

Project Synopsis
on
**Product Authentication
using Blockchain**

Submitted as a part of course curriculum for

Bachelor of Technology
in
Computer Science



Submitted by

Abhishek Singh Yadav (2000290120011)

Aditi Batra (2000290120012)

Anurag Tripathi (2000290120036)

Kshitij Pal (2000290310092)

Under the Supervision of

Prof. Shivani

Assistant Professor

KIET Group of Institutions, Ghaziabad
Department of Computer Science
Dr. A.P.J. Abdul Kalam Technical University
2022-2023

TABLE OF CONTENTS

	Page No.
TITLE PAGE	3
DECLARATION	4
CERTIFICATE	5
ACKNOWLEDGEMENT	6
ABSTRACT	7
CHAPTER 1: INTRODUCTION	8
1.1. Introduction	
1.2. Problem Statement	
1.2. Objective	
1.3. Scope	
CHAPTER 2: LITERATURE REVIEW	10
CHAPTER 3: PROPOSED METHODOLOGY	23
3.1 Flowchart	
3.2 Algorithm Proposed	
CHAPTER 4: TECHNOLOGY USED	25
CHAPTER 6: CONCLUSION	27
REFERENCES	28

KIET GROUP OF INSTITUTIONS

MINI PROJECT

2024 BATCH, SESSION 2022-23

APPROVAL OF TITLE BY GUIDE


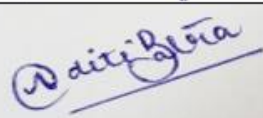
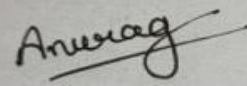
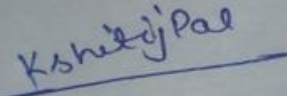
Guide Name: Prof. Ajay Kumar Shrivastava

Project ID: PCS24-12

Domain: Blockchain and Full Stack Development

Title: Product Authentication Using Blockchain



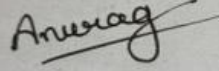
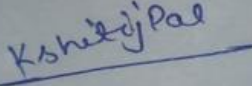
Date:

NAME	EMAIL	E-SIGN
Abhishek Singh Yadav	abhishek.2024cs1184@kiet.edu	
Aditi Batra	aditi.2024cs1002@kiet.edu	
Anurag Tripathi	anurag.2024cs1182@kiet.edu	
Kshitij Pal	kshitij.2024ec1064@kiet.edu	

Guide Sign:

DECLARATION

We hereby declare that this submission is our work and that, to the best of our knowledge and belief, it contains no material previously published or written by another person nor material which to a substantial extent has been accepted for the award of any other degree or diploma of the university or other institute of higher learning, except where due acknowledgment has been made in the text.

NAME	EMAIL	E-SIGN
Abhishek Singh Yadav	abhishek.2024cs1184@kiet.edu	
Aditi Batra	aditi.2024cs1002@kiet.edu	
Anurag Tripathi	anurag.2024cs1182@kiet.edu	
Kshitij Pal	kshitij.2024ec1064@kiet.edu	

CERTIFICATE

This is to certify that Project Report entitled “**Product Authentication using Blockchain**” which is submitted by **Abhishek Singh Yadav, Aditi Batra, Anurag Tripathi, and Kshitij Pal** in partial fulfillment of the requirement for the award of degree B. Tech. in the Department of Computer Science of Dr A.P.J. Abdul Kalam Technical University, Lucknow is a record of the candidates own work carried out by them under my supervision. The matter embodied in this report is original and has not been submitted for the award of any other degree.

Date:



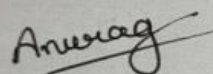
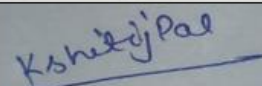
Prof. Shivani
Assistant Professor
Supervisor Signature

ACKNOWLEDGEMENT

It gives us a great sense of pleasure to present the synopsis of the B.Tech Mini Project undertaken during B.Tech. Third Year. We owe a special debt of gratitude to Prof. Ajay Kumar Shrivastava, Head of Department, Department of Computer Science, KIET Group of Institutions, Delhi- NCR, Ghaziabad, for his/her constant support and guidance throughout the course of our work. His sincerity, thoroughness, and perseverance have been a constant source of inspiration for us. It is only his/her cognizant efforts that our endeavors have seen the light of day.

We also take the opportunity to acknowledge the contribution of Dr. Ajay Kumar Shrivastava, Head of the Department of Computer Science, KIET Group of Institutions, Delhi- NCR, Ghaziabad, for his full support and assistance during the development of the project. We also do not like to miss the opportunity to acknowledge the contribution of all the department's faculty members for their kind assistance and cooperation during the development of our project.

Last but not least, we acknowledge our friends for their contribution to the completion of the project.

NAME	EMAIL	E-SIGN
Abhishek Singh Yadav	abhishek.2024cs1184@kiet.edu	
Aditi Batra	aditi.2024cs1002@kiet.edu	
Anurag Tripathi	anurag.2024cs1182@kiet.edu	
Kshitij Pal	kshitij.2024ec1064@kiet.edu	

ABSTRACT

Many sectors, like finance, medicine, manufacturing, and education, use blockchain applications to profit from the unique bundle of characteristics of this technology. Blockchain technology (BT) promises benefits in trustability, collaboration, organization, identification, credibility, and transparency.

