**KATHFORD INTERNATIONAL COLLEGE OF**

**ENGINEERING AND MANAGEMENT**

Balkumari, Lalitpur

A

Major Project Proposal

On

**“FAKE PRODUCT IDENTIFICATION USING QR CODE BASED BLOCKCHAIN SYSTEM”**

[Subject Code: EX707]

**Project Members**

Bharat Karki (003/BEX/2074)

Niranjan Tamang (007/BEX/2074)

Sagar Shrestha (011/BEX/2074)

**DEPARTMENT OF COMPUTER AND ELECTRONICS &**

**COMMUNICATION ENGINEERING**

**LALITPUR, NEPAL**

**AUGUST 2021**

Abstract

A counterfeit product results in huge loss to company. In Nepal, a lot of counterfeit is found in market. As a result of counterfeit product, it not only makes customer dissatisfaction but also a loss to retailer. A lot of solution to these problems has been addressed using various techniques. And most of solution is based on centralized system where information about products is stored in central server. In such centralized system, there are lots of problems such as a single point of failure, prone to attacks. Using the Blockchain, data is distributed over the peer-to-peer network instead of central server handling the all the data. In Blockchain, data is shared among the nodes in network. In our system, information about the product is stored in distributed ledger. So, any one on the network can watch the data. By scanning QR codes attach to product, a customer can query about the product that he is buying and check whether the product is genuine or not. After deciding to buy the product, customer needs to send a request to transfer the ownership of product to him/her. The main aim of this project to make decentralized application i.e. Dapps using the Ethereum framework using solidity programming language for writing the smart contract.

QR code that is to be attached to the product is generated using the serial no. of the products, time of manufacture, manufacturer name. After the product has been manufactured and ready for shipments, information about the product is added to distributed ledger. A customer can scan QR code and query the system whether the product is genuine or fake. If someone has attached QR code to product which is fake, then it will be easily identify using our system.

**Keywords:** Blockchain, Ethereum, Smart contracts, anti-counterfeiting, decentralization

Table of Contents

[Abstract i](#_Toc78739903)

[List of Figures iv](#_Toc78739904)

[List of Tables v](#_Toc78739905)

[List of Abbreviations vi](#_Toc78739906)

[1. Introduction 1](#_Toc78739907)

[1.1 Background 1](#_Toc78739908)

[1.2 Problem Statement 1](#_Toc78739909)

[1.3 Objectives 2](#_Toc78739910)

[1.3.1 Main Objective 2](#_Toc78739911)

[1.3.2 Specific Objectives 2](#_Toc78739912)

[2. Literature Review 3](#_Toc78739913)

[3. Feasibility Study 7](#_Toc78739914)

[3.1 Technical Feasibility 7](#_Toc78739915)

[3.2 Financial Feasibility 7](#_Toc78739916)

[3.3 Schedule Feasibility 7](#_Toc78739917)

[3.4 Operational Feasibility 8](#_Toc78739918)

[4. Project Methodology 9](#_Toc78739919)

[4.1 Block Diagram 9](#_Toc78739920)

[4.2 Flow Chart 10](#_Toc78739921)

[5. Implementation Plan 15](#_Toc78739922)

[5.1 Schedule 15](#_Toc78739923)

[5.2 Hardware and Software Requirements 16](#_Toc78739924)

[5.2.1 Hardware Requirements 16](#_Toc78739925)

[5.2.2 Software Requirement 16](#_Toc78739926)

[6. Expected Outcomes 17](#_Toc78739927)

[References 18](#_Toc78739928)

