Bilkent University

Department of Computer Engineering

Senior Design Project

Project Name: VerifiChain

Project Specification Report

Tuna Öğüt - 21803492
Erengazi Mutlu - 21803676
Bartu Teber - 21703460
Ömer Onat Postacı - 21802349
Arda Güven Çiftçi - 21801763

Supervisor: Özgür Ulusoy
Jury Members: Erhan Dolak, Tağmaç Topal
Innovation Expert: Nazan Kurt

October 17, 2022

This report is submitted to the Department of Computer Engineering of Bilkent University in partial fulfillment of the requirements of the Senior Design Project course CS491/2.

Contents

1. Introduction

Producing and selling counterfeit products has drastically increased in recent decades. This increase has a significant impact on not only the consumers but also the manufacturers, suppliers, and distributors in terms of economic status, as well as the well-being of the consumers. Hereby, companies can face problems like damaged reputation, customer satisfaction, and trust, extra budgets allocated to prevent counterfeit products, and economic shrinkage caused by sales that are likely to decrease in the long term, whereas consumers can also face hardships such as health problems that may be caused by poor quality products, not getting value for money, and extra expenses that may be caused by poor quality and fake products in the long run [1]. Even though there exist QR code-based solutions to solve this problem by demonstrating the product information, such solutions can still be exploited by using different techniques such as copying the QR codes.

VerifiChain aims to minimize this problem by integrating blockchain and QR code technologies into the supply chain and manufacturing process of products to increase the traceability and reliability of product verification. The factor that distinguishes VerifiChain from other QR code-based solutions is to create an immutable transaction flow on the supply chain by connecting each product with an owner in accordance with the logic of blockchain technology. While performing this process, it is aimed to increase traceability by using QR code technology to distinguish each product from the others.

This paper will describe the application VerifiChain with the boundaries of the constraints. Also, the functional requirements of VerifiChain will be explained to understand more about the motivation behind the application and how it solves the mentioned problem by determining the non-functional requirements to provide a mapping of the priorities of VerifiChain.

1.1 Description

VerifiChain is a web application that uses blockchain and QR code technologies. It provides product verification for individuals wanting to verify the authenticity of the products that they want to buy or they already have. The verification system works as follows; The manufacturer of the product will create a QR code to the product. Then, at the end of the manufacturing period, each product will be linked to their unique QR code through the system. The linking will be made using blockchain technology. Main reasons for using blockchain

technology is the security features that it provides and the wallet system that is used. By wallet technology, users can claim the ownership of the product. When users buy a product, the product's digital credentials will be transferred to the user's wallet. Thus, whenever user scans the QR code of the product, he/she will see the owner of that specific product. Which will add another layer of security to the system. Until a product is first transferred to a supplier, user or distributor, the product will seem like it belongs to its manufacturer. When it is sold there will be a transaction through the blockchain technology and the product will be assigned to its new user until he/she sells it again. The users who want to sell or buy a product should use the system provided. By using the system buyers will assure that the product is not counterfeit. Also, users can guarantee that the product is not stolen since you can not sell a product that you do not own and that is not in your wallet through the blockchain technology. Thus, if someone is trying to sell a stolen or a fake product he/she will be exposed. If the product is stolen, since the product will be assigned to some other user's wallet so that it will come out that it is stolen. On the other hand, if the product is fake, the QRcode will not have the credentials that indicates its authenticity so that it will be understood that the product is fake. This feature will also decrease the risks of buying fake products from unofficial distributors. Customers can easily scan the QR codes on the products and verify their authenticity.

The system will provide an interface that allows users to only buy, sell, monitor and verify the authenticity while authorized firms and brands can generate unique QR codes and link them to specific products. Which will assure if there is a product on the system it was made by an authorized brand.

Therefore, VerifiChain aims to decrease the risks of buying and selling counterfeit or stolen products by providing methods that are more secure to buy and sell products by allowing users to see the owner and the authenticity of the products.

1.2 Constraints

1.2.1 Implementation Constraints

- While implementation phase of the application, GitHub and Git will be used to collaborate and version control.
- Node.js and Express.js framework will be used for REST API.
- Ethereum Chain will be used for main chain; therefore, Solidity will be used for Smart Contracts.

- React.js and Ethers framework (a Web3 Framework) will be used for client side of the application.
- For personal data storage, PostgreSQL will be used as database management system.

