensus handling protocols. In major variations of Hyperledger, Consensus is being achieved through the use of lottery based algorithms including Proof of Elapsed Time (PoET) and Proof of Work (PoW) or through the use of voting based methods including Redundant Byzantine Fault Tolerance (RBFT) and Paxos [28]. Lottery based algorithms are said to be suitable when there are large number of Blockchain nodes exists. Voting based algorithms are said to be more suitable when there is a low latency requirement.

2.7 Discussion and Conclusion of the Chapter

As the first step, how the current organic process works has been analyzed. According to the findings of it, organic certification authorities are still using manual inspection process to validate organic food's status. Currently, they are not using any real time crop inspection mechanism to validate cultivation field's status in real-time – instead they perform random visits to cultivation fields for inspections.

As the next step, analysis on existing information systems has been carried out. As for the findings of this section, it is possible to say that most of information system / smart systems are tend to behave as smart farming solutions. However, most of the systems out there are not capable of providing their data for consumers in a presentable manner in which consumers can simply check for authenticity of crops which they purchase.

Then, the ways which can be used for environmental factor monitoring have been analyzed. Under this section sensors and integrated systems which are out there in the market that can be used for monitoring purposes have been studied.

As for the next step, current research domain has been explored to identify attempts which are taken to optimize trust factors in agriculture domain. In this section, it has realized that, in most cases trust issues are risen because of not having a proper way to identify the authenticity of food origin and conditions which they are being cultivated. Blockchain seems to be providing promising ways of ensuring trust issues which exists in current cultivation and supply chain systems due to the way of it is being architecture. Therefore, Blockchain platforms such as Ethereum and Hyperledger have been studied in abstract manner and will be studied indepth in order to formulate a solution under this research study.

Chapter 3

Problem Analysis

3.1 Introduction to the Chapter

In this chapter an in-depth analysis of issues which lead to improve distrust among end consumers about the organic food eco system will be carried out to find possible ways of solving them.

3.2 In-depth Analysis of Issues Exist in Current Eco-System

As per the introduction given to the problem in section 1.3 of this document, there are several issues existing in present context with respect to the transparency of how organic foods are being manufactured and they are being certified.

When considering about the issues identified from consumers' perspective in current organic agriculture eco-system, those can be broadly categorized into following categories.

1. Issues exist in verifying environmental constraints which organic crops are being manufactured.
2. Inability of verifying the authenticity and accuracy of data which are being collected from farms' data collection systems.
3. Not being able to trust organic certification authorities' processes.

According to the analysis done in literature review (Chapter 2) to analyze how the current organic eco system works, a hypothetical scenario can be formulated which can be considered as an ideal scenario for current organic eco-system verification process. However it is important to note that this hypothetical scenario has not yet been implemented at the present context and used only to illustrate issues which can exist in such optimum and ideal system. This hypothetical systematic process is depicted in figure 3.1.

Note: each step in figure 3.1 is marked with a placeholder for explanation purposes.

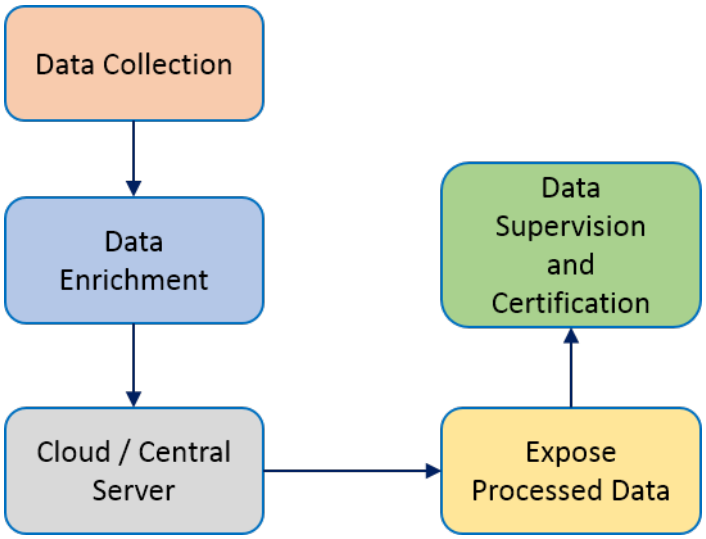


Figure 3.1: Ideal Organic Eco-System Data Flow

Following steps which represent each of the steps in figure 3.1 provides a brief description about each step and possible issues which could associates with them.

Step 1

This step involves in collecting data from cultivation fields with various methods. These methods might include data collection from an automated sensor network deployed in the fields, manual data reading and storing etc. Data collected from this step can be used to determine the quality of environment in which crops get manufactured and also to inspect whether there are any non-compliance materials are being used during the cultivation process. When looking at possible scenarios where this step leads to the original problem of "which factors improve the distrust among end consumers?", following points can be concluded.

- If this step includes manual data collection mechanism then collected data could have been entered in a wrong way.
- If this step involves with an automated system which captures environment factors and sends them for remote processing which in turn can be used by organic certification authorities to review compliances then data can be forged intentionally or non-intentionally in the middle. Therefore whatever the end results taken based on these data could be false.
- In a situation where collected data in this step needs to be transferred to other location for further processing then data could get corrupted and implies something else rather than what is originally intended.

Step 2

After collection of necessary data from farm field, it might require to send those collected data for further enrichment and data merges. This scenario can include operations such as data normalization and data conversion etc.

One of the potential security vulnerability which associates with this step is the data manipulation. This is because, data conversions and enrichments are usually based on set of business logics. Therefore if there is a requirement to alter data intentionally or unintentionally then this could be easily done with the help of small function tweaks at the processing place. This leads to produce falsify data at the end which can mislead end consumers.

Step 3

When looking at the present context of enterprise grade application development, it is obvious to note that in most of the cases people tend to use some level of centralized servers or cloud based services to implement their business logics. Having this kind of centralized closed and non-transparent systems will make it hard for consumers to believe in centralized authorities due to lack of transparency.

Step 4

Even though this step has been included in this diagram, according to analyzed literature this step cannot be found in most of the systems. The main reason for this could be identified as inability of exposing required data to outside in either anonymous or restricted manner. This is due to the fact that systems are not designed with the mindset of open transparency.

If there is a feature to provide necessary data to outside interested parties then organic certifiers could use those data and provide a better transparency to the end consumers.

Step 5

In this step organic certification authorities and other governing bodies need to look into the available data and provide decision/ certification based on them. This step is also not automated at the present context and done by manually at the moment.

One of the loop holes in this step is that if the certification authority is not properly audited over time then fraudulent activities could happen.

When looking at the literature, there are several attempts which have taken by several researches and organizations to make some supply chains transparent but those do not consider about organic agriculture business. These approaches include implementing integrated systems with distributed ledger technology etc.

3.3 Conclusion of the Chapter

Within this chapter, issues exists in current organic agriculture ecosystem have been identified and analyzed under three major sections. Those are : issues exists in verifying environmental constraints, issues exists when verifying authenticity of collected organic data and trust issues exists in current organic certification authorities. When looking at the current context, most of organic certification authorities are performing manual work to keep records of organic compliances and most of them do not provide a proper way for end uses to get know about certification process and organic crops' status in a transparent manner. These factors need to be addressed if it is required to provide a better solution with improved transparency.

Chapter 4

Solution Design

4.1 Introduction to the Chapter

In this chapter, an ideal solution design to the problems which have been identified in previous chapters will be formulated. Also, under this chapter several possible candidate system designs will be analyzed and an optimum solution will be chosen among them for future implantations.

4.2 Design Considerations

4.2.1 Basic Security Parameters Considered During Solution Design

In order to formulate a solution which will eventually optimize trust factors associated with organic agriculture ecosystem, it is required to consider following basic security fundamental concepts along with trust providing mechanisms.

Confidentiality

When data are being transmitted or handed over to another system / party, information must not be interpreted by the channel such as man in the middle and any other stakeholders (such as different farms). This feature is required for proposed solution because of multi tenancy support requirement that might be supported by the end solution in later stage of development. In other words this simply implies that data receiving from one farm must not be interpreted by another farm. This feature is important because farming agencies / companies might not want their data to be interpreted by each other to gain competitive advantages.

Data Integrity

Maintaining integrity in this kind of a solution takes high priority since the end result of whether the organic products are up to the acceptable standards or not is depending on the data that is being tested against set of defined rules. Therefore, necessary steps which need to ensure proper data integrity need to be taken with this regard.

Availability

Availability in this type of a system can be considered in two major ways. Those can be identified as follows,

1. Availability of summarized view of received data from a given entity - in this scenario it can be considered as data received from a specified farm / field which can be used to do a proper audit if required by the certification authorities or by the end consumers.

2. Availability of data upon request – typically this leads towards high availability aspects of end solution.

Non Repudiation

When considering about systems like this, data which are received from sensors are directly used to verify the compliance to organic certification regulations. Also, they can be exposed to outside to improve overall transparency within the system. Therefore, the end solution should consist of a mechanism to overcome plausible deniability.

Authentication

Having an authentication mechanism embedded in to the system helps getting right set of people to have right set of permissions to access and publish defined data. It does not matter whether the end solution has features to expose processed data to outside or not because, in order for data entries to get populated in the system, some entity has to publish data into it. Therefore, some level of authentication or user management is required in these kind of solutions.

4.3 Candidate System Designs

As for solutions, there are two major ways which this type of a system can be designed. Those can be identified as follows,

- Using a typical client server model to build a trustful system.
- Using an already proven trustful systems such as Blockchain to formulate a solution.

4.3.1 Typical Client-Server Model Design

In this scenario, clients are typically considered as IOT devices or edge devices. Edge devices usually do not have computing resources in order to perform sophisticated computations. Therefore, it is required for those devices to publish collected data into some sort of server for processing. This flow is illustrated in figure 4.1.

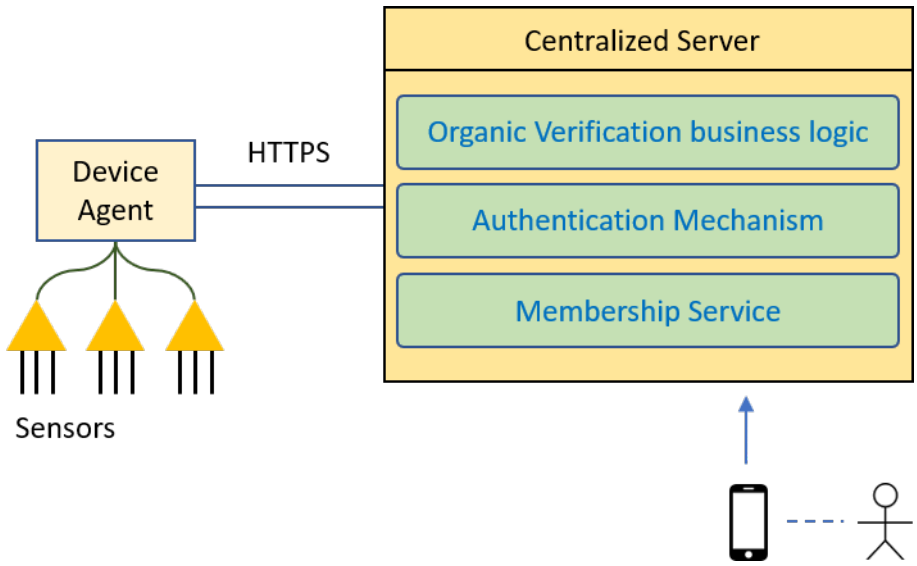


Figure 4.1: Client-Server Model

When looking into this option, clients (IOT Gateways etc. and IOT devices etc.) communicate with remotely deployed application servers (in which the entire system's model is implemented), the business model in this case includes the automatic verification of compliance to predefined organic certification rules and regulations.

Apart from the core business logic of validating the incoming data, this type of system also needs to provide a proper mechanism to make final and concluded details about organic crops to the end consumers during their purchases.

When looking at the mechanism which will be used to validate the final outcome of this solution, that is for end consumers to check whether the products they purchase are up to the required organic standard or not, has to be coded in the central server location as a business logic. In this case it is not possible to guarantee that this specific logics will provide required level of transparency to the end consumers.

4.3.2 Blockchain Based Design

Other way of formulating a solution for this kind of scenario is by using distributed ledger technology. Distributed ledger technology is used as the backbone technology in Blockchain platforms. When considering about Blockchain frameworks, there are various Blockchain systems which can be found in today's industry and almost all of them can be classified either into permissionless (public) Blockchain or permissioned (private) Blockchains.

