AHMAD HUSSAIN
01-134171-006
BUSHRA FAZAL
01-134171-020

Blockchain driven Food traceability system

Thesis submitted to the Department of Computer Science, Bahria University, Islamabad for fulfillment of the requirements of Bachelors of Science in Computer Science degree.

Supervisor: Ma'am Romana Talat

Department of Computer Science
Bahria University, Islamabad

August 2020

Abstract

. In past few years cases of forged academic certificates have increased and verification of certificates is lengthy and time consuming process.In this project we used blockchain as it provides immutability to the stored data.The aim of this project was to devise a system which will use blockchain to store academics certificates on it and provides a method for the verification of academic certificates eliminating manual verification process and thus saving time.

Chapter 1

Introduction

1.1 Project Background

Blockchain is incorruptible digital ledger of immutable transactions, that can be programmed, to record virtually everything of value. Blockchain stores record in a distributed database which spread across all the nodes of the network using peer-to-peer (P2P) network. In P2P network, all nodes are connected to each other and these nodes can directly share data without the need of central server. Blockchain only update the ledger via consensus mechanism. This attribute gives the power of decentralization to the blockchain. It uses cryptography to secure transaction and block. Each block in a blockchain is connected to the next block using hash of previous block. Genesis block is a first block of the blockchain. "Data can only be added in the blockchain with time-sequential order"[1]. Each single transaction is recorded in a block, and on reaching the capacity of block, the block is added to the ledger called blockchain. Each transaction and block have a unique hash code, if someone wants to change the data of a transaction, the hash code of transaction and the block changes which will make the chain invalid.

Growing threats to food security lead, us towards the need for an innovative traceability system. Such systems need to include some mechanism related to food quality control which help us in ensuring the safety of food supply chain product. Food customers/consumers are becoming more health-conscious and want to know more about the food they get. They want to know about the quality of the food and the time when the food was made or brought from the source. "Customers are more likely to switch to a brand that provides more in-depth product information beyond what's provided on the physical label" [2]. Right now, there is no easy way to check where your food e.g. rice or meat, came from and how fresh they are. The complex chain from raw material to consumer is not known to the consumer.

To address the problem of unsecured food supply chain, a blockchain based solution is proposed which empowers the customers with more data about the food they get .in this system we will use some smart contracts to handle and manage transactions and communication between all the network nodes, system will also be able to verifies all of the transactions stored in a centralized system database. A private blockchain will be introduce which will allow all the network nodes to encrypt their secret information but some major participants will get extra authority like Retailer and manufacturer to handle their customers. Proposed system will collect and manage data against each item included in supply chain process which help us in monitoring and liability for agricultural food quality and safety, can also be prolonged to all food sectors. The main purpose of the proposed system is to enhanced traceability performance, and public health safety also helps to encourage development about the advancement of an advanced business strategies based on blockchain and IoT.

1.2 Problem Description

With the help of emerging new technologies of internet food traceability systems are improving day by day but nearly all of advanced systems are centralized. These systems result in customer trust problem like falsifying customer information, fraud and corruption. Centralized systems are always controlled by single authority so there is more risk of their collapse as single point of failure can lead us toward crash of the whole system. Food borne diseases rate is increasing with time , there is a need for enhancing the trust of customers on food. Blockchain technology is providing efficient solution for secure food tracing system. Firstly, it will help us in keeping every transaction secure between food source, processing, warehouse, transportation, and retailers. Secondly, it will exchange the traditional system of tracking and manual monitoring system. As the traditional way of tracing food chain is not efficient enough to provide detailed information about food. Customers used to take interest in more detailed information specifically about the food they get.

