TEST PLAN
FOR
PRODUCT AUTHENTICATION USING BLOCKCHAIN

Guide Name: Ms. Shivani

Team Members Name:

Abhishek Singh Yadav(2000290120011), CS-7A
Aditi Batra(2000290120012), CS-7A
Anurag Tripathi(2000290120036), CS-7A
Kshitij Pal(2000290310092), EC-7B

ChangeLog

Version	Change Date	By	Description
version number	Date of Change	Name of the person who made changes	Description of the changes made
1.0.1	25-10-2023	Aditi Batra	Added the QR download button
1.0.2	25-10-2023	Anurag Tripathi	Scanning feature for QR

1. Introduction

The "Product Authentication Using Blockchain" project is designed to provide a robust solution for product authentication, leveraging blockchain technology to ensure product genuineness and transparency. The project's core functionality involves user registration, product registration, product verification, and integration with the blockchain network. This introduction outlines the test strategies, processes, workflow, and methodologies employed to validate and ensure the project's functionality and security.

Test Strategies:

Our test strategies for the project revolve around an end-to-end approach that encompasses user registration, product addition to the blockchain, and product verification. We emphasize both manual and automated testing to guarantee the system's correctness, security, and usability. To simulate real-world scenarios, we rely on Ganache, a personal blockchain, to create a controlled testing environment. Moreover, we focus on end-user satisfaction, aiming for a seamless and secure user experience.

Test Process:

The test process for this project adopts a well-defined methodology. It starts with meticulous test planning, followed by the creation of comprehensive test cases. The execution of these cases ensures that every facet of the system operates in harmony. Collaborative defect tracking and resolution are essential aspects of the process, as it involve tight coordination between testers and developers. Additionally, iterative testing is integrated to accommodate system refinements and feature enhancements.

Testing Workflow:

Our testing workflow is systematically structured. It commences with a thorough review and validation of project requirements to establish the scope of testing. Test cases are meticulously designed in line with these requirements. During execution, automated testing tools are utilized for efficiency, while manual testing validates the end-user experience. Testing results are comprehensively documented and reported to project stakeholders.

Methodologies:

In the project, we embrace a blend of testing methodologies, tailored to address diverse aspects of the system:

- Functional Testing: Ensuring that all system functionalities, including user registration, product addition, and verification, work as intended.
- Security Testing: Assessing the system's robust security measures, focusing on user authentication and blockchain integration.
- User-Centric Testing: Evaluating the system's user-friendliness, providing an intuitive and secure interface for manufacturers and customers.

- Blockchain Integration Testing: Verifying seamless integration with Ganache, testing data storage, immutability, and secure transactions.
- Data Integrity Testing: Ensuring that product data stored on the blockchain is accurate, reliable, and tamper-resistant.

Our methodologies are geared towards revealing potential issues, validating user requirements, and aligning with project objectives. The combination of these strategies, processes, and methodologies guarantees that the "Product Authentication Using Blockchain" project functions seamlessly, ensuring the authenticity of products and user satisfaction.

1.1 Scope

1.1.1 In Scope

The testing in scope for the "Product Authentication Using Blockchain" project encompasses the features, functional requirements, and non-functional requirements of the software that will be systematically tested to ensure its reliability and effectiveness. The project scope extends to:

1. User Registration and Authentication:

   - Verification of secure user registration with unique usernames and passwords.

   - Testing the user login process to confirm that registered users can log in securely.

   - Validation of the integration with Metamask for secure user interactions.

2. Product Registration:

   - Testing the product registration process by authorized entities.

   - Verification of the accuracy and security of product registration.

   - Confirmation of Metamask integration for secure product addition to the blockchain.

3. Product Verification:

   - Validation of product verification by end-users.

   - Confirmation that product authenticity can be correctly verified through scanning QR codes.

   - Verification of the seamless interaction between customers and the blockchain for product status retrieval.

4. Blockchain Integration:

   - Testing the correct storage of data on the blockchain, including product information.

   - Verification of the blockchain's immutability and security.

   - Validation of Metamask pop-ups for transaction confirmations and secure data handling.

