IJCRT.ORG ISSN : 2320-2882

INTERNATIONAL JOURNAL OF CREATIVE RESEARCH THOUGHTS (IJCRT)

An International Open Access, Peer-reviewed, Refereed Journal

Fake Product Detection Using Blockchain Technology

[1]Sakshi P. Hadole, [2]Ketki Ingole,
[1]Student , [2]Assosciate Professor
Department of Computer Science and Engineering
Sipna College of Engineering and Technology

Abstract: Blockchain innovations have acquired interest in the course of the most recent years. One of the most talked about issues is currency exchange, but its application is not limited only to Digital currency. So it has the potential to influence different business sectors. Blockchain technology has brought greater transparency and ease in large transactions. We can detect counterfeit goods using blockchain technology. The question arises when buying any item in today's world that the product is fake or genuine. And the lack of these things has been shown a huge impact on economic progress. Therefore, in order to curb all counterfeit goods, it is important to bring transparency about the goods to the notice of the consumers. The growing presence of counterfeit and unsafe products in the world is a cause for concern and blockchain technology has taken the next step towards its complete annihilation. Not only the use of technology will reduce the production of counterfeit goods, but everyone needs to be aware of this. By producing and packaging the right items each of those items needs to be given a digital code with its own identity. In this application, the supplier will register their products and customers will scan QR code using any QR scanning application and then the system will verify if the given product is counterfeit or not.

Index Terms **-** Blockchain Technology, Counterfeit Goods, Product Authentication, QR Code Verification, Transparency, Consumer Awareness

1. INTRODUCTION

Supply chain counterfeiting is a universal problem that plagues almost every industry. There are counterfeit electronic components, car parts, consumer goods, pharmaceuticals — even counterfeit wines. While manufacturers and distributors lose billions of dollars annually to counterfeit goods, the risks to consumers can be even greater. Faulty counterfeit auto parts or consumer products can overheat or catch fire, and more than 1 million people each year lose their lives due to counterfeit drugs.While manufacturers, distributors, shippers and government agencies are actively working to remove counterfeit goods from the supply chain, it's challenging to identify counterfeits. Counterfeit goods cost global brands more than $232 billion in 2018. The counterfeit drug market alone costs more than $200 billion per year - enough to bring 13 new drugs to market annually. Losses from counterfeit automotive parts are estimated to be $2.2 billion per year, not counting those from safety issues and legal liability. Counterfeit consumer electronics cost more than $100 billion per year, and bogus computer chips cost U.S. companies $7.5 billion annually, as well as 11,000 jobs. Identifying counterfeit goods that enter the supply chain can be difficult, if not impossible. The only way to beat counterfeiters is to apply a fool proof means of authenticating goods from their point of origin to final delivery. New cloud-based security technology is now available that can create unique, fool proof digital identifiers for products so that they can be tracked at every point in the supply chain. Identification of counterfeit merchandise in cutting-edge market is being a exceptional assignment for customers and it is very life threatening for the customers while this takes vicinity in pharmaceutical fields. Other fields like electronics, clothing, fashion-accessories additionally face a large effect on their emblem

because of counterfeit products. E-commerce has visible exceptional boom through the years from $39 billion in 2017 and it is projected to upward push to $200 billion via 2026[2]. This comes within the wake of extending penetration of the net and cell phones. After numerous market surveys it is observed that the counterfeit merchandise are growing rapidly and the rise of counterfeit products can badly affect the improvement and economic boom. Additionally because of this the many top companies have become bad comments and dropping their positions from the logo list.

Counterfeit merchandises are twins of the real merchandise in the marketplace. Often all reputed businesses are operating to forestall this system that is dangerous to all people in the entire international. The various branded or reputed groups are running on contemporary technology to identify the counterfeited products from the original product inside the market and to enhance this operating, the IT area can give them fine signals and can assist to prevent counterfeit items. Among those numerous technologies available inside the IT area blockchain is one of the promising Technologies which may be used for decreasing the counterfeiting of goods. A blockchain is a kind of dispensed ledger that is designed to prevent tampering. Primarily based on the allotted consensus Set of rules, clever contracts and encrypted algorithms [3]. Blockchain generation facilitates to clear up the Problem of counterfeiting of a product. And on this studies we proposed a product surveillance blockchain device with the intention to share statistics about merchandise from the manufacturer to the clients. We are growing such an application that will work on smart phones so one can Be giving all of the designated data about the products to the client who orders that product and help them to identify if the product is authenticated or counterfeited