1.3 Project Objectives

Our Project objective is to design a secure food tracking system which impose blockchain features and characteristics. Traditional systems for food traceability are used for isolating dirtied products from reaching to the end consumers and preventing consumers from causing risks to their health with the use of these unhealthy products. On the other hand, these systems are much more time consuming, more expensive, can be easily hacked and less secure. In order to overcome the problems of traditional food traceability system, blockchain technology is quite helpful. This system will allow access to the consumer to get the detail information including its quality, making time and other aspect related to the food that they are going to purchase. It will provide us maximum accountability throughout the entire transportation process of food products in the chain. Also provides transparency and traceability throughout the whole transaction process.

1.4 Project Scope

The proposed shared system with many nodes, such as farmer, manufacturer, transporter, distributer, retailer and customer. Where retailer and customers can negotiate for the best prices for their items, distributors can make payments directly to consumers without brokers and mediators. The aim is to provide the complete traceability of the food from farmer to customer. As the product goes through multiple stages, and at each stage, information about the product is recorded in distributed ledger. A customer scans a code of the product, in which a query is encoded. This query will show a complete traceability of the product.

Chapter 2

Literature Review

With the increase in use of internet of things, many researchers also consider relevant to utilize these IoT technologies for food traceability systems in supply chains. In 2006 Folinas et al. [?] discussed the effectiveness of a traceability system depends on the methodology of tracking and tracing each individual product, in such a way that we will be able to monitor the trace from primary production of product until the final discarding by the consumer. In 2017 a food traceability system was proposed by Tian and Feng. [?]based on blockchain and LoRa IoT technology, in which they talked about the integration of reliable blockchain verification mechanism into the low-power wide-area network (LPWAN) IoT system, for example smart agriculture system based on LoRa/NB-IoT technologies. They believe that this incorporation will help people to advance the food safety standards.

In 2017 lightweight blockchain based architecture was proposed for smart greenhouse farms in order to enhance the security and privacy in smart farms. The paper was named as A framework for blockchain based secure smart Greenhouse farming [?] The system also provides some framework of security based on the combination of blockchain technology and IoT devices which result in secure communication platform in Smart Greenhouse farming . IoT devices in greenhouse have the benefits of private ledger these devices act as blockchain by managing the energy consumption within the Greenhouse farms. A new approach was proposed in 2018 that enhance the agricultural food chains and lead us towards trusted applications and services within these chains. This approach helps us in allowing better interactions of farmers and other supply chain participants more specifically consumer, where blockchain is used for enhancing the transparency in the data flow between participants and the capacity of data management. The authors think the research will provide better result in chains performance by proposing new food-on-demand business model. The proposed model can help in decreasing the gap of subjective and objective food metrices based on quality standards. [?]

Atlams have discussed that leading the IoT systems toward the decentralized approach is a wise decision and also highlighted the benefits and challenges that we face while the integration of IoT devices and blockchain. [?] He also describes that blockchain is incorruptible power full technology of this era which is able to handle all management processes and decentralized computation overcome the IoT issues more specifically security issues In 2018 ,a decentralized, blockchain-based traceability system was proposed for Agricultural Food supply chain, which was named AgriBlockIoT. [?] The system is able to flawlessly integrate IoT devices dealing with digital data along the chain. The author has -define, develop and deployed some use cases such as from-farm-to-fork for achieving traceability, he has used Ethereum and Hyperledger Sawtooth, two different blockchains approaches for checking the results. At the end the author has compared the result of both blockchain approaches with respect to network usage ,CPU and latency ,and also explain the drawbacks and benefits of both approaches.

Chapter 3

Requirement Specifications

3.1 Existing System

The existing systems for food traceability in Pakistan are centralized. These systems are used to track and trace the products at various stages of distribution chain and supply chain In Pakistan there is traceability solution named as Meat Trax introduces by ZAUQ group ,its purpose is to trace and track the life cycle of meat from cattle till the end customer. Where they are providing information related to the health, immunization records, growth and ownership information. The main drawback of these centralized system is that they can be easily hacked, there is a single point of failure if the centralized server crashes the whole system will fail. Due to the centralized characteristic of existing system they are losing their customer trust as customer are keener about the food they get ,its quality and safety. Existing systems of food traceability in Pakistan are more time consuming ,much expensive, can be easily hacked and less secure.

