**Batch-17(SEC-3B)**

**FAKE PRODUCT IDENTIFICATION USING BLOCKCHAIN TECHNOLOGY**

Submitted in partial fulfilment of the requirements for the award of the degree of

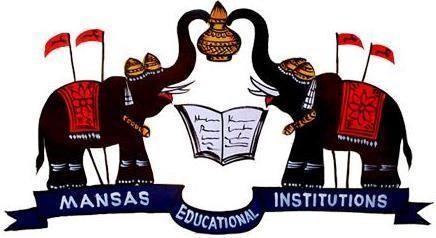
**Bachelor of Technology**

in

### **COMPUTER SCIENCE AND ENGINEERING**

#### BY

|  |  |
| --- | --- |
| **K. JYOTHSNA** |  |
| **20331A0582** |  |
| **I.SWATHI**  **20331A0572** | **N. SUSEEL KALYAN**  **20331A05C4** |
| **L.SRINIVAS**  **20331A0599** | **L.DHANUSH**  **20331A05A0** |
|  |  |



**DEPARTMENT OF COMPUTER SCIENCE AND ENGINEERING**

## MVGR COLLEGE OF ENGINEERING (Autonomous)

### **VIZIANAGARAM-535005, AP (INDIA)**

**(Accredited by NBA, NAAC, and Permanently Affiliated to Jawaharlal Nehru Technological University Kakinada)**

**2022-2023**

**Maharaj Vijayaram Gajapathi Raj (MVGR) College of Engineering (Autonomous)**

**Vizianagaram**

# **CERTIFICATE**

A picture containing text, clipart

Description automatically generated

This is to certify that the project report entitled “**FAKE PRODUCT IDENTIFICATION USING BLOCKCHAIN TECHNOLOGY”** being submitted by **K.Jyothsna,L.Srinivas,I.Swathi,N.Suseel Kalyan,L.Dhanush** bearing registered numbers **20331A0582, 20331A0599, 20331A0572, 20331A05C4,20331A05A0** respectively, in partial fulfillment for the award of the degree of “**Bachelor of Technology” in Computer Science and Engineering** is a record of bonafide work done by them under my supervision during the academic year 2022-2023.

#### 

#### 

**Dr P. Ravi Kiran Varma Mrs.K.Vindhya Rani**

**Head of the Department Assistant Professor**

**Dept. of CSE Dept. of CSE**

**Pg 2**

**ABSTRACT:**

In recent years, Counterfeiters create serious problems for authentic businesses and product manufacturing industries. This affects the companies name, sales, and profit of the companies. A company with a ledger developed by using blockchain can detect fake products and transfer the ownership of the real products through a safe and secured system. Our system also manages ownership of products.

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

Blockchain technology is the distributed, decentralized, and digital ledger that stores transactional information in the form of blocks in many databases which is connected with the chains. Blockchain technology is secure technology therefore any block cannot be changed or hacked. By using Blockchain technology, customers or users do not need to rely on third-party users for confirmation of product safety.

**Pg 3**

**TABLE OF CONTENTS**

**CHAPTER PG-NO**

**1. INTRODUCTION 5**

**2. REQUIREMENTS 13**

**3. IMPLEMENTATION 14**

**4. OUTPUTS 17**

**5. CONCLUSION 24**

**6. PROJECT OUTCOME 25**

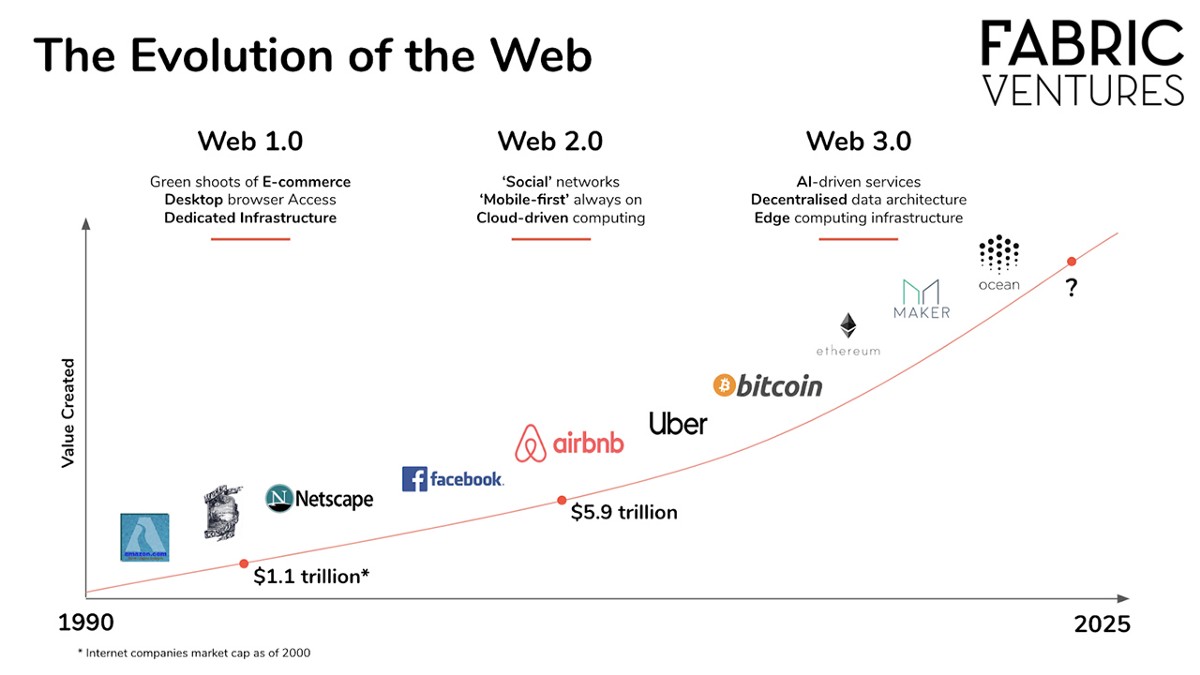
**REFERENCES 26**

**Pg 4**

**1.INTRODUCTION:**

Web 3.0 (Web3) is the third generation of the evolution of web technologies.

