

**PRCO304HK
Computing Project
2020/201**

**BSC(Hons) Computer and information Security
Li Hin Shing, Adam
20126318**

Project Title: Blockchain-based Fake Product Identification System

Word Count: 10039

Supervisors: Ronald K. MO, Ph.D., Dr Hafizul Asad

TRELLO LINK: <https://trello.com/b/aYZMInkW/prco304-adam-li>

GITHUB LINK: <https://github.com/AdamLi13/PRCO304>

TABLE OF CONTENTS

ACKNOWLEDGEMENTS.....	3
ABSTRACT	3
INTRODUCTION.....	3
BACKGROUND.....	4
2.1.1 what is the current issue	4
2.1.2 What is the ideal solution	4
2.2 Objectives.....	4
2.3 Study Goal.....	4
2.4 limitations of current solutions	4
3.Literature Review.....	5
3.1Blockchain Overview	5
3.2Blockchain Features	5
4.Legal, Social, Ethical and professional issues	10
5. Architecture and Design	15
5.1 Use-cases and functional requirement.....	15
5.2 Database based on blockchain's Data Architecture	16
5.2.1 Smart Contract Use Cases:	17
6. Development Technologies	17
6.1 Blockchain	17
6.1.2 Smart contract	18
6.1.3 Ethereum	20
6.1.4 Solidity	22
6.1.5 Brownie	23
7.Project Management	24
7.1.1Agile Development	24
7.1.2 GITHUB.....	24
7.1.3 TRELLO.....	24
7.3. TIME MANAGEMENT.....	25
7.4 Usability	26
8.Sprint plan and reviews.....	29
9.Overall Approach.....	52
10. Difficulties Encountered.....	53
11. Conclusions.....	55
Appendices	56

1. ACKNOWLEDGEMENTS

I would like to extend my sincere appreciation to my project supervisors, Ronald K.Mo and Dr Hafizul Asad for their guidance and support throughout this project. they guide me to solve the problems and have a clear path on how to achieve this project more effectively and efficiency.

1.1 ABSTRACT

this report describes a blockchain-based software development project to build a blockchain application for fake product identification. The application allows user to view the specific products with their own contact address and transaction records so they can clarify if that is a counterfeit.

The Report beings by defining the background, objectives and deliverables of the project, describing the aim and objectives of the project, current solution and the limitation of the current solutions. And then there is a section on literature review to explain an overview of current knowledge, relevant theories, methods and gaps in the existing topic.

Further on, the report describes the method of approach during the development process. And also, to look at the legal, social, ethical and professional issues of this project development.

The main body of the report discusses the project management of the application. The development was split into distinct stages, approaching each of these stages with an iterative approach which relies on the completion of the previous stage before moving on to the next. Also looks into how issues and challenges were met and overcome. The next section focuses on the testing/demonstration of the application.

The final sections of the report give a review of how the completeness of this project is by evaluating its architecture, design and the technologies used. Moreover, there is an appendices section which contains documents relevant to the project such as a user guide, project management document and sprint reviews.

2. INTRODUCTION

Block chain is one of the most significant technological innovations, and it has grown amazingly in the past few years. A renowned blockchain application is the cryptocurrency – Bitcoin. The Block chain technology is extremely powerful and effective to confirm the legitimacy of transparent records without relying on a centralized system. However, it's just a tip of the iceberg for it. It is ensured that the Blockchain technology can bring a lot more advantages to the systems/applications such as tamper-proofing/tamper resistance for the contents of the data.

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 Project is not only focused building an anti-counterfeiting system but also to explore the characteristic of the Blockchain (for example: Security and Privacy, Decentralization, Untraceability, Flexibility & Transparency) and understand how these characteristics make Blockchain becomes a disruptive technology and how it helps the industries.

2.1 Background:

2.1.1 what is the current issue

As found that almost every popular brand has fake manufacturers selling a counterfeit at cheaper rates nowadays. It's obvious that even the company experts may not be able to recognize between the real or fake electronic products so it makes the customers lack of confidence to purchase the popular brands' electronic products from the retailers especially when the customers are buying online.

2.1.2 What is the ideal solution

In this way, this phenomenon makes me think what if there's a decentralized Blockchain system with products anti-counterfeiting? in that way manufacturers can use this system to provide genuine electronic products without having to manage direct-operated stores, which can significantly reduce the cost of product quality assurance. And the customers can easily distinguish between fake ones and real ones by using the system and it is beneficial for both the buyers and the sellers as the buyer-seller relationship has been improved as the customers will have the ability to identify if it's a counterfeit.

To achieve this, what if the system can offer a digital signature or embedded barcode which is tied to a blockchain system? So, both the manufacturers and customers can rely on the embedded barcode or digital to help identify whether the product is fake or not. And it will be more user-friendly if the system can be used on the mobile devices.

2.2 Objectives

1. Build a Blockchain Based system to identify the fake product
2. Discover how identification system have benefited from blockchain technology
3. Discover what is the advantages for the data to be stored by using the decentralized blockchain technology.

2.3 Study Goal

The study goal of this project is to understand what is blockchain, how blockchain works and how it is transforming the software development. For example, understand why blockchain software is highly secure and the key features of block chain-based system (Data replication & Transaction Recording etc.) and also what are the differences between the traditional software development and block chain oriented software development.

2.4 limitations of current solutions

2.4.1 Lack of a user-friendly UI for user

As the current system is to use the Brownie & Solidity to create the smart contract and to build up a EVM (Ethereum Virtual Machine), it needs cost to put the system into the real Ethereum blockchain environment, without the money to perform the action, the system cannot link to the EtherScan (the block explorer and analytics platform for Ethereum) to store the transaction records on it. And it makes the user to lack of a user-friendly UI to review all the records that have been generated from the system.

3. Literature Review

3.1 Blockchain Overview

Blockchain – decentralized system, is essentially a distributed database of records or public ledger of all transactions or digital events that have been executed and shared among participating parties, each transaction in the public ledger is verified by consensus of a majority of the participants in the system [1]. Or it should be also considered as a distributed append-only timestamped data structure whether we can distribute peer to peer networks where the verifiable interaction can be made without the need for a trusted authority between the non-trusting members. (Christidis and Devetsikiotis, 2016).

One of the most important features which Blockchain has been provided is as to a set of interconnected mechanisms which generate signed transaction between peers. The transaction represents as the agreement between two participants/parties, which the transfer of physical or digital assets maybe involved. To complete a transaction task, for example there should be at least one party or participant signs the transaction, and it is distributed to its adjacent participant. Generally, Blockchain connects a set of entities which are called nodes. However, they are also called as full nodes for those nodes verify all the blockchain rules. The nodes group the transactions into blocks and they are in charge of identifying whether the transactions should be kept in the blockchain as they are valid, and also to decline or remove them if they are not. [figure.1]

How does a transaction get into the blockchain?

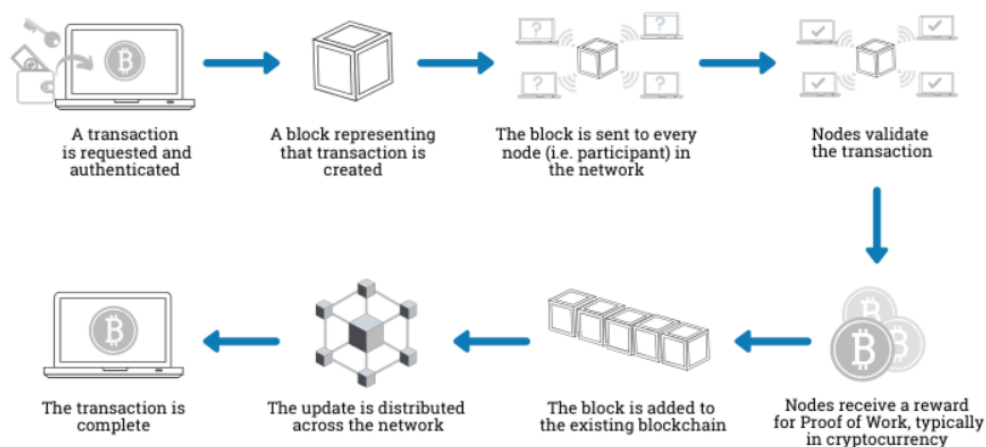


Figure.1 – How does a transaction get into the blockchain? – Euromoney Learning,2020

3.2 Blockchain Features

It's ensured that Blockchain technology owns special characteristics which are the key points to improve the transaction flow, interaction between party to party and their trust relationship etc.

It is important to understand the characteristics of Blockchain technology that help subvert the traditional human transaction foundation which has been implemented for few decades.

Using Blockchain once can create a data record system that does not depend on a trusted third party as a transaction intermediary. And that is reliable and shared openly at the same time.