Block chain Technology

Definitions

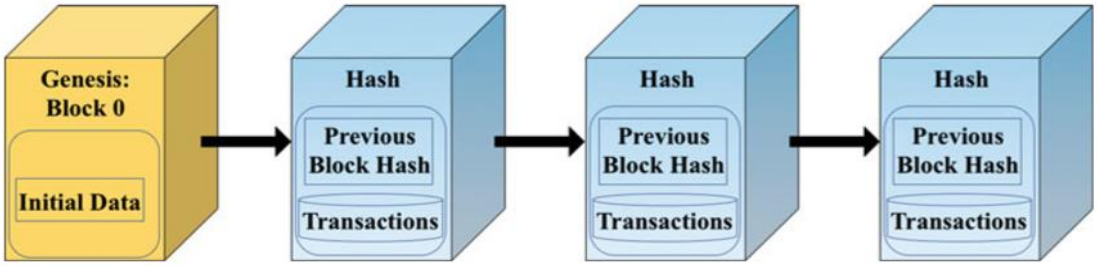
A blockchain is a linked list of immutable tamper-proof blocks, which is stored at each participating node. Each block records a set of transactions and the associated metadata. Blockchain transactions act on the identical ledger data stored at each node. Blockchain was first perceived by Satoshi Nakamoto (Satoshi 2008), as a peer-to-peer money exchange system. Nakamoto referred to the transactional tokens exchanged among clients in his system as Bitcoins.

Overview

In 2008, Satoshi Nakamoto (Satoshi 2008) came up with the design of an unanticipated technology that revolutionized the research in the distributed systems community. Nakamoto presented the design of a peer-to-peer money exchange process that was shared yet distributed. Nakamoto named his transactional token as Bitcoin and brought forth design of a new paradigm blockchain. The key element of any blockchain system is the existence of an immutable tamper-proof block. In its simplest form, a block is an encrypted aggregation of a set of transactions. The existence of a block acts as a guarantee that the transactions have been executed and verified. A newly created block is appended to an existing chain of blocks. This chain of blocks is predominantly a linked list which associates one block with the other. The initial block of any such list is a genesis block (Decker and Wattenhofer 2013). Genesis block is a special block that is numbered zero and is hard-coded in the blockchain application. Each other block links to some previously existing block. Hence, a blockchain grows by appending new blocks to the existing chain. A transaction in a blockchain system is identical to any distributed or OLTP transaction (TPP Council 2010) that acts on some data.

Traditional blockchain applications (such as Bitcoin) consist of transactions that represent an exchange of money between two entities (or users). Each valid transaction is recorded in a block, which can contain multiple transactions, for efficiency. Immutability is achieved by leveraging strong cryptographic properties such as hashing(KatzandLindell2007).Figure1presentsthe structure of a simple blockchain. A blockchain is a linked list in a true sense, as each block stores the hash of the previous block in its chain. Each block also digitally signs its contents by storing the hash of its contents inside the block. These hashes provide cryptographic integrity, as any adversary intending to modify a block needs to also modify all the previous blocks in a chain, which makes the attack cryptographically infeasible. A key design strategy is to construct a Merkle tree (Katz and Lindell 2007) to efficiently store and verify the hashes. Thus, each block only stores the root of the Merkle tree, as given the root, it is easy to verify the immutability. The preceding discussion allows us to summarize that a blockchain aims at securely storing a set of transactions. In the succeeding sections, we discuss in detail the transaction processing in a blockchain system. We also study mechanisms to validate these transactions and analyze some blockchain applications that employ the same servers of the blockchain system (Nawab 2018). These transactions act on the data stored on all the

participating servers. In its vanilla form, a blockchain transaction could be visualized as a set of read/write operations performed on each node of a replicated distributed database. To determine an ordering for all the incoming transactions, each blockchain application employs a consensus(SteenandTanenbaum2017)protocol. A distributed consensus algorithm (Lamport 1998; Gray and Lamport 2006) allows a system toreachacommondecision,respectedbythemajority of nodes. Recent blockchain technologies present several strategies for establishing consensus: Proof-of-Work (Jakobsson and Juels 1999; Satoshi 2008), Proof-of-Stake (King and Nadal 2012), Proof-of-Authority (Parity Technologies 2018), Practical Byzantine Fault Tolerance (Castro and Liskov 1999; Cachin 2016), and so on. To quantify the allowed set of nodes that can create a block (or participate in the consensus process), it is also necessary to characterize the topologies for blockchain systems.