* Web 3.0 is a possible future version of the internet based on public blockchains, a record-keeping system best known for facilitating cryptocurrency transactions. The attractiveness of Web 3.0 is that it is decentralized, meaning that rather than consumers accessing the internet through services mediated by companies.



* With the Peer-to-Peer networks that secure the Ethereum blockchain rather than centralized servers, bad actors will not have the same ability to disrupt Internet services as easily as they can now. There will no longer be single points of failure, allowing the network to function as normal regardless of participants being attacked.



**Pg 5**

**BLOCKCHAIN: THE NEW ERA OF TECHNOLOGY**

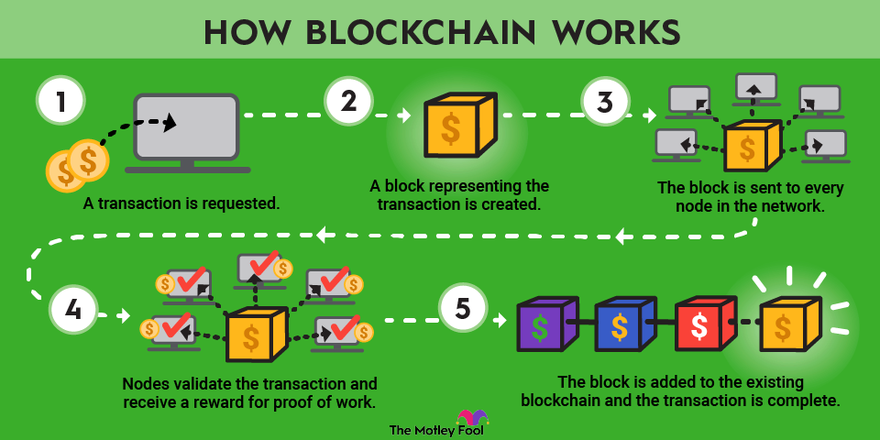


* **Satoshi Nakamoto** is the name used by the presumed [pseudonymous](https://en.wikipedia.org/wiki/Pseudonym) person or persons who developed [bitcoin](https://en.wikipedia.org/wiki/Bitcoin), authored the bitcoin [white paper](https://en.wikipedia.org/wiki/White_paper), and created and deployed bitcoin's original [reference implementation](https://en.wikipedia.org/wiki/Reference_implementation). As part of the implementation, Nakamoto also devised the first [blockchain](https://en.wikipedia.org/wiki/Blockchain) database.
* A blockchain is a distributed database or ledger that is shared among the nodes of a computer network. As a database, a blockchain stores information electronically in digital format. Blockchains are best known for their crucial role in cryptocurrency systems, such as [Bitcoin](https://www.investopedia.com/terms/b/bitcoin.asp), for maintaining a secure and decentralized record of transactions. The innovation with a blockchain is that it guarantees the fidelity and security of a record of data and generates trust without the need for a trusted third party.
* As new data comes in, it is entered into a fresh block. Once the block is filled with data, it is chained onto the previous block, which makes the data chained together in chronological order.
* Decentralized blockchains are immutable, which means that the data entered is irreversible.

Popularized by its association with cryptocurrency and [NFTs](https://builtin.com/blockchain/non-fungible-token-nft), blockchain technology has since evolved to become a management solution for [all types of global industries](https://builtin.com/blockchain/blockchain-companies-roundup). Today, you **Pg 6**

can find blockchain technology [providing transparency for the foodsupply chain](https://builtin.com/blockchain/food-safety-supply-chain), [securing healthcare data](https://builtin.com/blockchain/blockchain-healthcare-applications-companies), [innovating gaming](https://builtin.com/blockchain/gaming-video-games-esports) and overall changing how we handle data and ownership on a large scale.

**KEY TERMS OF BLOCKCHAIN:**



* **CRYPTOGRAPHY:**

[Cryptography](https://www.geeksforgeeks.org/cryptography-and-its-types/) is a technique or a set of protocols that secure information from any third party during a process of communication. It is also made up of two Greek terms, Kryptos term meaning “hidden” and Graphein, a term meaning “to write”. Some terminologies related to Cryptography:

**Encryption:**Conversion of normal text to a random sequence of bits.

**Key:**Some amount of information is required to get the information of the cryptographic algorithm.

**Decryption:**The inverse process of encryption, conversion of a Random sequence of bits to plaintext.

**Cipher:**The mathematical function, i.e. a cryptographic algorithm which is used to convert plaintext to ciphertext(Random sequence of bits).

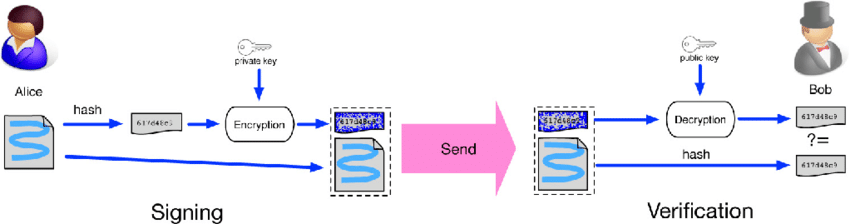
* **DIGITAL SIGNATURE:**

**Digital Signing in Blockchain** is a process to verify the user’s impressions of the transaction. It uses the private key to sign the digital transaction, and its corresponding public key will help to authorize the sender.