There are different kind of advantages and disadvantages associated with respect to each of these types. Solution formulation for this problem with Blockchain can be again broken down into another two subsystems as follows,

- A solution which involves in using permissionless (public) Blockchain as a backbone to provide transparency to the consumers.
- A solution which involves in using permissioned (private) Blockchain as a backbone to provide transparency to the consumers.

When looking at a solution with permissionless Blockchain, following points can be identified,

Decentralization

Permissionless Blockchains are always deployed in complete decentralized manner. Data are synchronized within network using various technologies. Almost all permissionless Blockchain systems include consensus protocols to come to a common consensus and typically require majority votes for consensus.

Digital assets

Most permissionless networks have some kind of user-incentivizing token mechanism. Currently, permissionless Blockchains employ either monetary or utility tokens, depending on the purpose they serve.

Anonymity

Permission less or public Blockchains typically provide anonymity. In most cases this factor cannot be considered as true anonymous but can be considered as pseudonymous where identity of a given entity is a pseudonym.

Transparency

Permissionless Blockchain systems are typically fully transparent with their nature.

Likewise, when looking at a solution with permissioned Blockchain, following characteristics can be identified,

Different level of decentralization aspects

When running a permissioned Blockchain, authorities can decide how much of decentralization aspects need to be satisfied by the system.

Transparency

Transparency aspects can be differed according to the context in which Blockchain is deployed. These type of Blockchains can be configured to be fully transparent or non-transparent.

Anonymity

Usually, permissioned Blockchains do not provide anonymity because in order to get into the system, one must be provisioned into the system beforehand.

Controlled Access

Almost all permissioned networks provide some level of controlled access mechanism to the network. This factor is important for some types of application such as trust systems because,

there can be various reasons to audit system logins rather than using sophisticated validation mechanisms such as proof of work or proof of concept to validate user data.

4.4 Proposed Solution Design

4.4.1 Determining the Nature of Solution

As stated in above section, either typical client server model or Blockchain based solution can be used to provide a solution to optimize the trust factor in organic agriculture business ecosystem.

If a solution is proposed with a typical client server architecture then it is necessary to provide a mechanism to collect and store incoming transactions (data) from various sources by the means of not crack-able and temper-proof ways. This results in implementing a system with data encryptions, signing and lot other basic cryptographic concerns in mind.

Therefore, if it is required to implement such system from the scratch and it might not be a feasible thing to do so.

Note: there might be a set of already available frameworks to do encryptions and other basic cryptographic features in programming contexts but, they need to be properly integrated and initialized in order to reach to the final goal.

On the other hand, if Blockchain based solution is chosen as the backbone for the proposed solution then its cryptographic nature which is included in its distributed ledger mechanism can be out of the box used to create more elegant outcome and also the amount of workload which needs to formulate final outcome is comparatively less when compared with other candidate solutions.

Since it is required to capture user details (device details) of which data is being transmitted, anonymity factor does not play a major role in this scenario. Therefore, when considering about two types of Blockchains, it is obvious to use permissioned Blockchain method over permissionless Blockchain due to its anonymity characteristics when formulating a solution for this type of application.

Also, Blockchain technologies provide shared business logic execution environment by the means of smart contracts. Therefore end user will get better transparency and visibility to what is under the hood and which will result in creating positive attitudes among end users who will be using this system.

By concluding the facts analyzed in previous sections and this section, it is recommended to use a permissioned Blockchain solution as the backbone for this project.

4.4.2 Abstract Solution Architecture

Figure 4.2 shows high level abstract overview of proposed solution which includes blockchain components.

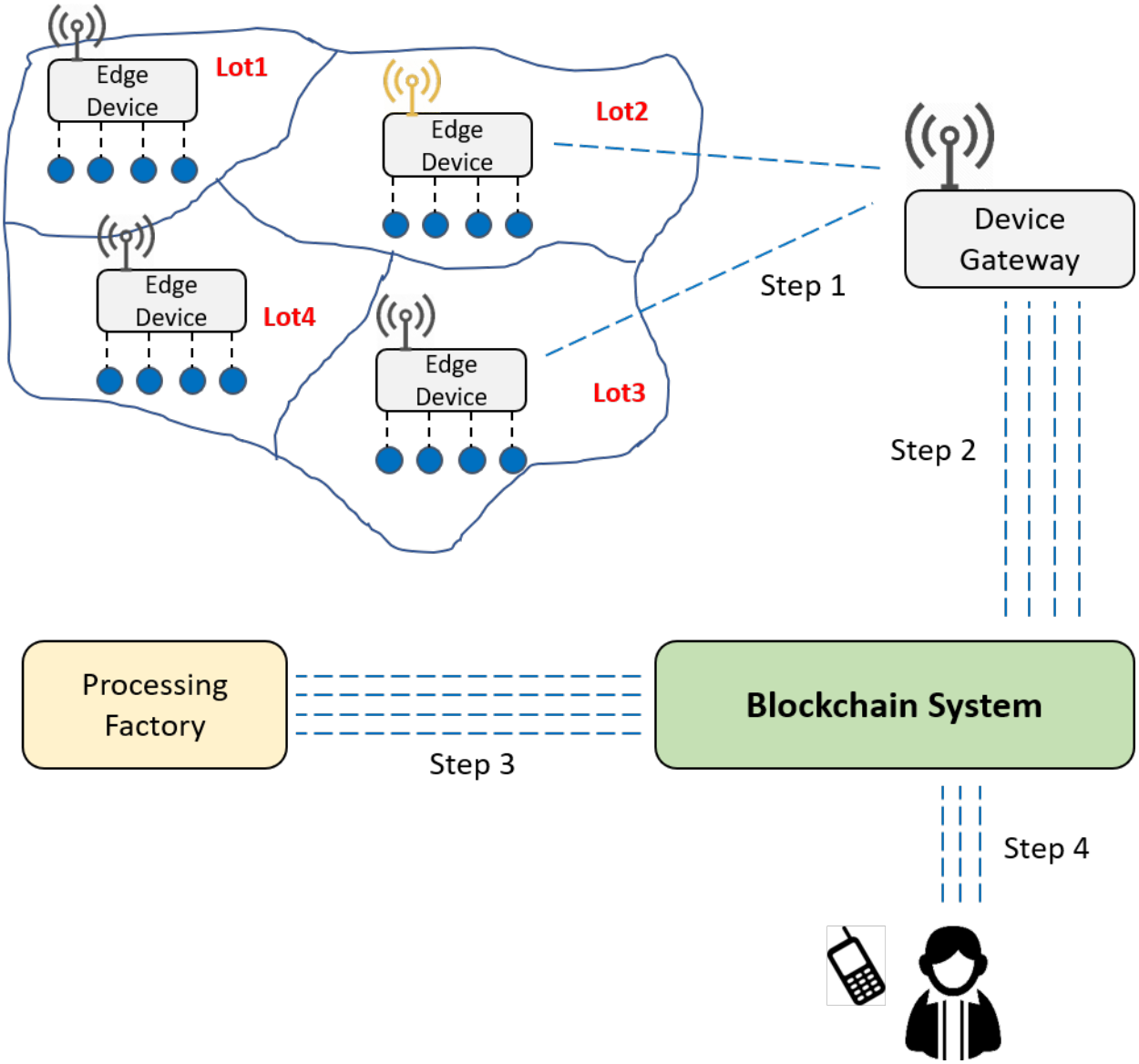


Figure 4.2: Abstract High-level Architecture of the System

Above proposed solution can be simply explained in following four steps (marked as in diagram).

Step 1

Sensor devices or edge devices which are deployed in cultivation farm fields transmit data into their respective gateways. As depicted in above diagram, entire farm field has divided into several sub farm fields namely as 'Lot1', 'Lot2',...etc. This has been done in order to ease off the validation process. Each of these sub-farm fields can have different types of crops cultivated in it. The deployed sensors in each sub farm fields will include respective farm field identifier

when transmitting data to its gateway. These identifiers will be used when performing final validations at the end of the process.

Step 2

Gateway device receives data from various sensors and aggregate them (if necessary). Then gateway devices transmit / send pre-processed data into Blockchain system.

Step 3

Crops processing factory which is responsible for collecting and performing necessary actions on crops feed data into the Blockchain system. This data consists of lot number to identify from which lot the particular crops (fruits and vegetables) have originated from.

Step 4

End users check for the validity of products to identify whether they were within the defined parameters to satisfy organic nature during their cultivation process by contacting Blockchain system. Note: during this step, an end user will query the Blockchain system to check whether the historic data from given farm field are having the correct data or not. This process might not be as straightforward as it depicted in the diagram but in order to reduce complexity in understanding, internal designs of final verification has been hidden from the diagram. However, detailed flow of this entire procedure will be presented in the next chapter.

4.5 Conclusion of the Chapter

In this chapter, several candidate designs have been identified and analyzed which can be used as a backbone to provide improved trust system for organic agriculture ecosystem. A Blockchain based system turns out to be a better solution when compared with typical client server system due to its built in cryptographic nature.

Chapter 5

System Implementation

5.1 Introduction to the Chapter

In this chapter, implementation related details for the Blockchain based design which have been formulated in design section will be discussed. In order to come up with a complete solution, first, required technology selection including determining the correct Blockchain framework will be discussed. Then business logic implementation details with respect to Blockchain will be discussed. Finally the overall system implementation related details together with deployment aspects will be discussed.

5.2 Overview of the Implementation Components

When considering about the overall solution architecture, following system components can be identified.

1. A permissioned Blockchain framework.
2. A system which is capable of transmitting collected data from devices to gateways.
3. A system which is capable of transmitting collected data from gateway to Blockchain system.
4. A mechanism to validate the organic food compliances or parameters.
5. A mechanism for end consumers to validate whether the products that they are purchasing are upto the standard or not.

5.3 Determining a Permissioned Blockchain System

5.3.1 Selecting a Blockchain System

As stated in above sections, there are two major types of Blockchain systems available to choose between. From those two, it is has been decided to use permissioned Blockchain system as the backbone to this solution stack.

When looking at present markert, there are various permissioned blockchain platforms available in the present markert. Some of them are free and open source whereas others are commercial products. In order to align with DAO concepts which leads to implement fully autonomous and transparent system for this kind of scenario, it is best to choose a Blockchain framework which has smart contract engine embedded into it, so that organic product verification related business logic can be implemented within the Blockchain itself.

According to [30] following comparison table 5.1 can be formulated for permissioned Blockchain networks.

	Hyperledger Fabric	R3 Corda	Ripple	Quorum
Governed By	Linux Foundation	R3 Consortium	Ripple Labs	JP Morgan and Ethereum
Ledger Type	Permissioned	Permissioned	Permissioned	Permissioned
Consensus Algorithm	Pluggable framework	Pluggable framework	Probabilistic Voting	Majority Voting
Smart Contract Availability	Yes	Yes	No	Yes

Table 5.1: Permissioned Blockchain Comparison

By analyzing the community articles [31][32][33] and due to following factors it has been decided to use Hyperledger Fabric permissioned Blockchain network as the backbone to this solution.

1. Hyperledger Fabric is governed by the Linux Foundation and being open source.
2. Built in smart contract capability with NodeJS and GO language support.
3. Better community support.
4. Highly scalable.
5. Development made easy with abstraction frameworks such as Hyperledger Composer.

5.3.2 Hyperledger Fabric as Backbone of the Solution

5.3.2.1 About Hyperledger Fabric

Hyperledger Fabric is an open source project maintained by linux foundation. Fabric is a variation of Hyperledger blockchain system. There are other variations of Hyperledger Blockchain systems available under Hyperledger umbrella such as: Hyperledger Sawtooth, Hyperledger Iroha etc. each of them are designed for various purposes. Hyperledger fabric is mainly designed to be act as permissioned distributed ledger and smart contract executor supporting the decentralized autonomous organization concept at its core level. Since it is a permissioned network there is no need for any computationally expensive tasks such as proof work (POW) which is available in permissioned distributed ledger systems such as Bitcoin.

5.3.2.2 Important Concepts in Hyperledger Fabric

Participants

Participants are the actual entities who involve in distributed ledger process. Typically, organizations and other stakeholders such as organic certification authorities, organic farms and other computation parties like back-end servers can be considered as participants in this solution.

