**IMPLEMENTING A BLOCCHAIN BASED ANTI-COUNTERFEIT SYSTEM**

**BY**

**VICTOR MBUGUA**

**EMMANUEL KIBET**

**CALENO ROSE**

**PAULINE MBUGUA**

**ABSTRACT**The growth of counterfeit goods has plagued the international community for decades. Nowadays, the battle against counterfeiting remains a significant challenge. Most of the current anti-counterfeiting systems are centralized. Motivated by the evolution of blockchain technology, we propose a decentralized anti-counterfeiting supply chain  
that exploits mobile,QR code and blockchain technologies.

In this project, with emerging trends in mobile and wireless technology, Quick Response (QR) codes provide a robust technique to fight the practice of counterfeiting the products. counterfeit products are detected using a QR code scanner, where a QR code of the product is linked to a Blockchain. So this system may be used to store product details and generated unique code of that product as blocks in the database. It collects the unique code from the user and compares the code against entries in the Blockchain database. If the code matches, it will give a notification to the customer, otherwise it will give the notification to the customer that the product is fake.

**Question 1: What is the main problem that you are solving?**

The ease of doing business in most parts of the globe is facilitating the growth of new businesses every day. Increasingly, small and medium-sized brands are sprouting across the world. Although globalization and advancement in technology have made it easier to establish brands, they are susceptible to umpteen challenges as well. While starting a new brand is easy, making it successful in today’s globalized economy is a big challenge for small and medium-sized companies.

Building a brand while adhering to the brand values is key; While every effort is focused on realizing this objective, when doing a analysis for the brands, most small and medium businesses ignore the threat of external factors including counterfeiting and brand abuse, which have a lasting impact on the brand and affect their sales and brand reputation. It is understood that small brands might have budget constraints that might compel them to overlook such areas, however, it is imperative that a budget be made available to implement a brand protection strategy that can fight the biggest and one of the most formidable competitors, and these are the counterfeiters.

Counterfeit products are widespread in many industries, for example, luxury handbags, perfumes, pharmaceutical products, and automotive components. The International Chamber of Commerce of Geneva claimed that the total global annual sale of counterfeit products is USD 650 billion.

Poor visibility, lack of transparency, incorrect recording and inefficient tracking are some of the challenges faced within the supply-chain ecosystem, which means that it has made it harder to understand where the problem arises. Thus with these reasons there have been loopholes in the supply-chains that are exploited for individual gain without adhering to the rules, regulations and standard of the global market.

With these inefficiencies in the supply-chain, there have been an increase in the production of counterfeit goods that may cause harm to consumers, exploitation of poor countries due to lack of proper oversight within countries, resale of expired products especially medical equipment and drugs that may be harmful to patients, consumers lose trust on companies deliverabity and companies making losses due to sale of counterfeit.

Several technologies that exist to solve the product-counterfeiting problem, such as  
radio-frequency identification, barcode scanning, and mobile technology. However, these technologies are mainly centralized and rely on trusted servers, which are vulnerable to cyberattacks, for example, replay and man-in-the-middle attacks. Blockchain technology has emerged as the best candidate to overcome these attacks. It can build a transparent, trustworthy, and secure supply chain that prevents the counterfeiting of products.

**Question 2: What is the importance of this problem?**

Economic sustainability refers to a status where an economy can achieve steady growth  
without sacrificing social and environmental sustainability. In the context of corporate  
and supply chain management, the economic sustainability pillar is often referred to as  
governance. It requires the company to develop a robust management structure that  
ensures overall transparency, traceability, and accountability, and ultimately can strengthen  
relations with external stakeholders and attract potential investors. Successful sustainable governance offers long term successes to the supply chains, because it can strengthen firms’ competitiveness, realize healthy and transparent corporate management, increase profit, and help the development of the other two pillars. However, it faces a range of challenges in practice. First, information asymmetry among partners along the supply chains could temper with the transparency management structure. This is particularly true for global supply chains, partly due to increased outsourcing.  
Second, the lack of reliability is another significant concern for the supply chain governance  
performance, which can lead to error or corruption issues due to the centralized transaction  
system. Lastly, it is often the case that traditional supply chain management hardly achieves traceability and reliability at the least possible cost, because it requires a substantial  
investment and management effort to monitor and trace the whole supply chain. Although  
most supply chains voluntarily self-regulate, such as the global management system (ISO  
14000), it is not a panacea for these challenges.