**Pg 7**

However, in this way, anyone with the sender’s public key can easily decrypt the document. Digital Signing targets the authenticity, not the security of the document. It’s a **way to ensure the source of the message transaction**. Keep this point noted for now.

Remember, here private key encrypts the message, and the public key decrypts the message.

****

* **NODES :**

Blockchain nodes are the moderators that build the infrastructure of a decentralized network. Their primary function is to maintain consensus of a blockchain’s public ledger, which varies from one type of node to the next.

“On the most basic level, a node is simply a device running the software of a specific blockchain”.

* **HASHING:**

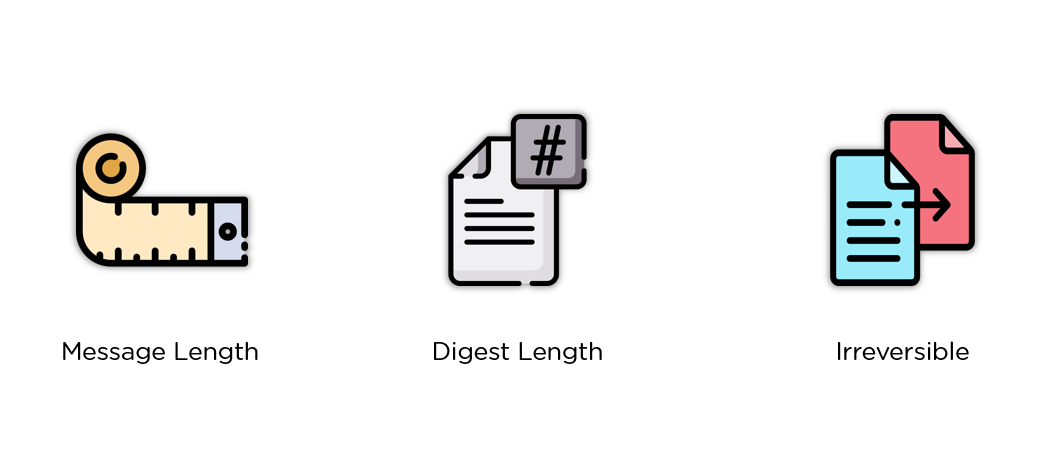
A hash is a mathematical function that converts an input of arbitrary length into an encrypted output of a fixed length. Thus regardless of the original amount of data or file size involved, its unique hash will always be the same size. Moreover, hashes cannot be used to "reverse-engineer" the input from the hashed output, since hash functions are "one-way" (like a meat grinder; you can't put the ground beef back into a steak). Still, if you use such a function on the same data, its hash will be identical, so you can validate that the data is the same (i.e., unaltered) if you already know its hash.

**Pg 8**

* **SECURE HASHING ALGORITHM:**

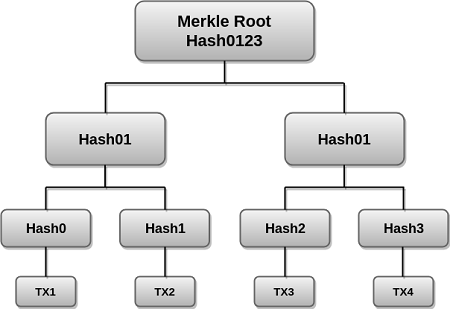
The family of SHA comprises four SHA algorithms: SHA-0, [SHA-1](https://www.geeksforgeeks.org/sha-1-hash-in-java/), [SHA-2](https://www.geeksforgeeks.org/difference-between-sha1-and-sha2/), and [SHA-3](https://www.geeksforgeeks.org/sha3-in-python/).

* SHA-0 is a 160-bit hash function that was published by the National Institute of Standards and Technology in 1993..
* SHA-256 is the most famous of all cryptographic hash functions because it’s used extensively in blockchain technology. The SHA-256 Hashing algorithm was developed by the National Security Agency (NSA) in 2001.



# **MERKLE TREE**

Merkle tree is a fundamental part of blockchain technology. It is a mathematical **data structure** composed of hashes of different blocks of data, and which serves as a summary of all the transactions in a block. It also allows for efficient and secure verification of content in a large body of data. It also helps to verify the consistency and content of the data. Both Bitcoin and Ethereum use Merkle Trees structure. Merkle Tree is also known as **Hash Tree**.