Blockchain Transaction Processing, Fig. 1 Basic blockchain representations

Problem Statement

The worldwide improvement of an item or innovation consistently accompanies hazard factors, for example, forging and duplication. Forging items can influence the organization's name and the client's wellbeing. Presently days discovery of phony item is the greatest test. Fake items are causing a significant impact on the organization and the client's wellbeing. Hence, item creators are confronting enormous misfortune. India and different nations are battling such fake and fake items. In the proposed framework, the framework produces QR codes utilizing Blockchain innovation. This innovation stores exchange records in blocks. These squares are secure and difficult to access and change the data from it. By utilizing a QR code we can recognize the fake item

2 . LITERATURE SURVEY

1. A Survey on Blockchain Technology: Evolution, Architecture and Security

Authors: Muhammad Nasir Mumtaz Bhutta, Amir A. Khwaja, Adnan Nadeem, Hafiz Farooq Ahmad , Muhammad Khurram Khan, Moataz A. Hanif, Houbing Song, Majed Alshamari , and Yue Cao

This survey paper has covered architecture of cryptocurrencies, smart contracts and general Blockchain based applications. The paper has provided a perspective to describe the Blockchain architectures in relation to cryptocurrencies, smart contracts and other applications. The research advances in consensus are also highlighted with some key development and application frameworks. A detailed discussion with respect to future and open research avenues is also performed, which could help to pave the way for researchers to explore the key challenging areas in the Blockchain field.

Disadvantages

- Doesn’t give idea about hashing and all consensus algorithms

2. Product Traceability using Blockchain

Authors: Rishabh Sushil Bhatnagar, Sneha Manoj Jha , Shrey Surendra Singh, Rajkumar Shende

The conventional SCM systems are widely used in the current market whereas blockchain is a relatively new system and is yet to be introduced in the industry on a large scale. The current SCM systems have prevailed so long in the market due to its easy and cheaper implementation on a large scale. Despite being used on a large-scale platform, these systems have their flaws which have prevailed since the existence of

these systems. The current system is opaque in nature and is very vulnerable to various frauds and scams due to poor maintenance of the records of the transactions within the system. Lack of trust between the participating entities is an issue yet to be resolved. The trust of the customer in the system is compromised by not providing a quality assured product even though it is a major factor in the growth of any business. Even with all these flaws, these systems are being used by various market giants as the prices of the products can be easily exploited with any credibility.

Disadvantages

Participation of too many entities makes it difficult for transactions.

3. A Blockchain-based Supply Chain Quality Management Framework

Author : Si Chen , Rui Shi , Zhuangyu Ren , Jiaqi Yan , Yani shi , Jinyu Zhang

In this appropriate paper, they proposed a framework for blockchain based SCQI. This framework will provide a theoretical basis to intelligent quality management of supply chain based on the blockchain technology. Furthermore, it provides a foundation to develop theories about information resource management in distributed, virtual organizations, especially distributed, cross-organizational and decentralized management theory. Disadvantages •Design of complex smart contract system which is much inefficient.

4. A Block Chain based Management System for Detecting Counterfeit Product in Supply Chain

Authors: M.C.Jayaprasanna, .V.A.Soundharya , M.Suhana, S.Sujatha

In this Paper, they have discussed about counterfeit products are growing exponentially in online and black-market. The block market is a biggest challenge in supply chain. The government has introduced several laws and regulations against fake products even though the government cannot control counterfeit products. Therefore, there is a need of an approach for detecting counterfeit products and providing security techniques to alert both manufacturer and consumer in supply chain. Manufacturers may use the block chain management system to store relevant product sales information within the block chain, which is accessible to all. The total number of sales the seller can sell and the rest left behind by the seller are transparent. The user can perform vendor-side verification using an encryption algorithm. Only way to decrypt is to use a private key of the owner. In this paper, we proposed block chain management system activates the consumer and enterprise vendor to track and identify the real product using a Smartphone. It also will detect counterfeit products as well as authenticity of manufacturer for both end user and enterprise vendor.

Disadvantages

- Using RFID (Radio frequency Identification) takes too much time for computing in a BCBM(Block Chain Based Management System).

5. A Blockchain-Based Application System for Product AntiCounterfeiting

Authors: Jinhua Ma , Shih-Ya Lin , Xin Chen , Hung-Min Sun

In this particular Paper, Manufacturers can use the system to store relevant information on product sales in Blockchain which is accessible to everyone. The total amount of sales that can be sold by the seller and the number of products currently left by the seller are transparent. The user can use the functions provided by our system to immediately perform vendor-side verification. The system provides identity verification by using digital signatures. There are no other means to decrypt the private key of the key owner unless the key owner accidentally leaks his key. In their system analysis result, the cost of the initial product record contract will only cost 1.2893394289 US dollars, and the cost of each product sale process will cost 0.17415436749 US dollars.