It is of significant importance to this research to systematically approach a review of the  
relevant literature in the field of counterfeited products in the fashion industry. Counterfeiting has been an ongoing issue for legitimate manufacturers since the 1970’s (Bian, & Moutinho, 2009, p.368). Since then, many companies have invested millions of dollars into developing their brand image only to have their profits reduced by copycat designers and knockoff enthusiasts. This has encouraged scholars to research the underlying causes behind this growing phenomenon. A significant portion of the research in this field focuses on the economic burden of counterfeiting as well as global intellectual property rights policies and how they apply to various products and industries. More recently researchers have shifted some of their focus to gaining an understanding of consumer behavior that is driving the demand for counterfeited goods

While government policies and anti-counterfeit legislation are at on all time high to combat the  
revenue losses faced by legitimate companies, an alternative approach to this issue can only be  
achieved through an understanding of the influence factors of consumer counterfeit purchase  
decisions.

**Question 3: What are the current solutions?**

**Anti-Counterfeiting Approaches**The current anti-counterfeiting works falls into two general camps:

(1)works that track-and-trace products to mitigate counterfeiting

(2) works that utilize cryptography to detect counterfeiting attacks.

**TRACK-AND-TRACE APPROACHES**  
This kind of approach uses Radio-Frequency Identification (RFID) tags to track the physical locations of a product, which are then stored in a centralized database. proposed one of the first track-and trace approaches, which uses Electronic Product Codes (EPC) to uniquely identify and track products in the supply chains. This approach can detect cloning attacks because the EPC of a counterfeit product will appear at least twice in the database. For example, a product with an EPC registered in Switzerland for sale cannot be registered in America at the same time. Nevertheless, the problem with approach is that it cannot detect tag reapplication attacks.  
The benefit of EPC is to quickly track products through the supply chain and make counterfeiting more difficult .This approach can detect cloning attacks by tracking and tracing the product with a complete product as the product moves from the manufacturer to retailers. In addition, it can detect modification attacks by using digital signatures. However, tag reapplication attacks remain a challenge for product-based approaches. This is because if a counterfeiter removes a tag from a genuine product and reapplies it to a counterfeit one, the product will remain valid, and the system therefore will not detect this attack.

**CRYPTOGRAPHIC APPROACHES**  
Cryptographic approaches use public or private key cryptography to authenticate products. propose an online approach that uses NFC tags and is based on public key cryptography. This approach allows customers to check the authenticity of products using their smartphones and does not require access to a database. Their approach assigns each instance of a product a unique public/private key pair, and uses a challenge-response protocol between the customer’s phone and the tag on the product. The tag contains the private key in a secure location that is accessible only to the tag’s processor. The corresponding public key is stored on the tag too, but can be obtained by the customer’s phone. The main benefit of this approach is that it involves customers in product authentication. However, this approach does not detect tag reapplication attacks, and requires expensive NFC tags that have processors, secure storage, and support encryption.  
Recently, TagPrint, an online cryptographic approach, was proposed to detect counterfeit products using RIFD. According to the authors, TagPrint is the first RFID-based online approach in existing anti-counterfeiting systems. This approach involves three parties: a tag provider, a product manufacturer, and a customer. First, the tags provider fingerprints its RFID tags by extracting some physical layer information to identify each tag. The tags and their fingerprints are ordered to the product manufacturer. Second, the manufacturer attaches a group of tags (at least four) to each product in randomized geometric locations. The manufacturer encrypts the tags’ fingerprints and geometric relationships and stores them in the tags’ memories. Third, the customer employs an RFID tag’s reader, which contains the manufacturer’s public key. The reader reads and decrypts the encrypted fingerprints and geometric relationships from the tags’ memories. After that, the reader obtains new tags’ fingerprints and geometric relationships and compares them to the decrypted ones to check if they are the same and hence determine the authenticity of the product. TagPrint can detect modification and cloning attacks using passive lowcost RFID tags and can be executed online. However, TagPrint cannot detect tag reapplication attacks. In addition, TagPrint is based on RFID tags, that require specialized readers, making this approach unsuitable for ordinary consumers.

**MONITORING AND BLOCKING OF SUSPICIOUS RESOURCES**The approach is that the manufacturer monitors Internet resources for infringing goods and their subsequent blocking. Monitoring such resources in automatic or semi-automatic modes requires developing specialized software, respectively, and resources for this development. Identification of the original is based on the buyer's confidence that all counterfeit resources are blocked. The manufacturer of the product can both monitor and entrust this process to another company. For example, Group-IB has been providing similar services for a long time and has a wide range of functionality. The company monitors the following areas: domain names, aggregators, bulletin boards, search engines, deep web, social networks, mobile application stores, messengers, contextual advertising. When a counterfeit is found, the company takes all necessary pre-trial measures to block resources and provides full legal support.  
**Pros of the approach:**• Reliability is above average;  
• You can entrust to another company;  
• Allows you to block many counterfeit resources effectively.  
**Cons of the approach:**• Requires considerable material investment;  
• Based on the trust of the buyer;  
• Works are only for online shopping

**Question 4: How will your solution solve the problem? What is new?**

We have come up with an idea that utilizes both blockchain technology and QRcode with a new form of algorithm that may enable one to validate products as they go through the production and distribution processes within the supply chain in order to weed out any counterfeit goods. Blockchain technology helps to solve the problem of counterfeiting a product. Blockchain technology is more secure. Once the product is stored on the network hash code is generated of that product and it is possible to maintain all transaction records of the product and its current owner as a chain will be created for that product transactions. All the transaction records will be stored in the form of blocks in the blockchain. In the proposed system we are assigning a generated QR code to a particular product and the end customer can scan that QR code to get all information about that product. After scanning the QR code we can identify that the product is real or fake.