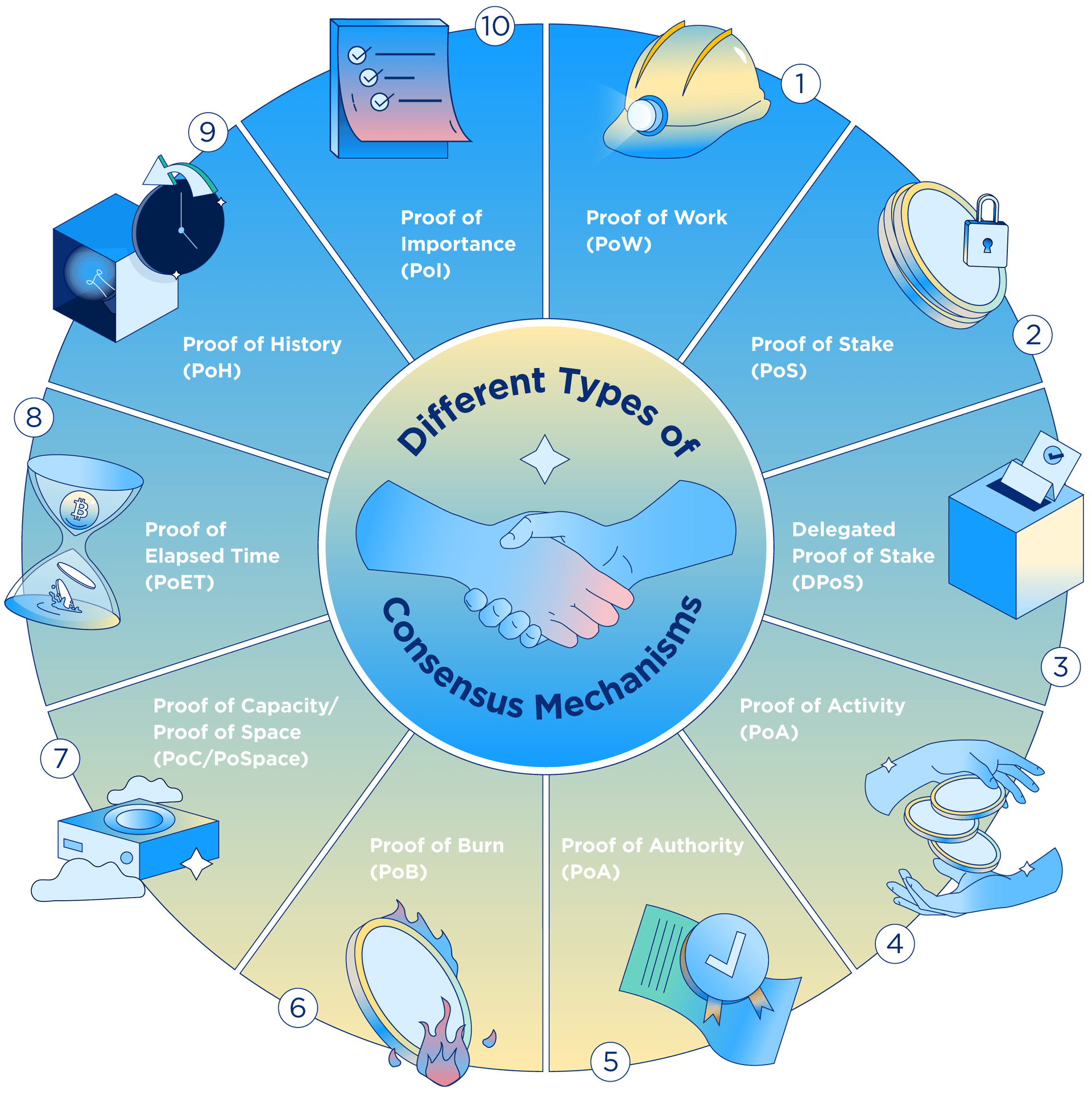


**Pg 9**

**CONSENSUS ALGORITHM:**

A consensus algorithm is a procedure that allows each peer of the blockchain network to set a shared agreement about the state of the decentralized ledger. In other words, The consensus algorithm is a protocol using which all the nodes in the blockchain network come to a common consensus (agreement) on the current data state in the ledger and can trust unknown peers in the network.

The consensus algorithm or mechanism is designed to acquire reliability in a network that consists of nodes or multiple users. So, consensus algorithms allow blockchain to achieve reliability and trust among nodes while ensuring security in the network environment. It is useful when it comes to record-keeping.



* **PROOF OF WORK:**

The Proof of Work consensus algorithm involves solving a computationally challenging puzzle in order to create new blocks in the Bitcoin blockchain. The process is known as ‘mining’, and the nodes in the network that engages in mining are known as ‘miners’.

The **purpose** of a consensus mechanism is to bring all the nodes in agreement, that is, trust one another, in an environment where the nodes don’t trust each other.

* All the transactions in the new block are then validated and the new block is then added to the blockchain.

**Pg 10**

* Miners(special computers on the network) perform computation work in solving a complex mathematical problem to add the block to the network, hence named, Proof-of-Work.
* **SMART CONTRACT**:

A Smart Contract (or cryptocontract) is a computer program that directly automatically controls the transfer of digital assets between the parties under certain conditions. A smart contract works in the same way as a traditional contract while also automatically enforcing the contract. Smart contracts are programs that execute exactly as they are set up(coded, programmed) by their creators. Just like a traditional contract is enforceable by law, smart contracts are enforceable by code.

* **HYPERLEDGER:**

Hyperledger is an open source project created to support the development of blockchain-based distributed ledgers. Hyperledger consists of a collaborative effort to create the needed frameworks, standards, tools and libraries to build [blockchains](https://www.techtarget.com/searchcio/definition/blockchain) and related applications.

* **NFT:**

Non-fungible tokens, often referred to as NFTs, are **blockchain-based tokens that each represent a unique asset like a piece of art, digital content, or media**. An NFT can be thought of as an irrevocable digital certificate of ownership and authenticity for a given asset, whether digital or physical.

**FAKE PRODUCTION IDENTIFICATION USING BLOCKCHAIN TECHNOLOGY**

* The idea of this project came into existence because of the increase in the counterfeit products. The objectives of this project are:

1.To Design Anti Counterfeit System using Blockchain.

2.To secure product details using a QR code.

3. Provide security to the clients by offering data to client.

**Pg 11**

* In this project, customer selects a product among the products displayed in the web page and pays to get ownership on it (buying from us) then we add a new transaction to blockchain stating the transfer of ownership
* In the proposed system QR code is generated for a particular product. Customers scan the QR code on the product or package using the smartphone’s QR code reader application or customer application have the option of QR code scanner. After scanning, we get the result of the product is real or fake. In the end, the Blockchain system holds these product details along with a history of transactions to enable the tracking of the product along the distribution chain. All the product details, block name, a hash value is stored in the blockchain.
* We can nodes and users to our blockchain at any time. There is a single blockchain that stores all the transactions. Each blockchain has several blocks and each transaction has several transactions. Each transaction consists of following details:

1. Date and time
2. Seller name and sender ID
3. Recipient name and recipient ID
4. Product name and product ID
5. Price

**Pg 12**

**2. REQUIREMENTS:**

**SOFTWARE REQUIREMENTS:**

* Spyder



**Spyder** is an [open-source](https://en.wikipedia.org/wiki/Open-source_software) cross-platform [integrated development environment](https://en.wikipedia.org/wiki/Integrated_development_environment) (IDE) for scientific programming in the [Python language](https://en.wikipedia.org/wiki/Python_(programming_language)). Spyder integrates with a number of prominent packages in the scientific Python.