3.2 Proposed System

The proposed system is a blockchain based system where users will be able to trace complete food supply chain and distribution chain within just minutes. In this system a decentralized approach will be used to store data and information related to all network attributes on the blockchain once it will be stored on blockchain, it cannot be altered because this new technology provides transparency and immutability to the data stored on it. Hence the blockchain based traceability system which cannot be tempered will be much faster and more secure because when we query the system and get the information about food traceability without going through the traditional centralized system and also manual monitoring system we get information without delay. The proposed system will be able to provide us a secure traceable food supply chain from farm till the end customer with the help of blockchain security methods.

3.3 Requirement Specifications

3.3.1 Functional Requirement

- Retailer's system administrator can add nodes to the network. Nodes will be of Distributors, Transporter, and manufacturer.
- Retailer's system administrator will deploy smart contracts.
- Manufacturer can register/add the food product information.
- Customers can view and verify the traceability of product with time stamp information.
- Registered Transporter and Distributor can add their own info to the product info, for traceability.
- User requirement of the system is to provide traceability for the product they purchased.

3.3.2 Non Functional Requirement

- The system must be secure enough to prevent the leakage of sensitive information and provide confidentiality.
- The system should have controlled the maintenance cost.
- The system should be able to maintain the data integrity.
- The system should must be scalable to manage large amount of data.
- The system should be more adaptable to the changing needs of users.
- The system should be secure to store sensitive data.
- The system should be able to handle spam attacks.

3.4 Use Cases

3.4.1 Add Network Entities

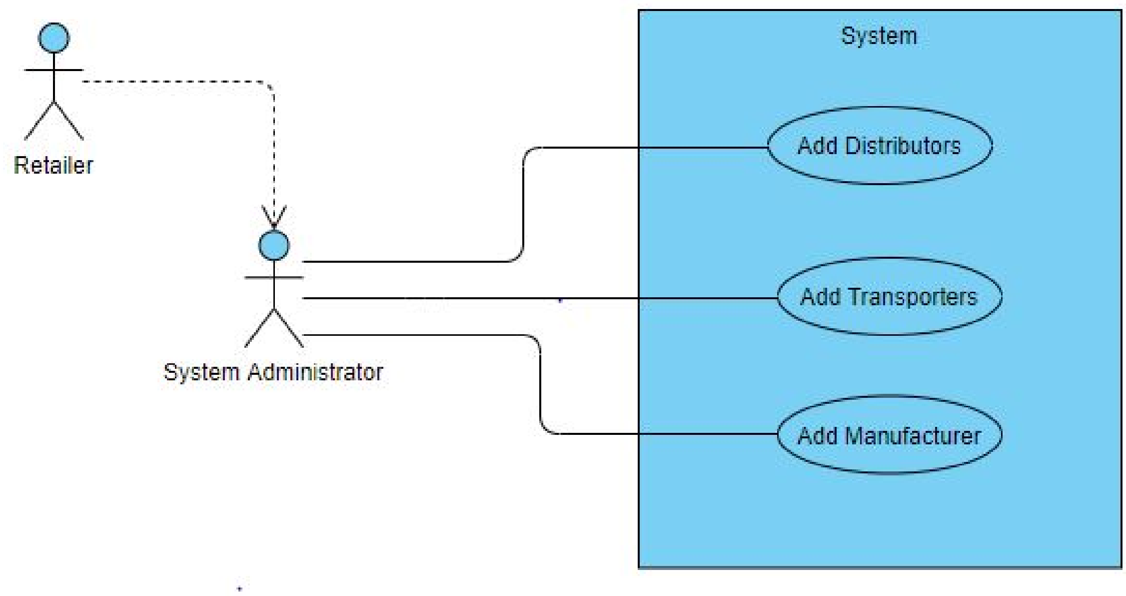

Figure 3.1: Add Network Entities

Use Case ID	UC 1
Use Case Name	Add Network Entities
Actor	Retailer, System Administrator
Pre Condition	A Hyperledger Iroha blockchain network should be build up and running.
Post Condition	Customers Manufacturer and Transporters are added to network
Success Scenario	Network nodes are successfully added to network