Peers

Peers can be considered as physical servers which carries distributed ledgers. However it is not required to have a ledger associated with every peer. Each participant who is involving in distributed ledger process needs to have access to the Hyperledger's ledger system. Smart contract can only be associated and invoked through peers, therefore participants who involved in this process need to have a peer belonging to them. Apart from providing access to distributed ledgers, Hyperledger peers are mainly responsible for endorsing transactions, distributing transaction among other peers etc.

When looking at peer terminology, it is possible to identify following major type of peers within the Hyperledger ecosystem.

- Endorser Peer : Endorsing peers can be considered as the primary contact point when initiating the transaction. When a participant or participating application wants to submit a transaction to the network, it first creates the transaction and submits it into the endorsing peer. Endorsing peers are responsible for endorsing the transactions which they endorse according to the endorsement policy defined during the smart contract creation. Also, endorser peers perform simulations for receiving transactions and create signed read write sets with respect to each transaction. Once above tasks have been performed, endorser peers will send endorsed (signed read-write set) back to the client/ application.

- Orderer Node : The primary purpose of orderer node is to maintain the order of transactions distributed across the network (among peers). Once client sends endorsed transactions to order node, it first assembles them into blocks. Adding transactions into blocks will be totally dependent on the block configuration settings. Once a block has been created within orderer node, it will be broadcasted across the network. Anchor peers will pick these broadcasted nodes in later stages.

- Anchor Peer : Anchor peers are responsible for capturing the transactions broadcasted by orderer nodes. Usually, anchor peers can be expected in every peer except for order peers. Orderer peers have inbuilt anchor peer capabilities. Once an anchor peer captures block from orderer peer, it distributes them among committing peers which are under them. When a committing peer received a transaction, it first simulates the transaction and verify endorsed read-write set values against block and if verified then, it will be added into local ledgers of peers.

Endorsement Policy

Endorsement policy defines the logic for transaction to be labeled as endorsed. Hyperledger fabric allows to define endorsement policies as rules within the system. Basically this involves in defining which peers or members need to endorse a given transaction before adding it into the ledger system. There are multiple ways which this can be defined by using combination of 'AND' and 'OR' operations. For an instance, following command defines one endorsement rule which specifies both peers of 'Org1' and 'Org2' need to sign transaction before they are being added into the ledgers.

```
peer chaincode instantiate -C <channelid> -n mycc
-P "AND('Org1.peer', 'Org2.peer')"
```

When a peer receives a transaction, it invokes the VSCC (Validation System Chaincode) associated with the transaction as part of the transaction validation flow to determine the validity of the transaction. Transaction contains one or more endorsements from one or more endorsing peers.VSCC is programmed to execute following tasks in order to determine the validity of transactions.

- To check whether all endorsements are valid (to check that all are properly signed etc.)

- To validate that there is an appropriate number of endorsements according to the defined endorsement policy.

- To verify endorsements' origin (whether they came from the expected source).

Membership Service Provider (MSP)

Membership service provider can be considered as the authentication and authorization handling mechanism within the system. There can be more than one MSPs for a given Blockchain system. In theory, it is required to have one MSP per organization and they are responsible for managing users within them.

In technical terms, a MSP can be considered as a certification authority (CA) which issues signature type known as business network cards to its participants. This business network card consists of security details which are required to authenticate each participant within the system.

Business Network Card

A Business Network Card provides all of the information needed for application / clients to connect to a blockchain business network. It is important to note that, the only way for application to access business network is through a valid business network card.

Business network card also contains connection profile details including URL to MSP service and endorser peers etc. which can be used by applications / participants to locate required services.

Channels

Hyperledger Fabric uses channels to communicate among its internal components. Each component within the hyperledger system needs to join to a specific channel in order to gain communication capability among internal components which have already joined to that particular channel. Each channel keeps its dedicated ledger synchronized with other distributed ledgers through a special synchronisation process.

Hyperledger also provides private channel concept which allows only defined set of participants to communicate with each other. This concept plays a major role since it allows set of users to achieve competitive advantage over others.

Smart Contracts

Smart Contracts can be considered as the major concept behind the decentralized autonomous organization (DAO). Smart contracts are programmatic logics which can be deployed into to Blockchain system. Smart Contracts can perform authorized CRUD operations on assets within the system and raise new transactions against them. However, it is important to note that, once a transaction is being created, only retrieval operation is permitted on it unlike in asset management.

When looking at the business functionalities offered in most of the organizations especially with respect to the automation domain including in organic food industry, it is obvious to mention that most of those functions can be automated using simple to complex smart contracts.

Transactions

Transactions can be considered as the actions which change assets' value from one state into another. In Hyperledger ecosystem asset's values can only be changed by invoking transaction on them. These transactions can be invoked from within a smart contract. In typical Blockchain system, once a transaction is made, it is treated as an immutable entry - means that once committed, it cannot be altered later. Therefore, transactions provide a robust way to handle historic events on all assets within the system. These transaction records can be later queried and analyzed for validity against given set of rules.

5.4 Proposed Solution Architecture

5.4.1 Detailed Flow of Execution

Figure 5.1 illustrates the proposed technology specific solution architecture. This architecture can be simply explained by following stages.

Stage - 1

As explained earlier, each farm will be divided into subfields as depicted in the diagram ('Field-1, Field-2 and Field-3' etc.). A sensor suite - a series of sensors will be installed in each of these fields to monitor status under different parameters. Then, a device agent which will be installed in a small hardware devices such as Raspberry Pis will collect data from its attached sensor suite.

Once necessary data have been collected from device agents, they will be sent out to a gateway for further processing. Gateways will be required because the edge devices (device agents) might not be capable of transmitting data (due to not having enough resources) to remote blockchain system.

During the data transmission process, as a protocol, MQTTS (MQTT over TLS later) will be used to transmit data from edge device to device gateway. Selection of MQTT protocol over other protocols can be justified with various reasons, among them, lightweightness and de facto standard for IOT domain can be considered as prominent reasons.

When considering about the data parameters which need to be sent to Blockchain for processing, basic parameters such as Potassium level (K), Phosphorus level (P), Nitrogen level (N), field number and device ID can be sent in as a simple JSON string as follows,

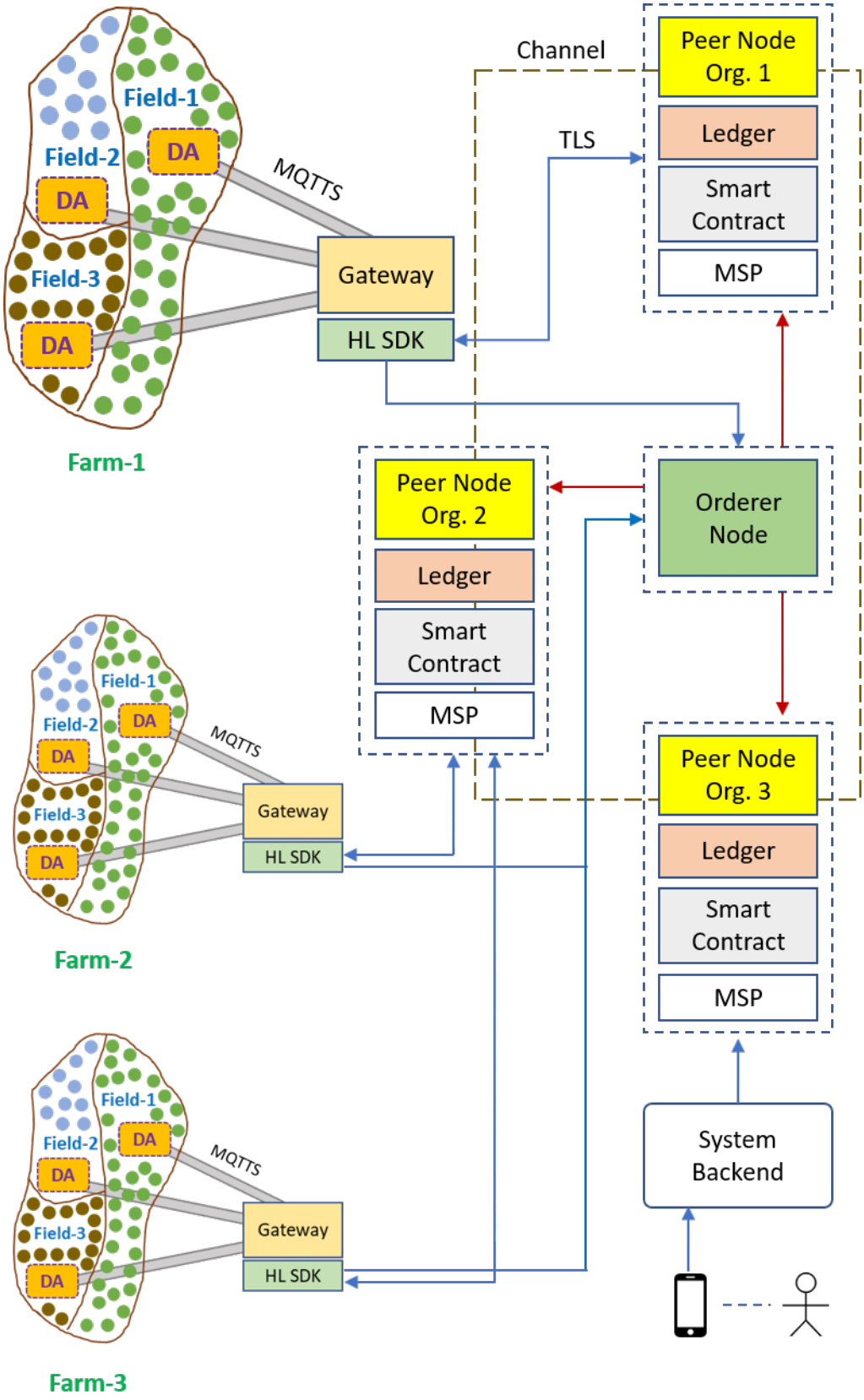


Figure 5.1: Proposed Solution Architecture

```
{
    "deviceId":"device001a",
    "fieldId":"lo24",
    "sensors":{
        "P":36.45,
        "K":41.25,
        "N":51.26
    }
}
```

Measurement of Potassium level (K), Phosphorus level (P), Nitrogen level (N) of soil can be considered as the minimum requirement to determine the organic level within a given farm field area. This is because, according to several studies conducted [34] [35], it is possible to detect whether some level of chemical fertilisers have been applied into a given farm filed by measuring above parameters.

Device agent or edge device at this stage needs to use the X509 digital certificate to encrypt sensor data and transmit them to the remote gateway. One of the important factor which needs to be emphasized in this context is the device agent software. As a part of solution, a device agent software / firmware which is capable of collecting sensor data on specific ports and pins on targeted hardware (such as RaspberryPi and Arduino) will be provided. It is advised to use these provided application agents / firmware on edge devices to avoid any data tampering during edge processing.

Data flow between device agent and device gateway can be more elaborately presented as in following figure 5.2,

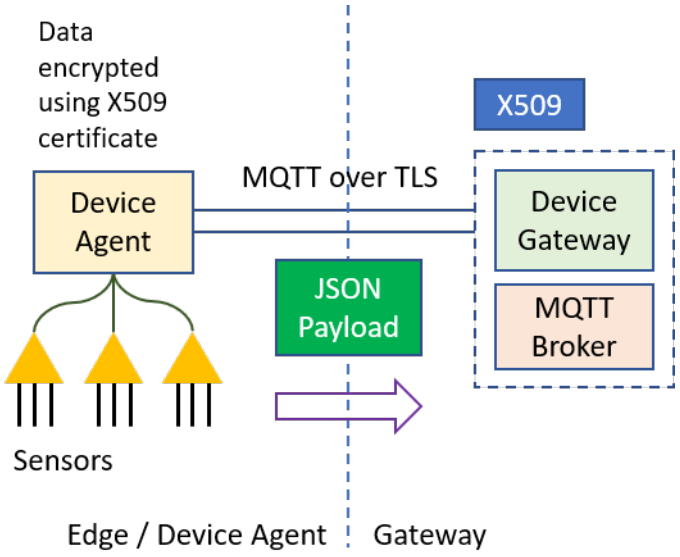


Figure 5.2: Device Agent and Device Gateway Communictaion

Stage -2

Once data have been received from edge devices to the gateway side, the next step would be to create transaction using those data. As a prerequisite, gateway agent appends farm identification to the JSON structure which will be used to create transactions.

In Hyperledger there are several SDK types which can be used to develop applications. For this solution development it has been decided to use Hyperledger Composer SDK as the core Hyperledger framework (selection details will be provided in future sections). As of writing this document, none of SDKs are providing out of the box encryption on data which are being transmitted to the hyperledger system.

Therefore one of the major task of this stage is to perform data payload encryption. For this purpose RSA key encryption together with diffie-hellman key exchange will be used.

Once a symmetric data encryption key has been shared between parties (device gateway and blockchain system), it will be used to encrypt transaction data which will be sent out to the hyperledger system. After necessary transaction data have been encrypted, new transactions will be created (one per farm-field data record) and submitted them to endorsing peers which are defined as part of endorsement policy defined in peer definition.

During this process, instead of encrypting entire message body which carries parameter values, a hashed string of that message body will be encrypted using the advanced encryption standard (AES) with cipher block chaining (CBC) mode and creates the signed signature. This generated signature will be sent along with the message body in the submitting transaction.

When submitting transactions to endorsing peers, it is required to provide Hyperledger card to validate the origin of each transaction. As explained earlier, these cards contains identities of respective participating actors provided by a specific MSP within the system. Participant authentication and authorization process can be achieved through card system where as data non repudiation aspects can be achieved through above mentioned singing mechanisms.

A sample transaction which will be submitted by the Hyperledger SDK to endorsing peer / Blockchain system can be given as follows,

```
{
    "farmId": "farm0001",
    "lotNum": "lot0002",
    "nitrogenLevel": "28",
    "phosphorusLevel": "31",
    "potassiumLevel": "33",
    "year": 2019,
    "month": 5,
    "day": 20,
    "hour": 10,
    "minute": 48,
```

```
    "encryptedHash": "5eaewcsT1cteaOU3kHDnyOxlEZiVON4IZpq
        /NjO5sxO/rLnHSwe2nAqAb68eX8cESmQqObNCctvaAZ5tYa8HKY="
}
```


Stage-3

When a transaction is received from a participant to endorsed peer, endorsing peer is responsible for endorsing it by labeling whether it is valid or not. In order for endorsing peer to specify a given transaction valid or not, first, it has to read incoming transaction data. However, some transaction data points at this point are encrypted but, it will not be a concern for transaction processing because endorsement process is not trying to interpret incoming data and instead, it just reads state of data and produce a read-write set for the transaction followed by a transaction signing process. Then signed read-write set will be sent back to the client.

Participants or applications, once received data back from respective endorsing peers, it will send endorsed transaction to orderer peer. Orderer peer will check for the validity of endorsement policy and if valid then adds transaction or set of transactions into a group called block.

Blocks will be distributed among other peer nodes within the channel by the help of broadcasting.

Operations explained in above stage 2 and 3 can be simply depicted in figure 5.3.

Stage 4

When other peer nodes receive blocks from orderer node, they will recheck for the validity of each block according to the endorsement policy. If blocks get validated then those blocks will be appended into their distributed ledgers.

Stage 5

Upon receival of transaction data to other peers, a scheduled smart contract will get triggered automatically to analyze received transaction data. These transaction data records include organic validity status measuring parameters such as different mineral levels.

Smart contract will check for each parameters' validity against set of defined rules. If it detected that parameters are getting out of defined ranges it will mark them as invalid and otherwise marked as valid. After determining the validity of each transaction record, smart contract will create a new transaction against a new asset which includes the validity status of a particular record.

Operations explained in above stage 4 and 5 can be depicted as in figure 5.4.

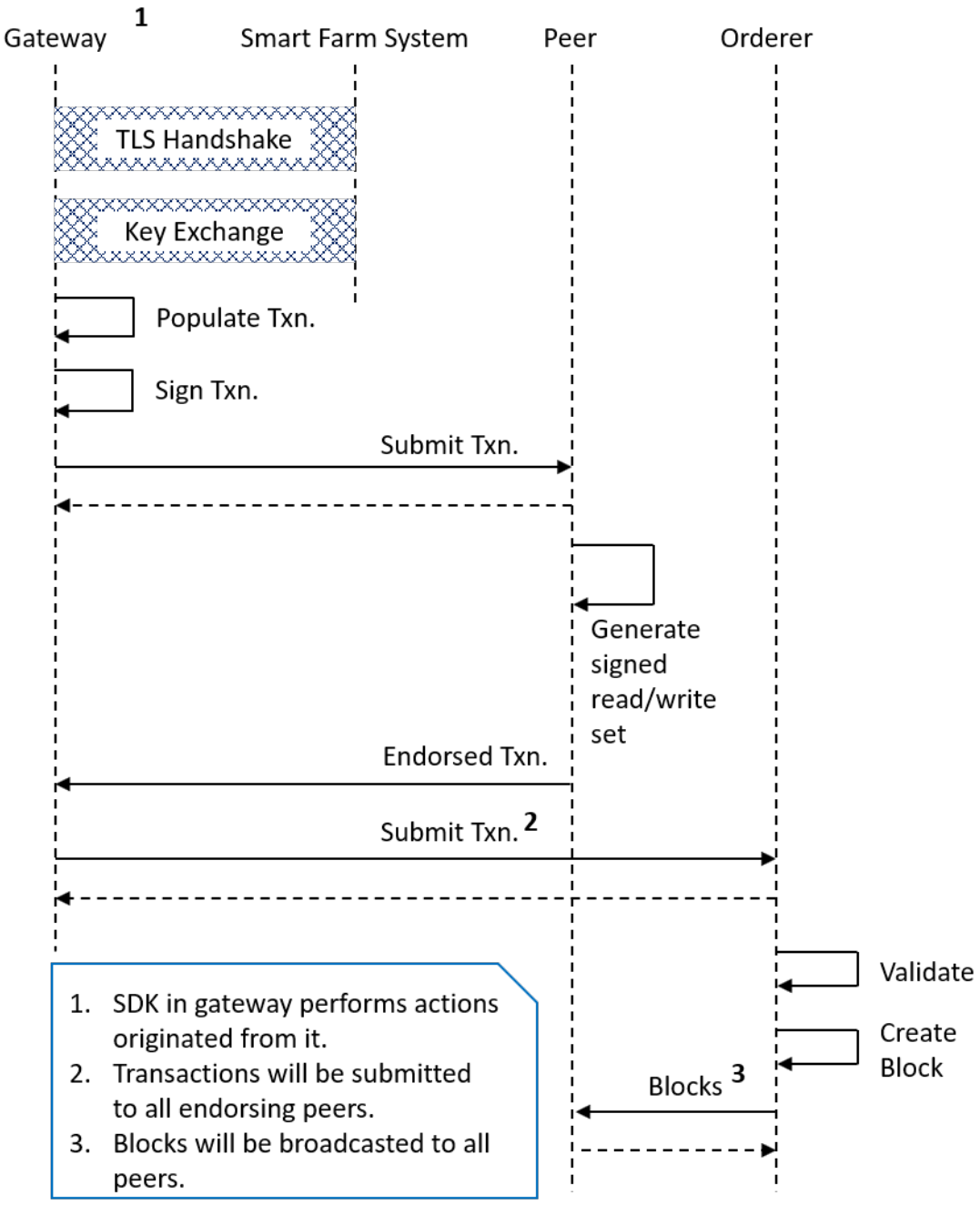


Figure 5.3: Operations between Gateway and Peers

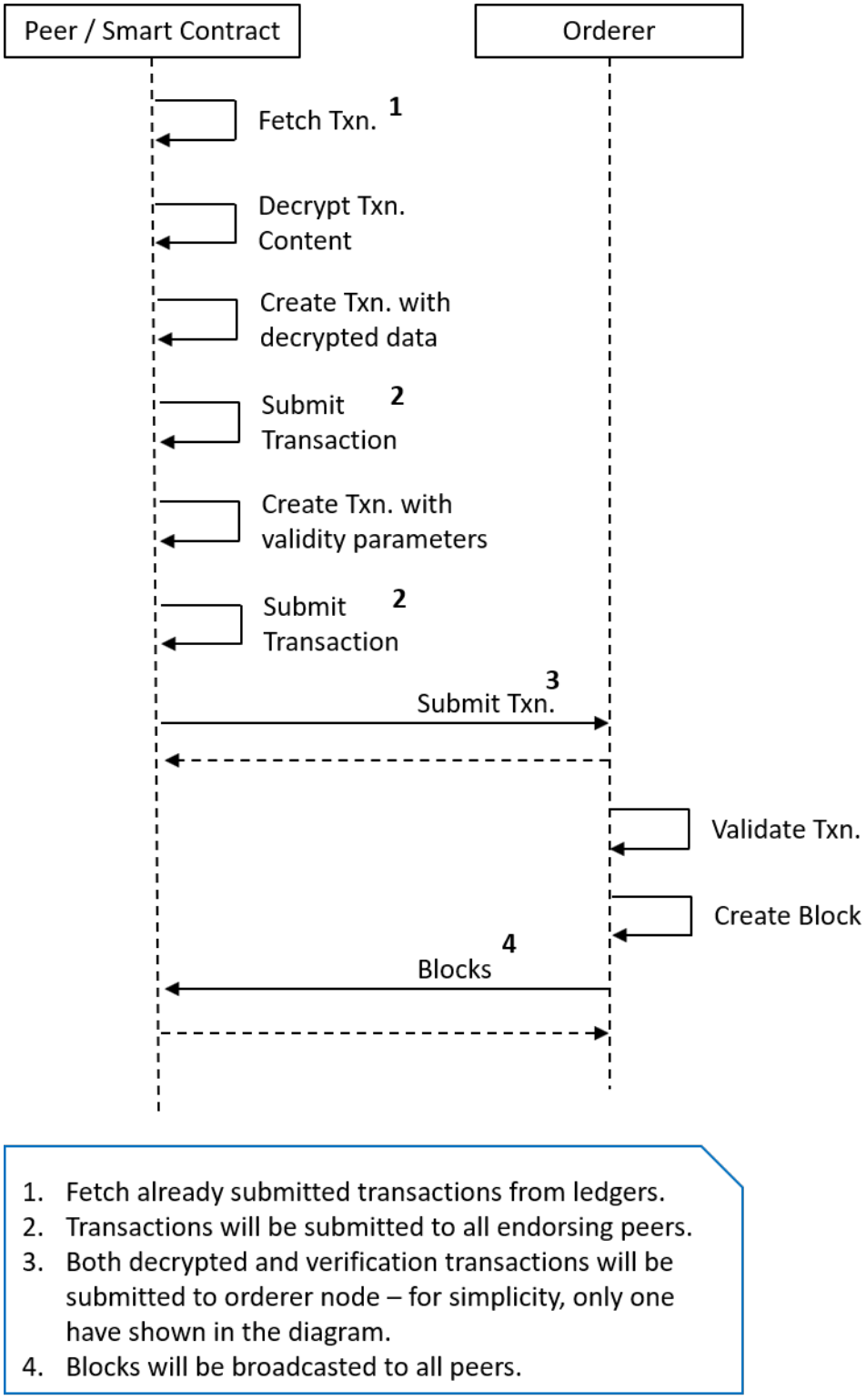


Figure 5.4: Operations between Peers and Orderer Node

5.4.2 Determining Blockchain Abstraction Layers

When looking at the vanilla version of Hyperledger Fabric, most of the tasks which need to be set up prior to using Hyperledger as well as tasks which need to perform after setting up it, require configuration and command execution on Hyperledger Fabric network itself. The commands which require to perform those tasks might require complex execution patterns and this can be considered as tedious set of tasks in some instances.

'Hyperledger composer' tool provides abstraction layer for development of business applications and configuring them. It abstracts complex process underneath and exposes simplified layer on top of it. Hyperledger Composer also carries community support to a greater extent through its open source initiatives. Therefore, it has been decided to proceed with Hyperledger composer as the development and configuration abstraction layer when developing this solution.

5.5 The Business Workflow

To summarize the lengthier process which was presented in last few chapters to harden the technology stack for better transparent system, following itemized steps can be presented. These steps need to be followed by solution users and system implementers in order to gain correct outcome of the proposed end solution.

Step - 1: Registering Process

As the first step, organic certification authorities get registered in the system. These certification authorities need to set up their local Hyperledger Fabric peers within their premises since they will be involved in the final endorsement which will happen in later stages in this process.

Once organic certification authorities get registered in the ecosystem, organic crops manufacturing farms then get registered in one of the available organic certification authorities. These organic certification authorities can be considered as different organizations or participants (more technically peers) within the final ecosystem.

Upon registering, each of organic farm will receive different and dedicated set of cards. These cards will be issued by the MSP (more technically, the CA) of respective organic certificate authority.

Step - 2 : Collecting Data from Farm Fields

Sensors deployed in farm fields will collect required data from its environment (including soil and moisture) and publish them via MQTT protocol to their respective gateways over encrypted tunnel. Before transmitting those data, each device will add their farm field ID into the message payload.

Step - 3 : Submitting data to Blockchain System

Farm gateways perform TLS handshake and exchange symmetric security keys for data encryption / signing process. A security key for each farm will be issued by the Blockchain solution (in this case security key can be either public key / private key pair or a simple symmetric key. However, for the implementation purpose of this solution, symmetric keys have been used).

Once farm gateway receives data payload from its subfields, it adds farm identification code into the message payload and sign it with previously obtained symmetric encryption keys. The important thing to note here is that, it might not require to exchange symmetric encryption keys every time the system is submitting the transaction, instead system can cache the security key for a defined amount of time.

As the next step, gateway will create a transaction and submit its signed payload into the Hyperledger Blockchain system. When submitting transactions to the blockchain system, device gateway application will provide card (obtained in above step 1) for each transaction.

Step - 4 : Transaction handling at Blockchain system

When a new transaction received to Hyperledger peer, it first checks whether the transaction is submitted with the correct business card. This process will include authorization and authentication handling at the Blockchain side, due to this process non-repudiation aspect of the entire ecosystem will be preserved. Then peers will go through the endorsement process (as explained in previous section). Once endorsement process complete, participant submits endorsed transaction to orderer node for block creation. Order node will then create blocks according to the block creation policy and distribute them among registered peers in the respective channel. At this point, peers do not decrypt any part of the transaction payload, instead it creates block out of encrypted / signed data.

Step - 5 : Peers updating distributed ledgers

Peers will receive blocks from orderer node and anchor peers will take them as the next step, then submit those to committing peers within the organization. Once committing peers receive blocks, they will update their ledgers. In this manner the entire system will have exact same distributed ledgers.

Step - 6 : Validating organic parameters of crops

A scheduled smart contract will get triggered against received transactions. These transactions will contain nothing but organic verification parameters and signatures received from farm fields. Therefore, as the first step, this smart contract will decrypt the encrypted parts in transaction payload by using the respective symmetric keys used during the encryption process.

Upon successful decryption, smart contract will create new transaction against a new asset type providing the organic validity of crops of each farm field. This smart contract will also create another set of transactions against new asset type with decrypted data for future reference.

It is important to note that, these new asset types which will carry the information about organic validity parameters and decrypted data can only be added to their respective ledgers through smart contracts. Therefore the end result of this ecosystem cannot be altered by external or internal parties.

During the verification process, more than one endorsing peers (conceptually, certification authorities) need to verify organic parameters (endorse transactions). Therefore, it is possible to say that more than one organic certification authorities are involving in verifying the organic nature of a given farm field which may belongs to a different organic certification authority. This leads to an improved organic certification mechanism.

Step - 7 : Validating Organic Parameters by End Users

End users will use applications based on mobile or web to query for specific crops' organic state by simply scanning the identification code like QR or barcode of the crops which they purchase. End user application will connect with a special peer node in Hyperledger Blockchain's ecosystem. This peer can be considered as a regular peer but it does not contain regular smart contracts in it. Instead this peer contains a special smart contract which is capable of providing a summarized output of organic nature of the respective organic crop.

Business logic involving in the final verification process of organic crop can be identified as follows,

- Once organic verification smart contract get invoked with a provided identification code (obtained from the end product), it first fetches decrypted organic status data of that particular crop for a defined period. Data fetch period is configurable and it should usually chosen as respective crop type's cultivation duration in days.
- When smart contract receive historic organic status data for a defined period, it will analyze each transaction data point. During the analysis if it detects a pattern of anomaly then smart contract will return negative response back to the caller - in this instance, the caller could be considered as the application used by end user. During this process it is important to adhere to a pattern of anomaly rather than just one anomaly event.

Above explained business verification process can be presented as in following figure 5.5.

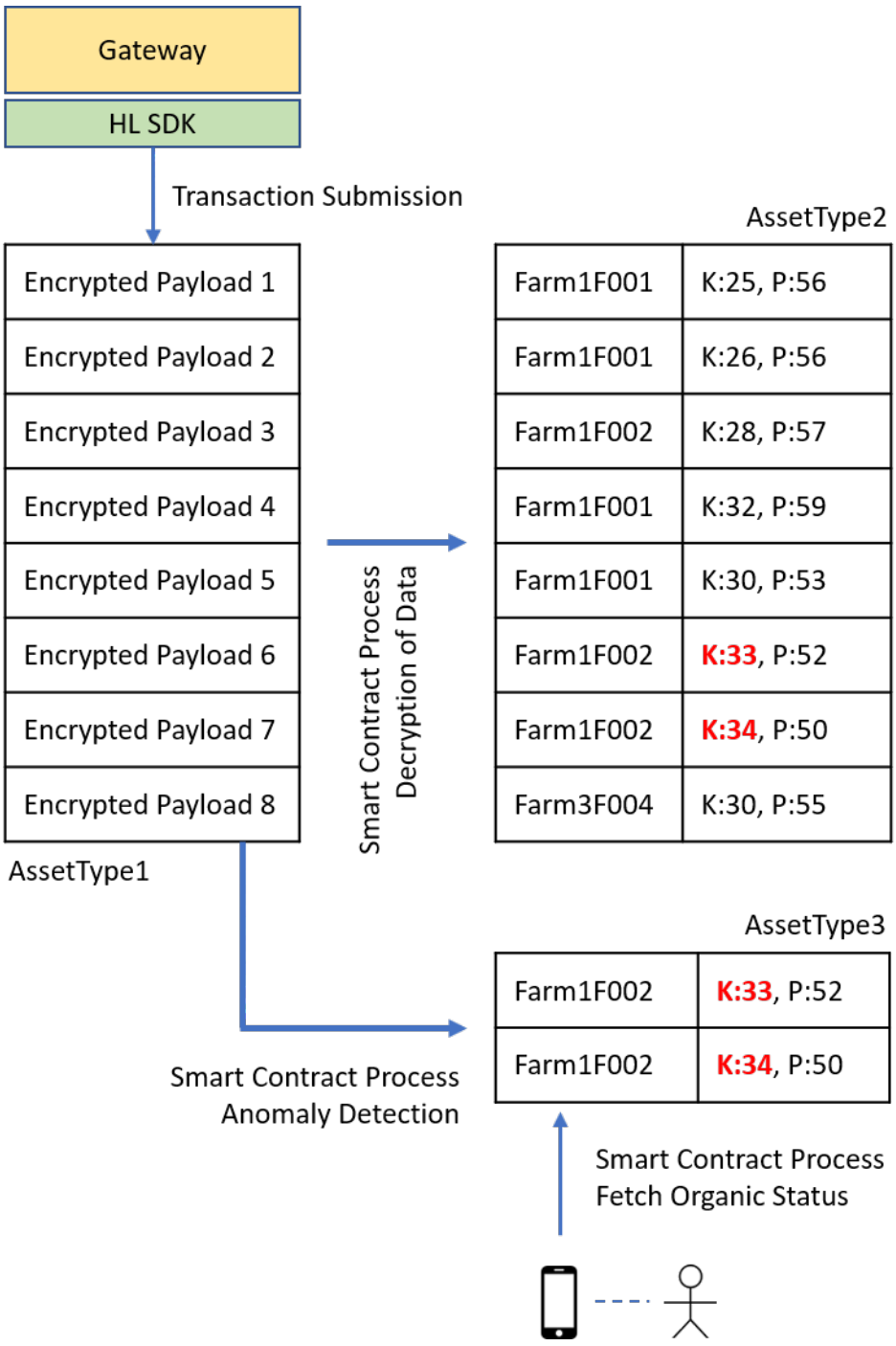


Figure 5.5: Organic Parameter Verification Process

5.6 Technologies Used

Following table5.2 lists down technologies / frameworks that have been used in order to develop the final solution.

Technology / Framework	Purpose
Hyperledger Fabric	As the underlying Blockchain (distributed ledger) backbone.
Hyperledger Composer	As the abstract SDK for Hyperledger Fabric.
Yeoman	As the client-side scaffolding tool.
Node.JS and Javascript	As the smart contract language.
Java 8 SE	As the data publisher agent development language.
Spring Boot	As the Java framework.
Moquette Broker	As the MQTT message broker.
Eclipse Paho	As the client side MQTT broker.
X509 Certificate	As the MQTT client authentication and for encryption purposes.

Table 5.2: Technologies Used

5.7 User Interface Designs

Since majority of the data ingestion part is handled automatically from the backend it is not required to have sophisticated user interfaces for it. However, once the system is in operational mode, it is required to have a web interface or a mobile application to check the validity of end products which are purchased by the end consumers. Therefore, following mobile application user interfaces (as shown in figure 5.6) have been implemented as part of the system implementation.

Figure 5.6: Screens of Mobile Application

5.8 Blockchain Related Data Models

Following Hyperledger Fabric blockchain related models and transactions have been used to implement the end solution.

```
namespace com.gbids.mcs.hlfarm.model.signedEntryData
asset SignedEntryData identified by entryId {
  o String farmId
  o String lotNum
  o String entryId
  o MineralLevel mineralLevel
  o Timestamp timestamp
  o String encryptedHash
}

concept MineralLevel {
  o String nitrogenLevel
  o String phosphorusLevel
  o String potassiumLevel
}

concept Timestamp {
  o Integer year
  o Integer month
  o Integer day
  o Integer hour
  o Integer minute
}

transaction createSignedFarmData {
  o String farmId
  o String lotNum
  o String nitrogenLevel
  o String phosphorusLevel
  o String potassiumLevel
  o Integer year
  o Integer month
  o Integer day
  o Integer hour
  o Integer minute
  o String encryptedHash
}
```

```
namespace com.gbids.mcs.hlfarm.model.decryptedEntryData

asset DecryptedEntryData identified by entryId{
  o String entryId
  o String farmId
  o String lotNum
  o String decryptedHash
  o MineralLevel originalMineralLevels
  o Timestamp originalTimestamp
  o Boolean signatureVerified
}

concept MineralLevel {
  o String nitrogenLevel
  o String phosphorusLevel
  o String potassiumLevel
}

concept Timestamp {
  o Integer year
  o Integer month
  o Integer day
  o Integer hour
  o Integer minute
}

transaction CreateEntry {
  o String farmId
  o String lotNum
  o String decryptedHash
  o String nitrogenLevel
  o String phosphorusLevel
  o String potassiumLevel
  o Integer year
  o Integer month
  o Integer day
  o Integer hour
  o Integer minute
  o Boolean signatureVerified
}
```

```
namespace com.gbids.mcs.hlfarm.model.validityEntryData

asset ValidityEntryData identified by entryId{
  o String entryId
  o String farmId
  o String lotNum
  o String valueFieldName
  o String valueFieldValue
  o String description
  o Boolean validity
  o Timestamp dataTimeStamp
}

concept Timestamp {
  o Integer year
  o Integer month
  o Integer day
  o Integer hour
  o Integer minute
}

transaction createEntry {
  o String farmId
  o String lotNum
  o String valueFieldName
  o String valueFieldValue
  o String description
  o Boolean validity
  o Integer year
  o Integer month
  o Integer day
  o Integer hour
  o Integer minute
}
```

```
function create_UUID() {
    var dt = new Date().getTime();
    var uuid = 'xxxxxxxx-xxxx-4xxx-yxxx-xxxxxxxxxxxx'
    .replace(/[xy]/g, function (c) {
        var r = (dt + Math.random() * 16) % 16 | 0;
        dt = Math.floor(dt / 16);
        return (c == 'x' ? r : (r & 0x3 | 0x8)).toString(16);
    });
    return uuid;
}


/**
 * @param
{com.gbids.mcs.hlfarm.model.signedEntryData.createSignedFarmData}
signedFarmData
 * @transaction
 */
function createSignedFarmData(signedFarmData) {
    return getAssetRegistry('com.gbids.mcs.hlfarm.model
    .signedEntryData.SignedEntryData')
        .then(function (signedEntryDataRegistry) {
            var assetFactory = getFactory();
            var NS = 'com.gbids.mcs.hlfarm.model
            .signedEntryData';

            var signedEntryId = create_UUID();
            var signedDataObj = assetFactory
            .newResource(NS, 'SignedEntryData', signedEntryId);

            signedDataObj.farmId = signedFarmData.farmId;
            signedDataObj.lotNum = signedFarmData.lotNum;
            signedDataObj.encryptedHash = signedFarmData
            .encryptedHash;

            var mineralLevelObj = assetFactory
            .newConcept(NS, "MineralLevel");
            mineralLevelObj.nitrogenLevel = signedFarmData
            .nitrogenLevel;
            mineralLevelObj.phosphorusLevel = signedFarmData
            .phosphorusLevel;
```

```
            mineralLevelObj.potassiumLevel = signedFarmData
            .potassiumLevel;
            signedDataObj.mineralLevel = mineralLevelObj;

            var timeStampData = assetFactory
            .newConcept(NS, "Timestamp");
            timeStampData.year = signedFarmData.year;
            timeStampData.month = signedFarmData.month;
            timeStampData.day = signedFarmData.day;
            timeStampData.hour = signedFarmData.hour;
            timeStampData.minute = signedFarmData.minute;
            signedDataObj.timestamp = timeStampData;

            return signedEntryDataRegistry
            .addAll([signedDataObj]);
        });
}


/**
 * @param
    {com.gbids.mcs.hlfarm.model.decryptedEntryData.CreateEntry}
    decryptFarmData
 * @transaction
 */
function createDecryptEntry(decryptFarmData) {
    return getAssetRegistry('com.gbids.mcs.hlfarm
    .model.decryptedEntryData.DecryptedEntryData')
        .then(function (decryptEntryDataRegistry) {
            var assetFactory = getFactory();
            var NS = 'com.gbids.mcs.hlfarm.model.decryptedEntryData';

            var decryptEntryId = create_UUID();
            var decryptDataObj = assetFactory
    .newResource(NS, 'DecryptedEntryData', decryptEntryId);
            decryptDataObj.farmId = decryptFarmData.farmId;
            decryptDataObj.lotNum = decryptFarmData.lotNum;
            decryptDataObj.decryptedHash = decryptFarmData
            .decryptedHash;
            decryptDataObj.signatureVerified = decryptFarmData
            .signatureVerified;
```

```
            var mineralLevelObj = assetFactory
            .newConcept(NS, "MineralLevel");
            mineralLevelObj.nitrogenLevel = decryptFarmData
            .nitrogenLevel;
            mineralLevelObj.phosphorusLevel = decryptFarmData
            .phosphorusLevel;
            mineralLevelObj.potassiumLevel = decryptFarmData
            .potassiumLevel;
            decryptDataObj.originalMineralLevels = mineralLevelObj;

            var timeStampData = assetFactory
            .newConcept(NS, "Timestamp");
            timeStampData.year = decryptFarmData.year;
            timeStampData.month = decryptFarmData.month;
            timeStampData.day = decryptFarmData.day;
            timeStampData.hour = decryptFarmData.hour;
            timeStampData.minute = decryptFarmData.minute;
            decryptDataObj.originalTimestamp = timeStampData;

            return decryptEntryDataRegistry.addAll([decryptDataObj]);
        });
}


/**
 * @param
    {com.gbids.mcs.hlfarm.model.validityEntryData.createEntry}
    validityEntryData
 * @transaction
 */
function createValidityEntry(validityEntryData) {
    return getAssetRegistry('com.gbids.mcs.hlfarm.model
    .validityEntryData.ValidityEntryData')
        .then(function (validityEntryDataRegistry) {
            var assetFactory = getFactory();
            var NS = 'com.gbids.mcs.hlfarm.model.validityEntryData';

            var validityEntryId = create_UUID();
            var validityEntryDataObj = assetFactory
    .newResource(NS, 'ValidityEntryData', validityEntryId);
```

```
            validityEntryDataObj.farmId = validityEntryData.farmId;
            validityEntryDataObj.lotNum = validityEntryData.lotNum;
            validityEntryDataObj.valueFieldName = validityEntryData
            .valueFieldName;
            validityEntryDataObj.valueFieldValue = validityEntryData
            .valueFieldValue;
            validityEntryDataObj.description = validityEntryData
            .description;
            validityEntryDataObj.validity = validityEntryData
            .validity;

            var timeStampData = assetFactory
            .newConcept(NS, "Timestamp");
            timeStampData.year = validityEntryData.year;
            timeStampData.month = validityEntryData.month;
            timeStampData.day = validityEntryData.day;
            timeStampData.hour = validityEntryData.hour;
            timeStampData.minute = validityEntryData.minute;
            validityEntryDataObj.dataTimeStamp = timeStampData;

            return validityEntryDataRegistry
            .addAll([validityEntryDataObj]);
        });
}
```

5.9 Edge Device Agent Implementation

As part of this solution, an edge device agents for selected hardware platforms will be implemented. The purpose of this edge device agents is to capture sensory data from attached sensors through their respective hardware input output pins. Once edge device agent starts to capture data directly from hardware input output pins, it does not matter whether there is any other program running in the same hardware device to capture the same set of data and alter them since those bogus applications cannot interfere with the edge device agent.

As a deliverable, an edge device agent running on Java has been designed for Raspberry Pi hardware type. It has the package structure as depicted in figure 5.7.

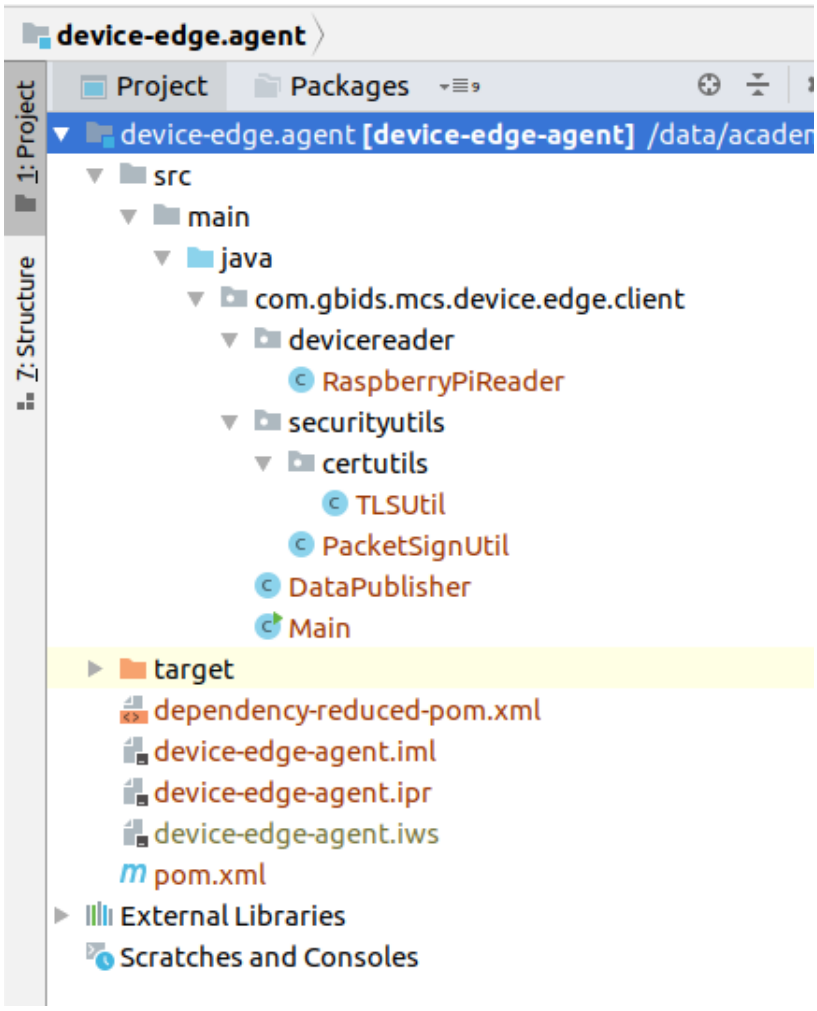


Figure 5.7: Device Agent Package Structure

5.10 Gateway Agent Development

Gateway agent is responsible for capturing incoming encrypted messages from devices which will be sent out by edge device agents. Upon receival of encrypted data, gateway agent first decrypt them and submit them as blockchain transaction to the Hyperledger Fabric peers.

Figure 5.8 depicts the package structure of device gateway agent which has been implemented by using Java components.

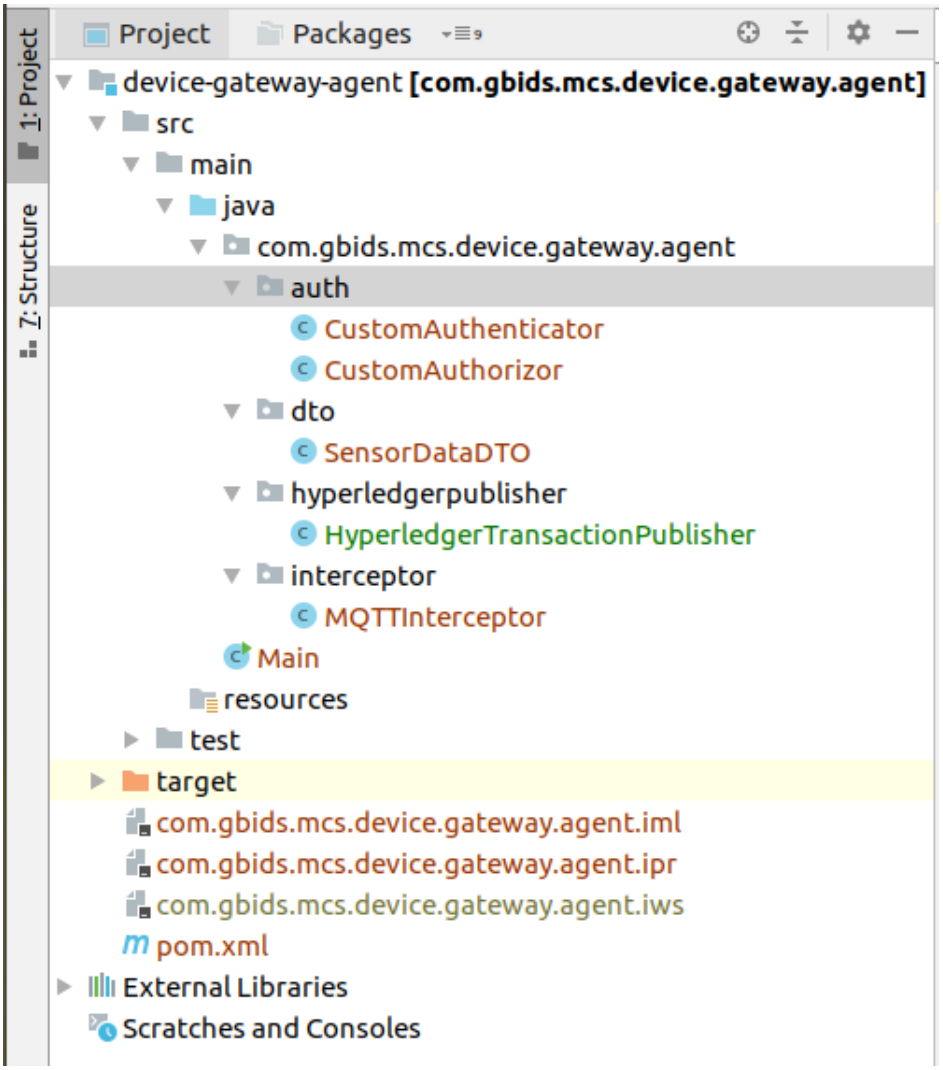


Figure 5.8: Device Gateway Package Structure

5.11 Conclusion of the Chapter

Within this chapter, the end solution which will formulate an entire ecosystem to optimize trust factors in organic agriculture business has been presented. Implementation related details including basic security fundamentals together with their implementation related details have also been presented. For the implementation of this endsolution, various technologies have been used and Hyperledger Fabric resides in the backbone of the solution to provide distributed ledger features. Entire solution have been developed by keeping the data transparency of the system as the first priority. Several Blockchain specific terminologies including smart contracts and read only asset registries have been used to optimize the end solution.