The main characteristics of Blockchain technology are Decentralization, Flexibility, Transparency, Security and Privacy and Untraceability. (Figure. 2)

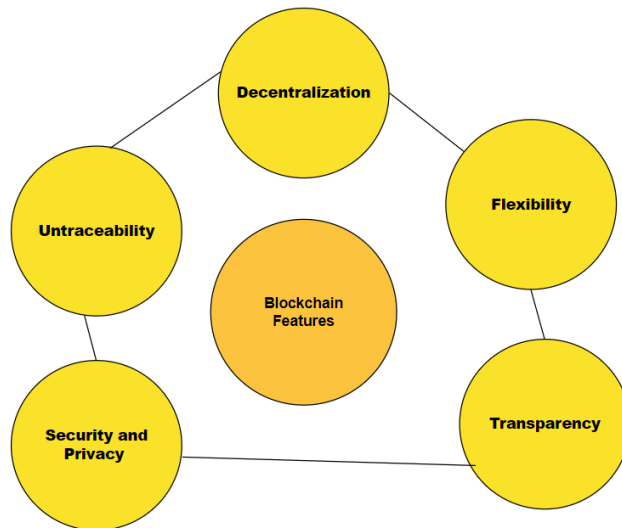


Figure.2 Blockchain Features

For the characteristics of Blockchain technology, the details have been described as below:

Decentralization: In Blockchain, decentralization refers to the transfer of control and decision-making from a centralized entity, it could be as individual or organization or group thereof to a distributed network.

In Blockchain, decentralized are to be able to decentralize the operations and storage. By decentralizing the operations and storage, each node of the Blockchain implements the information management, delivery and verification without connecting to a centralized center (third party.). it means those processes will be implemented at the local side and it does not rely on an additional third-party control, it is self-contained without centralized operations.

the advantages of Decentralization are providing a trustless environment, it does not mean it's not trustworthy but to provide an environment that nobody has to verify if each other is trustable or not. In the form of a distributed ledger, it provides the copy of the exact same data to each member, the majority of the members in the network will reject a member's ledger if it is altered or corrupted.

Besides, it improves data reconciliation by having a decentralized storage, every entity is able to access to view of the data which is real-time updated and shared. It can reduce the possibility and opportunity for data loss or any wrong data to be entered to the system. For example, the data will be often exchanged between the businesses and their partners and the data is generally transformed and stored in each company's data store, the data surfaces are not conciliated and the data loss may occur each time the data is transformed However this situation can be improve by using decentralization technology in blockchain.

Moreover, Decentralization can reduce points of weakness in systems where there may be too much reliance on specific actors. These weak points could lead to systemic failures, including failure to provide promised services or inefficient service due to the exhaustion of resources, periodic outages, bottlenecks, lack of sufficient incentives for good service, or corruption.

Furthermore, Decentralization can also help optimize the distribution of resources so that promised services are provided with better performance and consistency, as well as a reduced likelihood of catastrophic failure.

Flexibility: Blockchain has a high level of flexibility which is an open-source technology. It's capable to let anyone to use it and to develop the application/system from different aspects, such as for Cybersecurity, Healthcare, Financial Services, Manufacturing and industrial, Government and Retail. And there are already some amazing application & system right there such as:

“GuardTime”, which is a company creating “keyless” signature systems using blockchain which is currently used to secure the health records of one million Estonian citizens.

“ABRA”, a cryptocurrency wallet which uses the Bitcoin Blockchain to hold and track balances stored in different currencies.

Samsung. A famous south Korean multinational conglomerate that is one of the world's largest producers of electronic devices. They are also creating blockchain solution for the south Korean government which will be put to use in public safety and application of transportation.

Except cryptocurrencies, there are also lots of useful applications and systems have been developed or being developed. With more and more Blockchain platform are available, users can be re-build or develop the new systems, applications or even a new blockchain platform more flexible and easily. It is clear that blockchain is a world-changing technology.

Transparency: As mentioned the data in blockchain is completely clear and public. Its transparency makes it easy to search or recognize, or even for investigation.

Through the blockchain data flow, anyone is capable to see who is transferring the data to whom as Blockchain offers transaction log files which are continuous.

For example, all the transaction records can be viewed by either having a personal node or by using blockchain explorers that allow anyone to see transactions occurring live. Each node has its own copy of the chain, and it will be updated when there's new blocks have been confirmed to add to the blockchain. This means users are able to trace the whole transaction history of any physical or digital assets once their transaction flow data has been entered into the chain, if they desire to do so.

The transparency is also beneficial for risk management, let's say if a cryptocurrency exchange has been hacked/attacked and the cryptocurrencies which were held by the users on the exchange have been lost. While the identity of the attackers may not be verified, the cryptocurrencies that they have stolen are easily traceable. If the stolen cryptocurrencies have been moved or transferred to somewhere, users can view the where the cryptocurrencies go by using blockchain explorers.

Untraceability: although the transaction records have been recorded and stored in a permanent, inalterable public ledger – Blockchain. It doesn't mean all the records are fully traceable.

It is obvious that the blocks in the blockchain cannot be tampered with once they have been determined. Due to the restriction, if the block in the blockchain has been altered, it will be rejected by other nodes immediately.

Moreover, although everybody can see the transaction records, but it doesn't mean that they can see the identity behind a transaction as there is no needs to gather any personal information in order to perform the operations in blockchain. By strengthen the untraceability features, it makes it even virtually impossible for third-parties to follow the trail of transactions using services such as blockchain analysis.

Security and Privacy: In Blockchain, Cryptography is one of the most important elements which makes blockchain as such a special technology.

Public key cryptography is one the cryptographic system that has been adopted in Blockchain technology to protect data security. Users can create their own key pairs, including a public key (which may be known to others) and a private key (which may never be known by any except the owner). Typically, the public key is used to encrypt the data and the private key is to decrypt the data. In blockchain, the public key has also been used for authentication verification of the signed data and the private key is used to sign the data and also, to protect a user from theft and unauthorized access to funds such as depicted as a series of alphanumeric characters, which makes the hacker be more difficult to crack. As long as the user prevents the private key from leaking, the data will remain secure.

The security of Blockchain is relied on CIA Triad fundamental also:



Confidentiality — The blockchain provides spacious abilities and features to improves and ensure the anonymity. The linkage between the data and the user are the user keys only. And to improve the security level, the design of the user keys are also be capable to anonymize.

Among the various cryptographic techniques aiming to provide confidentially and privacy, the zk-SNARK, zk-STARK proofs are two noteworthy examples. zk-SNARK stands for zero-knowledge succinct non-interactive argument of knowledge, and zk-STARK represents zero-knowledge succinct transparent argument of knowledge. The former proofs are already being used on ZCash, a decentralized cryptocurrency focused on privacy and anonymity. While the latter proofs are being more and more emphasized as the improved version of the protocol is resolving many of the previous known limitation or weakness of Zk-Snark.

As a result, while being open and offering rich opportunities for transaction tracking, a blockchain allows users to maintain an unprecedented level of anonymity.

Data integrity — Blockchains are designed as public ledgers where every block is linked to nearby blocks using cryptographic hash functions. As a result, the transaction records cannot be tampered with or deleted. the transaction can only be created, but not altered. Any changes made to the records into the chain will be represented as a new transactions.

Availability — the resilience of blockchain has been ensured by having a huge amount of nodes, as the distributed ledger will create a copy to each node in the blockchain,

Having a large number of nodes ensures blockchain resilience even when some nodes are unavailable. And as each node in the network has a copy of the distributed ledger, the accessibility to other peers remains once the nodes verified that the transaction in blockchain is valid.

Blockchain technology addresses the security and trust issues from different aspects. First, new blocks are always stored linearly and chronologically. To explain more clearly, the blockchain records are always added as a N+1 symptom, for example the position of the new transaction will be counted as "101" if the previous record is counted as "100". And the position of the block on the chain is called as "Height", for example, the bitcoin's blockchain had reached 6855ch blocks so far which is a huge number.

After a block has been entered and linked to the end of the blockchain, it is nearly impossible to go back and alter the contents of the block. That's because each block contains its own hash, along with the hash of the block before it, and the block contains time stamp whenever it has been entered to the blockchain. The creation of the Hash codes involves in mathematics formulas which help to turn the separated data into a string of letters and numbers. The hash code will also be changed in case the information is edited any way.

So, the important of it for the security is, for example a hacker wants to steal the cryptocurrency from the blockchain (Bitcoin etc.). the action for the hacker is typically to alter the blockchain records and steal the crypto from any one of the owners. However, as each node has a copy in the current valid blockchain, if the hacker alters his/her own single copy, the copy will be no longer linked with everyone else's copy in that blockchain and as invalid. When everyone else reviews their copy with each other as the references, the hacker's copy and the invalid blockchain will be found out easily. so, in order for the hacker to steal the crypto successfully, the hacker will need to alter over a half of the total copies in the blockchain in order to tamper the records to forge the fake copies as the major copies and as same as the blockchain, and to re-build all of the blocks with the non-conflicting timestamps and hash codes into that "fake blockchain" However due to the needs of the enormous amount of the resources and cost it will be nearly impossible to implement it.

It is probably insurmountable to implement such kind of the attacks due to the fast-growing size of blockchain. Not only because the immense cost but also it would be worthless regarding the value ratio. The risk of being aware and the difficulty of the whole tasks makes the hackers hang back especially it is easily for the owners/members in the blockchain to move to a new valid blockchain that has not been attacked.

4. Legal, Social, Ethical and professional issues

It is obvious that Blockchain technology is growing rapidly nowadays however it will still be facing lots of the issues related to Legal, Social, Ethical and professional aspects:

Legal:

Jurisdiction: As blockchain is a decentralized system, it means the nodes exist into the global network, it is difficult for different countries to reach a consensus to establish a set of rules and laws to apply in order to control the blockchain. As different approaches to ownership, liabilities, contracts and titles have been adopted by different countries, it is hard to integrate them together without conflict and violation.