In today's world, Authentication and reliability of the product is a much-needed thing as the market of false products is growing drastically. In this project, we conducted an analysis on authentication of the products using the unbreachable Blockchain Technology. in which we show how blockchain can be used as a tool to authenticate products and provide security to the consumer that the product they are using is legitimate. open science can benefit from this technology and its properties. For this, we determined the requirements of an open science ecosystem and compared them with the characteristics of Blockchain technology to prove that the technology is suitable as an infrastructure. We will use Blockchain here because of its decentralized, secure, and immutable characteristics.

CHAPTER 1: INTRODUCTION

1.1 Introduction

Product certification can reflect product quality, maintain product reputation, and protect the legitimate rights and interests of consumers.

However, with the continuous increase in the number and types of products sold by online platforms, the possibility of consumers buying fake and shoddy products has gradually increased. This violates the consumers' legitimate rights and interests and leads consumers to question product brand reputation.

Therefore, the market demand for product certification is constantly increasing.

Blockchains are distributed and decentralized databases. On a blockchain, both parties do not need to reach a consensus or rely on third-party agencies to conduct transactions.

The transactions on the chain are traceable, undeniable, and nonmodifiable, which can well ensure the credibility of transactions. Currently, blockchains are widely used in different application scenarios, such as product certification, the Internet of Things, supply chain, and smart cities to ensure data security and traceability.

Therefore, In this project we came up with the idea of using unbreachable blockchain technology to verify or authenticate the credibility of a product.

For which we will store the information of the product, based on the blockchain technology and let the consumer view that the product they are about to use is legitimate or not.

1.2 PROBLEM STATEMENT

During the study for the project, we got acknowledged to various scenarios where the unauthenticated false products are handed to the consumer. Also, it is recognizable that people found themselves helpless when they are exposed to such conditions. So, by this project we aim to authenticate the product using the blockchain technology.

1.3 OBJECTIVE

The main objective of this project is to authenticate a product. Other specific objectives are

- This will reduce the number of false products in the market
- The image of company will not be tarnished.
- Producer-consumer relation will be better.
- Consumer will have the complete information about the product

1.4 SCOPE OF STUDY

This project includes deployment of blockchain technology and

- This study uses a blockchain approach to solve the problem of product authenticity which can reduce the validation time of a product by a company.
- In future work, the blockchain approach in the case of other product authenticity requires more research so that this technology can be further implemented and developed.

CHAPTER 2: LITERATURE REVIEW

Blockchain challenges and opportunities: a survey

Authors: Zibin Zheng and Shaoan Xie, Hong-Ning Dai, Xiangping Chen, Huaimin Wang

The blockchain technology has the key characteristics, such as decentralisation, persistency, anonymity and auditability. Blockchain can work in a decentralised environment, which is enabled by integrating several core technologies such as cryptographic hash, digital signature (based on asymmetric cryptography) and distributed consensus mechanism. With blockchain technology, a transaction can take place in a decentralised fashion. As a result, blockchain can greatly save the cost and improve the efficiency. Although Bitcoin is the most famous application blockchain application, blockchain can be applied into diverse applications far beyond cryptocurrencies. Since it allows payments to be finished without any bank or any intermediary, blockchain can be used in various financial services such as digital assets, remittance and online payment. Additionally, blockchain technology is becoming one of the most promising technologies for the next generation of internet interaction systems, such as smart contracts, public services, internet of things (IoT), reputation systems and security services.

Decentralisation: In conventional centralised transaction systems, each transaction needs to be validated through the central trusted agency (e.g., the central bank) inevitably resulting the cost and the performance bottlenecks at the central servers. Differently, a transaction in the blockchain network can be conducted between any two peers (P2P) without the authentication by the central agency. In this manner, blockchain can significantly reduce the server costs (including the development cost and the operation cost) and mitigate the performance bottlenecks at the central server.

Immutability: Since transactions are stored in different nodes in the distributed network, so it is nearly impossible to tamper the public blockchain. However, if the majority of the consortium or the dominant organisation wants to tamper the blockchain, the consortium blockchain or private blockchain could be reversed or tampered.

ArtChain: Blockchain-enabled Platform for Art Marketplace

Authors: Ziyuan Wang, Lin Yang, Qin Wang, Donghai Liu, Zhiyu Xu, Shigang Liu

The design of blockchain technology ensures that no one business entity can modify, delete, or even append any record to the ledger without consensus from other network participants, ensuring the immutability of data stored on the ledger. With \$200 billion of annual trading, the art market is one of the largest unregulated markets in the world, accounting for one-third of the amount of crime just behind drugs and guns. Tens of millions of dollars are transferred with little or no documentation and transparency.

Current challenges and issues in the art market are:

- (1) lack of transparency on prices and ownership history (provenance) and inadequate control of transaction data due to the information asymmetry;
- (2) the authenticity and appraisal of high-value works of art is difficult;
- (3) lack of the value of artworks at the primary art market and transparency trading at the secondary auction market (both online and offline).