Table 3.1: Use Case 1

3.4.2 Deploy Smart Contract by Network Administrator

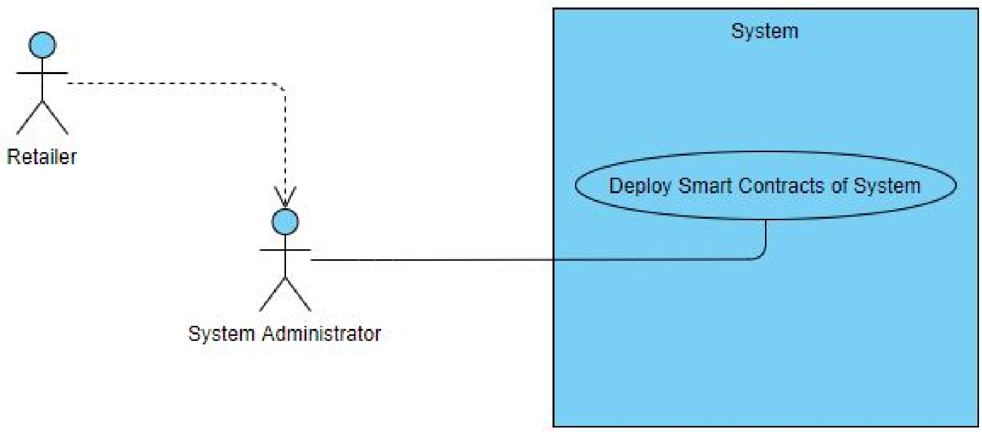

Figure 3.2: Deploy Smart Contract

Use Case ID	UC 2
Use Case Name	Deploy Smart Contract
Actor	Retailer, System Administrator
Pre Condition	A Hyperledger Iroha blockchain network should be build up and running.
Post Condition	Smart Contract are added to network
Success Scenario	Smart Contract nodes are successfully deployed

Table 3.2: Use Case 2

3.4.3 Access to Smart Contract

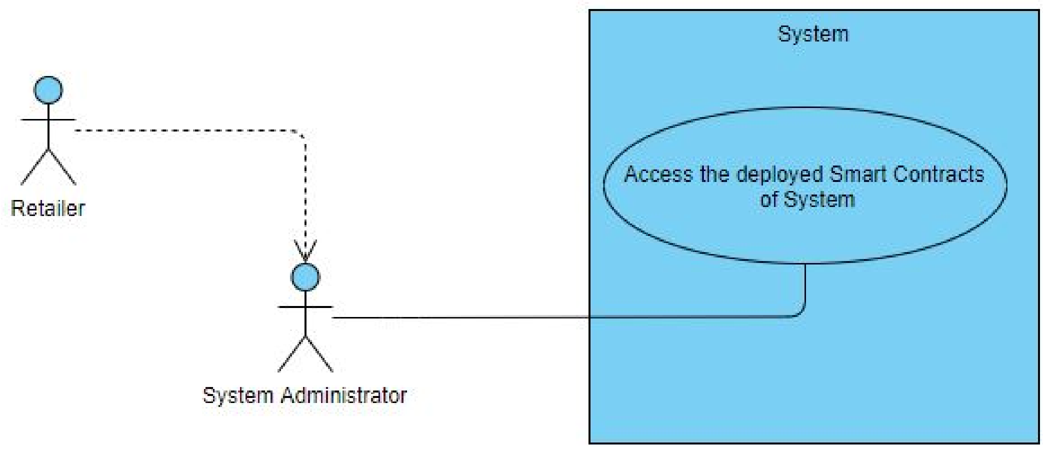

Figure 3.3: Access to Smart Contract

Use Case ID	UC 3
Use Case Name	Access to Smart Contract
Actor	Retailer, System Administrator
Pre Condition	A Hyperledger Iroha blockchain network should be build up and running and consumers distributors and manufacturers should be part of the blockchain network and smart contract must have been successfully installed, added nodes Peers by network administrator.
Post Condition	Smart Contracts are successfully deployed over the network
Success Scenario	Access to Smart Contracts is successfully added to network