Product information is permanently recorded by a blockchain, and cannot be altered, erased, or manipulated. A blockchain is a public decentralized ledger, so historical product information can be freely observed and verified by a user within the supply chain cycle. The transparency of the blockchain-supported e-commerce platform allows for a retailer to immediately know whether their goods are qualified; thus, counterfeit products cannot enter the supply chain. As blockchain technology ensures traceability and transparency, it can provide a trustful trading environment for enterprises in the supply chain; thus, it is an attractive solution for several supply-chain challenges.

**Question 5: What is the expected impact of your solution from various perspectives (social, commercial, environmental, etc)?**

A study on integrating blockchain in digital supply chains. The use of blockchain would provide better access to customers by sharing information about products effectively. Besides, products and service deliveries can be tracked to ensure visibility in the supply chain. Their analysis showed that many of the digital supply chains’ functionalities could be embedded in blockchain technology. In addition to that, blockchain provides security and cost-effective transactions in supply chains networks with no central system.

Blockchain can enable more explicit and more accurate tracking in supply chain: Organizations can digitalize digital assets and create a seamless record that separates everything that is made, making it possible to track assets from production to delivery or use by the end user. This increased supply of light supply gives more visibility to businesses and consumers. Blockchain can drive the supply chain transparency to help reduce the fraudulent assets of high value assets such as diamonds and pharmaceutical drugs. Blockchain can help companies understand how ingredients and finished goods are transferred through each subcontractor and reduce profit losses from fraudulent and gray market trading, as well as increase confidence in end-users by reducing or eliminating the impact of counterfeit products. In addition, entities may maintain additional control over the execution of an external contract. Blockchain provides all organizations within the network to provide appropriate access to the same information, which may reduce communication or data transmission errors. Less time can be spent verifying data and more can be spent on delivering goods and services — either to improve quality, reduce costs, or both. Finally, the blockchain can streamline management processes and reduce costs by enabling effective testing of supply chain data. Procedures that include self-assessment for compliance or credit purposes that may take weeks can now be accelerated using a spreadsheet of all relevant information.

**Question 6: Give a high level functional description of your solution. How will it be used?**

There is no good solution before to differentiate fake products from original products. Blockchain technology can be helpful to tackle such problems. The project’s main goal is to help people to identify the product is an original product or a fake product.  
We proposed a fake product detection system using blockchain technology as an android application for the detection of counterfeit products. The proposed system ensures that the detection of fake products in day-to-day life. The proposed system consists of three main parts, customer or user android application, Manufacturer’s or company’s android application, and Database.  
The first application is the Manufacturers or company side application in which we have to first  
register ourselves. After registration login into the application, we have some options. One option is to add a product in which the manufacturer can add the product details of which he/she can generate a QRCode that contains a unique code. Another option is to show the minting operation of the unique code to the blockchain. The manufacturer also can see the product is purchased or not.  
A second application is the Customer application in which we have to first register in-app after that we can log in to the application using id and password. In this application, there is an option to show products where customers can see the product details like name, total quantity, price of a product, details of the manufacturer. In this app we have a QR code scanner in which we scan the QR code of the product then it shows that the product is fake or real. There is another option which is a blockchain in which it displays the name of generated block product quantity, generated Hash Value, and the product is corrupted or not.

**Question 7: Give a high level technical description of your solution: architecture, technology, integration, innovative components, etc.**