**Pg 12**

* Postman API

Postman is a standalone software testing API (Application Programming Interface) platform to build, test, design, modify, and document APIs. It is a simple Graphic User Interface for sending and viewing HTTP requests and responses.



* Windows7 or higher
* Web Technologies-html,css,flask



**HARDWARE REQUIREMENTS:**

* 1GB RAM
* Diskspace 10GB

**Pg 13**

**3. IMPLEMENTATION**

**METHODOLOGY:** System is maintaining Status of product i.e., Manufacturer of product, current owner of product, and history of owners, time stamp i.e., at what time product was updated and a QR code.

**Stage 1**: **Product Enrollment Process:** Initially manufacturer will be the first owner of product. So, manufacturer will request administrator to add product on the network, at that time QR code will be generated. Administrator will enroll product and manufacturer on the network, and QR code is taken.

**Stage 2: Ship Product to Distributor:** In the next step manufacturer will ship the product to distributor. When distributor receives product will scan the QR code and update his details on the network, about product ownership, time Stamp and date.

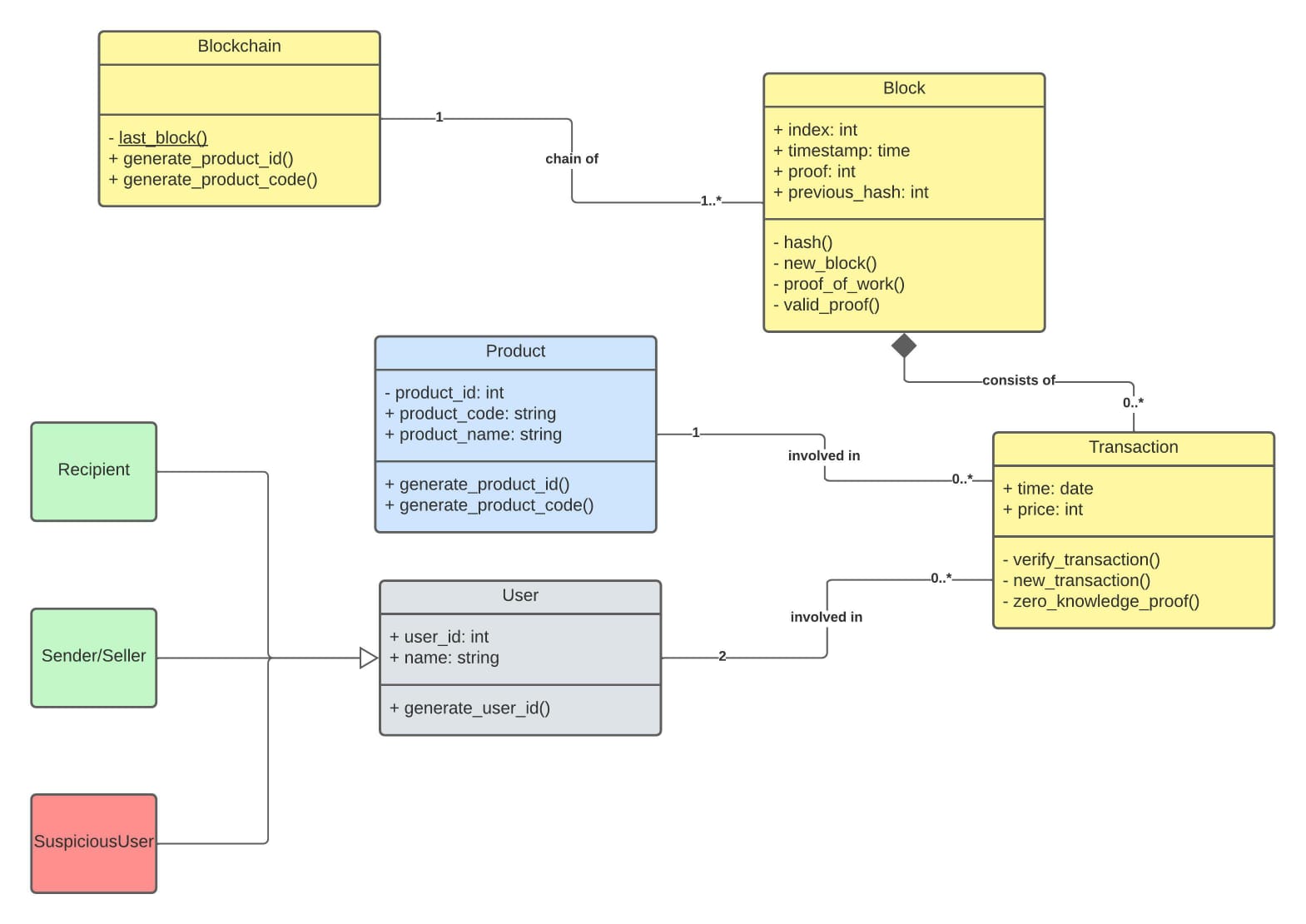
**Stage 3: Ship Product to Retailer:** At this Stage, the retailer receives product from Distributor and scan QR code assigned to product using QR code scanner, and will update owner details of the product on the network.

**Stage 4: End User Authentication Process:** At the end of the chain, customer will take the product, go to website and upload QR code over there, and customer will able to get all detail about product from manufacture to last retailer. And after getting details, it his question where to buy the product or not.

**UML DIAGRAM OF CLASSES USED:**

A UML diagram is a diagram based on the UML (Unified Modelling Language) with the purpose of visually representing a system along with its main actors, roles, actions, artifacts or classes, in order to better understand, alter, maintain, or document information about the system.