1.1.2 Out of Scope

The testing activities for the project have a defined scope, but it is equally important to clarify what is not included in the testing process. The following features, functional requirements, and non-functional aspects are out of scope for the testing phase:

1. Metamask Pop-up Behavior:
   - Detailed testing of Metamask itself, its functionalities, or any aspects unrelated to the integration with the system is out of scope. The focus is on confirming its interaction with the application but not testing Metamask's standalone features.
2. Blockchain Network:
   - Testing the underlying Ganache personal blockchain network, its security, or configurations is not within this project's scope. The focus is on the application's interaction with the blockchain, assuming a properly configured blockchain environment.
3. Performance Testing:
   - In-depth performance, load, or scalability testing is out of scope. This includes evaluating the system's response under heavy loads or the impact of concurrent user interactions.
4. Cross-Browser Testing:
   - Comprehensive cross-browser testing to validate the application's behavior on all web browsers is not within the scope. Testing will primarily focus on the system's performance in a specific browser environment.
5. Database and Blockchain Configuration:
   - Detailed testing of the database or blockchain configuration, maintenance, or setup is not part of the scope. The focus is on the application's interaction with these systems.

1.2 Quality Objective

The primary objective of our "Product Authentication Using Blockchain" testing project is to ensure that the application under test (AUT) aligns with its functional and non-functional requirements. In pursuit of this overarching goal, we have the following specific quality objectives:

1. Functional Requirement Conformance: Our testing aims to verify that the AUT conforms to all functional requirements defined in the project's scope. This includes ensuring that manufacturers can successfully register, log in, and add products to the blockchain and that customers can accurately verify product authenticity through QR code scanning or uploads.

2. Non-Functional Requirement Adherence: We intend to assess whether the AUT meets the specified non-functional requirements. This encompasses evaluating factors such as application security, user data protection, and the performance of the system in a controlled Ganache blockchain environment.

3. Quality Specifications: Our testing process seeks to ensure that the quality specifications defined by the client are met. This entails validating that the application operates seamlessly, offering a user-friendly experience, and upholding the integrity and security of the blockchain-based product authentication system.

4. Bugs and Issue Identification: One of our core objectives is to identify and address any bugs or issues before the system's go-live phase. We aim to conduct comprehensive testing to detect and report defects on time so that they can be rectified effectively.

By pursuing these quality objectives, we strive to deliver a robust and reliable product authentication system, ensuring that it aligns with client-defined requirements, industry standards, and user expectations. Ultimately, our goal is to enhance the application's quality, security, and overall performance.

1.3 Roles and Responsibilities

Detailed description of the Roles and responsibilities of different team members:

- Developers: Abhishek Singh Yadav and Anurag Tripathi (Blockchain), Aditi Batra (Frontend)
- Quality Analyst: Kshitij Pal

2 Test Methodology

2.1 Overview

AGILE MODEL
How the Agile model relates to your project:

1. Iterative and Incremental Development: Our project involves the development of a product authentication system that includes features like user registration, login, and product verification. The Agile model's iterative and incremental development approach allows you to build and enhance these features in small, manageable iterations. We can develop and release increments of the system with each iteration, ensuring that each increment is potentially shippable.
2. Flexibility and Adaptability: Agile is well-suited for projects with evolving requirements. Blockchain technology and user expectations may change over time. Agile's flexibility allows our team to adapt to these changes and implement new features or enhancements as needed. This is important in a project where technology and user needs are dynamic.
3. Regular Testing and Quality Assurance: Agile promotes continuous testing and quality assurance. Given the critical nature of product authentication and security in your project, regular testing and validation are essential. Agile enables our team to conduct testing throughout the development process, ensuring that each increment is thoroughly tested for quality and security.
4. Cross-functional collaboration: Our project involves multiple aspects, such as web development, blockchain integration, security, and user interface design. Agile encourages cross-functional collaboration among team members with diverse expertise. This collaborative approach ensures that all aspects of the project are addressed effectively.
5. Incremental Delivery: The Agile model promotes the delivery of functional increments at the end of each iteration. This aligns with our project's approach of gradually adding product authentication features. Manufacturers can start using the system as soon as the initial features are implemented, allowing for an early return on investment.

2.2 Test Levels

Considering the scope and functionality of the "Product Authentication Using Blockchain" project, we can define the following test levels:
1. Unit Testing:
- At this level, individual components and functions within the system will be tested in isolation.
- Specific functionalities, such as user registration, login, and product addition, will be tested for correctness.

- This level ensures that each part of the system works as intended.

