

# **Software Requirements Specification**

for

## **PRODUCT AUTHENTICATION USING BLOCKCHAIN**

**Prepared by**

Abhishek Singh Yadav

Aditi Batra

Anurag Tripathi

**KIET Group of Institutions**

**March 2023**

# Table of Contents

- 1. Introduction.....3**
  - 1.1 Purpose.....3
  - 1.2 Scope.....3
- 2. Overall Description.....3**
  - 2.1 Product Perspective.....3
  - 2.2 Product Functions .....3
  - 2.3 User Characteristics .....4
  - 2.4 Operating Environment.....5
  - 2.5 Constraints .....5
  - 2.6 Assumptions and Dependencies .....5
- 3. External Interface Requirements .....6**
  - 3.1 User Interfaces .....6
  - 3.2 Hardware Interfaces .....6
  - 3.3 Software Interfaces .....6
  - 3.4 Communications Interfaces .....7
- 4. Other Nonfunctional Requirements.....7**
  - 4.1 Performance Requirements.....7
  - 4.2 Security Requirements.....7
  - 4.3 Software Quality Attributes .....7
  - 4.5 Business Rules .....8
- 5. Other Requirements .....8**
  - 5.1 Appendix A: Glossary.....8
  - 5.2 Appendix B: Diagrams.....9

# 1. INTRODUCTION

## 1.1 Purpose

Several businesses have struggled for years with the problem of fake goods being marketed to unwary customers. Customers now find it more challenging to distinguish between real and phony goods due to the growth of e-commerce and online marketplaces. The selling of counterfeit goods is still a major issue, costing consumers and legitimate businesses money, despite the efforts of brands and regulatory organizations. Yet, there may be a solution to this problem with the development of blockchain technology. A secure and trustworthy method for product authentication can be developed by utilizing the transparency and immutability of blockchain, ensuring that customers can buy authentic products with confidence.

## 1.2 Scope

This software system's purpose is to offer a solution for product authentication that makes use of blockchain technology to guarantee the authenticity of products. Using blockchain technology, the system will let product makers give each product a digital identity that users can access via a smartphone application. Customers can scan a product's QR code with the mobile application to verify its authenticity. The system will also allow product makers to monitor the flow of goods via the supply chain, preventing the introduction of fake goods.

# 2. OVERALL DESCRIPTION

## 2.1 Product Perspective

Blockchain technology will be included in the software system to offer a reliable and secure mechanism for product authentication. Using blockchain technology, the system will let product makers give each product a digital identity that users can access via a smartphone application. Customers can scan a product's QR code with the mobile application to verify its authenticity. The system will also allow product makers to monitor the flow of goods via the supply chain, preventing the introduction of fake goods.

The software system will be compatible with existing systems and will provide an API for integration. The system will use secure cryptographic algorithms to protect the digital identities of products and will be compliant with relevant data protection regulations.

## 2.2 Product Functions

The software system will have the following functions:

1. **Product Identity Creation:** The system will allow product producers to build a digital identity for each product using blockchain technology.
2. **Product Movement Tracking:** The system will enable product manufacturers to track the movement of products through the supply chain.
3. **Mobile Application:** Customers will be able to scan a product's barcode to confirm its authenticity using the system's mobile application. The mobile application will be available for both Android and iOS platforms.