**Pg 14**

**INTERNAL CODE IMPLEMENTATION USING BLOCKCHAIN:**

Remember that a blockchain is an immutable, sequential chain of records called Blocks. They can contain transactions, files or any data you like. But the important thing is that they’re chained together using hashes.

**Building a Blockchain**

**Representing a Blockchain: The blueprint of blockchain class is depicted as:**

class Blockchain(object):

def \_\_init\_\_(self):

self.chain = []

self.current\_transactions = []

def new\_block(self):

# Creates a new Block and adds it to the chain

pass

def new\_transaction(self):

# Adds a new transaction to the list of transactions

pass

@staticmethod

def hash(block):

# Hashes a Block

pass

@property

def last\_block(self):

# Returns the last Block in the chain

pass

**Pg 15**

**What does a Block look like?**

Each Block has an index*,* atimestamp (in Unix time), a list of transactions, aproof (more on that later), and the hash of the previous Block.

block = {

'index': 1,

'timestamp': 1506057125.900785,

'transactions': [

{

'sender': "8527147fe1f5426f9dd545de4b27ee00",

'recipient': "a77f5cdfa2934df3954a5c7c7da5df1f",

'amount': 5,

}

],

'proof': 324984774000,

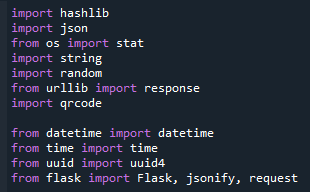
'previous\_hash': "2cf24dba5fb0a30e26e83b2ac5b9e29e1b161e5c1fa7425e73043362938b9824"

}

At this point, the idea of a chain should be apparent—each new block contains within itself, the hash of the previous Block. **This is crucial because it’s what gives blockchains immutability:** If an attacker corrupted an earlier Block in the chain then all subsequent blocks will contain incorrect hashes.

Make sure that [Python 3.6](https://www.python.org/downloads/?ref=hackernoon.com)+ (along with pip) is installed. You’ll also need to install Flask and the also other libraries.

Open up your favourite editor (here,Spyder). Create a new file, called blockchain.py.



pip install Flask==0.12.2 requests==2.18.4

**Pg 16**

## Interacting with our Blockchain

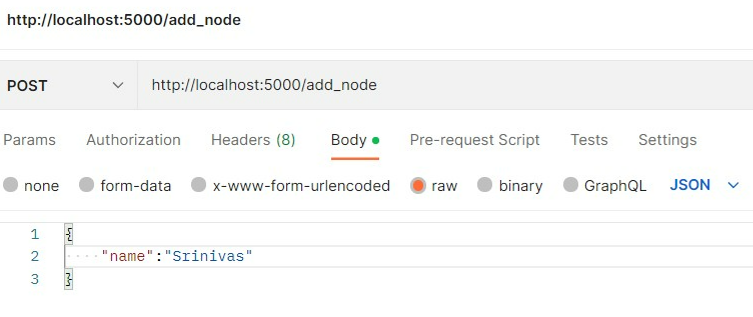
You can use Postman to interact with our Blockchain over a network.

$ python blockchain.py

\* Running on http://127.0.0.1:5000/ (Press CTRL+C to quit)

* Add node to blockchain:

When our Blockchain is instantiated we’ll need to seed it with a *genesis* block—a block with no predecessors. We’ll also need to add a “proof” to our genesis block which is the result of mining (or proof of work).

****

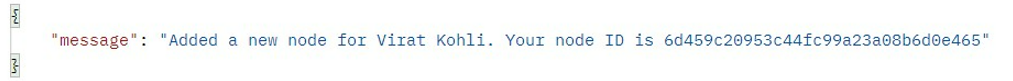
We’ve got a basic Blockchain that accepts transactions and allows us to mine new Blocks. But the whole point of Blockchains is that they should be decentralized*.* And if they’re decentralized, how on earth do we ensure that they all reflect the same chain? This is called the problem of Consensus*,* and we’ll have to implement a Consensus Algorithm if we want more than one node in our network.

****

**Output:**

****

**Pg 17**

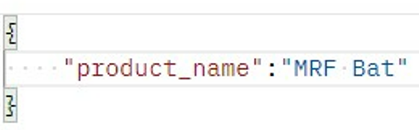
****

**The user list displayed from the added nodes are:**

****

**Pg 17**

* **Adding Products to Block**

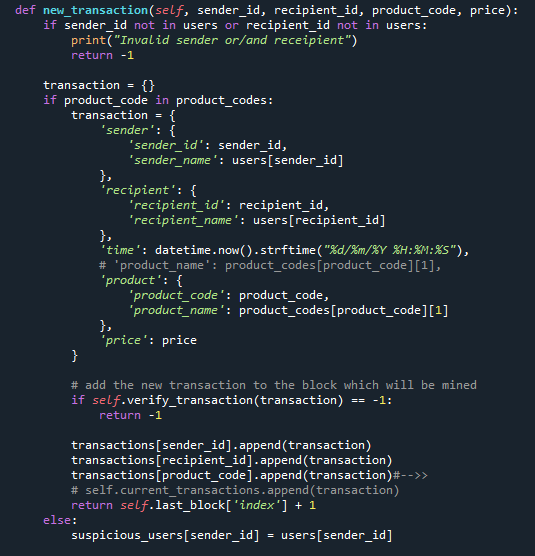




* **Get transaction:**

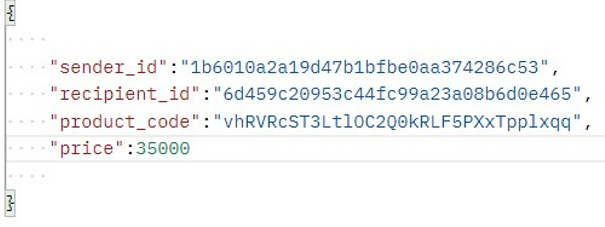
We’ll need a way of adding transactions to a Block. Create a new transaction by making a POST request to http://localhost:5000/transactions/new.

