SECURE COUNTERFEIT PRODUCT DETECTION SYSTEM USING BLOCKCHAIN

Pranav Gupta, Aditya Kesarwani, Divyanshu Tiwari
Supervisor: Dr. Sangeeta Mittal
Department Of Computer Science Engineering & Information Technology
Jaypee Institute of Information Technology

INTRODUCTION

Counterfeiting is the act of producing fake or imitation goods or currency with the intent to deceive or defraud. Counterfeiting is a significant issue that affects various industries, including fashion, electronics, pharmaceuticals, and even currency. In the current environment, detecting counterfeiting is crucial for a number of reasons:

1) **Consumer protection:** counterfeit products are often of lower quality, and using them can have serious negative effects, including health hazards and financial loss.
2) **Brand protection:** Losses in revenue, market share, and consumer loyalty may result from counterfeiting.
3) **Revenue protection:** Both businesses and governments lose money as a result of counterfeiting, when their items are imitated since counterfeiters don't pay taxes.

EXISTING APPROACHES

1) **Physical Verification:** It involves applying a unique holographic label on the product to visually indicate its authenticity. It includes overt features like texture, density and refraction and covert features read by Engage TM App.
2) **Centralised Databases:** Used by companies but suffer issues like the event of central server failure or comparatively slow searching complexity and the possibility of attacks on integrity and availability.
3) **Artificial Intelligence:** used to analyze data and detect patterns that may indicate counterfeit products. But, it needs a dataset prior to training which might not be available for new releases.

PROBLEM STATEMENT

To make a decentralized counterfeit product detection system and a tamper-proof data storage system to store product details and get the consumers to verify the same. The primary objective of this problem statement is to detect if a malicious/ unauthenticated user is selling the product. And, if an invalid/ ineligible user is detected, then the registration/transaction must be blocked by the contract itself. Only Authenticated users can perform Authorised actions.

IMPLEMENTATION

Ethereum-based blockchain was used to implement the solution as It has migrated to the Proof of Stake(POS) from the Proof of Work(PoW) because it is more secure, less energy-intensive, and better for implementing new scaling solutions compared to the previous PoW architecture. Here are the main functionalities.

1. addProduct() and addSeller(): These functions make use of the security provided by the "require" keyword. This leaves a scope of penalty even when the transaction for a user fails. Even if the registered user tries to add a product that has already been registered, the transaction would again fail leading to recurring gas fees. Product and seller can be added by manufacturer.
2. MfrSellProduct(), sellerSellProduct(): The relevant products are sold to the seller and then to the manufacturer.
3. verifyProduct(): This function checks whether the product whose Serial no. is scanned is sold to the same consumer verifying the product or not. Then based on the output of the above decision is made about if the product is authentic.

Below is the Use case Diagram and screenshot from the verification page of the application:

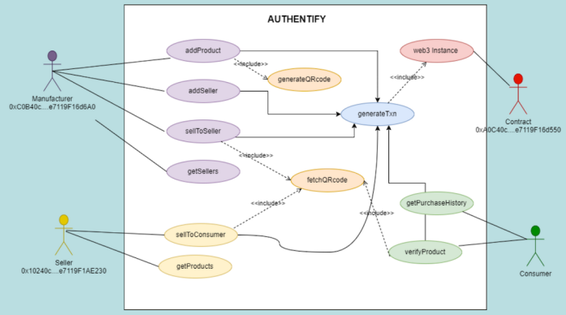
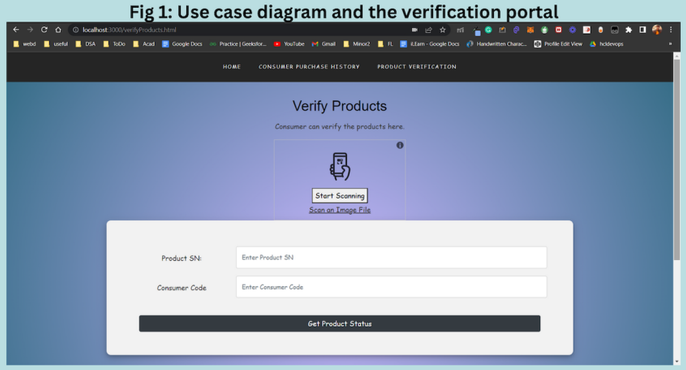


Fig 1: Use case diagram and the verification portal



CHALLENGES

1) Complexity of Blockchain Technology: The use of blockchain technology in the project introduced complexities that were not present in traditional software development projects.
2) Integration with Existing Systems: The project required the integration of the system with existing product authentication and counterfeit detection systems.
3) Security: The project involved the storage of sensitive information on the blockchain, which required careful consideration and implementation of security measures to prevent unauthorized access and tampering.

FUTURE SCOPE

1) Scalability: Apart from the scalability provided by distributed ledger technology and load balancing and scaling, we can implement other scalability techniques.
2) Complex Architecture: Currently we are considering a two level architecture i.e. manufacturer to seller and seller to consumer. Real life scenarios could consist of more levels and more complexity.
3) Mobile Application: The legitimacy of the product can be verified with much ease just by a few taps on the mobile application.
4) Expansion to Other Industries: The system's current field of use can be expanded to other industries.

REFERENCES

[1] Guo, Fangfang, Deqing Ma, Jinsong Hu, and Lu Zhang. "Optimized combination of e-commerce platform sales model and blockchain anti-counterfeit traceability service strategy." IEEE Access 9 (2021): 138082-138105.
[2] Hassija, Vikas, Vinay Chamola, Vatsal Gupta, Sarthak Jain, and Nadra Guizani. "A survey on supply chain security: Application areas, security threats, and solution architectures." IEEE Internet of Things Journal 8, no. 8 (2020): 6222-6246.