Decentralized Autonomous Organizations (DAOs):

Typically, a legal distributed or centralized system contains both individuals and organizations as the stakeholders and they should both have the equal rights to the system. However, for a decentralized autonomous organization (DAO), it is relying on smart contracts for the operation and it requires equally to nothing as the input from users. And behind the smart contract, it is just lines and lines of the codes as to maintain the whole operations. When a conflict or incident is occurred, it is hard to identify who or what should take the responsibility and what the responsibilities and consequences to bear.

Contract enforceability: As mentioned, the smart contract is the core of the decentralization system and it doesn't have an intermediate party to be involved. It is helpful for reducing the cost and even improving the security once the audit and legal concerns have been undertaken. However, before that as the smart contracts are just the programming codes eventually, it is difficult to define whether it's actually fit the definition of a contract in the common sense and the enforceability of a smart contract as it is quite far away from the control of the laws. It is sure that users will need to fully understand what the provisions and regulations are behind the smart contract before signing them.

Leaving a blockchain: supposing that you are using the blockchain-oriented system, as the personal information will not be saved in the blockchain, it is very difficult to retrieve the records and information back once you left the blockchain and forgot to hold a copy of the data on the ledger. Currently, there are no sufficient and complete provisions and protocols that supervise the information and records to be linked with a identification so that the information will be easily retrievable.

intellectual property

the blockchain's value is inevitable, and ownership of the IP in it will likely form an important consideration albeit that the limitations on the patentability of software and business processes. However, it is undeniable that the potential financial returns of blockchain technology is huge, the blockchain vendors will have to decide the strategy of intellectual property. That is a negotiated area which will need to be carefully noticed as if the vendors would like to take the benefits that generated from the Blockchain, including commercialization of the underlying data set which maybe involved in user's IP (data set).

In the same way, in the case of building a specific system or applications based on blockchain to meet customer's requirements, it is hard to define the ownership of the IP as the transparency of blockchain makes the software become public to use and everyone is able to own it. Without a competitive edge and/or guideline to strict whether it can be used by another customers or vendors, it is ensured that all the customers or users may insist on ownership on such developments. To solve this issue, it is better to license the customers and users for some terms of agreement to secure the IP possession in some way.

An "open innovation" approach is prevalent throughout fintech. The fintech companies are working towards a feasible blockchain POC. Traditionally the fintech companies have expected to own the intellectual properties in any developments. However there appears a consensus that the more the ideas have been shared, the more values of the technology will be gained.

Data privacy

As one of the key USPs (Unique selling points) of the blockchain is that the data is nearly impossible to be altered once it has been entered to the blockchain. In that way the personal data or metadata in the blockchain may enough to reveal someone's personal details. With the privacy needs of the banking sector, the transactions on the blockchain are not compatible with the banking currently due to its transparency. By using crypto-addresses only for identification is problematic as the banking secrecy must be kept by law however the blockchain is competitive with traditional regulations of banking.

In order to prevent this phenomenon becoming an obstacle, there's still many of concerns about the privacy protection that should be aware in blockchain. For example, to limit who can join the blockchain network, the definitions of trusted nodes and the permission of data encryption. Those limitation will definitely affects the transparency of the blockchain but it is an important topic on how to balance between the privacy and transparency.

Ethical:

Blockchain technology raises some ethical issues, with the two most prominent problems being

- 1) environment affects
- 2) criminal activity.

Firstly, the environment. It is ensured that blockchain is relying on raw computing power as all the encryption and calculation process need enormous amount of raw computing power to operate. It is ensuring that the blockchain could not be running without the power supply. For example, the Bitcoin Mining – consuming approximately 129 Twh per year which is higher than a country's annual electricity consumption.

The stats are mindboggling:

- In 2021, Bitcoin alone used more power than the entire country of the Norway.
- A single transaction uses as much power as a US household uses in 24 days.
- Bitcoin has the carbon footprint as Pakistan.
- Bitcoin is now responsible for 0.31 percent of the world's entire electricity usage.

It's clear that the enormous amount of power consumption is definitely not eco-friendly. It's needed to find a way to improve the efficiency and effectiveness of the transaction process to reduce the power

consumption. We will also need to think about if it is worth to harm the environment to earn the financial profits.

Secondly, even the mainstream adoption has increased nowadays, it is undeniable that the cryptocurrency like Bitcoin is more popular and common to be used in dark websites. The cybercriminals could sell weapons, drugs, personal information or any other banned items in there and using cryptocurrencies as payment because of its anonymity and transparency. It's difficult to trace the financial transactions records by using the cryptocurrencies in blockchain. It is ensured that the cryptocurrencies in blockchain are still the main payment method for illegally negotiation. For example, "WannaCry", a well-known ransomware crypto worm, is also asking the victims to pay Bitcoin as a way to retrieve their personal data back.

Social:

Blockchain has an environmental cost

As mentioned, Blockchain has an environmental cost, it is not only related to the ethical issue but also as a social issue. Blockchain relies on encryption to provide its security however it's relied on the raw computer power.

This essentially means that, in order to verify the processes of calculation, encryption and transaction of each blockchain, it requires a huge amount of computing power which may eventually bring a cost to the environment, for example to use Bitcoin as example, last year it has been calculated that the raw computing power required to keep it running in the network is as much as used by over 150 of the world countries including Netherlands, Philippines etc.

Although blockchain is a valuable network with huge potential, it brings an important consideration and the environmental implications to think about the energy consumption, as the blockchain market is growing rapidly, it is ensured different scale of blockchains and the derivatives will be developed and the power consumption will be inevitably growing. Without any supervision, it is inevitable that the blockchain technology will be harmful to the environment as the carbon footprint produced is enormous and it end up brings a lot of the social and environmental issues to the society.

The "Establishment" has a vested interest in blockchain failing

Currently, to be honest- despite the immense interest in adoption to blockchain for those fintech companies, the blockchain technology and its products are not having good comments from "the establishment" – the dominant group that controls a policy or an organization. Most of them may want the blockchain technology to be disappeared quietly.

Over the centuries, Banks have been making huge amounts of profit from representing as the middle-man role, and because the cost is distributed among their over millions of users, the users usually pay very little individually.

Banks carry huge lobbying power with governments and legislators. It's imageable that the established financial services industry could want to find ways to kill blockchain, or even it is not possible to do it but dramatically, reduce its usefulness by restricting it to be able to use in main stream and restrict its availability by restricting the way the people to use blockchain technology.

However, Charity organizations, non-profits and non-governmental organizations (NGOs) often do not Lack of technology to reach the corporate donors who are willing and able to help. Whether it is problematic to get fund to get more advanced IT devices or skills training for them to address the problem, Blockchain technology is an advanced technology that can help them to create shared system or records to reach the corporate donors and store their information without paying a huge cost.

Professional:

Lack of regulation creates a risky environment

this is a large professional issue within the value-based blockchain networks, for example, as many investors in cryptocurrencies blockchains nowadays and those blockchains become more and more valuable, without the regulations for the value-based blockchain, scams and market manipulation are commonplace. One of the most high-profile cases is onecoin – recently revealed as a ponzi scheme which is believed to have robbed millions from the investors who thought they were able to earn a huge profit by investing to the coin at the very early stage.

As with many areas of tech in recent years, legislators have largely failed to keep pace with innovators (or scammers), leading to rich pickings for those seeking to exploit “FOMO” – the “fear of missing out”.

Moreover, as an investor in blockchain, if you choose to hold your properties to the exchange or online wallet, it is inevitable that you will need to take the risk of being hacked. Or even the exchange is being shut down or the properties you have invested is a scam. as lack of regulatory oversight, you will not have any compensation and there's not action you can take in order to get back your properties.

Furthermore, its complexity means end users find it hard to appreciate the benefits

Although its potentially revolutionary applications are apparent once one has made the effort to understand how the blockchain technology and its special characteristics can benefit to the world and bring the immense amount of profit, it just takes a while, or even quite long time for the general public to understand what makes blockchains potentially so useful. Tech pundits talk about replacing the middle-man facilities traditionally provided by the financial services industry – such as clearing

payments and fraud prevention. But as far as many are concerned, banks provide this service adequately well, at an apparently low cost to the end user.

5. Architecture and Design

5.1 Use-cases and functional requirement

Below are the functional requirements for the anti-counterfeit system, due to the time restriction and the limitation of the knowledge to the system, there are some of the requirements which may enhance the functionality of the system have not been added. However, they would be added to any future development of the project.