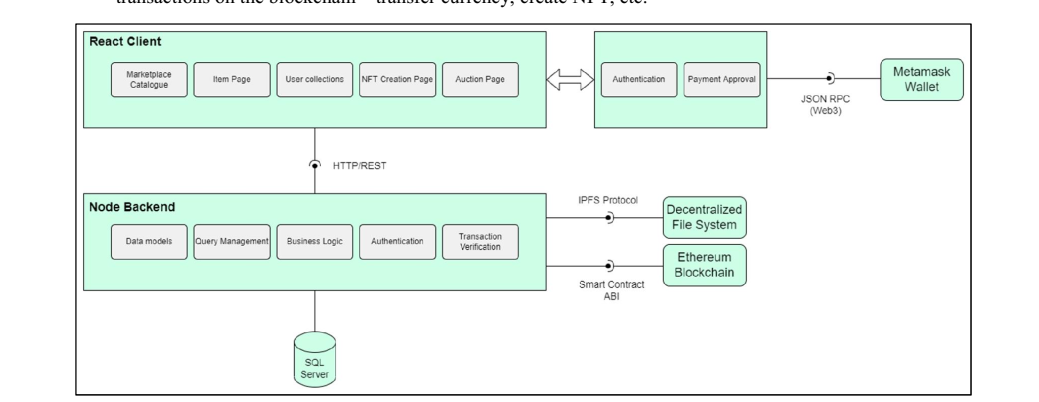
Blockchain Technology  
The blockchain is a distributed ledger that stores data through a chain structure. It establishes a trusted environment via consensus algorithms, asymmetric encryption, and smart contracts, giving it characteristics of transparency, decentralization, traceability, and anonymity. The blockchain is divided into three different application modes, namely, public, private, and consortium, depending on the level of centralization. A blockchain is chosen according to the different requirements of information confidentiality and transparency under different application scenarios. A public blockchain is completely decentralized, in which each node can participate in the process of data verification, storage, and update without the need to gain access from anyone else. A private blockchain is centralized, and all its related nodes are strictly  
controlled in specific institutions; the central organization is controlled by a limited number of nodes. A consortium blockchain is partially centralized, in which some specific nodes control the consensus process. Compared with private and public blockchains, the authority of nodes in a consortium blockchain can be flexibly set, and information processing is faster. Thus, consortium blockchains are widely applied. The adoption of blockchain technology could eradicate the moral-hazard problem under a markdown sponsor contract. A new anticounterfeit system based on blockchain technology could facilitate companies to effectively build a supply chain.

### QRCode

The symbol known as a Quick Response (QR) code is a two dimensional (matrix) that was introduced in 1994, initially as a means to track parts used in automobile manufacturing in Denso Wave - one of Japan’s Toyota group of companies (Brindha and Gopikaarani, 2014). The patent was made available for public use and an international standard was approved by the International Standards organization in 2000 and is regularly being updated (ISO, 2015).  
Similarly to the original use of QR codes in the automobile industry, QR codes can be used in a  
number of areas as a means to support interaction in controlled situations such as in supply chain process.

Architecture Overview React Client: This is a webapp built with ReactJS. It is primary interface between the user and the backend. It provides an easy-to-use graphical interface allowing the user to use all features of the software with ease. It communicates with the backend server using REST APIs. It also lets the user to access the wallet using Web3 libraries and JSON-RPC.

Metamask Wallet: This is a popular wallet that is used to store cryptocurrency. The client-side webapp communicates with this wallet using Web3 protocol. It lets the user approve payments.  
 Nodejs Backend: This server contains all the business logic of Bricklin. It communicates with the client through REST APIs, with the distributed file system using IPFS protocol and with the Ethereum Blockchain using the smart contracts. It also has a SQL database.  
 Distributed File System: This is a peer-to-peer network of devices which stores files. The files uploaded by the users for tokenization will be stored on this network. The backend can access this network using the IPFS protocol.  
 Ethereum Blockchain: It will store the URIs of NFTs. It also stores the smart contract and all the transactions performed by users.  
 Smart Contract: It is a piece of code with some business logic that is deployed on the blockchain. It performs all transactions on the blockchain – transfer currency, create NFT, etc.

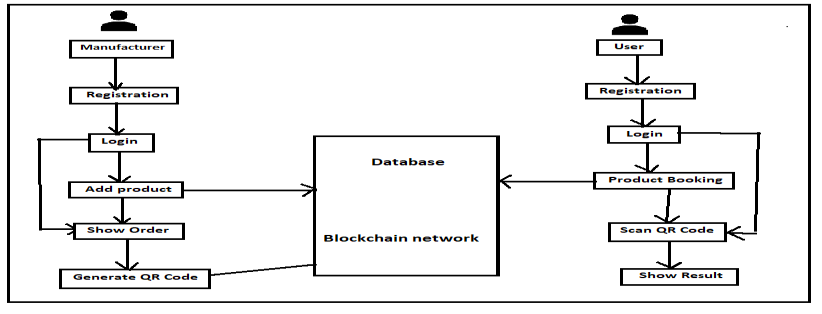


Four things are built here. An nft maretplace website, QRcode generator ,QRcode reader and smart contracts. The websites are built using Angular, javascript, CSS and HTML for the front end and springboot and node.js for the backend.

Android Studio is the official integrated development environment (IDE) for Googles Android  
operating system, built on IntelliJ IDEA software and designed especially for Android development. It is available for download on Windows, macOS and Linux based operating systems. It is placement for the Eclipse Android Development Tools (ADT) as primary IDE for native Android application development.