A blockchain-based art trading system, which has been piloted and operated as a working product in practice. It is expected to provide a complete solution towards these challenges by creating a new ecosystem for the art keeping, trading and transferring. ArtChain fundamentally builds up the underlying architecture of blockchain to support a commercial-level trading platform centered around art assets.

- A. **Tokenization**: Tokenization refers to converting an asset into a digital token on the blockchain system, so that ownership of the asset can be transferred via smart contracts.
- B. **Transaction security**: ArtChain network assures the security of users' accounts and funds by using blockchain consensus, digital signatures and end-users encrypted wallets. The artwork trading platform provides security services that are likened to those offered by financial institutions.
- C. **Privacy and Confidentiality**: ArtChain makes public all ledger nodes and their state in the network in real time. The transaction history (block content) and state

information in ArtChain are publicly visible. However, in case of any privacy requirements for some transactions, such privacy information will be processed.

The Supply Chain Has No Clothes: Technology Adoption of Blockchain for Supply Chain Transparency

Authors: Kristoffer Francisco and David Swanson

Blockchain technology allows two parties to transact directly using duplicate, linked ledgers called blockchains. This makes transactions considerably more transparent than those provided by centralized systems. As a result, transactions are executed without relying on explicit trust [of a third party], but on the distributed trust based on the consensus of the network (i.e., other blockchain users). Applying this technology to improve supply chain transparency has many possibilities. Every product has a long and storied history. However, much of this history is presently obscured. Often, when negative practices are exposed, they quickly escalate to scandalous, and financially crippling proportions.

There are many recent examples, such as the exposure of child labor upstream in the manufacturing process and the unethical use of rainforest resources. Blockchain may bring supply chain transparency to a new level, but presently academic and managerial adoption of blockchain technologies is limited by our understanding.

Now, as supply chain managers begin to recognize the possibilities of this new technology, there is high potential for elevating transparency. The arrival of this technology is timely because consumers are demanding supply chain transparency. For example, consumers often want guarantees that fish purchased and consumed are not farmed using illegal netting practices or from closed waters.

The first traceability application evaluated is a project enabled by Ethereum. From January to June 2016, yellowfin and skipjack tuna fish were tracked throughout the entire supply chain, from fishermen to distributors. End users could then track the “story” of their tuna fish sandwiches via a smartphone and determine information about the producers, suppliers, and procedures undergone by the end product. Every unit of measure (by fish or by catch) was associated with a digital “token” to confirm a given fish’s origin and tracked

throughout the supply chain, presenting a viable model for product certification to an end consumer.

Everledger is another blockchain-enabled traceability application for the global diamond industry. The company, which partnered with Barclays, created a database of over a million diamonds registered on their blockchain to certify the final cut diamond was ethically-sourced from “conflict-free” regions. Similar measures are being used to create an anti-counterfeit database for other valuable goods such as fine wine and art.

Where Is Current Research on Blockchain Technology?—A Systematic Review

Author: Jesse Yli-Huumo, Deokyoan Ko, Sujin Choi, Sooyong Park, Kari Smolander.

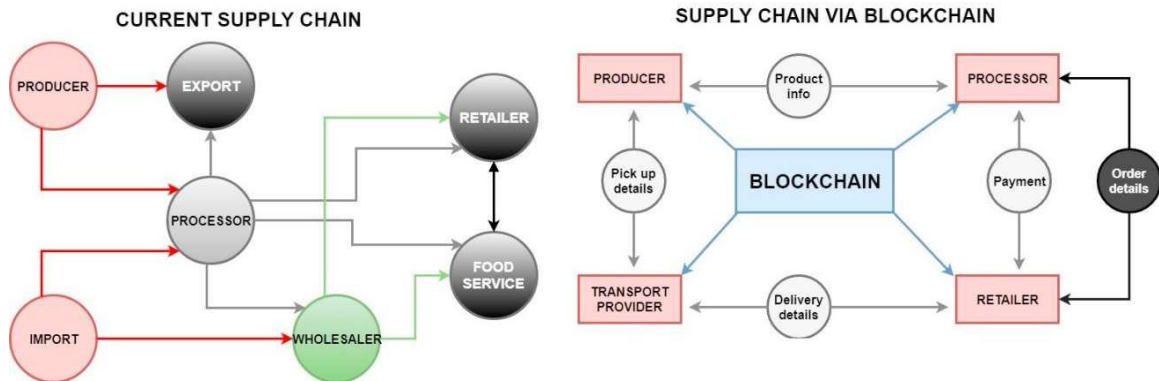
The idea of blockchain was first coined in the year 2008 for the very famous Bitcoin Cryptocurrency. Since blockchain is a decentralized transaction, the interest in Blockchain technology has been increasing gradually. However, even though Blockchain seems to be a suitable solution for conducting transactions by using cryptocurrencies, it has still some technical challenges and limitations that need to be studied and addressed. High integrity of transactions and security, as well as privacy of nodes are needed to prevent attacks and attempts to disturb transactions in Blockchain. Then the question arises - that what is the security percentage of the current blockchain technology? Answer happens to be that the current Blockchain has a possibility of a 51% attack. In a 51% attack a single entity would have full control of the majority of the network's mining hash-rate and would be able to manipulate Blockchain. To overcome this issue, more research on security is necessary. But the fact that conducting a 51% level attack is a extremely tough task on its own that sometimes seems next to impossible but it still can be done and it can definitely not be ignored. Another problem that comes with blockchain technology is its size and bandwidth. Bitcoin community assumes that the size of one block is 1MB, and a block is created every ten minute which can go out of control if more amount of blocks are to be created therefore there is a limitation in the number of transactions that can be handled (on average 500 transaction in one block). If the Blockchain needs to control more transactions, the size and bandwidth issues have to be solved. Another problem happens to be its usability. The