5.1.1 Functional requirements:

Core:

- The user should be able to add the product items
- The user should be able to add the product to the blockchain
- Each user and the product should have their own address
- The manufacturer of the product should have its own address
- the product should be able to store the transaction records
- the product should be a QR code for users to identify whether it is real or fake by confirming its address

Desirable:

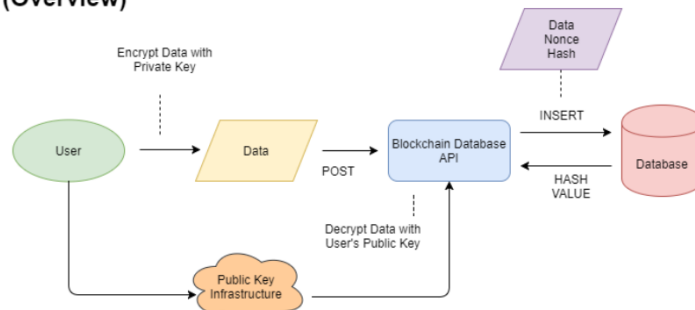
- the user will be able to view the location of the product.
- The system will be able to display whether the product is fake or real (by comparing the manufacturer address and the original address)

5.1.2 Non-functional Requirements

- Documentation – there should be appropriate documentation or video guide for the system
- Performance – system must be responsive to user's actions
- Privacy – the data should not be shared to any third party, or it would be better to be encrypted
- Security – ensure there is no any malicious code in the system
- Usability – the system should be user-friendly such as to provide a console for user to input the commands.

5.2 Database based on blockchain's Data Architecture

Database based on Blockchain's Data Architecture (Overview)



In the blockchain database, is a combination of traditional database and distributed database where data is transacted and recorded via Database Interface (also known as Compute Interface) supported by multiple-layers of blockchains. The database itself is shared in the form of an encrypted/immutable ledger which makes the information open for everyone. And the blockchain database meets the CIA triad fundamental.

When the transaction has been made by the user, the data will be encrypted by user's private key and transfer to the blockchain Database API. then the blockchain Database API will decrypt the user data with user's public key. User' identity can be verified during this process. And the above processes achieve the objectives of confidentiality and accountability.

After that, the Data Nonce hash value will be generated and assign to the transaction. The blockchain API insert the data & transaction to the database and the database will re-verify the hash value each time a new transaction has been inserted. Therefore, by comparing the previous hash and the new hash value, the database can be able to detect if any change is unauthorized. And users are able to be notified by using the blockchain database API. therefore, the integrity of the data will be guaranteed.

5.2.1 Smart Contract Use Cases:



The parties involved in a transaction decide to use an options contract. It includes the preset price and pre-defined rules that have to be met in order to complete the transaction and change the ownership of the goods.



When a triggering event (e.g. an expiration date or strike price) is hit, the contract is exercised according to the coded terms.



Regulators use Blockchain to monitor the market activity and maintain the privacy of individual actors' positions.

Smart contract is the core of blockchain technology, it represents the computer codes on top of a blockchain which includes set of pre-defined rules unite the parties to interact with each other. In case those pre-defined rules are met, the agreements will be enforced automatically even without the “middleman”.

The Flow of use case:

1. The parties involved in a transaction decide to use an options contract. It includes the preset price and pre-defined rules that have to be met in order to complete the transaction and change the ownership of the goods.
2. When a triggering event (e.g., an expiration date or strike price) is hit, the contract is exercised according to the coded terms.
3. Regulators use blockchain to monitor the market activity and maintain the privacy of individual actors' positions.

6. Development Technologies

During the project development, the investigations was carried out to find out the most suitable technology and platform to develop the fake product identification system. As the blockchain technology has been developed rapidly and more and more versions of the blockchain have been developed, it is hard to define whether which platform, blockchain network or proof is best suited for the project. Anyway, the technologies that have been adopted for this project management are shown as below:

6.1 Blockchain

Blockchain – decentralized system, is essentially a distributed database of records or public ledger of all transactions or digital events that have been executed and shared among participating parties, each transaction in the public ledger is verified by consensus of a majority of the participants in the system.

One of the most important features which Blockchain has been provided is as to a set of interconnected mechanisms which generate signed transaction between peers. The transaction represents as the agreement between two participants/parties, which the transfer of physical or digital assets maybe involved. To complete a transaction task, for example there should be at least one party or participant signs the transaction, and it is distributed to its adjacent participant. Generally, Blockchain connects a set of entities which are called nodes. However, they are also called as full nodes for those nodes verify all the blockchain rules. The nodes group the transactions into blocks and they are in charge of identifying whether the transactions should be kept in the blockchain as they are valid, and also to decline or remove them if they are not.

The flow of a transaction get into the blockchain are as below:

1. A transaction is requested and authenticated.
2. A block representing that transaction is created.
3. The block is sent to every node (i.e., participant) in the network.
4. Nodes Validate the transaction and process the next action.
5. Nodes receive a reward for proof of work, typically in cryptocurrency.
6. The block is added to the existing blockchain.
7. The update is distributed across the network.
8. The transaction is complete.

6.1.2 Smart contract

A smart contract is an automatically executed contract in which the terms of the agreement between the buyer and the seller are directly written into the code line. The codes and protocols contained therein exist in a distributed, decentralized blockchain network. Code control execution, transactions can be traced and irreversible.

Smart contracts allow credible transactions and agreements between different anonymous parties without the need for central authority, legal systems, or external execution mechanisms.

Although blockchain technology is mainly considered to be the foundation of Bitcoin, its development goes far beyond the scope of supporting virtual currencies.

There are some key points of the smart contract which need to be notified:

A smart contract is an automatically executed contract, and the terms of the agreement between the buyer and the seller are directly written into the code line.

American computer scientist Nick Szabo invented a virtual currency called "Bit Gold" in 1998. He defined smart contracts as computerized transaction agreements that enforce contract terms.

Smart contracts make transactions traceable, transparent and irreversible.

In reality, smart contract use case can vary from sector to sector based on where companies are using them, for examples:

- **Digital Identity** – provides individual identity in digital assets, removes **counterfeits** and also makes KYC frictionless.
- **Financial security** – can be used for liability management, automatic payments, stock splits, dividends.
- **Trade Finance** – can be used for cross border payments, international trade.
- **Financial Service** – offer error-free services, automating many aspects.
- **Financial Data Recording** – Improves data recording, accuracy, saves reporting and auditing costs.
- **Government** – help automate operations, improves transparency and efficiency.
- **Supply Chain Management** – automates supply chain with visibility and transparency, leads to fewer frauds
- **Insurance** – automates claims and resolves disputes with proof
- **Clinical Trial** – offers cross-institutional visibility, automate data share and improves privacy
- **Escrow** – automates escrow amount, authenticates and improves trust
- **Trading Activity** – Trades can be automated without the need for intermediaries
- **Mortgage System** – Automates mortgage and fastens the process

6.1.3 Ethereum

Ethereum is a decentralized open source blockchain with smart contract functions. Ether (ETH) is the native cryptocurrency of the platform. In terms of market value, it is the second largest cryptocurrency after Bitcoin. Ethereum is the most active blockchain and also an open access to data-friendly services for everyone – there is no limitation with location and identity. It's community-based technology behind its own cryptocurrency – ETH and thousands of applications that are being used.

The characteristics of Ethereum are shown as below:

Censorship-resistant

Ethereum has not controlled by any company and government. This decentralization makes it nearly impossible to be stopped for the services and the payment receipt on the Ethereum.

Commerce guarantees

Ethereum has created a more level playing field. The customer has a built-in guarantee of security, and the funds will only change hands when you provide the content. You don't need the influence of a big company to do business.

Compatibility for the win

It is ensured that all Ethereum products are compatible by default so the companies can develop or improves each other's creation or learn from each other's success. As the results, the developers are having better experiences and they are building better products all the time.

Banking for everyone

Typically, not everyone has access to the financial service as there's a minimum requirement for the traditional financial services. However, to access Ethereum, all you need is an internet connection to use its lending, borrowing and saving services.

A more private internet

There is not necessary to provide all or even any personal details for you to use the Ethereum, Ethereum is building its economy environment to be based on value but not surveillance.

A peer-to-peer network

Ethereum allows directly move money or make agreements to someone else without any intermediary companies. It's likely a P2P network.

Like all cryptocurrencies, Ethereum operates on a blockchain network. Blockchain is a decentralized distributed public ledger in which all transactions are verified and recorded. In a sense, it is distributed, and everyone participating in the Ethereum network holds the same copy of the ledger, allowing them to see all past transactions. It is decentralized because the network is not operated or managed by any centralized entity-it is managed by all distributed ledger holders.

Blockchain transactions use cryptography to ensure network security and verify transactions. People use computers to "mine" or solve complex mathematical equations to confirm every transaction on the network and add new blocks to the blockchain that is the core of the system. Participants will be rewarded with cryptocurrency tokens. For the Ethereum system, these tokens are called Ether (ETH).

Ether can be used to buy and sell goods and services, such as Bitcoin. Its price has also risen rapidly in recent years, making it a de facto speculative investment. But the unique feature of Ethereum is that users can build applications that "run" on the blockchain, just like software "runs" on a computer. These applications can store and transmit personal data or process complex financial transactions.

"The difference between Ethereum and Bitcoin is that the network can use computing as part of the mining process," said Ken Fromm, Director of Education and Development of Enterprise Ethereum Alliance. "This basic computing power transforms value storage and exchange media into a decentralized global computing engine and publicly verifiable data storage."