Disadvantages

- This proposed system even though it uses a ethereum Blockchain which is best for smart contracts. It uses digital signatures for transactions. Everytime Using a digital signatures for all transactions becomes clumsy.

6. A Blockchain-based decentralized system to ensure the transparency of organic food supply chain

Authors: B. M. A L. Basnayake, C. Rajapakse

This study is based on the applicability of Blockchain concept to improving transparency and validity of agricultural supply chain and its process. Since recent past, there has been a rapid change in the production of food and its raw materials. An efficient method to bridge the gap between the farmer producing commodities in the market and the end customer was studied. Blockchain based architecture and its concepts were taken for implanting trustworthiness and transparency within the users and their transactions. In this paper as there is a drawback of farmers may not be knowing about the product traceability once they register.

Disadvantages

• In this blockchain only farmers has the access to start or end transaction at any moment. As most of the farmers being an illiterates they don't have much understanding of blockchains.

7. User Interface of Blockchain-Based Agri-Food Traceability Applications

Authors: Atima Tharatipyakul and Suporn Pongnumkul

A Review: Blockchain technology is seen as a way to improve agri-food supply chain traceability and deliver food quality, safety, and nutrition information to stakeholders. Limited knowledge on how to design the user interface for the traceability application could lead to usability issues. As a step towards more usable blockchain-based agri-food traceability applications, this paper reviewed existing works from a user interface perspective.

Disadvantages

• Gives an idea about only existing user interface which are inefficient and ambiguous for users. The design proposed in this system requires high cost.

Proposed System

Objectives

- **To develop an online blockchain based fake product identification system**
- **To implement blockchain for transparency and security**
- **To implement SHA and AES algorithms**

Users

- **Admin**
- **Manufacturer**
- **Supplier**
- **consumer**

Algorithms

- **SHA**
  - **This algorithm will be used to find out unique hash value of every block**
  - **We proposed SHA2 which will generate 32 byte hash value**
  - **SHA2 generate unique representative value, if any single bit changed the hash value will also changed**
  - **The Secure Hash Algorithm 2 (SHA-2) is a computer security cryptographic algorithm. It was created by the US National Security Agency (NSA) in collaboration with the National Institute of Science and Technology (NIST) as an enhancement to the SHA-1 algorithm. SHA-2 has six different variants, which differ in proportion with the bit size used for encrypting data.**

- **AES**
  - **This algorithm will be used to encrypt block data**
  - **We will use AES 32 byte key encryption to encrypt block data on blockchain server**
  - Advanced Encryption Standard (AES) is a specification for the encryption of electronic data established by the U.S National Institute of Standards and Technology (NIST) in 2001. AES is widely used today as it is a much stronger than DES and triple DES despite being harder to implement.
  - **AES is a block cipher.**
  - **The key size can be 128/192/256 bits.**
  - **Encrypts data in blocks of 128 bits each.**

SHA

SHA-2 is a set of cryptographic hash functions designed by the United States National Security Agency and first published in 2001. They are built using the Merkle–Damgård construction, from a one-way compression function itself built using the Davies–Meyer structure from a specialized block cipher. SHA-2 is a family of hashing algorithms to replace the SHA-1 algorithm. SHA-2 features a higher level of security than its predecessor. It was designed through The National Institute of Standards and Technology (NIST) and the National Security Agency (NSA). Entrust uses the SHA-1 hashing algorithm to sign all digital certificates. Entrust is introducing the SHA-256 variant of the SHA-2 family as a signing option for all certificates. Due to possible backwards compatibility issues with older Operating Systems, Entrust is also leaving the SHA-1 the default hashing algorithm and allowing the customer to

optionally choose SHA-2 when signing or to set SHA-2 as the default in the Certificate Management Service (CMS).

One of the major benefits of using SHA-2 is that it addresses some weaknesses in the SHA-1 hashing algorithm. SHA-1 is not considered to be unsafe at this time; however, the weaknesses that have been identified make the algorithm vulnerable to possible exploitation over the coming years.