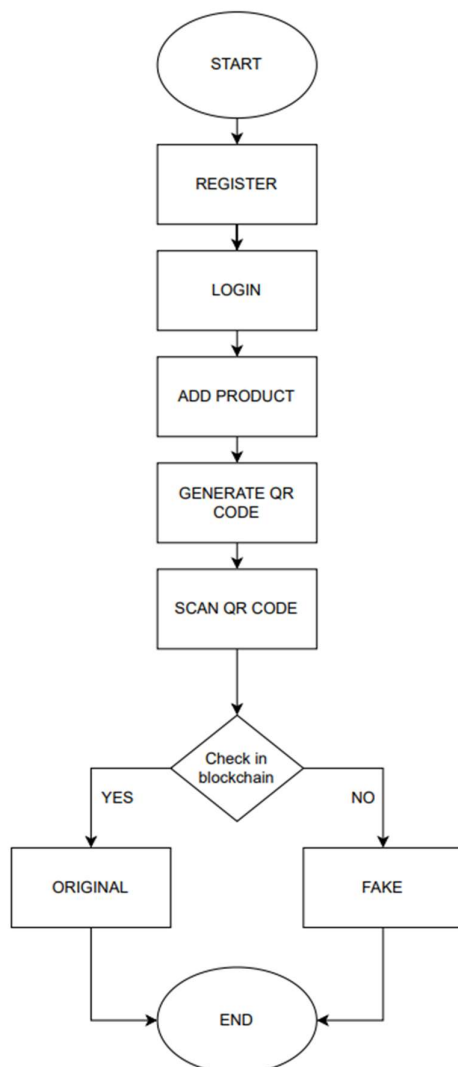
4. **Real-Time Authentication:** The system will be able to authenticate products in real-time, allowing customers to quickly and easily verify the authenticity of a product.
5. **API Integration:** The system will provide an API for integration with existing systems.
6. **Data Protection:** The system will use secure cryptographic algorithms to protect the digital identities of products and will be compliant with relevant data protection regulations.

## 2.3 User Characteristics

**Customers:** Customers will be the primary users of the system. They should have basic experience in utilizing a mobile application and the ability to scan barcodes.

**Product manufacturers** will use the system to give their goods digital identities and follow their progress through the supply chain. They ought to be familiar with supply chain management and blockchain technology on a fundamental level.

**System Administrators:** System administrators will be responsible for managing the software system. They should be highly skilled in database management, blockchain technologies, and software development.



## 2.4 Operating Environment

The software system will operate in the following environment:

**Hardware:** The system will require a server to host the blockchain network and the database for product authentication and supply chain tracking. To process large numbers of transactions, the server needs to have enough processing power and memory.

**Software:** The system will require blockchain software, database management software, and a mobile application for customers. The database management software should be able to handle large amounts of data, and the blockchain software should be compatible with the server's operating system.

**Network:** The system will require a secure network connection to ensure the privacy and integrity of data. The network should be protected with firewalls and other security measures to prevent unauthorized access.

**Operating system:** The blockchain software and database management software should work together with the server's operating system. Both the Android and iOS operating systems should be supported by the customer's mobile application.

**Maintenance:** The system will require regular maintenance and updates to ensure optimal performance and security. This includes updating software versions, keeping an eye out for bugs and security holes, and applying patches and fixes as necessary.

**Backup and recovery:** In the event of a system failure or disaster, the system should have a backup and recovery plan in place to guarantee that data is not lost. A recovery plan should be created to restore the system in the event of a failure, and regular backups should be made and stored offsite.

## 2.5 Constraints

- **Security:** The software system must be designed with robust security measures to ensure the protection of digital identities and prevent unauthorized access to the system. The system must be compatible with current devices and systems and must offer APIs for simple integration.
- **Data Privacy:** The system must comply with relevant data privacy regulations, such as GDPR, and ensure that customer data is protected.
- **Performance:** The system must be designed to handle high numbers of product authentication requests in real-time.
- **Cost:** The system must be cost-effective and provide value to both customers and product manufacturers.
- **Scalability:** The system must be designed to scale as the number of products and users grows.

## 2.6 Assumptions and Dependencies

Assumptions

- Product manufacturers will be willing to participate in the system and create digital identities for their products.

- Customers will be willing to use the mobile application to authenticate products and will have access to mobile devices and internet connectivity.
- Product barcodes will be unique and accurately depict the product's identification.
- The blockchain network and database will be secure and reliable, and capable of handling high volumes of transactions.
- The system will comply with relevant regulations and industry standards for data privacy and security.
- The system will be scalable and versatile to adapt to changing company needs and technology improvements.