For example, from each transaction record you are able to see the below attributes:

Attribute Name	Description
Transaction Hash	A unique 66 characters identifier that is generated whenever a transaction is executed
Status	The status of the transaction (success, failed etc.)
Block	The number of the block in which the transaction was recorded. Block confirmation indicate how many blocks since the transaction is mined.
Timestamp	The Date and time at which a transaction is mined.
From	The sending party of the transaction (could be from a contract address)
To	The receiving party of the transaction (could be a contract address)
Value	The value being transacted in Ether and fiat value (for example how many Ether has been valued from this transaction and how many US Dollars they are referred to.
Transaction Fee	Amount paid to miner for processing the transaction
Gas Price	Cost per unit of gas specified for the transaction, in Ether and Gwei. The higher the gas price the higher the chance of getting included in a block.

Transaction Details	
Overview	State Comments
Transaction Hash:	0x8eadd043ea004b93b29eb62405d01276935541b922c5e22e5b220693683af9cd 🔗
Status:	Success
Block:	12491524 2 Block Confirmations
Timestamp:	35 secs ago (May-23-2021 04:02:04 PM +UTC) Confirmed within 21 secs
From:	0x18916e1a2933cb349145a280473a5de8eb6630cb (Huobi 21) 🔗
To:	0x98465371f60a67c5ccea750e48f1f06c97133124 🔗
Value:	0.013335 Ether (\$25.60)
Transaction Fee:	0.002793 Ether (\$5.36)
Gas Price:	0.000000133 Ether (133 Gwei)
Click to see More ↓	
Private Note:	To access the Private Note feature, you must be Logged In

Figure 1. – transaction details on Ethereum Blockchain Explorer

6.1.4 Solidity

Solidity is an object-oriented high-level language used to implement smart contracts. A smart contract is a program that manages the behavior of accounts in the state of Ethereum. Solidity is a curly brace language. It is influenced by C++, Python and JavaScript, and is designed to target the Ethereum Virtual Machine (EVM).

Entities are statically typed and, in addition to other functions, support inheritance, libraries, and complex user-defined types. With Solidity, you can create contracts for voting, crowdfunding, blind auctions, and multi-signature wallets.

When deploying the contract, you should use the latest version of Solidity. This is because of the regular introduction of major changes as well as new features and bug fixes. We currently use the 0.x version number to indicate this rapid rate of change.

6.1.5 Brownie

Brownie is a Python-based development and testing framework for smart contracts targeting the Ethereum Virtual Machine.

Brownie is a powerful, user-friendly framework for developing smart contracts on Ethereum. Use case includes:

Deployment: Automatically deploy many contracts on the blockchain, and any transactions required to initialize or integrate them.

Interaction: Write a script or use the console to interact with the contract on the mainnet, or perform a quick test in the local environment.

Debugging: Obtain detailed information when the transaction is restored to help you quickly identify the problem.

Test: Write unit tests in python and evaluate test coverage based on stack trace analysis. We make no promises.

Besides, Brownie has specific features that are helpful to

Full support for Solidity and Vyper

Contract testing via pytest, including trace-based coverage evaluation

Property-based and stateful testing via hypothesis

Powerful debugging tools, including python-style tracebacks and custom error strings

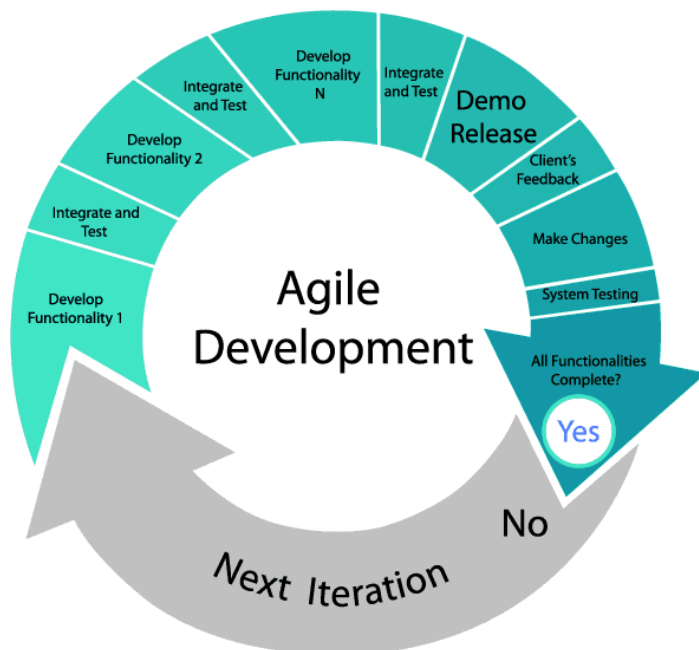
Built-in console for quick project interaction

Support for ethPM packages

7. Project Management

7.1.1 Agile Development

Agile is a term used to describe approaches to software development emphasizing incremental delivery, team collaboration, continual planning and continual learning, instead of trying to deliver it all at once near the end.



Agile development methodology has been adapted during this product development this time, as we have included the below development practices for ensuring the project is under the development cycle.

- ▶ User Story Board
- ▶ Product Vision Board
- ▶ Road Map
- ▶ Scrum Artefacts

During the development of the project, understood that it was difficult to manage the progress of the project without a suitable method. To address the problem, the project has been adapted to use a scrum board that helped to make sprint backlog item visible. The scrum board is as important as the focal point of the project as it helps for leading the direction of the project development and keeps me focused on the tasks that remain and their priorities.

By keep updating the scrum board, it is effective to review the total percentage of project completion so I can easily to review the different parts of the project such as the completed tasks, in-progress tasks and remaining tasks weekly and to adapt it to the agile development cycle – design, development, testing and deployment.

7.1.2 GITHUB

GitHub is a code hosting platform for version control and collaboration that has been adapted into this project.

the main benefit of blockchain using version control is that you can develop new features without interrupting

Version control provides a “checkpoint” function for the develop to revert their development to the save point easily, so in case there is any problem during the project development, the developers can let the system to be in normal once again by reverting it to the save point. GitHub also provides an online repository for the developers to prevent any data loss in the event of local hardware failure.

7.1.3 TRELLO

In addition to following general project management practices, the project management tool Trello was used to help with the organizational aspect of the project.

Trello gives the users a visual workflow diagram which is helpful for user to review the progression of the whole project. For example, by using the Trello, the user can be able to view the what tasks are being worked on and who took the responsibility, and whether what things will need to be reviewed and what tasks are completed.

Each sprint has its own Trello board, which included a list of completed tasks or important events in the sprint.

Each of the main tasks can be separated to multiple subtask which gives the users a better understanding of how the project is going and how to main tasks is going to be finished. To specific the progression of the tasks, users can also create the sprint boards as “In Progress” and “Completed” for understanding the status of each task easily.

7.3. TIME MANAGEMENT

Meeting with supervisor was scheduled for the Wednesday of almost every week during the past three months. Each time supervisor was asking for the progression of the project development and if there were any difficulties occurred. Although the project development may still need lots of the improvements, However as guided by the supervisor, it was very helpful for the time management of the project as we were able to know how to fix the problem during the project development and when to move to the next stage of the project to avoid being running out of time.

7.4 Usability

HCI

HCI is the study, planning and design of what happens when you and a computer work together. As it names implies, HCI consists of three parts: the user, the computer itself and the ways they work together.



Clarity

One of the cores of usability is clarity. I maintained the system's simplicity and readability has been maintained as the UI of the system is using the command line interface

As this is a blockchain-based fake product identification system so we want the user to understand what is the purpose of the system once they get into the it. So, there is nothing extra else but the system is aimed to help users to understand the product details and its transaction flow so the user can be able to let the customers to identify the anti-counterfeit.

For the color scheme, the layouts have not been designed but with dark purple as the main colors, as this color can be matched with the output fonts' colors (blue and white. These colors are not only attention-seeking, but also

being readable.

```

Transaction sent: 0xed474c04919740abcf16aedd2c0aae79c5b273dcc721c2401c790f7d2463e6c8
Gas price: 0.0 gwei Gas limit: 12000000 Nonce: 8
Reports.addUser confirmed - Block: 9 Gas used: 67469 (0.56%)

Transaction sent: 0x1422b0070b04d1963fd6e8e7b913fd7b185efd2068fc264441ccac7d424c1ebb
Gas price: 0.0 gwei Gas limit: 12000000 Nonce: 9
Reports.addUser confirmed - Block: 10 Gas used: 67481 (0.56%)

Transaction sent: 0xd1ebfef9754614518ce0d7b09100f0715af0b55782351656c39eae55f1239a96
Gas price: 0.0 gwei Gas limit: 12000000 Nonce: 10
Reports.addUser confirmed - Block: 11 Gas used: 67433 (0.56%)

Transaction sent: 0x053ff6805be94e39258a3309ee3f8572f04600ee18548522d7b25078ddaef37
Gas price: 0.0 gwei Gas limit: 12000000 Nonce: 11
Reports.addProduct confirmed - Block: 12 Gas used: 243619 (2.03%)

Transaction sent: 0x0ac52e0c0f1306c23daa3794726bbc78df32035d2df85c476b54a58ef4e6bc66
Gas price: 0.0 gwei Gas limit: 12000000 Nonce: 12
Reports.addProduct confirmed - Block: 13 Gas used: 243619 (2.03%)

Transaction sent: 0x4918293d47891d570adbc9d9e5c008a1f04169689bee7c9752b520f0e0036b69
Gas price: 0.0 gwei Gas limit: 12000000 Nonce: 13
Reports.addProduct confirmed - Block: 14 Gas used: 243619 (2.03%)

Transaction sent: 0x4ec8de33a74884e4115cc74844541220510f31881c61f600166bd94f65d0d433
Gas price: 0.0 gwei Gas limit: 12000000 Nonce: 14
Reports.getItemById confirmed - Block: 15 Gas used: 43602 (0.36%)

(True, '0001', 'shoes', 'A_manufacturer', 'A_manufacturer', 'manufacturer')
Transaction sent: 0xa9b488228a443e2a18308a4b6ed0198b17921184c95dc51c4c4654a47972e2fe
Gas price: 0.0 gwei Gas limit: 12000000 Nonce: 15
Reports.getItemById confirmed - Block: 16 Gas used: 43602 (0.36%)

(True, '0002', 'shoes', 'A_manufacturer', 'A_manufacturer', 'manufacturer')
Transaction sent: 0xbffebaa240887096928eaa2be85d6b615894eea0e1914e366962f7452f11c282
Gas price: 0.0 gwei Gas limit: 12000000 Nonce: 16
Reports.getItemById confirmed - Block: 17 Gas used: 43602 (0.36%)

```

Learnability

No matter how good is the system design, it is meaningless if the users feel difficult to operate the system. So, we understand it's important to maintain the system's learnability.