Table 3.3: Use Case 3

3.4.4 Registration of Food Product

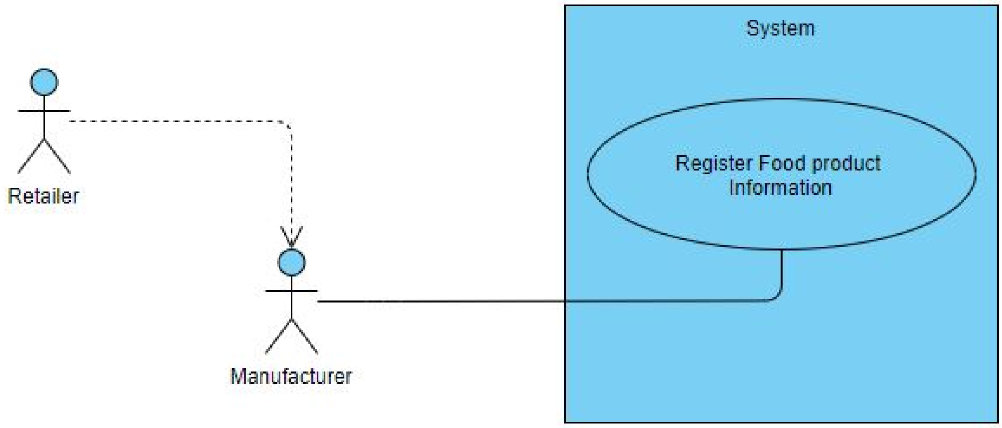

Figure 3.4: Register Food Product

Use Case ID	UC 4
Use Case Name	Register Food Product
Actor	Retailer,Manufacturer
Pre Condition	A Hyperledger Iroha blockchain network should be build up and running, all network nodes are added to network.
Post Condition	Food Product are added to hyperledger
Success Scenario	Food Product nodes are successfully Register to network