# List of Figures

Figure 4‑1 Block Diagram 9

Figure 4‑2 Flowchart of seller sign data 10

Figure 4‑3 Flowchart of verifying the seller's identity 11

Figure 4‑4 Flowhart customer signed data 12

Figure 4‑5 Flowchart of Manufacturer verifying the customer address 12

Figure 4‑6 Flow Chart of overall system 13

List of Tables

Table 5.1 Gantt Chart 15

List of Abbreviations

Dapps Decentralized Application

IPFS Inter Planetary File System

DSA Digital Signature Algorithm

ECC Elliptic Curve Cryptography

QR code Quick Response Code

# Introduction

## Background

In context of Nepal, lots of fake product of renowned company is found in market. Because of this it causes a lot of renowned company a huge loss and also breaks trust about the product for a customer. Individual customer also gets in loss because they get the fake product not the genuine one. Also, retailer who is selling a genuine product may have to compete with the retailer who is selling a Counterfeiting product. As a result, retailer who is selling a genuine product may result to his/her business loss. In order to resolve these problems, one popular technology that can be used is Blockchain. One of the renowned Blockchain applications is Bit coin crypto currency. Blockchain is simply a chain of blocks connected together with hash value. If any of data gets changed in one block, whole of the block following that blocks gets wrong. Any application built using Blockchain technology ensures that contents in data are tamper-proof.

The main goal of our project is to make a decentralized Blockchain system to keep the record of information of manufactured product such as ownership of the product, model number, Date of Manufacture and so on. At the customer side, we tends to use the QR code scanner to get the information about product and check whether or not the product is genuine or not which indeed help the customer decide to buy the given product or not.

## Problem Statement

Many fake products have been generated in existing supply chain in Nepal. In order to resolve these problems, there must be a system for end user to check details about the product and determine whether to buy the product or not by checking whether the product is genuine or not. In past, the information about the products is stored in centralized manner. So, hacker can attack on the just a single system and cause the whole system to fail i.e. cause single point of failure. Due to this single point of failure, we fail to track the information about the products. In some of case, QR code is being used but the information about the products is stored in centralized database which is not so good because bad people can attack such system easily than the decentralized system. So, our main aim is to build the decentralized blockchain system for sharing the information about the product for product anti-counterfeiting. In such a system, it is impossible for attacker to change information about the products and get their fake products in the market.

## Objectives

### Main Objective

* To design and develop a decentralized Blockchain system for fake product identification using QR code.

### Specific Objectives

1. To make a smart contracts using solidity programming language
2. Design and develop Dapps
3. To make a Blockchain with each block containing necessary data.
4. To generate QR code for a product

# Literature Review

Satoshi Nakamoto (Nakamoto, 2008) explained that a purely peer-to-peer version of electronic cash would allow online payments to be sent directly from one party to another without going through a financial institution. Digital signatures provide part of the solution, but the main benefits are lost if a trusted third party is still required to prevent double-spending. He proposes a solution to the double-spending problem using a peer-to-peer network. The network timestamps transactions by hashing them into an ongoing chain of hash-based proof-of-work, forming a record that cannot be changed without redoing the proof-of-work.

A. Funde (A. Funde, 2019) described about how IPFS(Inter Planetary File System) which is Distributed Web can be used to manage the ownership of products. IPFS is more useful than http as it can distribute huge volume of data efficiently and IPFS doesn’t allow duplication. IPFS and the Blockchain are similar. You can address large amounts of data with IPFS, and place the immutable, permanent IPFS links into a blockchain transaction. This timestamps and secures your content, without having to put the data itself on the chain.

Product anti-counterfeiting solutions are developed and implemented with centralized system architecture relying on centralized authorities or any form of intermediaries. Vulnerabilities of centralized product anti-counterfeiting solutions could possibly lead to system failure or susceptibility of malicious modifications performed on product records or various potential attacks to the system components by dishonest participant nodes traversing along the supply chain (Yiu, 2021).

J. Leng introduces about new decentralized blockchain-driven model, named Makerchain, is presented to handle the cyber-credit of social manufacturing among various makers. An anti-counterfeiting method composed of chemical signature is proposed to represent unique features of personalized products. Twinning unique signature data to blockchain and other functional databases is realized and anticipated to make manufacturing service transactions among makers more trustworthy. Based on an automated execution mechanism of smart contracts among makers, a decentralized manufacturing network can be enabled for automating transactions among makers, as well as third-party verification of product lifecycle through a trail of historic events (J. Leng, 2019).