**Pg 18**



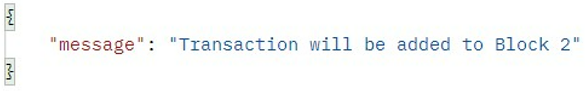
**Pg 18**



****

**Pg 19**

****

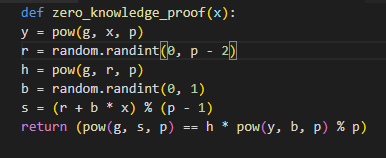
****

After new\_transaction() adds a transaction to the list, it returns the *index* of the block which the transaction will be added to—*the next one to be mined.* This will be useful later on, to the user submitting the transaction.

**Understanding Proof of Work**

A Proof of Work algorithm (PoW) is how new Blocks are created or *mined*on the blockchain*.*The goal of PoW is to discover a number which solves a problem. The number must be difficult to find but easy to verify—computationally speaking—by anyone on the network. This is the core idea behind Proof of Work.

**Pg 19**



* **Mining the block:**

Let’s try mining a block by making a GET request to

<http://localhost:5000/mine>:

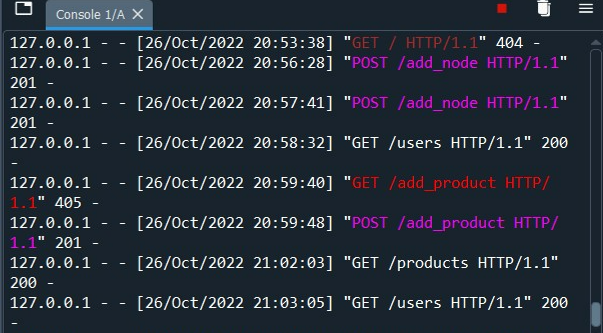
|  |
| --- |
| **Pg 20** |
|  |
|  |
|  |
|  |
|  |
|  |
|  |
|  |
|  |
|  |
|  |
|  |
|  |
|  |
|  |
|  |
|  |
|  |  |

****

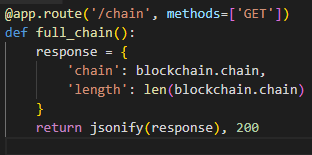
**The Mining Endpoint:** Our mining endpoint is where the magic happens, and it’s easy. It has to do three things:

* Calculate the Proof of Work
* Reward the miner (us) by adding a transaction granting us 1 coin
* Forge the new Block by adding it to the chain