The smart contracts are written using solidity, a programming language used for ethereum smart contracts. These are converted to byte code and then stored in the Ethereum Virtual Machine(EVM).The website will make calls to the smart contract in the EVM via the web3.js library.A smart contract is a program stored on the blockchain,that only runs when predetermined conditions are met.

The classes in the middle layer, which is sometimes called the business rules layer, act as an interface between the classes in the presentation and database layers are the middle layer. The objects created from these business classes are called business objects. In this case the middle layer are the objects connecting the user interface with the backend system

This real-time system can be implemented to check the received product is a counterfeit product or original product. After the creation of QR Code Scanner application and integrating it with our blockchain database, we were able to scan for an authentic product and also distinguish between fake products. The manufacturer uses the algorithm to generate a QR code in blockchain technology. We used transaction hashes as a means to test the authenticity of the product and also converted them to QR Code so that the hashes could be scanned easily and the authenticity of the product can be checked. 

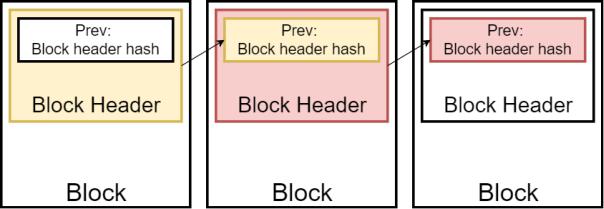
**Question 8: Give a high level description of your solution development environment, platform, tools, etc.**

### blockchain overview

A study on integrating blockchain in digital supply chains. The use of blockchain would provide better access to customers by sharing information about products effectively. Besides, products and service deliveries can be tracked to ensure visibility in the supply chain. Their analysis showed that many of the digital supply chains’ functionalities could be embedded in blockchain technology. In addition to that, blockchain provides security and cost-effective transactions in supply chains networks with no central system.

Blockchain is a decentralized system. It refers to the col-lective maintenance of a technical solution that maintains a continuous record file as a reliable database through decen-tralization. It was initially used extensively on Bitcoin[2]. II-A The block generation method of Blockchain is to collect and verify the data and then generate a new block through. We first describe the Blockchain consensus mechanism using Bitcoin as an example, its Blockchain consensus mecha-nism is a proof of work algorithm (POW). Each node com-petes based on their respective computing power to solve a SHA256 math problem that is complicated to solve but easy to verify. The first node that solves this problem will get the new block accounting right.

Blockchain data is stored on each node, then the nodes exchange information with each other over the network. Each node maintains an entire Blockchain data. The node will verify the received transactions and include them in the new block based on its own Blockchain data, and try to obtain the accounting rights of the new block in the above manner.



**BLOCKCHAIN FEATURES**

In today’s social system a large part of the economic behavior of individuals depends on trust where regularly two sides interact with a third party, thus forming a trust relationship. Usually, there is a mutual non-trust between these two parties that have long been based on trust guarantees provided by third parties, therefore it is important to take notice of the characteristics of Blockchain technology that help subvert the foundation of human transactions that have been conducted for thousands of years.

Using Blockchain one can create a data record system that does not depend on a trusted third party as a transaction intermediary, and that is openly shared and reliable at the same time. The characteristics of Blockchain technology are described in detail below.

1. Security and Privacy: Public key encryption in cryp-tography is used in Blockchain to protect data security. Users can generate their own key pairs, including a private key and a public key. Private key is used to sign data, and public key is used to verify the authenticity of not rely on an additional third-party control, has no centralized control, and is self-contained.
   1. Untraceability: After a block has been determined in the Blockchain, it cannot be tampered with. Due to the following circumstances, once a block in the Blockchain is altered, it will be immediately detected and rejected by other nodes.
   2. Transparency: The data in Blockchain is completely public and anyone can inquire. Within the Information flow one can clearly see who is passing data to whom as Blockchain maintains a continuous transaction log file.
   3. Flexibility: The technology of Blockchain is open source and anyone can use it to modify it into their own version. There are already numerous flexible Blockchain platforms available, and users can also redevelop a new Blockchain platform if they desire so. Blockchain is an unlimited technology meaning that users can create multiple applications based on Blockchain.

**ETHERIUM**

Ethereum is an open- source public service that uses blockchain technology that allows smart contracts and cryptocurrency trading securely without a third party. There are two accounts available through Ethereum externally possessed accounts ( controlled by private keys made by human users) and contract accounts. Ethereum allows developers to deploy all kinds of decentralised apps.