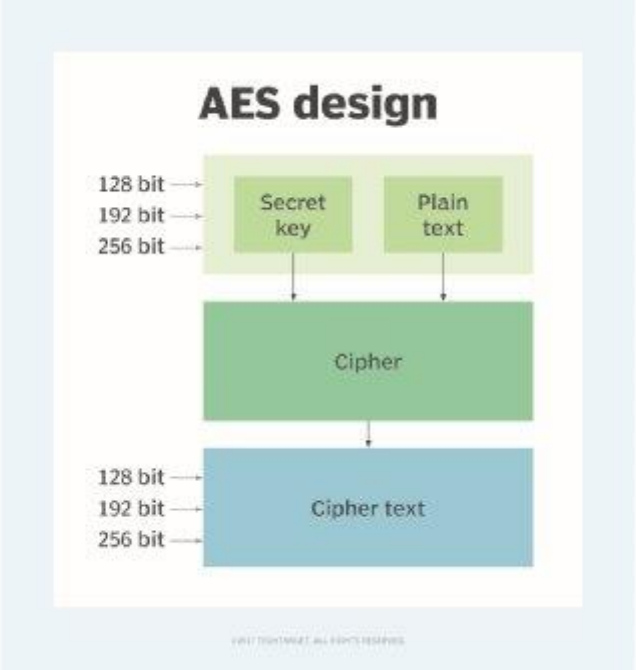
AES Working

AES includes three block ciphers:

1. AES-128 uses a 128-bit key length to encrypt and decrypt a block of messages.
2. AES-192 uses a 192-bit key length to encrypt and decrypt a block of messages.
3. AES-256 uses a 256-bit key length to encrypt and decrypt a block of messages.

Each cipher encrypts and decrypts data in blocks of 128 bits using cryptographic keys of 128, 192 and 256 bits, respectively.Symmetric, also known as secret key, ciphers use the same key for encrypting and decrypting. The sender and the receiver must both know -- and use -- the same secret key.The government classifies information in three categories: Confidential, Secret or Top Secret. All key lengths can be used to protect the Confidential and Secret level. Top Secret information requires either 192- or 256-bit key lengths.

There are 10 rounds for 128-bit keys, 12 rounds for 192-bit keys and 14 rounds for 256-bit keys. A round consists of several processing steps that include substitution, transposition and mixing of the input plaintext to transform it into the final output of ciphertext.



uses 128-, 192- or 256-bit keys to encrypt and decrypt data.

The AES encryption algorithm defines numerous transformations that are to be performed on data stored in an array. The first step of the cipher is to put the data into an array, after which the cipher transformations are repeated over multiple encryption rounds.The first transformation in the AES encryption cipher is substitution of data using a substitution table. The second transformation shifts data rows. The third mixes columns. The last transformation is performed on each column using a different part of the encryption key. Longer keys need more rounds to complete.

What are the features of AES?

NIST specified the new AES algorithm must be a block cipher capable of handling 128-bit blocks, using keys sized at 128, 192 and 256 bits.

Other criteria for being chosen as the next AES algorithm included the following:

- **Security.** Competing algorithms were to be judged on their ability to resist attack as compared to other submitted ciphers. Security strength was to be considered the most important factor in the competition.
- **Cost.** Intended to be released on a global, nonexclusive and royalty-free basis, the candidate algorithms were to be evaluated on computational and memory efficiency.
- **Implementation.** Factors to be considered included the algorithm's flexibility, suitability for hardware or software implementation, and overall simplicity.

Choosing the new AES algorithm

Fifteen competing symmetric algorithm designs were subjected to preliminary analysis by the world cryptographic community, including the National Security Agency (NSA).

In August 1999, NIST selected five algorithms for more extensive analysis:

1. **MARS**, submitted by a large team from IBM Research;
2. **RC6**, submitted by RSA Security;
3. **Rijndael**, submitted by two Belgian cryptographers, Joan Daemen and Vincent Rijmen;
4. **Serpent**, submitted by Ross Anderson, Eli Biham and Lars Knudsen; and
5. **Twofish**, submitted by a large team of researchers from Counterpane Internet Security, including noted cryptographer Bruce Schneier.

Implementations of all of the above were tested extensively in American National Standards Institute (ANSI), C and Java languages for:

- speed and reliability in the encryption and decryption processes;
- key and algorithm setup time; and
- resistance to various attacks -- both in hardware- and software-centric systems.

Detailed analyses were conducted by members of the global cryptographic community, including some teams that tried to break their own submissions.After much feedback, debate and analysis, the Rijndael cipher was selected as the proposed algorithm for AES in October 2000. It was published by NIST as U.S. Federal Information Processing Standards (FIPS) PUB 197, which was accepted by the secretary of commerce in December 2001.