1.2.2 Security Constraints

- Generated and transferred QR codes and their transaction history information will be visible both in VerifiChain and Ethereum Chain which can be seen in EtherScan; therefore, transaction history will be immutable [2].

1.2.3 Technological Constraints

- Users must use Chromium-based web browsers to have the MetaMask Wallet application in their browsers to interact with Smart Contracts [3}.
- Therefore, users must download and create an account in MetaMask Wallet. It can be downloaded from the store of the related browser.

1.2.4 Language Constraints

- VerifiChain will be launched in English initially; however, new languages can be added to the system according to the demand of the users.

1.2.5 Economic Constraints

- Since the transaction of each product will be done using MetaMask wallet and Ethereum chain, there will be Gas fees to make a transaction for each product. However, VerifiChain aims to minimize the Gas fees in the Smart Contracts.

1.3 Professional and Ethical Issues

VerifiChain is an application to detect counterfeit products, the most significant issue is to provide transparent data for each product. During the development, sub-systems like MetaMask Wallet and Ethereum Chain will be used to create and interact with transaction data. Since blockchain technologies are adopted, data transparency will be ensured by the network.

In cases of theft and similar situations that may occur during the manufacturing phase, the exploit of the features of application by the criminals cannot be guaranteed, therefore the necessary contract will be presented to the users.

Since MetaMask is a third-party application that is being used in VerifiChain, some vulnerabilities come with it such as anonymous links that are sent from malicious people. Unfortunately, this is a problem that comes from the nature of using "Hot Wallet" [4]. However, VerifiChain will provide the necessary information for its users to minimize the occurrence of such cases.

2. Requirements

2.1 Functional Requirements

VerifiChain is planned to meet the following functionalities:,

2.1.1 QR Code Execution and Product Matching

In VerifiChain, all products will be associated with a single, unique QR code. For reliability and traceability reasons, the access to generate a unique QR code and to match the QR code with a product is given to the manufacturer. Authorizing just the manufacturer to generate a QR code increases the reliability and traceability of VerifiChain since:

- Manufacturer is the most reliable stakeholder to generate a QR code since it is directly related to the brand. Suppliers and distributors may manipulate the authorization of generating QR codes.
- Generating QR codes at the first step of the supply chain increases the traceability of VerifiChain since a supply chain of the product from the manufacturer to a distributor is fully traceable.

2.1.2 Product Transfer and Displaying Transaction History

The products in VerifiChain will be transferred via their QR code. The transactions will execute in the blockchain. The possession of the QR code will be transferred from one user to another user. Using blockchain increases the reliability and traceability of transactions. Every node in the blockchain will be able to see the full transaction history of the product and the history is unalterable. For example, the manufacturer will transfer all products to the supplier and the

supplier will transfer all products to the distributor. If the products are not sold in the season, the distributor will transfer these products to the outlet store. Therefore, when a customer goes to an outlet store and scans the QR code, the customer will be able to see the full transaction history of the product along with if the product was really on the market the previous season even with the information in which store it was on market. Moreover, VerifiChain will allow users to sell products peer to peer on second hand along with a high assurance of originality. However, the main vision of VerifiChain is to make the supply chain of products reliable and traceable rather than handling second-hand product selling. Therefore, the features of second-hand product selling will be limited and basic on delivery but it will be possible in the future to scale the features of second-hand product selling.

2.1.3 Wallet Integration and Displaying All Products

A MetaMask wallet will be integrated with VerifiChain. The stakeholders in the supply chain will be able to list all the products they have and how many of them they have. Moreover, a customer will also be able to see which products they purchase. The QR code of every product will also be available on the product list.

2.1.4 Fake Product Report

In doubtful circumstances, every user regardless of having the product can report the product that can be fake. For example, let someone enter a shop and scan the QR code of a product. Then, he/she sees that the product is supposed to be in another shop in the transaction history. In this doubtful circumstance, if he/she reports the product, that product will be labeled as suspicious and will be investigated.

2.1.5 User Reviews

VerifiChain gives value to the opinion of its customers and uses their feedback for improvement and bug tracking. For this purpose, VerifiChain periodically gets reviews and feedback from users. For example, once a month after the subscription, a pop-up requesting user feedback appears on the window.

2.2 Non-Functional Requirements

2.2.1 Accessibility

- Since as a third-party application MetaMask Wallet will be used, the web browser that VerifiChain is running on must be able to support the requirements of MetaMask Wallet. Therefore, Chromium-based web browsers such as Google Chrome and Brave could be used as well as Mozilla Firefox because such web browsers are integrated with MetaMask Wallet [3].
- React.js will be used for the front-end development of VerifiChain.
- Node.js will be used for the back-end development of VerifiChain.