Ethereum’s mission is to create another shared work protocol, to provide a unique set of trades that we believe will be truly useful in the external division of segregation operations, with special emphasis on conditions where time for rapid development, security of small and unusual jobs; Ethereum does this by establishing what is the last non-authoritative base name for unauthorized power, marketing formats and country conversion activities. A blank definition of a word coin is usually written in two lines of code, and some principles such as currencies and currency systems are usually made up of less than twenty. Smart contracts, cryptographic "boxes" contain value and are only open if certain conditions are met, can also be built on stage, with greater force than those given Bitcoin scripting due to increased Turing-absoluteness, value- mindfulness, value blockchain - mindfulness and -state blockchain in the programming language embedded in Turing-complete, which allows anyone to write smart contracts and assigned tasks in an environment where they will produce their own authorized laws, marketing formats and land reform activities.

**SMART CONTRACTS**  
Bitcoin as the first cryptocurrency was proposed in 2008 by Satoshi Nakamoto, who is presumably an anonymous person or group of persons hiding by this pseudonym. The difference from traditional payment systems is that electronic currency could be transferred in a peer-to-peer manner without a central party that needs to check the records of ownership. Blockchain technology helps to prevent the double-spending problem and enforce the validity of transaction records . One more crypto-asset “token” is almost the same as the cryptocurrency – a bearer instrument used to transfer value between parties over the blockchain network; whereas tokens are created by a single party to represent a certain value, cryptocurrency is generated by the network as the reward for miners or validators.  
Token technology was introduced and standardized by Ethereum and its smart contracts, which  
code describes how each token should work . However, Ethereum was planned as a globally  
distributed computing network that uses publically stored immutable programs – smart contracts also referred to as decentralized applications. However, decentralized applications usually include a client-side created using markup, style sheets, and JavaScript (JS). Decentralized applications (or DApps) use the Web3 JS library to interact with the smart contracts deployed on the blockchain. DApps are immutable (as any data stored on the blockchain) and perform exactly as they were developed, without the possibility of fraud, downtime, censorship, or interference.

**TOKENIZATION**  
In the context of blockchain, tokenization means a representation of real physical or electronic  
assets digitally on the blockchain. There could be commodities, real estate, ownership rights for  
arts or other collectibles, currency, or any other kinds of assets. As advantages tokenization offers  
faster and cheaper transaction processing, flexibility, decentralization, security, an transparency, but there are disadvantages, such as regulatory and legality issues, as well as technical barriers caused by the use of DApps. There are two types of crypto-tokens:  
• Fungible Tokens (FT), which value is identical among all tokens, and which are exchangeable  
to each other (i.e. one FT token could be replaced by another FT token similarly to digital cash).

Non-fungible Tokens (NFT) are unique and not equal to each other in value (i.e. each NFT  
token is different from others and cannot be replaced by any of them).

Another explanation of FT and NFT given in says that dollar bills are exchangeable to other  
dollar bills, so they are fungible, whereas baseball cards or other collectibles are unequal in their value and cannot be replaced with another one.  
From the technological point of view, both FT and NFT are implemented as smart contracts, which are programmed in a specific way. Several smart contract standards for tokens were developed by the Ethereum community . The most popular contract standards are:  
• ERC20 standard for fungible tokens, which is suitable for multiple use cases, such as payment  
tokens, loyalty coins, gift cards, etc. A great example of NT implemented as the ERC20 token on  
the Ethereum blockchain is Tether USD, a stable cryptocurrency (also referred to as the  
“stablecoin”) that digitally represents USD (United States Dollar) [18].  
• ERC721 standard for non-fungible tokens, which is suitable for documents, land titles, digital  
identities, real estate, collectibles, etc. A great example of NFT implemented as the ERC721 token on the Ethereum blockchain is CryptoKitties, an Ethereum-based game in which players buy, sell,and breed collectible digital cats [19].  
Nowadays OpenZeppelin organization provides extensive references for the development of  
ERC20, ERC721, and other smart contract standards [20].

Blockchain technology helps eliminate the problem of counterfeiting. Blockchain technology is much safer. Once the data is stored in the network hash code is generated in that product and you are likely to take care of all the sales records of the current owner and its owner as the sequence will be created for those product agreements. All sales records will be stored within the block type within the blockchain. Within the proposed system we assign the QR code generated to a particular product and thus the end client ignores that QR code in order to disclose all the information for that product. After checking the QR code we will identify whether the product is genuine or counterfeit.