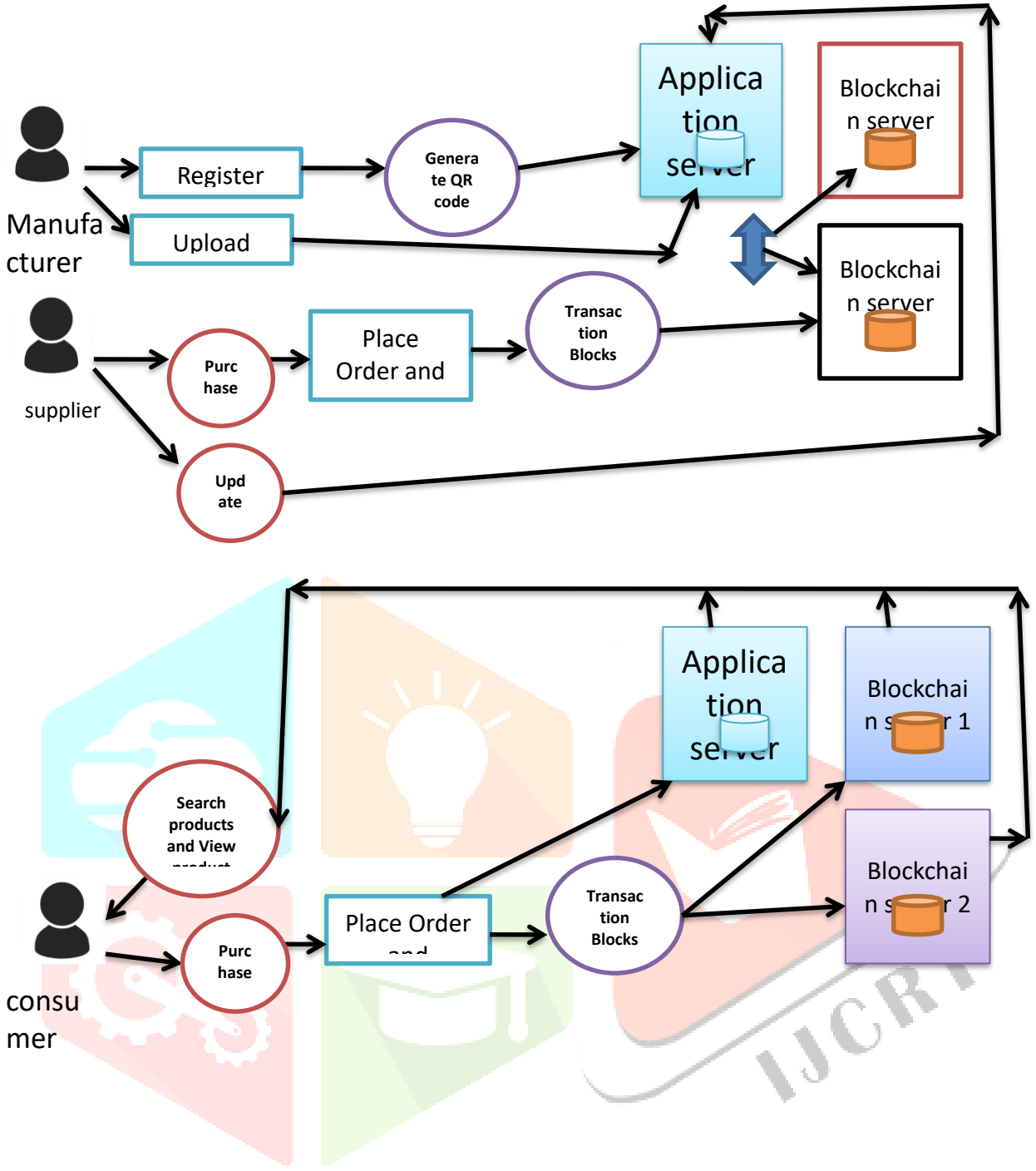
AES became effective as a federal government standard in 2002. It is also included in the International Organization for Standardization (ISO)/International Electrotechnical Commission (IEC) 18033-3 standard, which specifies block ciphers for the purpose of data confidentiality.

In June 2003, the U.S. government announced that AES could be used to protect classified information. AES soon became the default encryption algorithm for protecting classified information, as well as the first publicly accessible and open cipher approved by the NSA for Top Secret information. The NSA chose AES as one of the cryptographic algorithms to be used by its Information Assurance Directorate to protect national security systems.

The successful use of AES by the U.S. government led to the algorithm's widespread use in the private sector. AES has become the most popular algorithm used in symmetric key cryptography. The transparent selection process established by NIST helped create a high level of confidence in AES among security and cryptography experts.

3. Working

In this project, we proposed fake product detection using blockchain technology. This will be a web application in which manufacturer will be able to do registration. After registration, manufacturer will logged in into the system and register their products. At the time of product registration, our system will generate QR code for registered product. Supplier is another user in this system that will purchase products from manufacturers and register products again for customers. The customers will do registration and after login, they will be able to view supplier’s products with qr codes. Customers will scan QR code, and our system will check whether the product is present in our database. If the product exists, the product will be genuine otherwise we can declare it as fake product.