Blockchain paradigm when coupled with cryptographically-secured transaction has demonstrated its utility through a number of projects with Bit coin being one of the most notable ones. Ethereum implements this paradigm in generalized manner. Furthermore, it provides a plurality of such resources each with distinct state and operating code but able to interact through a message-passing framework with others (WOOD, 2021). The algorithm that makes Blockchain system secure is hash algorithm.

Current anti-counterfeiting supply chains rely on a centralized authority to combat counterfeit products. This architecture results in issues such as single point processing, storage, and fail-ure. Blockchain technology has emerged to provide a promising solution for such issues. N. Alzahrani (Kamat)proposed the block-supply chain, a new decentralized supply chain that detects counterfeiting attacks using blockchain and Near Field Communication (NFC) technologies. Block-supply chain replaces the centralized supply chain design and utilizes a new proposed consensus protocol that is, unlike existing protocols, fully decentralized and balances between efficiency and security.

Although there has been many related studies focusing on supply chain quality management, the technologies used still have difficulties in resolving problems arising from the lack of trust in supply chains. The root reason lies in three challenges brought to the traditional centralized trust mechanism: self-interests of supply chain members, information asymmetry in production processes, costs and limitations of quality inspections. Si Chen and his team (Si Chen, 2017) discussed how to improve the supply chain quality management by adopting the blockchain technology, and propose a framework for blockchain-based supply chain quality management.

QR i.e. “Quick Response” code is a 2D matrix code that is designed by keeping two points under consideration, i.e. it must store large amount of data as compared to 1D barcodes and it must be decoded at high speed using any handheld device like phones. QR code provides high data storage capacity, fast scanning, omnidirectional readability, and many other advantages including, error-correction (so that damaged code can also be read successfully) and different type of versions. Different varieties of QR code symbols like logo QR code, encrypted QR code, iQR Code are also available so that user can choose among them according to their need. QR code is applied in different application streams related to marketing, security, academics etc. (Tiwari, 2016).

Smart contract are self-executing contracts with the terms of agreement between interested parties. The contracts are written in form of program codes that exist across a distributed, decentralized blockchain network. Smart contract allow transaction to be carried out between untrusted parties without the need of central authority. Early work on the smart contract has been done by Szabo and Miller. Blockchain technology represented by bit coin and other crypto currencies is called a blockchain 1.0 which is temper-resistant, decentralization (S. Wang, 2018). However, writing a complex logic is not possible due to the limitations of the Bit coin scripting language which has only 256 instructions set. So, bit coin is considered as prototype of smart contracts. Recent blockchain platforms such as Ethereum introduce the idea of running user-defined programs on the blockchain. The codes of Ethereum smart contract are written in stack-based byte code language and executed in Ethereum Virtual Machine. Ethereum is currently the most popular platform for developing smart contracts, so called as Blockchain 2.0. Smart contract are more like an autonomous agents that live inside the EVM, always executing a specific piece of code when called by message or transaction, and having a direct control over their own ether balance. The term transaction is used in Ethereum to refer to signed data package that stores a message to be sent from an externally owned account

The main intent of Ethereum is to create an alternative protocol for building decentralized application. While building such decentralized system, it has two types of account: externally owned accounts, controlled by private keys and contract accounts, controlled their contract code. An externally owned account has no code, and can send messages from an externally owned account by creating and signing a transaction; in contract account, every time the contract account receives a message its code activates, allowing it to read and write to internal storage and send other messages or create contract in turn. Externally owned account address is calculated as:

Externally owned account address = SHA3 (public key)

Also, note that contract address is calculated as:

Contract address = SHA3 (EOA + nonce)