Table 3.4: Use Case 4

3.4.5 View Product Traceability

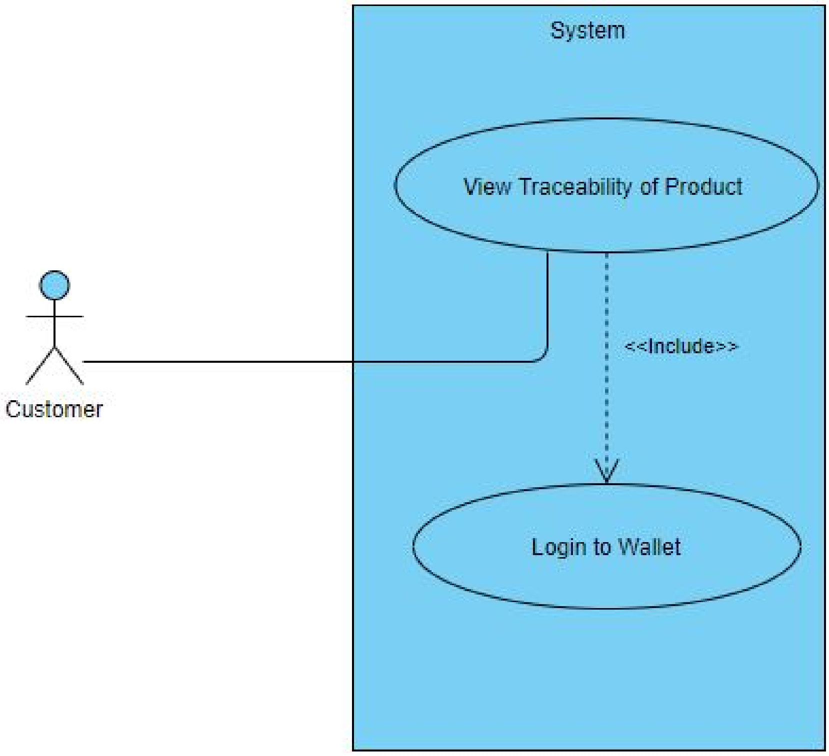

Figure 3.5: View Product Traceability

Use Case ID	UC 5
Use Case Name	View Product Traceability
Actor	Customer
Pre Condition	A Hyperledger Iroha blockchain network should be build up and running, all network nodes are added to hyper ledger and food products are registered.
Post Condition	Product Traceability is visible to Customers
Success Scenario	Product Traceability is successfully viewed to Customer

Table 3.5: Use Case 5

3.4.6 Verify Product Traceability

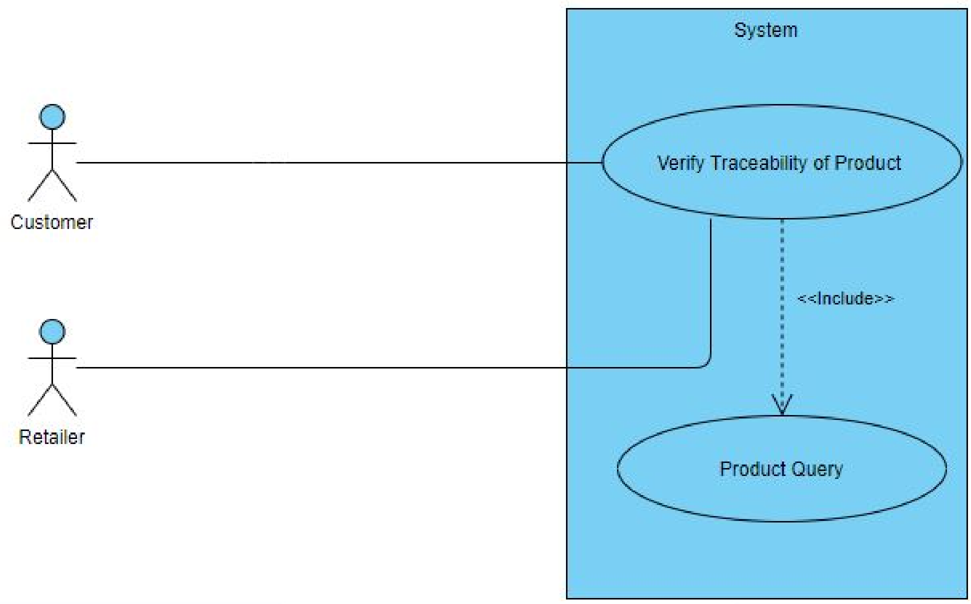

Figure 3.6: Verify Product Traceability

Use Case ID	UC 6
Use Case Name	Verify Product Traceability
Actor	Customer,Retailer
Pre Condition	A Hyperledger Iroha blockchain network should be build up and running, all network nodes are added to hyper ledger food products are registered and viewable .
Post Condition	Product Traceability is verified
Success Scenario	Product Traceability is successfully verified by Customer and Retailer