2.2.2 Availability

- VerifiChain will be operable in any location with an internet connection.
- Operations in software systems of VerifiChain will be done during periods of least intensity of use to make the application optimally available for the users.

2.2.3 Backup and Recovery

- VerifiChain will use Ethereum Chain for the main chain to store transaction history for each product; therefore, Ethereum Chain undertakes backup and recovery of the transaction history data for each product.
- MetaMask Wallet has its own recovery procedure for each user [5].
- The database of the VerifiChain is PostgreSQL; therefore, the backup and recovery is undertaken by the database service of VerifiChain. Personal Data will be stored in both global and local storage systems to prevent data loss.

2.2.4 Extensibility

- VerifiChain must be open to developments for adopting new features with new functionalities such as second-hand exchange.
- Other blockchains such as the Solana chain, can be integrated along with Ethereum.

2.2.5 Data Integrity

- Since the system will use Ethereum Chain to store transfer and transaction data for each product, the maintenance and the assurance of the data accuracy is undertaken by Ethereum Chain and be visible in EtherScan [2].

2.2.6 Security

- There are mandatory private credentials for the users to be signed up, connect their wallets, and make a transaction.
- Since VerifiChain uses blockchain technologies, the data storage system will be decentralized in terms of wallet information. Therefore, a more secure system is provided compared to a centralized data storage system.

2.2.7 Exception Handling

- If any error occurs during the execution of the program, users will be informed in regards to what is the error, why the error occurs, and how to solve such error. Hereby, users will be guided to handle the exceptions during a flow of actions.

2.2.8 Usability

- The GUI of the VerifiChain will be clear and user-friendly to direct the users to take accurate actions.
- Users will be able to score determined parameters, and convey their thoughts via a feedback system.

2.2.9 Maintainability

- Integrated sub-systems will work in a harmony to provide functionality as complementary factors; therefore, the maintenance of VerifiChain can be ensured.
- Since each sub-system will serve for a goal, new sub-systems can be added to the cumulative system and maintained easily.

2.2.10 Transparency

- VerifiChain is a web3 based application. Transactions are kept under Ethereum network. Therefore, all of the product's transaction history will be visible in both VerifiChain and EtherScan in which all transactions on Ethereum chain are visible [2].

2.2.11 Legal and Regulatory Requirements

- A contract signed by the users will prevent exploiting the application for their own benefit.

2.2.12 Integrability

- VerifiChain uses a third-party application, which is MetaMask Wallet, to integrate users to Ethereum blockchain.
- Ethereum Chain will be used as an integrated blockchain to store data and interact with MetaMask Wallet.
- Such sub-systems will be bringed together into the system of VerifiChain.

2.2.13 Response Time

- Since VerifiChain uses Ethereum blockchain, Ethereum's transactions per second will apply to all the transactions. Therefore, tps relies on Ethereum's tps speed.

3. References

[1] “What are the biggest impacts of counterfeits on brands?,” *Red Points*, 08-Jun-2022. [Online]. Available: https://www.redpoints.com/blog/what-are-the-biggest-impacts-of-counterfeits-on-brands/. [Accessed: 16-Oct-2022].

[2] “Ethereum (ETH) Blockchain Explorer.” [Online]. Available: https://etherscan.io/. [Accessed: 16-Oct-2022].

[3] D. P. Matt Hussey, “What is metamask? how to use the top Ethereum Wallet,” *Decrypt*, 04-Jun-2022. [Online]. Available: https://decrypt.co/resources/metamask. [Accessed: 16-Oct-2022].

[4] F. G., “What is a WEB3 wallet? ,” *Online IT Bootcamp; Learn Coding, Data Science, AWS, DevOps, Cyber Security & Salesforce*, 15-Aug-2022. [Online]. Available: https://clarusway.com/what-is-a-web3-wallet/. [Accessed: 16-Oct-2022].

[5] “What is a ‘secret recovery phrase’ and how to keep your crypto wallet ...” [Online]. Available: https://metamask.zendesk.com/hc/en-us/articles/360060826432-What-is-a-Secret-Recovery-Phrase-and-how-to-keep-your-crypto-wallet-secure. [Accessed: 16-Oct-2022].