Bitcoin API for developing services is difficult to use. There is a need to develop a more developer-friendly API for Blockchain. But despite of these problems we cannot ignore advantages and facilities that it offers and since it is a decentralized environment for transactions where all the transactions are visible to everyone.

It provides anonymity, security, privacy, and transparency to all its users. However, it also comes up with some technical challenges that need more researches on them and by this they definitely can be overcome.

How blockchain improves the supply chain: case study alimentary supply chain

Authors: *Roberto Casado-Vara, Javier Prieto, Fernando De la Prieta, Juan M. Corchado*



In current supply chain there is lack of mutual information to each user or linked persons through this chain but with the help of blockchain technology each linked person with that supply chain can check the data regarded the product on which this supply chain is applied. A new model for agriculture tracking is presented in this paper. The proposed model involves blockchain ,smart contract and a MAS to co-ordinate the tracking of food in the agriculture supply chain through the implementation of this new model the current agriculture supply chain has an improvement based on the addition of blockchain. In figure are the current supply chain and supply chain architectures via BLOCKCHAIN. This enables a higher security in the transactions in addition this new model corrects the disadvantages of current supply chain. The data is decentralized and each member can read important

data for its operations in the blockchain for instance the producer can view the product information of the processors and the pickup details of the transport provider.

Effective scheme against 51% Attack on Proof-of-Work Blockchain with History Weighted Information

Authors: Xinle Yang, Yang Chen and Xiaohu Chen

Blockchain is considered to be the distributed data processing protocol for retaining a public distributed ledger in a Peer-to-peer network. There is a popular protocol used in blockchain systems which resolves the double-spending problems known as Proof-of-work (PoW). If an attacker is given an access to calculate the hash power greater than half of the total hash power then the attacker can create a double-spending attack or 51% attack. In PoW, each node competes to find a nonce value to produce a hash which meets the certain criteria and once this value is found, a block is generated and broadcasted to peer-to-peer network. NiceHash provides an open market in exchange of hash rate. Anyone can easily pay with cryptocurrency to rent available hash rate to mine for the target blockchain. The entire process takes approximately 50 to 500 blocks and then the attacker can release the rented hash rate and can earn the profit.

To perform 51% attack, malicious miners have 2 choices: either to mine the longer branch or build up the miner representation in previous blocks to build up the credibility. Historical Weight Difficulty (HWD) scheme works to defend the 51% attack. Only unique miner's generation frequency is counted. This discourages single high hash rate miners and thus encouraging the decentralization of mining and ultimately increasing the difficulty of attack. With HWD scheme, the cost of attacking the Ethereum Mainnet blockchain is increased by more than 100 times if one set the window size to 1M or 2M blocks. HWD calculation algorithm is used. If the attacker wishes to make nodes to switch his fraudulent branch, he needs to produce higher HWD value. The attacker needs to mine in the original branch for a while to make itself included in the history. Therefore, when it switches to hidden branch, its HWD will be greater.

ETH Relay: A Cost-efficient Relay for Ethereum-based Blockchains

The novel relay scheme employs the validation-on-demand pattern with the economic incentives to be reduced by 92%. Relays operate on off-chain clients forward block headers of source blockchain to a destination blockchain virtually replicating one blockchain within the other. Eth relay is secure and decentralized as long as there is at least one off-chain client acting honestly.

Simplified payment verification (SPV), is used in the light nodes like wallet software, is a technique used to cryptographically verify that a particular transaction is part of a blockchain while having the knowledge of a blockchain's block headers but not of the individual blockchain transactions. The light node has access to the Merkle root hash. Merkle proof of membership consists of all tree nodes that make up the path from the transaction up to the root node and can be retrieved. Then hashes of all the nodes is recalculated) up to the root node. If the final hash matches the Merkle root hash of the block header stored by the light node, the membership of the transaction within the corresponding block is successfully verified. Light nodes thus are able to verify the existence of transactions such as payments. BTC Relay is a Bitcoin light node that runs on the Ethereum blockchain in the form of a smart contract, called relay contract. The relay contract is able to verify the inclusion of Bitcoin transactions on the Ethereum blockchain by means of SPVs. PeaceRelay, a relay for Ethereum-based blockchains that mitigates high validation cost. The accurate functioning of ETH Relay is ensured when off-chain clients continuously submit block headers of the source blockchain to the relay contract on the destination blockchain and dispute any invalid block headers entering the relay contract. To hold clients that submit invalid block headers accountable, clients are required to deposit a stake for every submitted header. The stake is locked for the duration of the lock period of newly submitted block headers and it cannot be withdrawn neither be used for submitting further block headers. To encourage the submission of block headers, clients receive a fee every time their submitted headers are used for SPVs. The relay contract performs the 4 steps:

- Determining the Main Chain
- Verifying Main Chain Membership
- Counting Block Confirmations
- Verifying the Merkle Proof of Membership

ETH Relay uses a validation-on-demand pattern combined with a sophisticated incentive structure to motivate honest participation. ETH Relay does not require trust in a centralized party.

A Hybrid Blockchain Architecture For Privacy-Enabled And Accountable Auctions

A novel hybrid blockchain architecture that combines private and public blockchains to allow sensitive bids to be opened on a private blockchain so that only the auctioneer can learn the bids, and no one else. The hybrid blockchain based auction system is significantly faster and cheaper than an all public blockchain based auction system.

Smart Contracts

There are three smart contracts deployed in order to enable our architecture - the auction contract, the Public Declare contract and the Congress Factory contract. The auction contract is deployed on the private blockchain by the auctioneer. The public blockchain

hosts two smart contracts namely the Public Declare contract and the Congress Factory contract. The former is used to declare the highest and second highest bidders along with their respective bids of the auction and for the secure auction participants bid on the items in the form of commitments. When a breach is suspected, the Congress Factory has an automated check that requires the auctioneer to send its data to it. For the implementation of hybrid architecture, we have chosen Ethereum for both the private and public chains.

The Genesis Block: a genesis file for the private blockchain is written in json format. This file is a customized unique genesis file that contains details regarding the gas limit, the chain id, difficulty, nonce and most importantly the participating account ids with pre-funded balances. The genesis block is the first block in the blockchain or block 0 and is created using this genesis state file. The gas limit is the highest amount of gas. Every participant address is pre-funded by 100,000 gas for initial bidding purposes. Once the participant joins the system, it is enforced to become a miner.

Commitments over Private Chain: The commitments are generated offline by the participants by a JavaScript application portal. The participants then with the help of the web3 application send the generated commitments to the auctioneer.

Miners over the Private Chain: Commitments are mined as transactions by the miners over the private blockchain. Each participant is enforced to become a miner on the private chain. Each participant is pre-funded with a necessary amount of ether to participate in transaction and each participant has to become a miner on its acceptance to the private chain.

Ether over Private Chain: Although the ether on the private chain has no significant effect on the economic ecosystem of the blockchain, every entity on the private blockchain should be provided with equal amount of ether as every other entity.

Mechanism of Formation of a Bid Commitment: The bit commitment scheme implemented using a hash function scheme. Let f be a one-way hash function with hard-core predicate B . Let m be the binary form of the bid. Each participant randomly selects r which is a string of 0's and 1's. The bid is parsed before acceptance by the contract. If there is any discrepancy in the bid example, the commitment does not match the required length or it contains any invalid characters, the bid is rejected. Integrating Public and Private Blockchains: Nodejs, a JavaScript run-time environment and npm package manager is being used for the frontend UI for the participants and the auctioneer to call the blockchain. Testrpc is used as a testing framework for the private chain.

Blockchain Technologies And Their Applications In Data Science And Cyber Security

Blockchain technologies essentially provide a platform for the secure transfer of the data that are part of any transactions including financial transactions and contracts. One of the most popular applications of blockchain is Bitcoin which is essentially financial cryptocurrency. Another popular application of blockchain is Ethereum. Blockchain

essentially consists of a collection of blocks that are linked together via chains. A block is essentially a file that contains data pertaining to a transaction. The data from one block may be transferred to multiple blocks. A block may receive data from multiple blocks. The data in each block is permanent and immutable. Blocks can be added to the blockchain as the transaction progresses. Each transition has to be verified. An important component of blockchain is cryptographic hash functions. This is a form of a message digest where checksums are computed based on the contents. This is one of the key components that provide security (e.g., confidentiality, integrity, authenticity) for blockchains. Blockchains use asymmetric key technology which is essentially public key cryptography. Blockchains may also use network addresses which are derived from the public key cryptography.

BLOCKCHAIN FOR DATA SCIENCE

Blockchain is emerging as a key technology for securing the data science techniques. That is, securing the data collection, data processing, data management, data analytics and data sharing activities via blockchain is being examined. With the decentralized nature of blockchain, trust can be ensured by a collection of processes in the peer-to-peer network. For data sharing, blockchain technologies enable multiple parties to access and share the data securely. The distributed ledger at the heart of blockchain can also determine the provenance of the data which is an important aspect of data science. Blockchain is key to keeping track of all the transactions in a supply chain process and this also includes the data supply chain. Additionally, data generated through blockchain is validated, structured and immutable. Since the data that is provided by blockchain is ensured of data integrity, it enhances big data. The topological feature computed from the blockchain graphs can be used to predict Bitcoin price dynamics.

BLOCKCHAIN FOR CYBER SECURITY

Blockchain technologies were developed mainly to execute secure transactions including the secure transfer of cryptocurrencies. The distributed ledger-based architecture for blockchains facilitates distributed data storage. Cryptographic checksums are used to ensure security. The key can be revoked any time and this way one can enforce dynamic security. Another application of blockchain is in providing IoT security where billions of devices are connected which facilitates distributed processing. As a result, blockchain technologies can be used for the secure communication between the devices and not have centralized control. A third area is in DNS (Domain Name System). DNS systems are usually centralized and therefore hackers can break into such systems without difficulty. However, due to the distributed nature of blockchains, hackers will find it more difficult to find the single point of entry. Finally, most messaging systems use end-to-end encryption. It is stated that blockchains could potentially help enhance cyber defence as the platform can prevent fraudulent activities via consensus mechanisms, and detect data tampering depending on its underlying characteristics of operational resilience, data encryption, auditability, transparency and immutability. It also adds that blockchains enhance security by eliminating humans in the authentication process, reduce distributed denial of service attacks (DDoS), provide traceability, and support decentralized storage.

Hybrid Blockchain Design for Privacy Preserving Crowdsourcing Platform

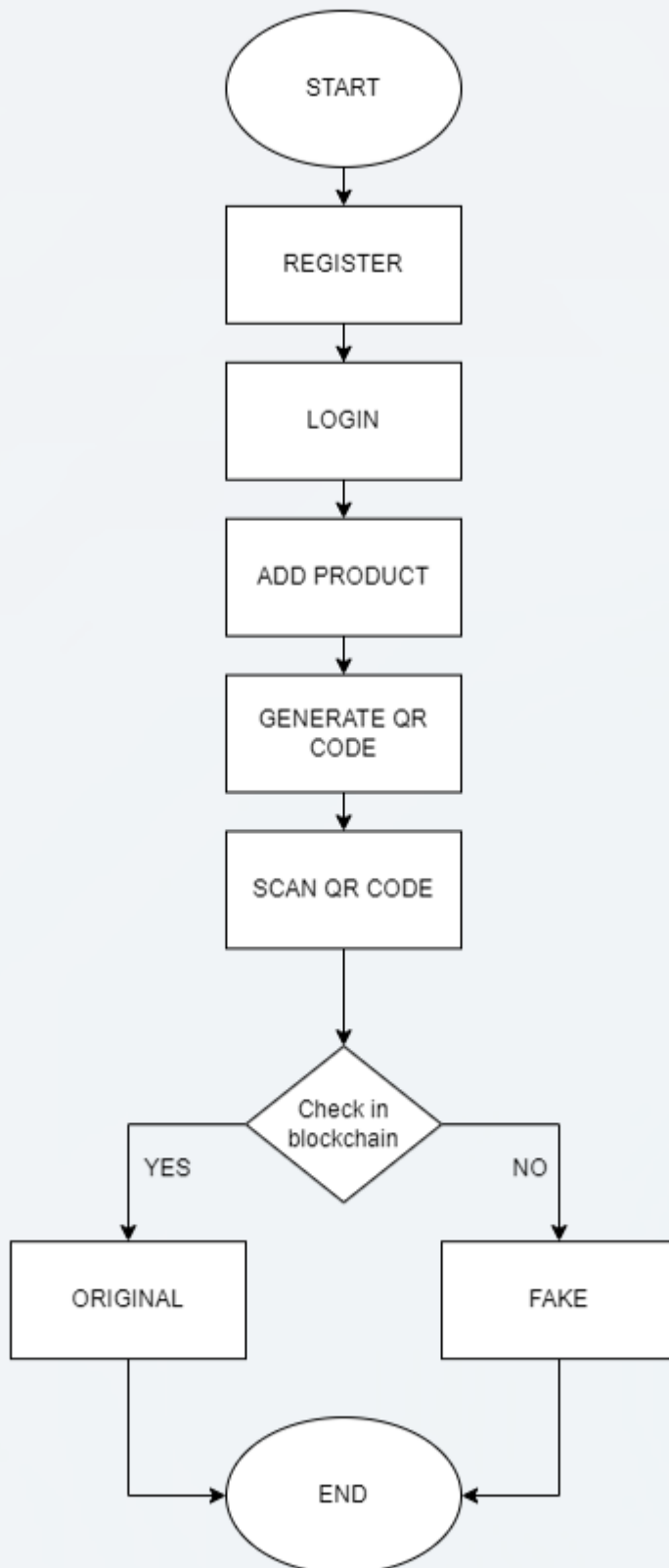
Authors: Saide Zhu, Huaifu Hu, Yingshu Li, Wei Li

Blockchain is considered to be the most promising technologies to promote crowdsourcing by providing new features, such as decentralization and accountability. To enhance transaction verification throughput, Delegated Proof of Stake (DPOS) and Practical Byzantine Fault Tolerance (PBFT) consensus are respectively deployed on the public chain and the sub-chains, and smart contracts of the public chain and the sub-chains are designed accordingly. The core of the blockchain is the consensus protocol. In DPOS consensus, there are three roles, including stakeholders, witnesses (block producers or validators), and alternative nodes. The advantages of DPOS in verification speed, energy consumption and security, DPOS provides the finality feature. The stability of the network. By respectively employing DPOS and Practical Byzantine Fault Tolerance (PBFT) consensus on the public chain and the sub-chains, platform can achieve higher transaction throughput and less execution time compared with traditional PoW/PoS-based blockchain. PBFT consensus algorithm can be divided into five steps: request, pre-prepare, prepare, commit and reply. Advantages of PBFT includes that it is more efficient and can reach to high transaction verification speed when the volume of the transaction is not so high, transaction finality is achieved and it can achieve network agreement without any intensive computations.

Smart contract is written in the form of code and stored on a blockchain and inherits features like accountability and decentralization. Once written can be trusted by the users. Crowdsourcing platform is based on a hybrid blockchain network that consists of a public chain and multiple sub-chains, in which public tasks are posted on the public chain and private tasks are uploaded to the sub-chains for privacy protection. There are 3 types of entities on the platform: requester, worker and validator. In blockchain-embedded crowdsourcing platform, there are six phases of implementation: Identity Authentication, Public Chain Setup, Sub-chain Setup, Smart Contract Deployment, Zero-Knowledge Poof, which are illustrated in this section.

CHAPTER 3: PROPOSED METHODOLOGY

3.1 Flowchart:



3.2. Algorithm Proposed:

1. Manufacturer initiates the registration process on the website by providing a unique ID and password.
2. Clicking the register button triggers the MetaMask confirmation prompt for blockchain validation.
3. Manufacturer logs in using the same credentials and proceeds to register a product.
4. During product registration, the manufacturer inputs a unique product ID and name.
5. Confirmation of addition to the blockchain is done by clicking the "add" button, prompting MetaMask confirmation again.
6. Upon successful registration, a corresponding QR code is generated for download by the manufacturer.
7. Manufacturer affixes a QR code to the product for authentication purposes.
8. Users or customers scan/upload QR code on the website.
9. The system verifies product authenticity and displays relevant information.
10. Confirmation is provided as to whether the product is genuine or counterfeit.

CHAPTER 4: TECHNOLOGY USED

BLOCKCHAIN

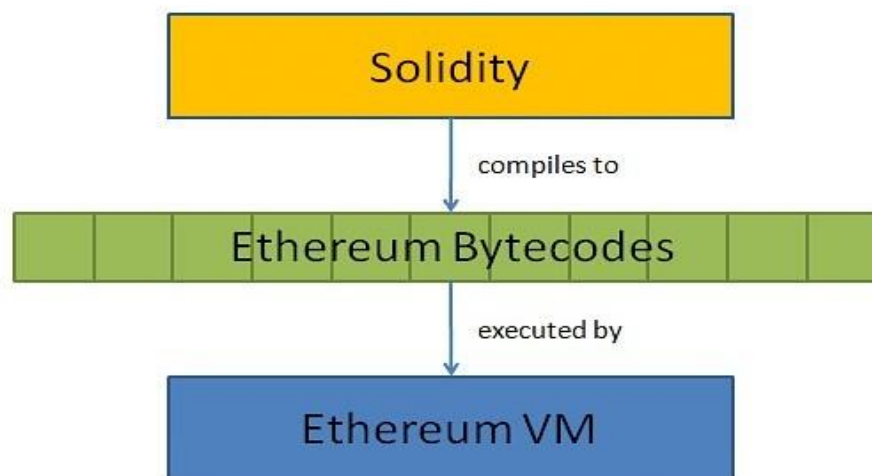
Blockchain is **a system of recording information in a way that makes it difficult or impossible to change, hack, or cheat the system**. A blockchain is essentially a digital ledger of transactions that is duplicated and distributed across the entire network of computer systems on the blockchain.

Ethereum is a blockchain-based computing platform that enables developers to build and deploy decentralized applications—meaning not run by a centralized authority. You can create a decentralized application for which the participants of that particular application are the decision-making authority.