Table 3.6: Use Case 6

3.4.7 Add network nodes information

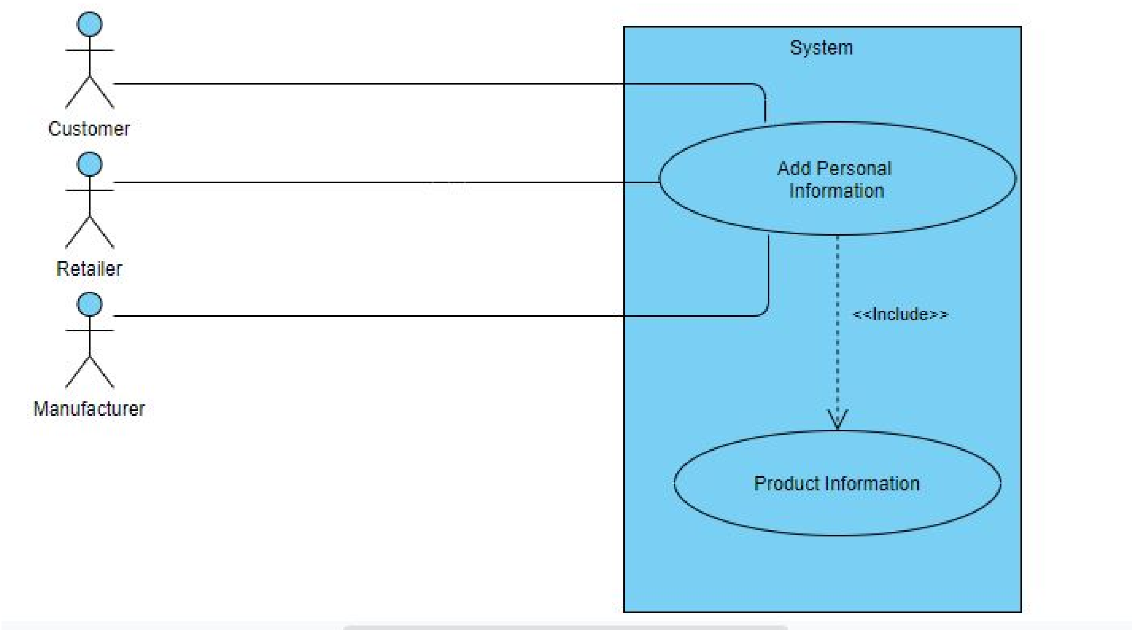

Figure 3.7: Add network nodes information with product

Use Case ID	UC 7
Use Case Name	Add network nodes information with product
Actor	Customer,Retailer,Manufacturer
Pre Condition	A Hyperledger Iroha blockchain network should be build up and running, all network nodes are added to hyper ledger food products are registered,viewable and verified .
Post Condition	Network nodes information is added with product over the network
Success Scenario	Network nodes information is successfully added with product over the network.

Table 3.7: Use Case 7

Chapter 4

Design

Systems design is the process of defining the architecture, components, modules, interfaces, and data for a system to satisfy specified requirements. This chapter should have the following sections:

4.1 System Architecture

This section describes the system in narrative form using non-technical terms. It should provide a high-level system architecture diagram showing a subsystem breakout of the system, if applicable. The high-level system architecture or subsystem diagrams should, if applicable, show interfaces to external systems. Supply a high-level context diagram for the system and subsystems, if applicable.

4.2 Design Constraints

This section describes any constraints in the system design (reference any trade-off analyses conducted such, as resource use versus productivity, or conflicts with other systems) and includes any assumptions made during the developing the system design.

4.3 Design Methodology

Summarize the approach that will be used to create and evolve the designs for this system. Cover any processes, conventions, policies, techniques or other issues which will guide design work. This is for deciding whether you will use structured, object-oriented or other specific methodologies. Most people will use some object-oriented technique with UML.

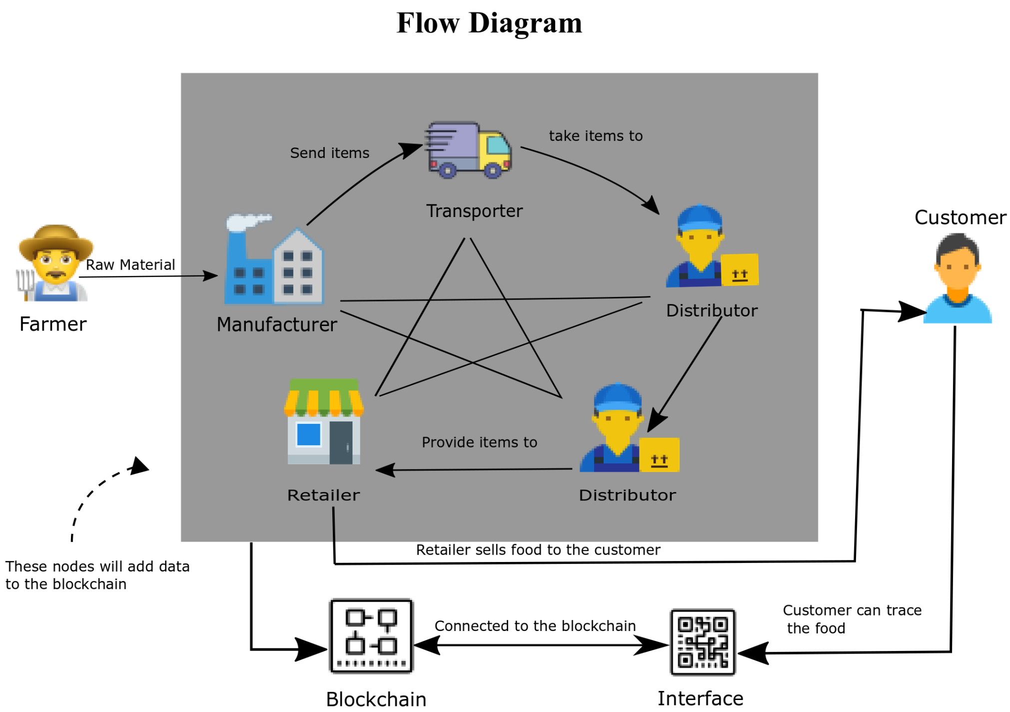

Figure 4.1: System Achitechture

4.4 High Level Design

This section describes in further detail elements discussed in the Architecture. High-level designs are most effective if they attempt to model groups of system elements from a number of different views. Typical viewpoints are:

1. Conceptual or Logical: This view shows the logical functional elements of the system. Each component represents a similar grouping of functionality. For UML, this would be a component diagram or a package diagram.

2. Process: this view is the runtime view of the system. The components are threads or processes or distributed applications. In UML, this would be a process interaction diagram.

3. Physical: this view is for distributed systems. The components are physical processors that have parts of the system running on them. For UML, this would be a deployment diagram.

4. Module: this view is for project management and code organization. The components are typically files or directories. This picture shows how the directory structure of the build and development environment will be designed.

5. Security: this view typically focuses on the components that cooperate to provide security features of the system. It is often a subset of the Conceptual view.

4.5 Low Level Design

This section provides low-level design descriptions that directly support construction of modules. Normally this section would be split into separate documents for different areas of the design. For each component we now need to break it down into its fundamental units or modules. For an OO implementation in Java, our components would become packages. Then the low level design will take each package and break it down into its classes. For smaller systems, you may have a single UML class diagram that each module description refers to.

4.6 Database Design

The section should reveal the final design of all database management system (DBMS) files and the non-DBMS files associated with the system under development. Provide a comprehensive data dictionary showing data element name, type, length, source, validation rules, maintenance (create, read, update, delete capability), data stores, outputs, aliases, and description.

4.7 GUI Design

This section provides the detailed design of the system and subsystem inputs and outputs relative to the user. Depending on the particular nature of the project, it may be appropriate to repeat these sections at both the subsystem and design module levels.

4.8 External Interfaces

External systems are any systems that are not within the scope of the system under development. In this section, describe the electronic interface(s) between this system and each of the other systems and/or subsystem(s), emphasizing the point of view of the system being developed.

References

[1] Peter J. Denning. Is computer science science? *Commun. ACM*, 48(4):27–31, April 2005. No Citations.