**Pg 21**

****

* **Final chain**

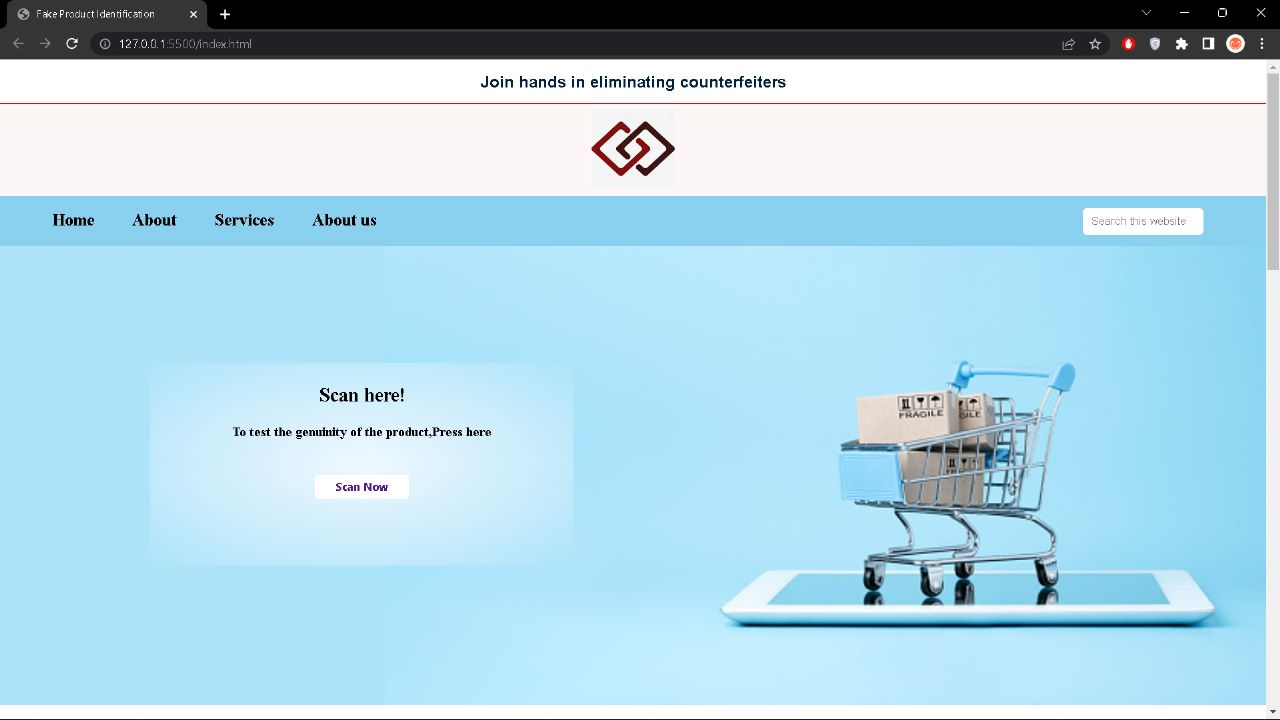
****

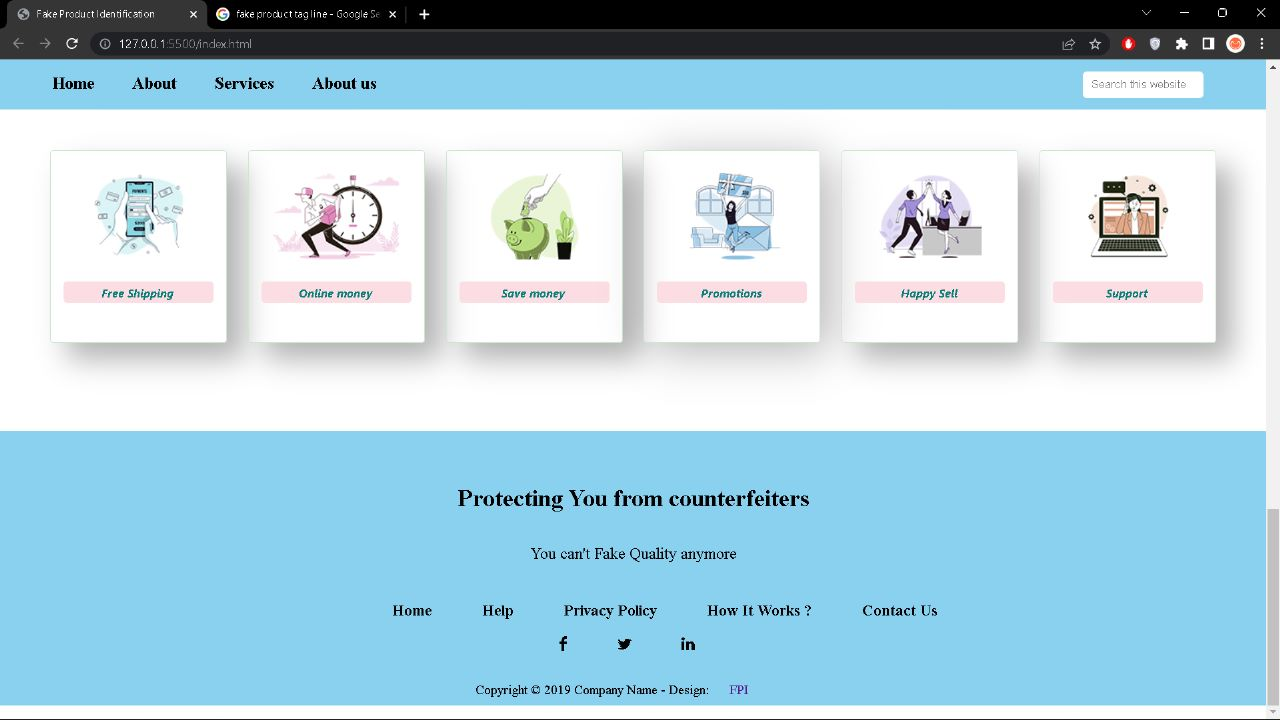
****

**Pg 22**

**FUTURE IMPLEMENTATION:**

This project can be practised in reality using front end technologies so that customer can easily scan the product’s QR CODE and test its genuinity via company’s website.

****

****

**Pg 23**

**5. CONCLUSION:**

This project allows both manufacturers and suppliers to interact with the system to add their respective block containing the transaction details to blockchain without modifying other’s block. Blockchain is a decentralized system, therefore the local suppliers cannot interfere with the checking or counterfeiting of the product in the proposed system. Manufacturers and Suppliers can use the system to store product details in Blockchain which adds certain properties such as data consistency and confidentiality that assure the security and privacy of the data on the network. The customer views the product supply chain history and verifies if the product is genuine. Customers can be sure about the integrity of goods they purchase. The proposed system can effectively lower the rate of counterfeiting of branded goods and provide the companies with an easier approach to provide consumers with the confidence that they will not purchase counterfeit goods. This system will help to build trust and good bonding between manufacturer and customer and indeed it will help in improving economy and reducing corruption

**Pg 24**

**6. PROJECT OUTCOMES**

✓ From this project, we have learnt that how can we identify the problem of fake products and how can we help in tackling and giving a solution to this day-to-day problem using blockchain technology.

✓ There might be many solutions to a problem but choosing the optimum solution is possible through blockchain which is more secure,trustworthy,immutable.

✓ From this project, we have learnt how to improve our presentation skills, how to make an effective presentation and even learnt how to present our thoughts and implementation through this.

✓ From this project, team management skills improvised a lot, each one of us enthusiastically took each part of theirs and worked on it. We learnt how coordination can help make a bigger problem into a smaller problem and each person was the leader of the team in their way.

✓ From this project, communication skills have got better and how to represent ourselves in front of a crowd improved, communicating among ourselves also helped in making our work easier.

✓ From this project, we have learnt to use various python modules and interacting with blockchain using postman API.

✓ Finally, this project helped us in learning new skills, helped us to think out of the box, improve our thoughts towards society and how to take up a problem from our daily life and put some work on it to give a minimal solution which would positively benefit the society.

**Pg 25**

**REFERENCES:**

[**https://www.tutorialspoint.com/python\_blockchain/index.htm**](https://www.tutorialspoint.com/python_blockchain/index.htm)

[**https://ijariie.com/AdminUploadPdf/Fake\_Product\_Detection\_Using\_Blockchain\_Technology\_ijariie14881.pdf**](https://ijariie.com/AdminUploadPdf/Fake_Product_Detection_Using_Blockchain_Technology_ijariie14881.pdf)

[**https://ijarcce.com/papers/fake-product-detection-using-blockchain-technology/**](https://ijarcce.com/papers/fake-product-detection-using-blockchain-technology/)

**Pg 26**