#### Dependencies

- **Blockchain Technology:** The system depends on the availability and reliability of blockchain technology to provide a secure and tamper-proof method of tracking products through the supply chain.
- **QR code Scanners:** The system depends on the availability of barcode scanners to scan product barcodes and verify their authenticity.
- **Mobile Devices:** The system depends on the availability of mobile devices to run the mobile application for customers.
- **Internet Connectivity:** The system depends on the availability and reliability of internet connectivity to connect to the blockchain network, database, and mobile application.

## 3. EXTERNAL INTERFACE REQUIREMENTS

### 3.1 User Interfaces

**Mobile Application for Customers:** The mobile application will allow customers to scan the product's QR code and check their legitimacy. The interface will be intuitive and user-friendly, providing clear instructions and feedback to the user.

**Web Application for Product Manufacturers:** The web application will allow product manufacturers to create digital identities for their products and track them through the supply chain. The interface will be secure and accessible only to authorized users.

### 3.2 Hardware Interfaces

**QR code Scanners:** To scan the product's QR code and confirm its authenticity, the system will interface with barcode scanners.

**Mobile Devices:** To access the camera and internet connectivity features, the mobile application will interface with mobile devices.

**Server:** The system will require a server to host the blockchain network and the database for product authentication and supply chain tracking. The system will interface with the server's hardware components, such as processors, memory, and storage devices.

### 3.3 Software Interfaces

**Blockchain Software:** The system will utilize blockchain software to provide a secure and tamper-proof method of tracking products through the supply chain. The blockchain software will interface with the database management software to store and retrieve product information.

**Database Management Software:** The system will utilize database management software to store and retrieve product information. The database management software will interface with the blockchain software to ensure data integrity and security.

### 3.4 Communication Interfaces

**Mobile Data Network:** The mobile application will communicate with the blockchain network and the database management software through the mobile data network.

For the system to authenticate products in real time, it will need a strong and dependable mobile data connection.

**Internet Protocol (IP) Network:** Using the IP network, the web application for manufacturers of goods will interact with the blockchain network and the database management program.

The system will require a stable and reliable IP network connection to create and track digital identities for products.

**Application Programming Interface (API):** The system will offer an API that enables access to the database management system and the blockchain network by third-party applications. The API will enable integration with other systems, such as e-commerce platforms, to provide seamless product authentication and supply chain tracking.

**Secure Sockets Layer (SSL):** The system will utilize SSL to provide secure communication between the mobile application, the web application, and the server hosting the blockchain network and the database management software. SSL will ensure data confidentiality and integrity during transmission.

**Messaging Protocol:** The system will utilize a messaging protocol to provide real-time notifications to customers and product manufacturers regarding product authentication and supply chain tracking. The messaging protocol will ensure timely and accurate communication between the system components.

## 4. Other Non-Functional Requirements

### 4.1 Performance Requirements

The system shall be able to authenticate products in less than 3 seconds. A daily minimum of 10,000 authentication requests must be handled by the system. The system shall have a 99.9% uptime.

### 4.2 Security Requirements

The system shall use secure cryptographic algorithms to protect the digital identities of products and multi-factor authentication for user accounts. The system shall be compliant with relevant data protection regulations.

### 4.3 Software Quality Attributes

**Scalability:** The system will have a strong capacity for growth, allowing it to support an increasing quantity of goods and users on the blockchain network. Also, the system will be able to process a large number of transactions instantly.

**Usability:** The system will be user-friendly, offering customers and product makers a straightforward and intuitive interface to obtain product information and follow supply chain data. Also, the system will give the user feedback and clear directions.

Product data and transactions on the blockchain network will be processed swiftly and accurately thanks to the system's high performance. Additionally, the technology will offer quick supply chain tracking and product authentication responses.

**Maintainability:** With a modular and scalable design that enables simple upgrades and improvements, the system will be simple to maintain. In the event of a problem, the system will also be simple to troubleshoot and diagnose.

Customers and product producers will be able to access the system from a variety of platforms and devices because of the system's compatibility with different operating systems, browsers, and mobile devices.

## 4.4 Business Rules

- Throughout the production process, a special identifying number must be assigned to each product.
- Any transactions involving the supply chain, such as product transfers and ownership changes, must be documented on the blockchain network.
- Access to and modification of product data on the blockchain network is restricted to authorized parties such as product makers and distributors.
- To confirm a product's validity, customers must be able to scan or input its unique identification number.
- On the blockchain network, any attempt to alter or tamper with product data must be found and stopped.
- In the event of any suspicious activity or product fraud, the system must immediately notify product makers and distributors.
- Product authentication and supply chain tracking laws and regulations must be adhered to by the system.
- Every product transaction and activity on the blockchain network must have a clear and verifiable audit trail provided by the system.
- Customers and product makers must be able to obtain product information and track supply chain data through the system's user-friendly interface.
- All product data and transaction privacy and security on the blockchain network must be guaranteed by the system

## 5. Other Requirements

### 5.1 Appendix A: Glossary



1. **Blockchain:** It is a shared, immutable ledger that facilitates the process of recording transactions and tracking assets in a business network. An *asset* can be tangible (a house, car, cash, land) or intangible (intellectual property, patents, copyrights, branding). Virtually anything of value can be tracked and traded on a blockchain network, reducing risk and cutting costs for all involved.

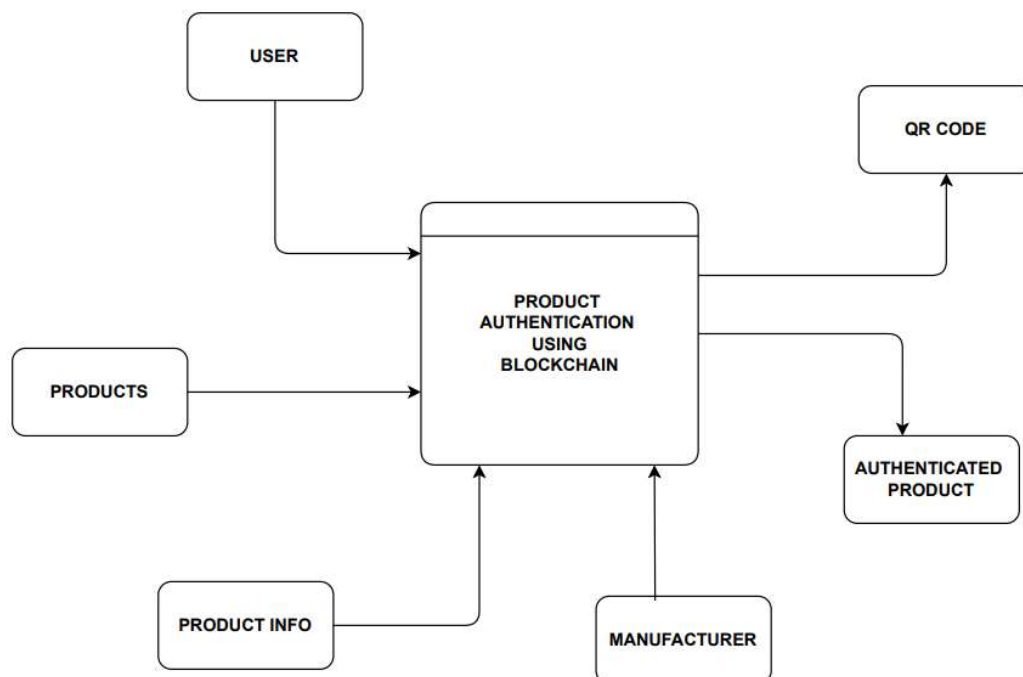
➤ Key elements of a blockchain

- **Distributed ledger technology**  
All network participants have access to the distributed ledger and its immutable record of transactions. With this shared ledger, transactions are recorded only once, eliminating the duplication of effort that's typical of traditional business networks.
  - **Immutable records**  
No participant can change or tamper with a transaction after it's been recorded in the shared ledger. If a transaction record includes an error, a new transaction must be added to reverse the error, and both transactions are then visible.
  - **Smart contracts**  
To speed transactions, a set of rules — called a smart contract — is stored on the blockchain and executed automatically.
2. **Ethereum:** Ethereum is a decentralized blockchain platform that establishes a peer-to-peer network that securely executes and verifies application code, called smart contracts. Smart contracts allow participants to transact with each other without a trusted central authority.
  3. **QR code:** A QR code (Quick Response code) is an array of black and white squares or pixels set in a grid that stores data for a machine to read. A smartphone or camera can quickly process the information contained in a QR code's specific arrangement of pixels, making it a convenient way to store and access data.

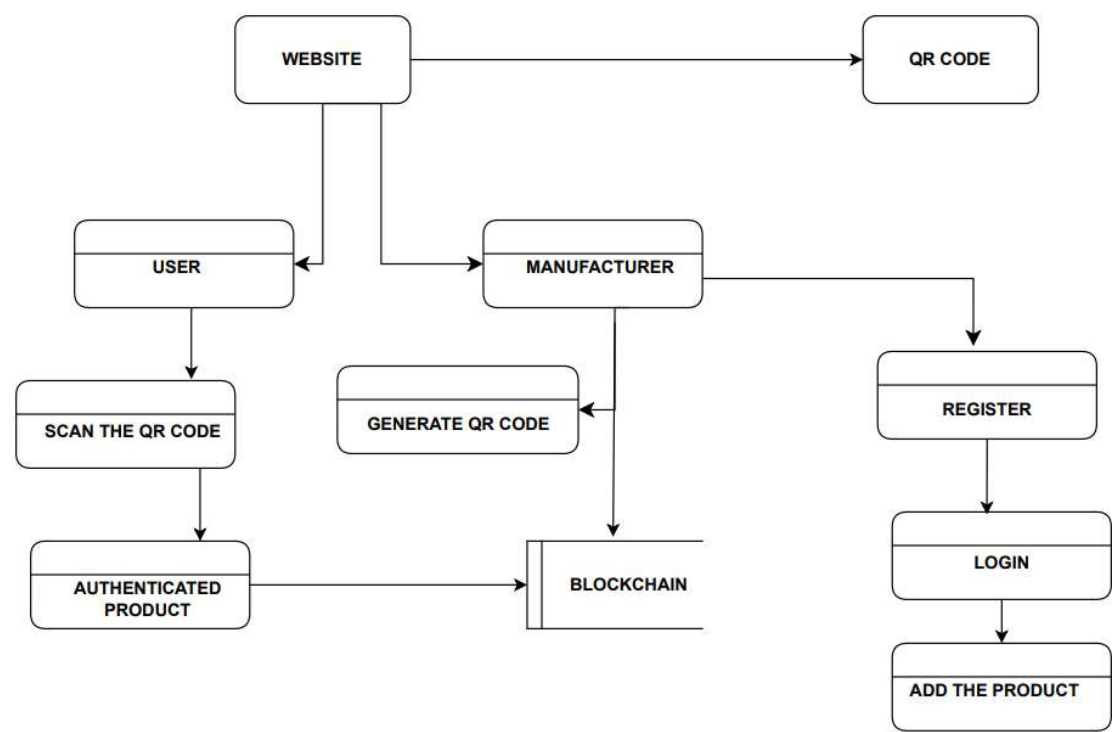
## 5.2 Appendix B: Diagrams

### 5.2.1 DATA FLOW DIAGRAMS

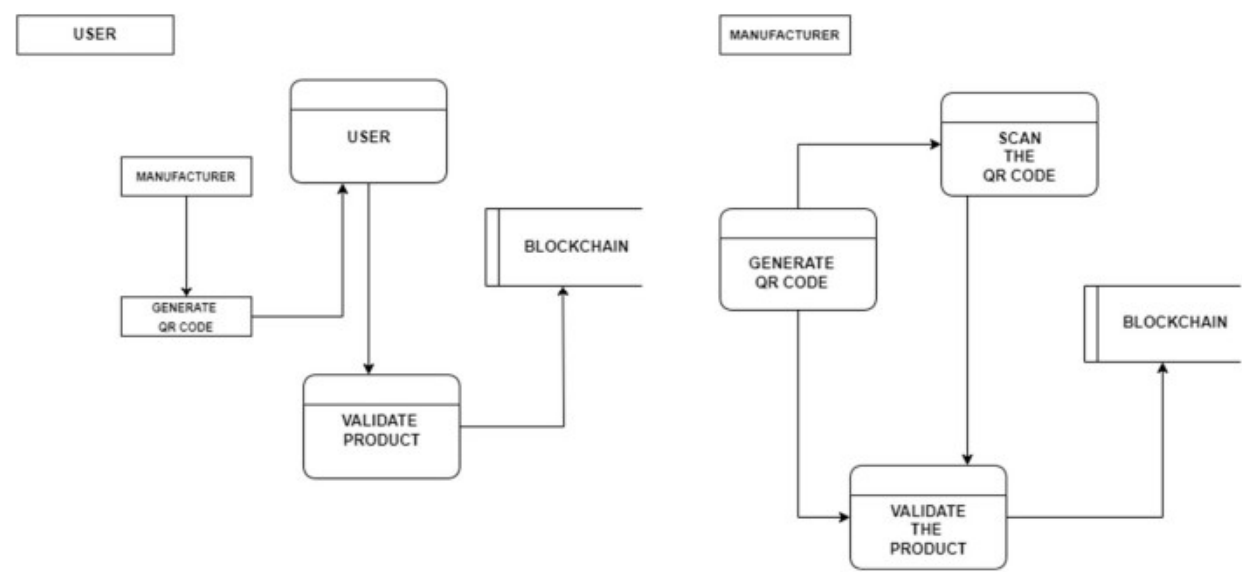