Chapter 6

Evaluation

6.1 Evaluation Plan

In order to evaluate proposed ecosystem for this solution, as a primary method, a scenario-based approach has been used. This method includes evaluation of any possible loopholes / weaken points associated with every data processing / collection point in the proposed flow. After a thorough analysis of each data processing / collection point, a conclusion will be provided at the end of this chapter.

6.2 Evaluation Procedure

The primary objective of this project is to improve the transparency of organic agriculture business. It is important to note that there exists several software solutions developed by various vendors to automate farming process by introducing smart farm solutions. However improving transparency in the flow was not their primary concern. Therefore, evaluation of mechanisms which have been taken in order to improve transparency within the ecosystem will be more focused in this chapter rather than focusing on process automation features provided by other applications.

Following scenarios can be evaluated for the transparency improvements.

Scenario 1: Weak points which associate when an edge device collects real time data from farm fields

Data tampering can be considered as one of the major security loophole that can be associated within this stage of the data flow. The only way which can be used to evaluate whether this fraudulent activity can happen or not during this stage is, by assuring that there is no way of tempering data at this level. To address this issue, following mechanisms have been introduced.

- Usage of out of the box firmware for edge devices
  Every edge device agent which is responsible for capturing sensor readings need to be installed with a firmware which has been provided as part of the solution. In this manner, it is possible to reduce data tampering happen at device-end because, this firmware directly captures sensor readings from device itself (such as Raspberry Pi, Arduino etc.) without relying on any external applications or libraries.

- Performing data encryption
  Data encryption will be performed within the edge device agent (and decrypted at the gateway). During this process secret key which will be used for encryption of parameters will be embedded into the edge device agent. Therefore, if any bogus application tries to send fraudulent data to gateway then it can be detected as tempered.

Scenario 2: Weak points which associate when edge devices sending data to device gateway

Data corruption and tempering which could happen during the data transmission can be identified as the major weak point which associates in this phase of the data flow.

To overcome this concern, this solution uses secure tunnel to transmit data from edge device to device gateway. Once edge device agent collects data from sensors it creates MQTT data packets and send them to remote MQTT broker which is deployed in respective gateway agent through a TLS layer. Hence, it is not an easy task for bogus users / applications to temper transmitting data.

Also, message signature adds additional security measures into the system which helps to identify any data tampering issues. Following figure 6.1 of transaction illustrates how message signatures are being kept in the original transaction when submitting them to the blockchain system.


```
{
    "farmId": "farm0001",
    "lotNum": "lot0002",
    "nitrogenLevel": "28",
    "phosphorusLevel": "31",
    "potassiumLevel": "33",
    "year": 2019,
    "month": 5,
    "day": 20,
    "hour": 10,
    "minute": 48,
    "encryptedHash": "5eaewcsT1cteaOU3kHDnyOxlEZiVON4IZpq/Nj05sxO/LOX/Jme
}
```


Figure 6.1: Signed Signature in Submitting Transactions

Scenario 3: Data tampering issues at the transaction processing

Usually, almost every available smart farm solution out there store their data in a centralized database system and most of the systems available are designed as centralized systems. Therefore, anyone who is having higher privileges in those systems can change persisted data within the system and thereby create false outcomes.

To address this issue, a blockchain based backbone has been used for the end ecosystem. As described in system design and system implementation chapters, once organic validity parameters have been added into the Hyperledger Fabric peers as transactions, there is no way of altering or reverting that particular transaction record from the system. Following figure 6.2 provides a proof that there is no way to change added transaction in the blockchain system since there is no any 'PUT' or 'DELETE' HTTP method available in Hyperledger Fabric's Composer rest server.

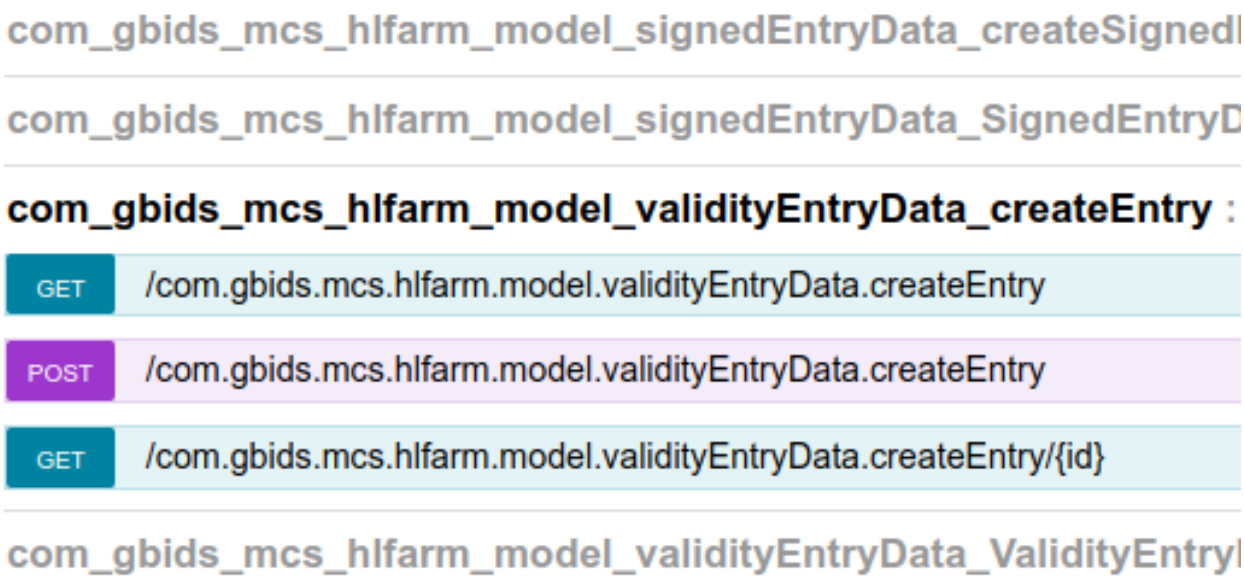


Figure 6.2: Methods Supported for Transactions

Scenario 4: Authentication related issues

Not being able to verify the authenticity of operations carried out within the system might leads to unwanted security issues.

To overcome this issue, when performing any transaction related operation, edge application or device gateway need to provide business network card issued by MSP within the peer organization. These card include X509 based certificates of each respective participant which can be used to authenticate participants within the system.

Following sample console output depicts the process of creating new X509 based certificates for participants by the MSP service in hyperledger.

```
2019-05-30 15:49:45.386 UTC [msp] newBccspMsp
-> DEBU 02c Creating BCCSP-based MSP instance
2019-05-30 15:49:45.386 UTC [msp] New -
> DEBU 02d Creating Cache-MSP instance
2019-05-30 15:49:45.386 UTC [msp] loadLocaMSP
-> DEBU 02e Created new local MSP
2019-05-30 15:49:45.386 UTC [msp] Setup
-> DEBU 02f Setting up MSP instance Org1MSP
2019-05-30 15:49:45.387 UTC [msp/identity] newIdentity
-> DEBU 030 Creating identity instance for cert

-----BEGIN CERTIFICATE-----
MIICQjCCAemgAwIBAgIQDJbOh88U+tlJ9He5sjUwBDAKBggqhkjOPQQDAjBzMQsw
CQYDVQQGEwJVUzETMBEGA1UECBMKQ2FsaWZvcm5pYTEWMBQGA1UEBxMNU2FuIEZy
YW5jaXNjbzEZMBcGA1UEChMQb3JnMS5leGFtcGxlLmNvbTEcMBoGA1UEAxMTY2Eu
b3JnMS5leGFtcGxlLmNvbTAeFw0xNzA2MjYxMjQ5MjZaFw0yNzA2MjQxMjQ5MjZa
MHMxCzAJBgNVBAYTAlVTMRMwEQYDVQQIEwpDYWxpZm9ybmlhMRYwFAYDVQQHEw1T
YW4gRnJhbmNpc2NvMRkwFwYDVQQKExBvcmcxLmV4YW1wbGUuY29tMRwwGgYDVQQD
ExNjYS5vcmcxLmV4YW1wbGUuY29tMFkwEwYHKoZIzj0CAQYIKoZIzj0DAQcDQgAE
kQ216YBD8kks+IzKJyBmdLqh/L/sEZ5twTqYpsK1ztNhIUDplsletAFOJQWRH+kb
hzFFNvS1qwveGRU6ztN5haNfMF0wDgYDVR0PAQH/BAQDAgGmMA8GA1UdJQQIMAYG
BFUdJQAwDwYDVR0TAQH/BAUwAwEB/zApBgNVHQ4EIgQgGatlq7sEgH2tEuTAqaqm
ZJ5who46vQIXoyLYnkfhpq4wCgYIKoZIzj0EAwIDRwAwRAIgCyrj/lUjtBYaEgMt
x98l5z+iLU6r+gp4CsdcDYzKLugCIGXlcU56avWSUtRAGn8Avpb6TOxtkrKIpeTE
QfM8VsS/
-----END CERTIFICATE-----

2019-05-30 15:49:45.388 UTC [msp/identity] newIdentity ->
DEBU 031 Creating identity instance for cert

-----BEGIN CERTIFICATE-----
MIICGjCCAcCgAwIBAgIRANuOnVN+yd/BGyoX7ioEklQwCgYIKoZIzj0EAwIwczEL
MAkGA1UEBhMCVVMxEzARBgNVBAgTCkNhbGlmb3JuaWExFjAUBgNVBAcTDVNhbiBG
cmFuY2lzY28xGTAXBgNVBAoTEG9yZzEuZXhhbXBsZS5jb20xHDAaBgNVBAMTE2Nh
Lm9yZzEuZXhhbXBsZS5jb20wHhcNMTcwNjI2MTI0OTI2WhcNMjcwNjI0MTI0OTI2
WjBbMQswCQYDVQQGEwJVUzETMBEGA1UECBMKQ2FsaWZvcm5pYTEWMBQGA1UEBxMN
U2FuIEZyYW5jaXNjbzEfMB0GA1UEAwwWQWRtaW5Ab3JnMS5leGFtcGxlLmNvbTBZ
MBMGByqGSM49AgEGCCqGSM49AwEHA0IABGu8KxBQ1GkxSTMVoLv7NXiYKWj5t6Dh
WRTJBHnLkWV7lRUfYaKAKFadSii5M7Z7ZpwD8NS7IsMdPR6Z4EyGgwKjTTBLMA4G
A1UdDwEB/wQEAwIHgDAMBgNVHRMBAf8EAjAAMCsGA1UdIwQkMCKAIBmrZau7BIB9
rRLkwKmqpmSecIaOOr0CF6Mi2J5H4aauMAoGCCqGSM49BAMCA0gAMEUCIQC4sKQ6
```

```
CEgqbTYe48az95W9/hnZ+7DI5eSnWUwV9vCd/gIgS5K6omNJydoFoEpaEIwM97uS
XVMHPa0iyC497vdNURA=
-----END CERTIFICATE-----
.......
.......
.......
```

Following sample console output depicts the authentication error which will be returned by the MSP service once tried to submit transaction with invalid / wrong business network card. This also provide a proof that, without a proper authentication, this solution will not accept any transaction into the system.

```
buddhi@buddhi-ideapad:~/applications/hyperledger/fabric-dev-servers$
composer transaction submit -c PeerAdmin@hlfv1 -d
'{"$class": "com.gbids.mcs.hlfarm.model
.signedEntryData.createSignedFarmData",
"farmId": "farm0001", "lotNum": "lot0002", "nitrogenLevel": "28",
"phosphorusLevel": "31", "potassiumLevel": "33", "year": 2019,
"month": 5, "day": 20, "hour": 10, "minute": 48, "encryptedHash":
"5eaewcsT1cteaOU3kHDnyOxlEZiVON4IZpq/Nj05sxO/LOX/jFuZq+30mr3rLn
HSwe2nsrf68eX8cESmQq0bNCctvaAZ5tYa8HKY=" }'

Error: Error trying to ping.
Error: No business network has been specified for this connection
```

Apart from above evaluated facts, it is also important to look at how this system improves transparency when it comes to the organic verification process. As explained in system implementation chapter, this ecosystem suggests to have several organic certification authorities when it comes to the final farm field organic parameter verification process - which will eventually leads to improved certification process. Also, every peer share the same smart contract for organic parameter verification process. Therefore, it is impossible to alter business logic independent of others.