Modules

- **Admin Panel**
- Login
- Reports
- View suppliers
- View manufacturers
- View consumers
- **Products Management**
- Product Registration
- Product Cost Management
- Upload Product Photos
- **Order Processing**
- Buyer will Place product order
- View order details (For buyer and product owner)
- Process order (current product owner will process the pending order)
- **Supply Chain Management in Blockchain**
- Product Supply chain transactions will be maintained on distributed servers in the form of blocks

- The blocks will be maintained in sequence so that the consumer can view complete product details by scanning QR code

4. Result Analysis

The implemented system was tested using multiple product entries and user roles to examine its behavior under real usage conditions. The evaluation focused on QR verification, blockchain record validation, and encryption performance.

1. Product Registration and QR Code Generation

Manufacturers ran tests and managed to register several products through the system interface without any issues. Every time they added an entry, the system created a unique QR code and connected it to a blockchain record. They then scanned these QR codes using regular mobile apps, and all the products matched up with the right data. Looking at the screenshots, you can see that each product has its own identifier—no duplicates anywhere. So, the system does a good job keeping everything unique when products are registered.

2. Verification of Genuine vs Fake Products

To evaluate detection capability, two types of inputs were tested:

- Valid QR codes generated by the system
- Invalid or tampered QR codes

When valid QR codes were scanned, the system retrieved product details such as manufacturer, supplier, and transaction history. In contrast, tampered or unregistered QR codes returned no matching records and were flagged as invalid. This behavior shows that the system can effectively differentiate between authentic and counterfeit items.

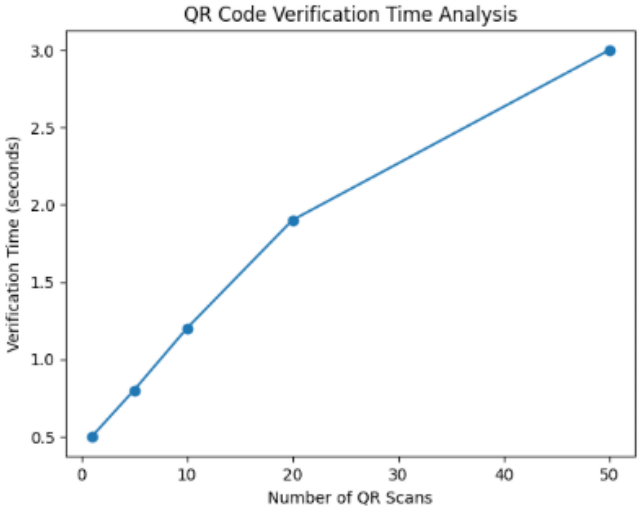
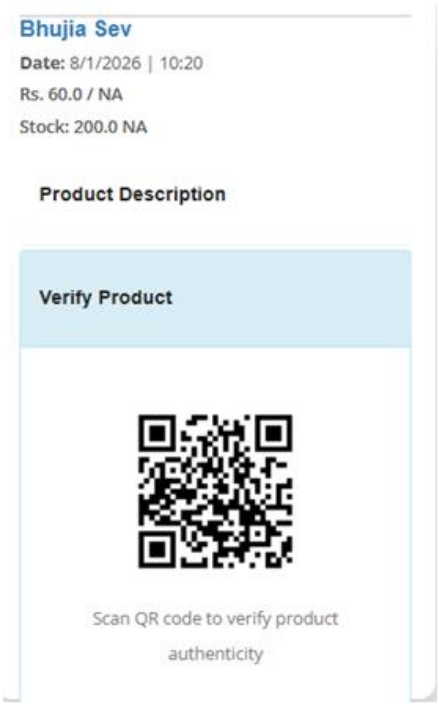


Fig.1: QR Code Verification Time Analysis

The graph shows the relationship between the number of QR code scans and the time required for verification. It can be observed that the verification time increases gradually with the number of scans, while still remaining within an acceptable range for real-time applications.



After Scanning Customer **will get Products result if product exists on server**

If QR verification Failed Product Detected as Fake

3. Blockchain Record Validation (SHA-2)

Every transaction in the system got hashed with SHA-2. Even the smallest tweak—like changing a product's price or updating the supplier—completely changed the hash value. That shows how sensitive the hashing really is. The blockchain used these hash links between blocks to keep everything connected. Whenever someone tried to mess with the stored data, the whole chain broke, and it was obvious right away. The tests clearly show that this hashing approach keeps the data consistent all the way through the chain.

4. AES Encryption Performance

Block data was encrypted using AES before storage. The encryption and decryption process was tested with multiple data sizes.

Observed results:

- Encryption time remained low for standard product data
- Decryption successfully restored original data without loss
- No readable data was exposed without the correct key

The performance measurements (as shown in your AES evaluation screenshots) indicate that AES adds security without introducing significant delay. This makes it suitable for real-time applications.

5. Transaction Flow in Supply Chain

The system was tested across different roles:

- Manufacturer → Supplier → Consumer

Each transaction was recorded as a block. When a product moved from one entity to another, a new block was added to the chain. The recorded results show that the full history of the product could be retrieved at any stage by scanning the QR code.

Screenshots demonstrate that users can view:

- Product origin
- Ownership changes
- Transaction timestamps

This confirms that the system ensures end-to-end traceability.

6. Response Time Analysis

The time taken for QR verification and data retrieval was measured during testing. The average response time was within a few seconds, depending on network conditions. No major delays were observed during normal operation.

7. Observations from Test Results

- All valid products were verified successfully
- Fake or unregistered products were consistently rejected
- Hash values changed instantly on data modification
- Encrypted data remained secure and inaccessible without keys
- Blockchain maintained proper sequence of transactions

The experiments show the system consistently catches fake products. Using QR codes, SHA-2 hashing, and AES encryption keeps the product data safe and easy to track, while also protecting it from tampering. The system's results match what it was supposed to do, proving it works well in real-world situations.

5. Conclusion

This system offers a real-world way to spot fake products by blending blockchain tech with QR code checks. Give each product its own digital ID, log everything on a distributed ledger, and you've got a solid method for tracking authenticity all along the supply chain.

Tests show it can reliably tell real products from fakes or ones with tampered records. SHA-2 hashing keeps the data solid, and AES encryption locks down any sensitive info so others can't poke around where they shouldn't. Every transaction gets tracked, so you can follow a product all the way from the manufacturer right through to whoever actually buys it.

Response times in testing stayed quick and the system didn't bog down. Checking a product's authenticity is easy—just scan the QR code with your phone. Plus, using blockchain makes it much harder for anyone to mess with the records, which helps cut down on fraud.

Still, there are a few things to work out before this could go truly big. The system depends on each product getting registered correctly, and you'll need a network connection, which can be tricky in some places. Adding offline checks and finding better ways to handle huge amounts of data could help deal with these issues.

In the end, this kind of blockchain-based tracking does what it's supposed to do: it makes it tougher for counterfeit goods to circulate. With some tweaks and more widespread use, it could make supply chains safer, more open, and a whole lot more trustworthy.

6. REFERENCES

[1] Muhammad Nasir Mumtaz Bhutta, Amir A. Khwaja, Adnan Nadeem, Hafiz Farooq Ahmad , Muhammad Khurram Khan, Moataz A. Hanif, Houbing Song, Majed Alshamari , and Yue Cao , "A Survey on Blockchain Technology: Evolution, Architecture and Security", IEEE special section on intelligent big data analytics for internet of things, services and people,2021, pp. 61048 – 61073.

[2] Rishabh Sushil Bhatnagar, Sneha Manoj Jha , Shrey Surendra Singh, Rajkumar Shende "Product Traceability using Blockchain", 2020 2nd International Conference on Advances in Computing, Communication Control and Networking (ICACCCN).

[3] Si Chen , Rui Shi , Zhuangyu Ren , Jiaqi Yan , Yani shi , Jinyu Zhang," A Blockchainbased Supply Chain Quality Management Framework", 2017 IEEE 14th International Conference on e-Business Engineering (ICEBE).

[4] M.C.Jayaprasanna, .V.A.Soundharya , M.Suhana, S.Sujatha," A Block Chain based Management System for Detecting Counterfeit Product in Supply Chain" ,IEEE 2021 Third International Conference on Intelligent Communication Technologies and Virtual Mobile Networks (ICICV).

[5] Jinhua Ma , Shih-Ya Lin , Xin Chen , Hung-Min Sun,A Blockchain-Based Application System for Product Anti-Counterfeiting" International Journal Of Scientific & Technology Research Volume 8, Issue 12, December 2019 issn 2277-8616.

[6] B. M. A. L. Basnayake, C. Rajapakse," A Blockchain-based decentralized system to ensure the transparency of organic food supply chain" ,IEEE 2019 International Research Conference on Smart Computing and Systems Engineering (SCSE)

[7] Atima Tharatipyakul and Suporn Pongnumkul, "User Interface of Blockchain-Based Agri-Food Traceability Applications", IEEE vol 9, 2019,pp.82909-82929