SOLIDITY

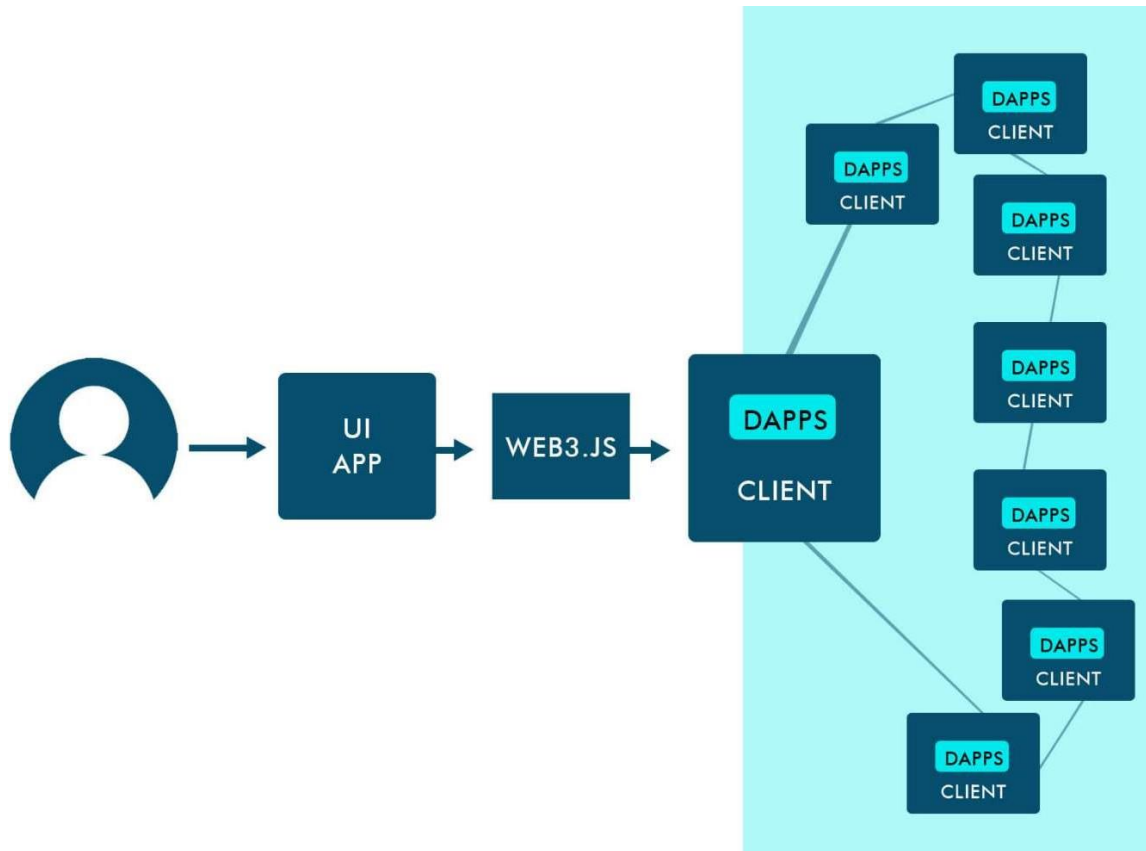
Solidity is an object-oriented programming language for implementing smart contracts on various blockchain platforms, **Solidity is the primary language on Ethereum** as well as on other private blockchains, such as the enterprise-oriented Hyperledger Fabric blockchain.

- It's used to create smart contracts that implement business logic and generate a chain of transaction records in the blockchain system.
- It acts as a tool for creating machine-level code and compiling it on the Ethereum Virtual Machine (EVM).



WEB3.JS

Web3 is a **collection of JS libraries that lets you interact with an Ethereum node remotely or locally**. Simply, it provides us with an API to use so we can easily work with the blockchain. Web3 works as a wrapper for JSON RPC to connect to a remote or local Ethereum node with either a HTTP or IPC connection.



CHAPTER 6: CONCLUSION

In conclusion of this project, we would conclude that this project will provide a great help to the future as discussed earlier. Exploring the use of public blockchains, known for their accessibility and transparency, is a pathway to further elevate trust. This shift not only embraces technological advancement but also signifies a commitment to transparency and diversity, fostering increased consumer confidence.

This project will be based on Blockchain algorithms and full-stack development. With the help of this project, authentication of the product can be done by providing proper information about the product on the blockchain network. The project aims to reduce the false products from the market. The immutable nature of blockchain establishes an unassailable foundation of trust by safeguarding product data against unauthorized alterations. Integral to this method, smart contracts serve as vigilant guardians, meticulously validating product information against predefined criteria, thereby fortifying the market against counterfeit infiltrations. The emphasis on transparency extends beyond mere transactional interactions, fostering a trustful relationship between consumers and manufacturers. By effectively exposing counterfeiters, this approach diminishes the market value of fraudulent goods, acting as a formidable deterrent to illicit production. This dual protection shields consumers and legitimate producers alike.

REFERENCES

[1] **Ethereum.org**

<https://ethereum.org/en/>

[2] **Physical Assets on the Blockchain : Linking a novel Object Identification Concept with Distributed Ledgers**

Thomas Hepp, Patrick Wortner, Bela Gipp

[3] **Effective scheme against 51% Attack on Proof-of-Work Blockchain with History Weighted Informationy**

Xinle Yang, Yang Chen and Xiaohu Chen

[4] **The Supply Chain Has No Clothes: Technology Adoption of Blockchain for Supply Chain Transparency**

Kristoffer Francisco and David Swanson

[5] **Where Is Current Research on Blockchain Technology?—A Systematic Review**

Jesse Yli-Huumo, Deokyoon Ko, Sujin Choi, Sooyong Park, Kari Smolander.

[6] **ArtChain: Blockchain-enabled Platform for Art Marketplace**

Ziyuan Wang, Lin Yang, Qin Wang, Donghai Liu, Zhiyu Xu, Shigang Liu

[7] **How blockchain improves the supply chain: case study alimentary supply chain**

Roberto Casado-Vara, Javier Prieto, Fernando De la Prieta, Juan M. Corchado