#### DFD LEVEL 0



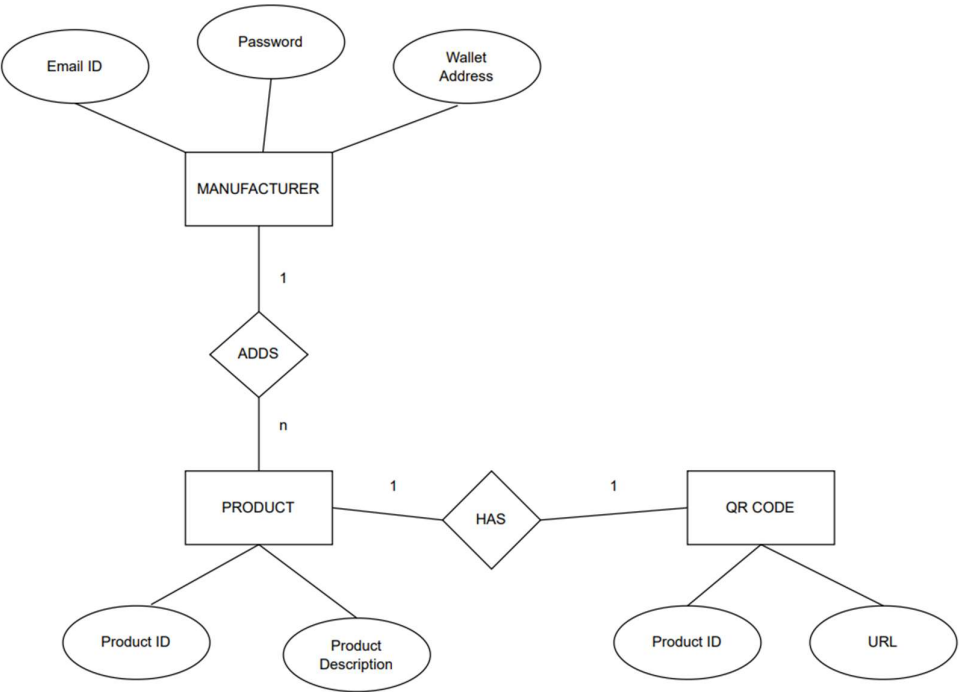
**DFD LEVEL 1**



**DFD LEVEL 2**



5.2.2 ENTITY- RELATIONSHIP DIAGRAM



5.2.3 Sequence Diagram