The number of bits outputted by the SHA3 hashing algorithm is of fixed sized 256 bit number. Hash algorithm is one of most important algorithm that plays a significant role in the blockchain network because it helps to maintain the integrity. For example, if you change the only 1 bit of information to input to hash algorithm, then whole hash value becomes total different than the previous one. Due to this important feature, Blockchain system cannot be tampered with. Since, blockchain is nothing but the decentralized database in the peer to peer to network consisting of chain of blocks. A single block is made of multiple transactions. If any changes is made in past block, the whole forward blocks needs to compute the hash value so as to make the chain valid. Here, way to generate the public and private key in Ethereum blockchain is by using ECC (elliptical curve cryptography) algorithm other than RSA algorithm because key generated using ECC algorithm is much more secure than the key generated by the RSA algorithm. The main intent of public private key cryptography is to make the communication system between two parties much more secure. One of key properties of the public private key cryptography is that one cannot generate the private key given the public key. In other words only public key can be generated from private key but the vice versa is almost impossible for today’s computing system. It is much more like a trap door function that is, given private key you can generate the public key. But once you get the public key, you cannot generate private key. How the encryption and decryption is done is given as:

Encrypted message = Encryption(private\_key, message)

message= Decryption(public\_key, Encrypted message)

Once the message is encrypted using the private key it can only be decrypted using the public key or vice versa. In the most of Blockchain system, this concept of public private key cryptography is used for validation of transaction in the blockchain. In simple way, the concept of digital signature plays a huge role in making blockchain system in storing and transferring of information in system (Buterin, 2015).

# Feasibility Study

## Technical Feasibility

All the technical resources required for the project including hardware and software are easily available in the market. Also, most of the equipment that is required for the project is there. And there must not be a problem for us to get those things that are required for the project. Evaluating the technical feasibility is the most intricate part of the feasibility study. Here, as we will be making a smart contract or decentralized application using solidity programming language on Ethereum. We will change their smart contract Solidity code into Ethereum byte code, add the byte code into a transaction and deploy the transaction into the network. When miners of Ethereum receive the transaction, they will record the transaction in a block and run the byte code in the Ethereum virtual machine each time a transaction of this smart contract is called. Since our project require resources that are easily available, so our projects is technical feasible.

## Financial Feasibility

The project we are going to work on is economically feasible and is within the range of affordable expenditure as most of the equipment and electronic devices are already available. Once the system setup is done and it starts functioning as it is supposed to, then all the expenses that are made during the project would look worth it. A simple financial analysis which gives the actual comparison of costs and benefits are much more meaningful in every project. This gives the top management economic justification for the new system. Since we do have to use mobile with internet connection with camera able to scan QR code in our project so, the total cost for our project is very low which makes it financially feasible and easy to complete within deadline.

## Schedule Feasibility

The project is currently in the analysis and requirement gathering phase. So, in 9 months, the project is expected to be completed within the proposed schedule.

## Operational Feasibility

Our final project will need the computer and mobile with internet connection to utilize it.

# Project Methodology

## Block Diagram

Block 1

Smart contract

Block 3

Block n

User Interface

Admin

Manufactured Product

Details

Block 2

User

**Figure 4‑1 Block Diagram**

Admin, who is manufacturer, keeps the record of the product such as time at which the product is manufactured, current ownership of product, product name in the blockchain server. As the blockchain system is immutable, not tampered with and is secure in the sense that if any of past transaction data is changed by some bad parties in his blockchain and tries to make his blockchain domain in the network. Then, his blockchain is rejected by network because he needs to follows the rules written in smart contract in code. If he doesn’t follow the rules and business logic written in the smart contract then his transaction will become invalid or in other words blockchain network will not validate his transactions.

After the information about product has been added to network then, customer will scan the QR code attached to product and make a query to blockchain server whether the product is real or not. If customer wants to buy a product then he/she will ask for manufacturer to transfer the ownership of the product to him

## Flow Chart

Verified Data

Uint8 v

Byte32 r

Byte32 s

Customer message

Current Date (UTC)

Hash value

Signed Hash

Seller sign

SHA3

**Figure 4‑2 Flowchart of seller sign data**

Seller mismatch

Seller match

Hash value

Smart Contract

Input

v, r, s

Seller address

Customer message

Current Date

**Figure 4‑3 Flowchart of verifying the seller's identity**

In order for customer to make sure that seller is the one who he claims to be. For this case, seller will send the signed hash of the customer message and current date. In other words, it uses the concept of digital signature. Signed Hash value can be decomposed into v, r, and s. Now, consumer will acquire necessary information then call our system for verification of whether the seller identity is correct one. Customer will only need to send v, r, s, time, the message the customer asked seller to encrypt.

Verified Data

Uint8 v

Byte32 r

Byte32 s

Seller Address

Recipient

Mail address

Phone number

Hash value

Signed Hash

Customer sign

SHA3

**Figure 4‑4 Flowchart customer signed data**

Customer mismatch

Customer match

Hash value

Smart Contract

Input

v, r, s

Seller address

Customer Address

Recipient

Mail Address

Phone number

**Figure 4‑5 Flowchart of Manufacturer verifying the customer address**

After verifying the seller, then customers need to ask for manufacturer for transfer the ownership of the product. For this, customer needs to send the seller address, recipient name of the product, phone number of the recipient. Along with this information, customer need to send the digital signature associated with given information. The manufacturer will use our system to verify that encrypted message from valid customer or not. The manufacturer will use our system whether the customer is one who he claims to be.

No

Scan QR code

Information about product

Transfer the ownership of Product

Real

Fake

Is information there in Blockchain?

Yes

**Figure 4‑6 Flow Chart of overview of proposed system**

First things first, while verifying whether the product he/she is going to buy, customer needs to make sure the sellers is one who he/she claims to be. After verifying seller, customer needs to query the blockchain server whether information about the product is there in blockchain or not. If the product information is there in blockchain, then provide the information about the product, seller address, customer information to the manufacturer for transfer of ownership of the product to customer. If the product information is not found in the blockchain, then our system will provide the information that product is fake.

# Implementation Plan

## Schedule

**Table 5.1 Gantt chart**

|  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- |
| **S.N.** | **ACTIVITY** | **JUL-SEPT** | **OCT-NOV** | **DEC-JAN** | **FEB-MAR** |
| 1 | Feasibility Study |  |  |  |  |
| 2 | System specification |  |  |  |  |
| 3 | Requirement Analysis |  |  |  |  |
| 5 | Designing and Building Prototype |  |  |  |  |
| 6 | Documentation |  |  |  |  |
| 7 | Testing |  |  |  |  |
| 8 | Implementation |  |  |  |  |

## Hardware and Software Requirements

### Hardware Requirements

* + A computer with internet connection
  + Mobile Device with Camera with internet connection

### Software Requirement

* + Ethereum
  + solidity
  + Node.js
  + HTML
  + CSS
  + Ganache
  + GIT
  + JavaScript
  + React
  + Web3.js

# Expected Outcomes

The following outcomes have been presumed for this project:

* + Get the information from QR code attach to product using QR code scanner
  + By querying to Blockchain server by providing the information of product to manufacturer, Customers can verify that the product is genuine or not.
  + By providing necessary information and data to manufacturer for transfer of ownership of the product.

# References

A. Funde, P. N. (2019). Blockchain Based Fake Product Identification in Supply Chain. *International Research Journal of Engineering and Technology.* Maharashtra, India.

Buterin. (2015). *Ethereum white paper*. Retrieved from Ethereum.org: https://ethereum.org/en/whitepaper/

J. Leng, P. J. (2019). Makerchain: A Blockchain with Chemical Signature for Self-Organizing.

Kamat, A. A. (n.d.). Using QR codes to track and identify counterfeit products.

Nakamoto, S. (2008). Bitcoin: A Peer-to-Peer Electronic Cash System.

S. Wang, Y. Y. (2018). An Overview of Smart Contract: Architecture, Applications, and Future Trends. Suzhou, China: IEEE.

Si Chen, R. S. (2017). A Blockchain-based Supply Chain Quality Management Framework.

Tiwari, S. (2016). An Introduction To QR Code Technology. *International Conference on Information Technology.*

WOOD, D. G. (2021). ETHEREUM: A SECURE DECENTRALISED GENERALISED TRANSACTION LEDGER.

Yiu, N. C. (2021). Toward Blockchain-Enabled Supply Chain Anti-Counterfeiting and Traceability. *IEEE.*

|  |
| --- |
|  |
|  |
|  |