There's no such useless buttons/process in our system. We want it to be as simple as possible to use in order to improve user's experience.

For example, user can see the whole blockchain transaction and the product transaction details easily by entering the system.

Also the brownie has provided a console for user to easily run the commands for further actions and management into the blockchain and it provides a clear view for users to understand how to run the functions they need to use in the system.

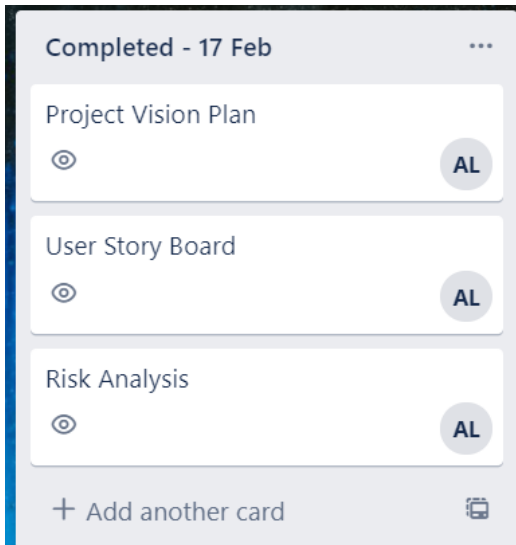
8.Sprint plan and reviews

Link For **Trello** :

<https://trello.com/b/aYZMlnkW/prco304-adam-li>

Sprint 1

Date: 17/Feb



Plan	Start date	Expected completion date	To be completed by
define the system requirements & concerns	17/2	3/3	Adam Li
The Project Management Plan	17/2	3/3	Adam Li
Study on blockchain technology	17/2	3/3	Adam Li

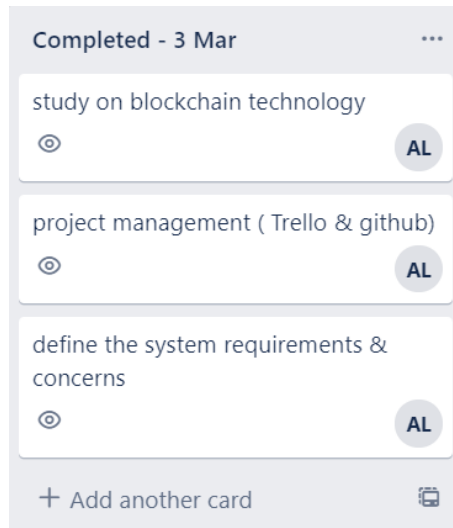
Review	Start date	Expected completion date	Status	Notes

Risk Analysis	NA	NA	completed	
Project Vision Plan	NA	NA	completed	
User Story Board	NA	NA	completed	

Sprint 2

Date:

3/Mar



Plan	Start date	Expected completion date	To be completed by

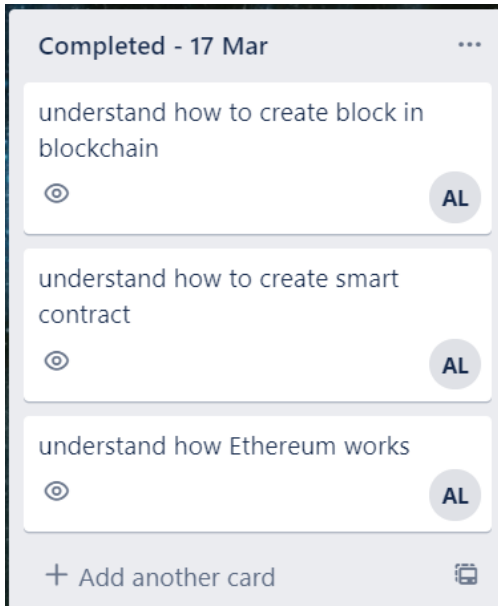
Understand how to create block in blockchain	3/3	17/3	Adam Li
Understand how to create smart contract	3/3	17/3	Adam Li
Understand how Ethereum works	3/3	17/3	Adam Li

Review	Start date	Expected completion date	Status	Notes
Define the system requirements and concerns	25/2	3/3	Completed	Completed by Adam Li
The project management plan	25/2	3/3	Completed	Completed by Adam Li
Study on blockchain technology	25/2	3/3	Completed	Completed by Adam Li

Sprint 3

Date:

17/3



Plan	Start date	Expected completion date	To be completed by
Add blockchain function Testing	17/3	24/3	Adam Li
Learn how to create own blockchain	17/3	24/3	Adam Li
Mid-term review report	17/3	24/3	Adam Li

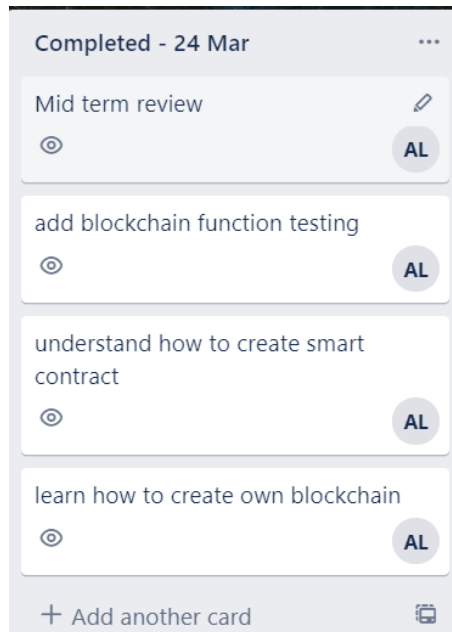
Review	Start date	Expected completion date	Status	Notes
Understand how to create block in blockchain	3/3	17/3	Completed	
Understand how to create smart contract	3/3	17/3	In-progress	It was more time-consuming than the expectation and it needed more time to understand how to

				create the smart contract.
Understand how Ethereum works	3/3	17/3	Completed	

Sprint 4

Date:

24/3



Plan	Start date	Expected completion date	To be completed by
Review block chain System Design	24/3	31/3	Adam Li
study on blockchain security	24/3	31/3	Adam Li

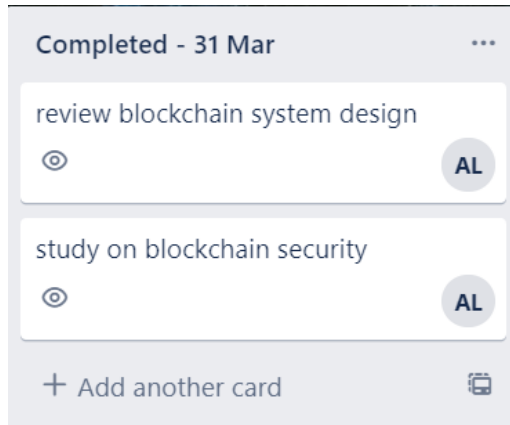
Review	Start date	Expected completion date	Status	Notes
Add blockchain function Testing	17/3	24/3	Completed	
Understand how to create smart contract	3/3	17/3	Completed	Understood how to create the smart contract
Learn how to create own blockchain	17/3	24/3	Completed	

Mid-term Review Report	17/3	24/3	Completed	
------------------------	------	------	-----------	--

Sprint 5

Date:

31/3



Plan	Start date	Expected completion date	To be completed by
Learn how to build the blockchain-based system using python	31/3	7/4	Adam Li
Product Management in blockchain	31/3	7/4	Adam Li
Understand how to use Solidity	31/3	7/4	Adam Li
Understand how to use Brownie	31/3	7/4	Adam Li

Review	Start date	Expected completion date	Status	Notes
Review block chain System Design	24/3	31/3	Completed	
study on blockchain security	24/3	31/3	In-progress	the task was in-progress at the time there are so many references to study however it didn't affect the progress of the

				project development
--	--	--	--	---------------------

Sprint 6

Date: 7/4

Completed - 7 Apr

learn how to build the blockchain-based system using python

AL

product management in blockchain

AL

understand how to use Solidity

AL

understand how to use Brownie

AL

+ Add another card

Plan	Start date	Expected completion date	To be completed by
Create Smart Contract	7/4	14/4	Adam Li
Create Ethereum blockchain	7/4	14/4	Adam Li
QR code generation function	7/4	14/4	Adam Li
Testing the transaction behavior on blockchain	7/4	14/4	Adam Li