2. Integration Testing:
   - Integration testing focuses on verifying the interactions between different system components.
   - It will ensure that the website, Metamask integration, and blockchain communication work seamlessly together.
   - Testing at this level validates the flow of data between various modules.
3. System Testing:
   - System testing evaluates the end-to-end functionality of the entire "Product Authentication" system.
   - This level will test the complete user journey, from registration and login to product addition and QR code scanning.
   - It ensures that the system as a whole meets the specified requirements.
4. Security Testing:
   - Given the importance of secure transactions and data integrity, security testing is crucial.
   - This level assesses the security measures in place, including user data protection, Metamask integration security, and blockchain data security.
   - Vulnerability assessments, penetration testing, and data encryption validation are performed.

3 Test Deliverables

3.1 Test Cases

- Test Case 1: User Registration

Test Case ID	Test Case Description	Test Steps	Expected Result	Pass/Fail
TC-1	Test user registration process	Go to the registration page.	User can access the registration page.	Pass
		Enter a valid username and password.	Username and password fields are accepted.	Pass
		Click the “Register” button.	Confirmation pop-up of metamask appears.	Pass
		Confirm the registration.	The user successfully registered.	Pass
TC-2	Test User registration with invalid credentials	Go to the registration page	User can access the registration page.	Pass
		Enter an invalid username and password.	Username and password fields are accepted.	Pass
		Click the “Register” button.	Confirmation pop-up of metamask appears.	Pass
		Cancel the registration.	The registration process is canceled.	Pass

- Test Case 2: User Login

Test Case ID	Test Case Description	Test Steps	Expected Result	Pass/Fail
TC-3	Test user login process	Go to the login page.	User can access the login page.	Pass
		Enter a valid username and password.	Username and password fields are accepted.	Pass
		Click the “Login” button.	Logged in successfully.	Pass
TC-4		Go to the login page.	User can access the login page.	Pass
		Enter an invalid username and password.	Username and password fields are accepted.	Pass
		Click the “Login” button.	Error message displayed.	Pass

- Test case 3: Product Registration

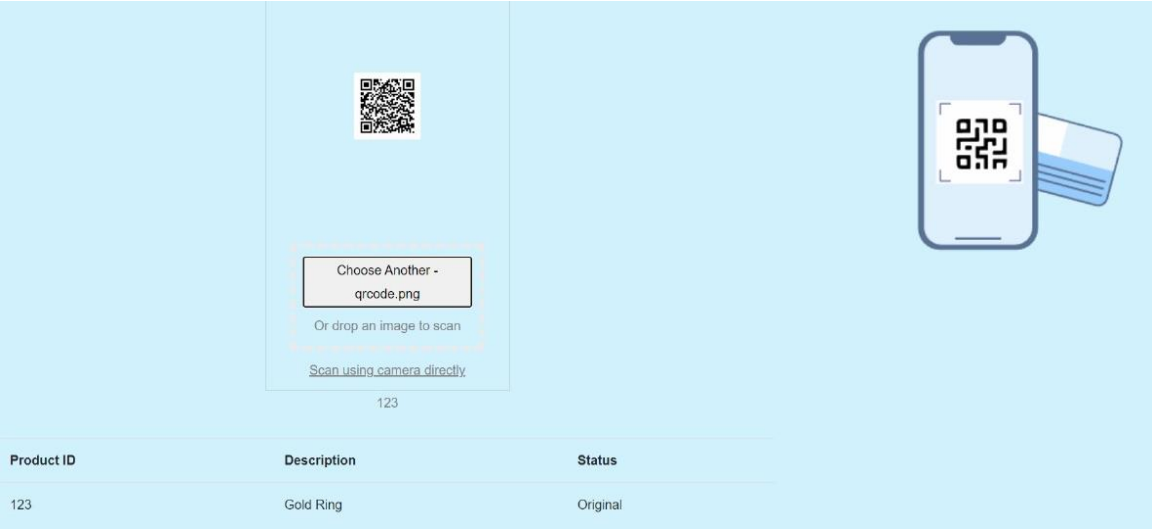
Test Case ID	Test Case Description	Test Steps	Expected Result	Pass/Fail
TC-5	Test product registration by manufacturer	Log in as a manufacturer.	Successful Login.	Pass
		Navigate to the product registration page.	Access to the registration page.	Pass
		Enter the unique product ID and Name.	Information accepted.	Pass
		Click the “Register Product” button.	Confirmation pop-up of metamask appears.	Pass
		Confirm the product registration.	The product is successfully registered on the blockchain.	Pass
TC-6	Test product registration with invalid credentials	Log in as a manufacturer.	Successful Login.	Pass
		Navigate to the product registration page.	Access to the registration page.	Pass
		Enter the unique product ID and Name.	Information accepted.	Pass
		Click the “Register Product” button	Confirmation pop-up of metamask appears.	Pass
		Confirm the product registration.	Error message.	Pass

- Test Case 4: Product Verification

Test Case ID	Test Case Description	Test Steps	Expected Result	Pass/Fail
TC-7	Test product verification by users	Go to the product verification page.	Access to the verification page.	Pass
		Upload the valid QR code.	Product ID accepted.	Pass
		Click the “verify” button.	The product’s authenticity verified.	Pass
TC-8	Test product Verification with an invalid product ID	Go to the product verification page.	Access to the verification page.	Pass
		Upload the invalid QR code.	Product ID accepted.	Pass
		Click the “verify” button.	Error message.	Pass

3.2 Requirement Traceability Matrix

Requirement ID	Requirement Description	Test Case ID(s)
REQ-1	User Registration	TC-1, TC-2
REQ-2	User Login	TC-3, TC-4
REQ-3	Product Registration	TC-5, TC-6
REQ-4	Product Verification	TC-7, TC-8

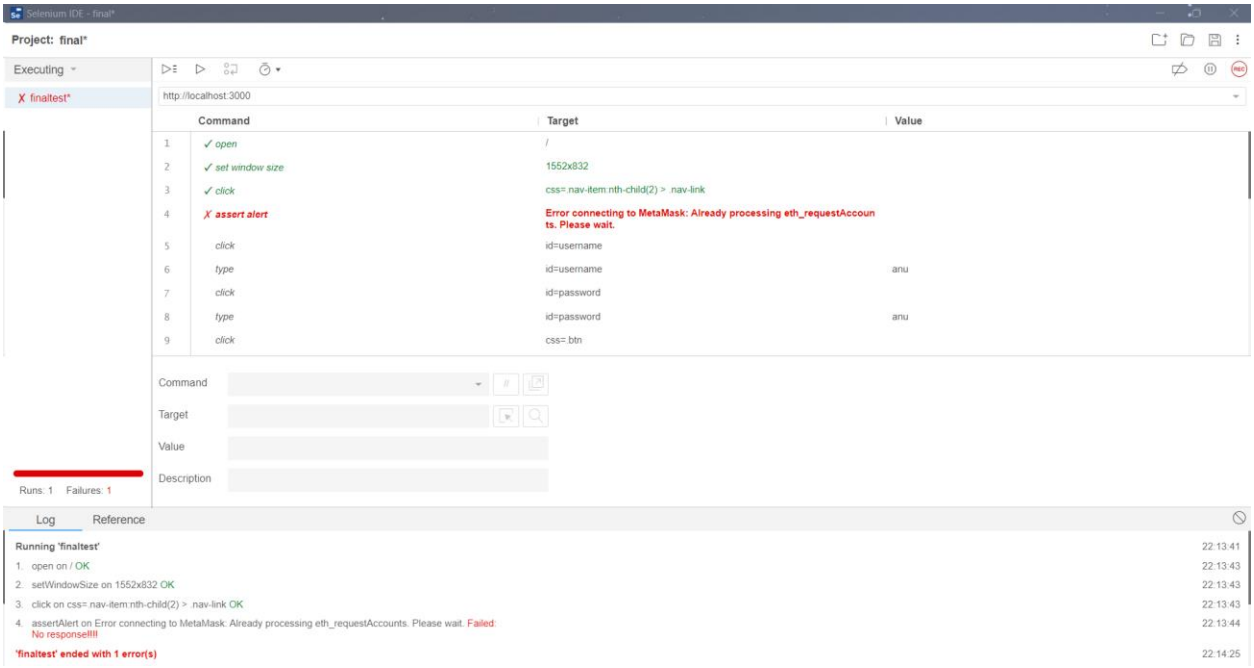


4 Resource & Environment Needs

4.1 Testing Tools

Required Testing Tools to test the project are as follows:

- Automation Tool: Selenium



4.2 Test Environment

- Operating System: Windows 10 (64-bit)
- Web Browsers: Google Chrome (latest version)
- Blockchain Environment: Ganache (for local blockchain simulation)
- Ethereum Wallet: MetaMask (for secure blockchain transactions)
- Development Server: XAMPP (for local web hosting)
- Testing Framework: Selenium (for automated testing)
- Version Control System: Git (latest version)
- Documentation: Microsoft Office Suite (for test plan and documentation)

5 Terms/Acronyms

TERM/ACRONYM	DEFINITION
API	Application Program Interface
AUT	Application Under Test
UAT	User Acceptance Testing