Publicly viewable ledgers provide ability for end users to look for actual data directly without using any mobile or web application. This feature improves the transparency aspect within the ecosystem in a greater scale. However, mobile and web application ease off viewing verification process of transactions.

Following figure 6.3 shows how an end user would see the publicly available ledger and transactions from the blockchain system.

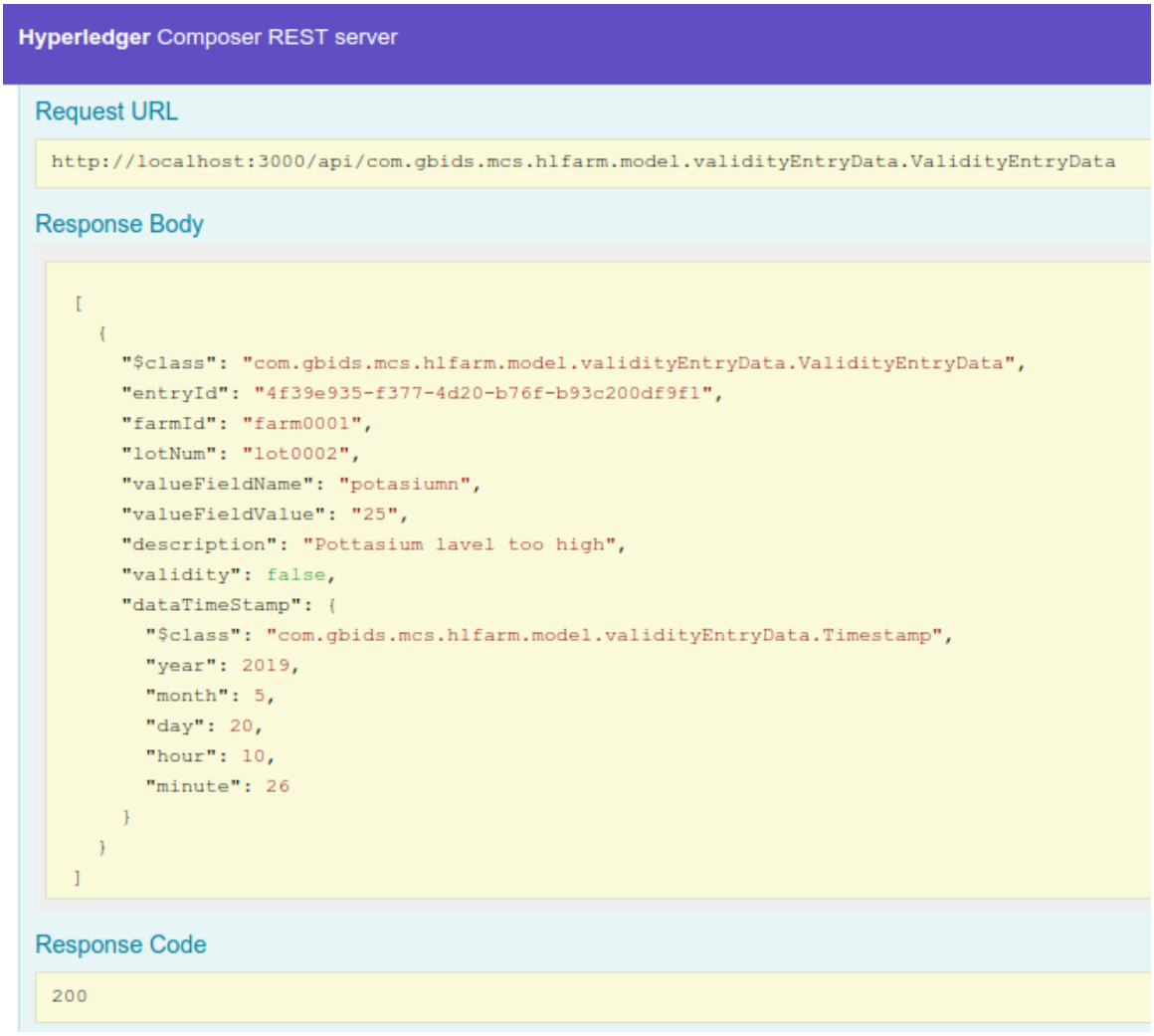


Figure 6.3: Public Assets and Transaction View

Conclusion

Throughout this study, issues and concerns which leads to improve distrust among end consumer regarding the organic crops which they purchase over regular market have been analyzed. After the analysis, it was clear that majority of consumers are losing their trust on so-called organic crops due to not having transparent certification process associated with organic certification authorities. Therefore, it has been decided to address this concern by approaching with a computer science based model to provide a better trustful system for organic agriculture ecosystem. As a result, possible candidate solutions including typical client server model and state of the art blockchain systems have been analyzed.

It has been concluded that building a solution with permissioned blockchain system for this type of scenario can be beneficial in many areas specially from development perspective as well as in consumer perspective. The Hyperledger Fabric blockchain system has been selected to proceed with the end solution. During the system design and system implementation phases, smart contract based solution has been formulated to optimize the trust factors within the organic agriculture ecosystem.

Mainly, within this proposed solution, trust factors have been improved by introducing smart contract based organic parameter verification mechanism where more than one pre registered certification authorities have to endorse a given crop in a particular farm field.

During the evaluation phase, it was clear that above proposed system meets basic cryptographic concerns as well as fundamental concepts with respect to improving trust factors to its extent and proved to be consistent for production usage.

Bibliography

[1] J. Lewin, "BBC goodfood," 01 02 2013. [Online]. Available: https://www.bbcgoodfood.com/howto/guide/organic. [Accessed 24 05 2018].

[2] J. Lewin, "What does organic mean?," BBC - GoofFood, [Online]. Available: https://www.bbcgoodfood.com/howto/guide/organic. [Accessed 11 08 2018].

[3] "Organic Foods," Food safety authority of Iraland, Dublin, 2015.

[4] "9 Amazing Benefits Of Organic Food," OrganicFacts.net, [Online]. Available: https://www.organicfacts.net/organic-products/organic-food/health-benefits-of-organic-food.html. [Accessed 15 08 2018].

[5] "15 Advantages of Organic Food," Sustainable Baby Steps, [Online]. Available: http://www.sustainablebabysteps.com/advantages-of-organic-food.html. [Accessed 15 08 2018].

[6] "The World of Organic Agriculture Statistics and Emerging Trends 2018," Research Institute of Organic Agriculture, Frick, Switzerland, 2018.

[7] K. Mathews, "Global Organic Food Market to Grow at Over 16% by 2020," 23 01 2016. [Online]. Available: https://www.techsciresearch.com/news/462-global-organic-food-market-to-grow-at-over-16-by-2020.html. [Accessed 24 05 2018].

[8] N. Amarasingam and A. Sugirtharan, "Demand for Organic food Products in the urban areas of the Batticaloa District, Sri Lanka," in Research Journal of Agriculture and Forestry Sciences, 2015.

[9] "Food Safety Authority of Ireland," 17 05 2017. [Online]. Available: https://www.fsai.ie/faq/organic_food.html. [Accessed 24 05 2018].

[10] J. Doward and A. Wander, "If you buy 'organic produce', can you trust what you get?," The Guardian, 21 08 2005. [Online]. Available: https://www.theguardian.com/uk/2005/aug/21/foodanddrink.organics. [Accessed 24 05 2018].

[11] "Organic Certification Procedures Manual," Organic Certifiers, Inc., CA, 2016.

[12] M. McEvoy, "Organic 101: Five Steps to Organic Certification," U.S. Department of Agriculture, 10 10 2012. [Online]. Available: https://www.usda.gov/media/blog/2012/10/10/organic-101-five-steps-organic-certification. [Accessed 15 09 2018].

[13] "Steps to Organic Certification," Sask Organic, 04 05 2018. [Online]. Available: http://saskorganics.org/steps-to-organic-certification. [Accessed 15 09 2018].

[14] Z. Liqiang, Y. Shouyi, L. Leibo, Z. Zhen and W. Shaojun, "A Crop Monitoring System Based on Wireless Sensor Network," Procedia Environmental Sciences, vol. 11, pp. 558-565, 2011.

[15] "Collection Tree Protocol," Wiki, 2018. [Online]. Available: https://en.wikipedia.org/wiki/Collection_Tree_Protocol. [Accessed 14 09 2018].

[16] "OnFarm," OnFarm, 2018. [Online]. Available: http://www.onfarm.com. [Accessed 15 09 2018].

[17] "Plant nutrients in the soil," Department of Primary Industries, [Online]. Available: https://www.dpi.nsw.gov.au/agriculture/soils/improvement/plant-nutrients. [Accessed 14 09 2018].

[18] "Smart Agriculture Sensors: Helping Small Farmers and Positively Impacting Global Issues," Mouser Electronics, 05 06 2018. [Online]. Available: https://www.mouser.com/applications/smart-agriculture-sensors/. [Accessed 14 09 2018].

[19] "Arable Mark," Arable, 2018. [Online]. Available: http://www.arable.com/. [Accessed 14 09 2018].

[20] "Products," Observant, 2018. [Online]. Available: https://observant.net/products/. [Accessed 14 09 2018].

[21] "Sensors," Pycno, 2018. [Online]. Available: https://pycno.co/sensors. [Accessed 14 09 2018].

[22] S. Nakamoto, "Bitcoin: A Peer-to-Peer Electronic Cash System".

[23] C. Roberto and P. Javier , "How blockchain improves the supply chain: case study alimentary supply chain," International Workshop on IoT Approaches: for Distributed Computing, Communications and New Applications, vol. 134, pp. 393-398, 2018.

[24] P. Lucena, A. Binotto, F. Da Silva and H. Kim, "A case study for grain quality assurance tracking based on a blockchain business network," in Symposium on Foundations and Applications of Blockchain, CA, 2018.

[25] S. A. ABEYRATNE and R. P. MONFARED, "Blockchain ready manufacturing supply chain using distributed ledger," in International Journal of Research in Engineering and Technology, 2016.

[26] M. P. Andersen, J. Kolb, K. Chen, G. Fierro, D. E. Culler and R. A. Popa, "WAVE: A Decentralized Authorization System for IoT via Blockchain Smart Contracts," University of California, Berkeley, 2017.

[27] K. Christidis and M. Devetsikiotis, "Blockchains and Smart Contracts for the Internet of Things," in PLETHORA OF RESEARCH IN INTERNET OF THINGS (IoT), 2016.

[28] "Introduction to Hyperledger Business Blockchain," Hyperledger Architecture Working Group, 2017.

[29] "Hyperledger Business Blockchain Technologies," Hyperledger, 2018. [Online]. Available: https://www.hyperledger.org/projects. [Accessed 21 07 2018].

[30] "The top 5 enterprise blockchain platforms you need to know about," Horses for Sourses, 18 03 2018. [Online]. Available: https://www.horsesforsources.com/top-5-blockchain-platforms_031618. [Accessed 20 02 2019].

[31] "Why Hyperledger Fabric?", Medium, 2019. [Online]. Available: https://medium.com/coinmonks/why-hyperledger-fabric-1b1479d483b4. [Accessed: 30- Feb- 2019].

[32] "Top 6 technical advantages of Hyperledger Fabric for blockchain networks", IBM Developer, 2019. [Online]. Available: https://developer.ibm.com/tutorials/cl-top-technical-advantages-of-hyperledger-fabric

-for-blockchain-networks/. [Accessed: 30- Feb- 2019].

[33] "5 advantages of using Hyperledger Fabric for your Enterprise Blockchain - DEV Community", Dev.to, 2019. [Online]. Available: https://dev.to/skcript/5-advantages-of-using-hyperledger-fabric-for-your-enterprise

-blockchain--302a. [Accessed: 30- Feb- 2019].

[34] S. Haneklaus, E. Schnug, H. Paulsen and I. Hagel, "Soil Analysis for Organic Farming", Communications in Soil Science and Plant Analysis, vol. 36, no. 1-3, pp. 65-79, 2005. Available: 10.1081/css-200042968 [Accessed 20 March 2019].

[35] N. Miller and K. Gleason, "Fertilizer in the Identification and Analysis of Cultivated Soil", The Archaeology of Garden and Field, pp. 25-43, 1994. [Accessed 13 March 2019].