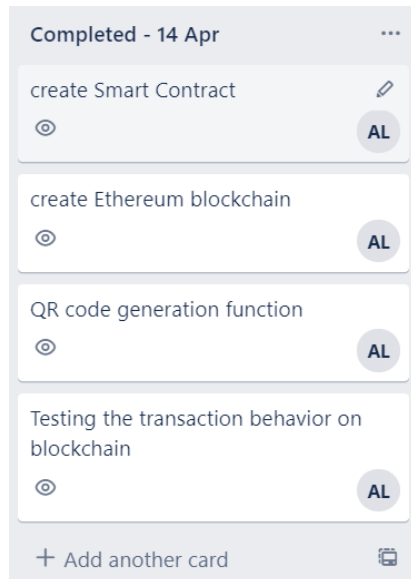
Review	Start date	Expected completion date	Status	Notes
Learn how to build the blockchain-based system using python	31/3	7/4	Completed	

Product Management in blockchain	31/3	7/4	Completed	
Understand how to use Solidity	31/3	7/4	Completed	
Understand how to use Brownie	31/3	7/4	Completed	

Sprint 7

Date:

14/4



Plan	Start date	Expected completion date	To be completed by
Review the functions and project development progress	14/4	21/4	Adam Li

Review	Start date	Expected completion date	Status	Notes
Create Smart Contract	7/4	14/4	Completed	
Create Ethereum blockchain	7/4	14/4	Completed	
QR code generation Function	7/4	14/4	In-progress	The QR code cannot be display as expectation (it will be blur or broken)

Testing the transaction behavior on blockchain	7/4	14/4	Completed	
--	-----	------	-----------	--


Sprint 8

Date:

21/4


Completed - 21 Apr

Review the functions and project development progress



AL

+ Add another card



Plan	Start date	Expected completion date	To be completed by
Add the production details into QR code	21/4	28/4	Adam Li

Review	Start date	Expected completion date	Status	Notes
Review the functions and project development progress	14/4	21/4	Completed	

Sprint 9

Date:

28/4

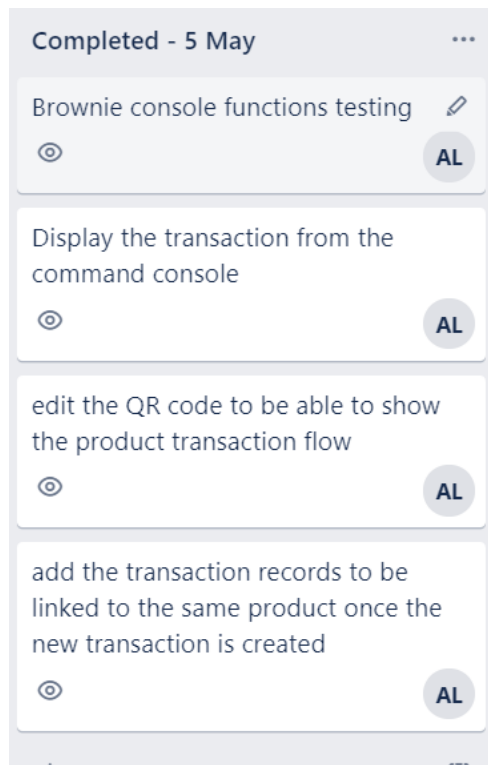


Plan	Start date	Expected completion date	To be completed by
Brownie Console functions testing	28/4	5/5	Adam Li
Display the transaction from the command console	28/4	5/5	Adam Li
Edit the QR code to be able to show the product transaction flow	28/4	5/5	Adam Li
Add the transaction records to be linked to the same product once the new transaction is created	28/4	5/5	Adam Li

Review	Start date	Expected completion date	Status	Notes
Add the production details into QR code	21/4	28/4	Completed	

Sprint 10

Date: 5/5



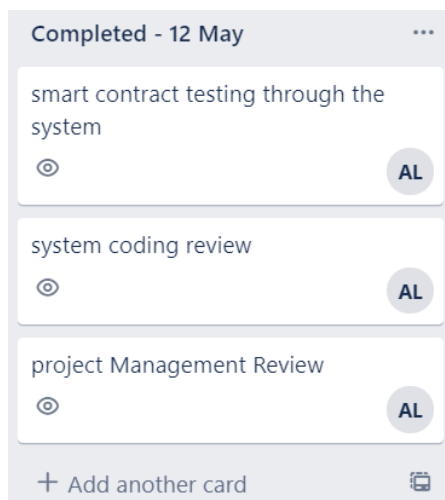
Plan	Start date	Expected completion date	To be completed by
Smart Contract Testing through the system	5/5	12/5	Adam Li
system coding Review	5/5	12/5	Adam Li
Project Management Review	5/5	12/5	Adam Li

Review	Start date	Expected completion date	Status	Notes
Brownie Console functions testing	28/4	5/5	Completed	
Display the transaction from the command console	28/4	5/5	Completed	

Edit the QR code to be able to show the product transaction flow	28/4	5/5	Completed	
Add the transaction records to be linked to the same product once the new transaction is created	28/4	5/5	Completed	

Sprint 11

Date: 12/5



Plan	Start date	Expected completion date	To be completed by
The project Report	12/5	31/5	Adam Li
Test if the transaction records can be view from the Ethereum blockchain explorer (online Ethereum blockchain)	12/5	19/5	Adam Li

Review	Start date	Expected completion date	Status	Notes
Smart Contract Testing through the system	5/5	12/5	Completed	

system coding Review	5/5	12/5	Completed	
Project Management Review	5/5	12/5	Completed	


Sprint 12

Date:

19/5


Completed - 19 May

Test if the transaction records can be view from the Ethereum blockchain explorer (online Ethereum blockchain)



AL

+ Add another card



Plan	Start date	Expected completion date	To be completed by
System Functions Review	19/5	26/5	Adam Li
Blockchain Security Features testing	19/5	26/5	Adam Li
System Design Review	19/5	26/5	Adam Li
System usability Testing	19/5	26/5	Adam Li
System Vulnerabilities checking (if any)	19/5	26/5	Adam Li

Review	Start date	Expected completion date	Status	Notes
The project Report	12/4	31/5	In-Progress	Task is in-progress and the expected date to finish is end of May
Test if the transaction records can be view from the Ethereum blockchain explorer (online	12/5	19/5	Completed	

Ethereum blockchain)				
----------------------	--	--	--	--

Sprint 13

Date:

26/5



Plan	Start date	Expected completion date	To be completed by
N/A			

Review	Start date	Expected completion date	Status	Notes

System Functions Review	19/5	26/5	Completed	
Blockchain Security Features testing	19/5	26/5	Completed	
System Design Review	19/5	26/5	Completed	
System usability Testing	19/5	26/5	Completed	
System Vulnerabilities checking (if any)	19/5	26/5	Completed	
The project Report	12/4	31/5	In-Progress	Task is in-progress and the expected date to finish is end of May

9.Overall Approach

An overall approach - used to describe the planning, methodology and tools we have adapted to bring out the deliverables.

It is important to have a good project management methodology to handle the project development in order to make sure the progress of the project can be visible so it will be easier to review and manage.

As the project has been suggested to adapt APM (agile project methodology) to break down the whole project into a small piece, so we can review each part of the project weekly to discuss with supervisor whether which part of the project need to be improved or modified. And also, it was more efficient to manage the resources, greater flexibility and adaptability to change needs. As I was able to go through the design, development, testing and deployment of the project every single week.

It is ensured that to communicate with supervisor, it's better to understand the status of the whole project development, it ended up bringing more effectiveness and efficiency for the project development and management.

As it is a personal project so it's undeniable that without a good communication, it is impossible to handle the whole project development without any mistakes and obstacles, and it is also problematic to solve all the problems by oneself.

So, we decided to have a weekly conversation to discuss about the main tasks for each part of the project and the ideas or suggestions for the project design. It was a great start for the project management as I could be able to know what should be the direction of the project and how to complete the project effectively.

It was inevitable to have difficulties during the project development, and I came across the obstacle by discussing the problem with the supervisor. Sometimes it is just impossible to solve the problem by your own as limited knowledge and due to the project requirements restriction.

However, as affected by COVID-19 we didn't have any face-to-face communication during the time of the project development so it was more difficult to fully receive the supervisor's requirements and suggestions. It took self-discipline to ensure the works is done in time with quality.

10. Difficulties Encountered

As this is the first time for me to develop a project with mainly concerned with the blockchain technology, it is inevitable that I encountered some difficulties during the project.

The first difficulty was I had no idea how to build a block-oriented system at the beginning. So, I did take a lot of time to study on how to make a blockchain system with different methods. One example was I did spend lots of time to understand how the blockchain works and its architecture. For example, what is the brownie, Solidity, Ethereum and smart contract.

However, as the more time I spent on the project development, the more I learnt how to develop the blockchain system and it helped me to develop basic functions on the blockchain system at least.