Software requirements

* **Database**:
* XAMMP - helps a local host or server to test its website and clients via computers and laptops before releasing it to the main server. It is a platform that furnishes a suitable environment to test and verify the working of projects based on Apache, Perl, MySQL database, and PHP through the system of the host itself. Among these technologies, [Perl](https://www.javatpoint.com/perl-tutorial) is a programming language used for web development, [PHP](https://www.javatpoint.com/php-tutorial) is a backend scripting language, and MariaDB is the most vividly used database developed by MySQL.
* MySQLi - API used as a connector function to link the backend of the PHP app to the MySQL database**.**
* **Android studio**:for delopment of android apps
* **Languages**

**Java-** we will utlize java to develop powerful APIS for front end utilization

• **Node.js** - A JavaScript runtime environment for server-side programming. Node.js is needed for testing the functionality of your Ethereum smart contract and ensuring its proper and secure operation. Along with Node.js, installation of a package manager called Yarn will be done.

• **HARDHAT** - A popular Ethereum development framework that allows you to write and test smart contracts. Truffle is written in JavaScript and contains a compiler for the Solidity programming language. hardhat Contract is a JavaScript library that facilitates importing of compiled smart contracts.  
• **Ganache CLI** - An Ethereum remote procedure call (RPC) client within the Truffle framework; formerly known as TestRPC.  
• **Web3.js** - An Ethereum JavaScript API that communicates with the Ethereum network through RPC calls.  
• **Metamask** - A fast and secure Ethereum client for managing accounts, tokens, and so on.  
• **Visual Studio Code** - A functional code editor.  
• **Remix.ethereum IDE** will be used to manually test the smart contract and Meta mask will be used to send transactions to the blockchain. Remix.ethereum will help remove all the syntax errors and for debugging all transactions debugger of remix IDE will be used.

**Question 9: How will you manage your product development cycle, your quality assurance process, your solution deployment logistics, etc?**

The researcher will employ the Agile model during the development stages of the system. This model aims to produce high quality systems that meet the client’s expectation. Development is done in form of sprints. Each sprints ensures functional and non-functional requirements are met.

### Data Collection Methods :

The researcher will identify all the requirements for the development of a blockchain based counterfeit system. Questionnaire and schedule will be used to collect the primary data.

We also plan to involve a manufacturing company in gathering the required information to help us understand the day to day tasks in afactory and how our system may be intergrate with existing ones.

### System Design:

The researcher lists down the hardware and software required for the development of the anti-Counterfeit system. Software processes and task will described. The input, process, output and storage hardware are specified. Server configuration and coding will also be done during this stage.

### Implementation:

With inputs from system design, the system is first developed in small programs called units, which are integrated into the next phase. Each unit is developed and tested for its functionality which is referred to as Unit Testing

### Integration and Testing:

Units developed in the implementation phase are integrated into a system after testing of each unit. The software designed, needs to go through constant software testing to find out if there are any flaws or errors. Testing is done so that the client does not face any problem during the installation of the software.

**Question 10: Give the most relevant plans that you have developed for your project (for example, time schedule, resource plan, training plan, risk management, contingency plan, etc.)**

**Project Budget**

|  |  |  |  |
| --- | --- | --- | --- |
| **No** | **Item Description** | **Available** | **Estimated cost(Kshs)** |
| 1 | Personal computer (HP ELITEBOOK 840) | **🗸** |  |
| 2 | Flash memory | **🗸** |  |
| 3 | Smartphone | **🗸** |  |
| 4 | Documentation printing and binding | ☒ | 30,000 |
| 4 | Documentation, apis and cloud services | ☒ | 15,000 |
| 5 | Etherium sevices | ☒ | 50000 |
| 6 | Intellij(Community) | **🗸** |  |
| 7 | XAMPP Server | **🗸** |  |
| 8 | Android Studio | **🗸** |  |
|  | Browser(Chrome 2020) | **🗸** |  |
| 9 | Research Expenses | ☒ | 10,000 |
| 9 | QR printer | ☒ | 30,000 |
| Grand Total | | | 108,000 |

# **Project Schedule**

|  |  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- | --- |
| **Activity** | **Duration**  **(Hrs)** | **Expected**  **Start Date** | **Expected**  **End Date** | **Actual**  **Start Date** | **Actual**  **End Date** | **Deliverables** |
| Project  Identification | 10 Hrs | 3rd  2022 | 7th December 2022 | 10th December  2022 | 14th December  2022 | Project identification writeup-draft |
| Requirements  Identification | 8 Hrs | 10th Decmber  2022 | 12th December  2022 | 10th December  2022 | 12th December  2022 | Project abstact form document-draft |
| Data Collection |  |  |  |  |  |  |
| * Tools Development | 15 Hrs | 17th December  2022 | 20th December  2022 |  |  |  |
| * Implementation | 10 Hrs | 21st December  2022 | 28th December 2022 |  |  |  |
| * Feedback Collection | 11 Hrs | 29th December  2022 | 11th January  2023 |  |  |  |
| Analysis |  |  |  |  |  |  |
| * User\_needs analysis | 20 Hrs | 14th January  2023 | 25th |  |  |  |
| * Timeline specifications | 10 Hrs | 28th  January  2023 | 2nd  February  2023 |  |  |  |
| Design |  |  |  |  |  |  |
| * Required Hardware& software specification | 15 Hrs | 5th February  2023 | 16th February  2023 |  |  |  |
| * Processing procedures outline | 5 Hrs | 19th February  2023 | 6th  March  2023 |  |  |  |
| Implementation |  |  |  |  |  |  |
| * Module development   (coding) | 65 Hrs | 9th  March  2023 | 20th March  2023 |  |  |  |
| * Module testing | 10 Hrs | 23rd March  2023 | 27th March  2023 |  |  |  |
| Testing  &Integration |  |  |  |  |  |  |
| * Units integration | 10 Hrs | 30th  March  2023 | 11th April  2023 |  |  |  |
| * Verification &Validation   Procedures | 5 Hrs | 14th April  2023 | 18th April  2023 |  |  |  |
| Documentation | 30 Hrs | 30th April  2023 | 3th  May  2023 |  |  |  |
| Final Presentation | 4 Hrs | 8th May  2023 | 12th  May  2023 |  |  |  |

# **Gantt chart showing the project schedule.**

|  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- |
|  | Duration  (In Weeks) | 1 | 2 | 3 | 4 | 5 | 6 | 7 | 8 | 9 | 10 | 11 | 12 | 13 | 14 | 15 | 16 | 17 | 18 | 19 | 20 | 21 | 22 | 23 | 24 | 25 | 26 | 27 | 28 |
| 1 | Project  Identification |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |
| 2 | Requirements  Identification |  | |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |
| 3 | Data Collection  -Tools Development  -Implementation  -Feedback Collection |  |  |  | | | |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |
| 4 | Analysis |  |  |  |  |  |  |  | | |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |
| 5 | Design |  |  |  |  |  |  |  |  |  |  | | | | |  |  |  |  |  |  |  |  |  |  |  |  |  |  |
| 6 | Implementation |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  | | |  |  |  |  |  |  |  |  |  |  |  |
| 7 | Testing  &Integration |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  | | |  |  |  |  |  |  |  |  |
| 8 | Documentation |  |  |  |  |  |  |  |  |  | | | | | | | | | | | | | | | | | |  |  |
| 9 | Final Presentation |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  | |

**REFERENCE**1. Si Chen, Rui Shi, Ren, Jiaqi Yan, Yani Shi, “A Blockchain-based Supply Chain QualityManagement  
2. Framework”, 14th, IEEE International Conference on e-Business Engineering, 2017.  
3. Blockchain Based Fake Product Identification in Supply Chain www.irjet.net: Ajay Funde, Pranjal Nahar, Ashwini Khilari.  
4. Fake News Detection In Social Media using Blockchain: - Shovon Paul, Jubair Joy, Shaila Sarkar. OECD and EUIPO, *Trade in Counterfeit and Pirated Goods – MappingThe Economic Impact*. OECD Publishing, 2019.  
5. K. Dégardin, Y. Roggo, and P. Margot, “Understanding and fighting the medicine counterfeit market,” *Journal of pharmaceutical and  
biomedical analysis*, vol. 87, pp. 167–175, 2014.  
6. OECD and EUIPO, *Trade in Counterfeit Goods and Free Trade Zones– Evidence From Recent Trends*. OECD Publishing, 2018.  
7. Social Bakers**,** (2012-03-01), *"Facebook statistics by country",*http://www.socialbakers.com/facebook-statistics/ [2012-03-21]

8.Statistiska Centralbyrån, SCB(2012), *"Sveriges befolkning efter kön och ålder 31  
december 2011"* [Electronic] Stockholm, SCB, Available:  
http://www.scb.se/Pages/TableAndChart\_\_\_\_262459.aspx [2012-03-20]  
  
9. Anti-Counterfeiting and Neo C. K. Yiu, IEEE Department of Computer Science, University of Oxford “Toward Blockchain-Enabled Supply ChainTraceability” fi13040086 (2021 , March 29)  
Neo C.K. Yiu, Member, IEEE Department of Computer Science, University of Oxford “Toward Blockchain-Enabled Supply Chain Anti-Counterfeitingand Traceability” 2102.00459 (2021 , January 31)

10. M. Swan, Blockchain, Blueprint for a new economy. O’Reilly Media Inc.,2015.

11. M. Biella, V. Zinetti. Blockchain technology and applications from a financial perspective. Unicredit Tech. Rep., February 26, 2016.  
12. S. Porru, A. Pinna, M. Marchesi, R. Tonelli. Blockchain-oriented SoftwareEngineering: Challenges and New Directions, Proc. 2017 IEEE/ACM 39th IEEE International Conference on Software Engineering Companion, Buenos Aires, Argentina, May 2017, IEEE Press.