The second difficulty was to understand different features and

limitations of the blockchain technology and how to use them properly to build the own system so the development speed of the Project has been decreased for a while.

The problem has been resolved by having discussion and research more frequently, so I could gather all of the knowledge together in order to learn more about the blockchain technology and how to solve the problems I met.

The third difficulty was lack of experience with project management such as I did take times to define the goals and the plans of the project at the very beginning as I don't have any experience on how to effectively manage a blockchain-based system.

However, by using the project management tool like Trello scrum Board tool. It was helpful to let me be able to manage the project more effectively as I was able to manage the tasks by having a schedule, things-to-do board and weekly completed tasks boards.

11. Conclusions

This project set out to develop a blockchain-based fake product identification system to give user a powerful to enter the product details into the blockchain, and the blockchain will help to generate the independent address for each product so customer can identify whether the product is a counterfeit or not by verifying the original address of the product. The system used Solidity and Brownie for creating the blockchain Virtual environment and smart contract in order to meet its aims and objectives.

I am very glad that the application can be fulfill the requirements as the expectations and I think it's a good idea for me to choose blockchain as the project title as I think it's a world-changing technology which is worth to learn more about it. However as there are still lots of the improvements can be made to the system. It is ensured that additional features can be added at a later date which can improve the user experience.

Appendices

Reference List:

- [1]Blockchain Technology Beyond Bitcoin – Michael Crosby, Nachiappan, Oct 2015.
2. A systematic literature review of blockchain-based applications: Current status, classification and open issues – Fran Casino, Thomas K.Dasaklis, Constantinos Patsakis, March 2019
3. Systematic Literature review of blockchain in requisites of big data and its applications - Umair Aslam, Saad Manzor, Muhammad Imran Babar, August 2019
4. A Blockchain-Based application system for product anti-counterfeiting – Jinhua Ma, Shih-Ya Lin, Xin Chen, Hung-Min Sun, May 2020
5. Etherscan - <https://etherscan.io/>
6. A systematic literature mapping on secure identity management using blockchain technology – Tripti Rathee, Parvinder Singh, March 2021
7. What is Decentralization in Blockchain? - <https://aws.amazon.com/blockchain/decentralization-in-blockchain/>
8. The Advantages and Disadvantage of the Blockchain Technology – Julia Strebko, Andrejs Romanovs – November 2018.
9. 35 Amazing Real World Examples of How blockchain is changing our world – Bernard Marr, 2020 - <https://www.bernardmarr.com/default.asp?contentID=1302>
10. Blockchain Explained – Luke Conway, November 2020.

Mid Term Review Report

Aim and Objectives

This project is aimed to develop a fake electronic product identification System As found that almost every popular brand has fake manufacturers selling a counterfeit at cheaper rates nowadays. It's obvious that even the company experts may not be able to recognize between the real or fake electronic products so it makes the customers lack of confidence to purchase the popular brands' electronic products from the retailers especially when the customers are buying online.

Objectives:

1. Build a Blockchain Based system to identify the fake product
2. Discover how identification system have benefited from blockchain technology
3. Discover what is the advantages for the data to be stored by using the decentralized blockchain technology.

Summary of Progress

Preliminary Study

As so far, I've done many research on the mechanism of the blockchain technology to understand how it is different with the general centralized system, for example as to use smart contract to fully disclose the information so anyone can easily prove the legitimate source of the related product and the owner's information. And it's such beneficial to an identification system as it is possible to prove whether the product is a genuine goods by using the anti-counterfeit blockchain system.

It is ensuring that there are 3 things that blockchain can do very well:

1. **Data Authentication & Verification**
2. **Smart Asset Management:**
3. **Smart Contracts:**

And 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.

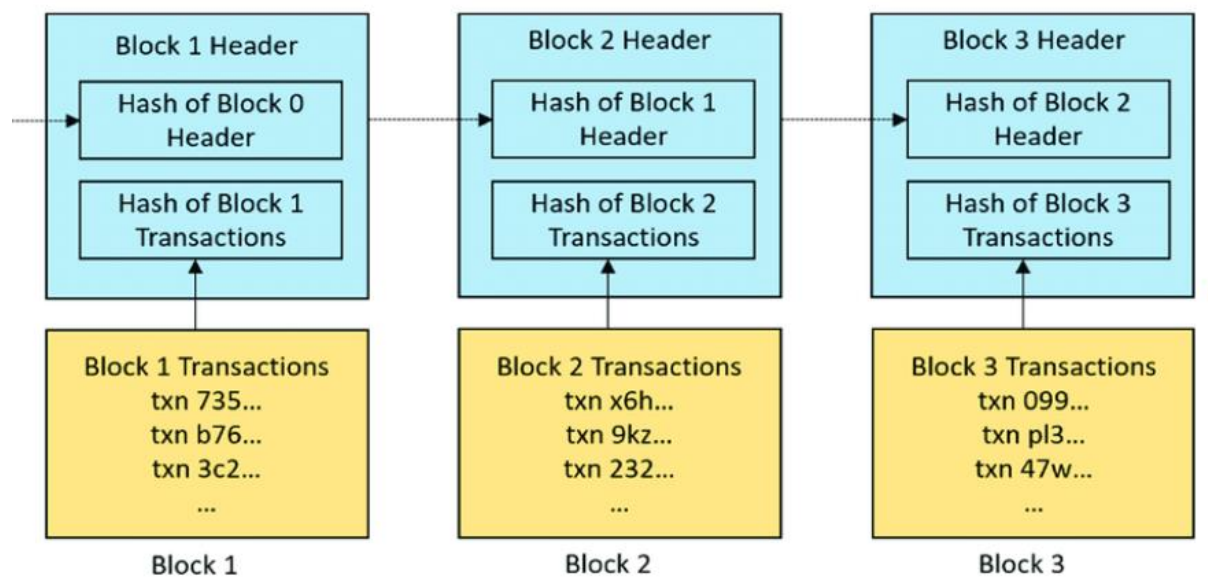


Figure1: How blocks are chained to form a blockchain

In order to build the blockchain fake product identification system, the **project setup plan** will be as follows:

1. Identify the suitable use-case
2. Identify the suitable platform (E.g Ethereum)
3. Design the Nodes/Blocks
4. Design the Blockchain
5. Design the API

As mentioned, choosing a suitable platform is also an important element for building a Blockchain system and for me it will be better to choose a more famous and popular platform for doing the project as it will be much easier to find out more information related to the platform.

Ethereum will be as a good choice as Ethereum is a Blockchain platform that can build smart contracts using a Turing-completeness programming language. Anyone can write smart contracts or other decentralized applications on Ethereum. Users can set access permissions, transaction formats, state conversion equations, and so on, and build any desired rules.

To understand more about the relationship between the blockchain and the platform, and the features of the blockchain technology (Flexibility, security and privacy, transparency, untraceability and decentralized) and its programming algorithm, it helps me to enhance the completeness of the project.

Planned Work:

So far, I've planned and working at the below works:

1. Understood how Ethereum works with the blockchain technology.
2. Understood how to build a basic node/block using python
3. Understood how to build a basic blockchain using python.
4. Understand how to create a smart contract

Vision

Blockchain is one of the most significant technological innovations, and it has grown amazingly in the past few years. A renowned blockchain application is the cryptocurrency – Bitcoin. The Blockchain technology is powerful and effective to confirm the legitimacy of transparent records without relying on a centralized system. However, it's just a tip of the iceberg for it. It is ensured that the Blockchain technology can bring a lot more advantages to the systems/applications such as tamper-proofing/tamper resistance for the contents of the data.

This project is aimed to develop a fake electronic product identification System As found that almost every popular brand has fake manufacturers selling a counterfeit at cheaper rates nowadays. It's obvious that even the company experts may not be able to recognize between the real or fake electronic products so it makes the customers lack of confidence to purchase the popular brands' electronic products from the

retailers especially when the customers are buying online.

In this way, this phenomenon makes me think what if there's a decentralized Blockchain system with products anti-counterfeiting? in that way manufacturers can use this system to provide genuine electronic products without having to manage direct-operated stores, which can significantly reduce the cost of product quality assurance. And the customers can easily distinguish between fake ones and real ones by using the system and it is beneficial for both the buyers and the sellers as the buyer-seller relationship has been improved as the customers will have the ability to identify if it's a counterfeit.

To achieve this, What if the system can offer a digital signature or embedded barcode which is tied to a blockchain system? So both the manufacturers and customers can rely on the embedded barcode or digital to help identify whether the product is fake or not. And it will be more user-friendly if the system can be used on the mobile devices.

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 Project is not only focused building a anti-counterfeiting system but also to explore the characteristic of the Blockchain (for example: Security and Privacy, Decentralization, Untraceability, Flexibility & Transparency) and understand how these characteristic make Blockchain becomes a disruptive technology and how it helps the industries.

RISK PLAN:

Estimating Error - the actions/behaviours to achieve the project goals or project parts do not work as expected / the expected actions/behaviours actually can't achieve the project goals.

for example: the programming cannot achieve the expected functions.

Schedule Error: the scheduled tasks are spending much more time which is out of the expectation

for example: scheduled to finish task A within a week, but ended up finishing the tasks by three weeks etc....

lack of references resources for the project E.g. different electronic products for testing.

Deadlock to the technology implementation

Meeting capture screens:

