AuthentiGuard: Decentralized Product Authentication System using Blockchain for Counterfeit Detection

Dr.V. Dhanakoti[1], Dejaswarooba B[2], Gokul M[3], Dev Preeth Singh R[4]
[1]*Professor, SRM Valliammai Engineering College*
[2,3,4]*Student, SRM Valliammai Engineering College*

***Abstract*— Counterfeit items are a major threat to consumer safety, brand reputation, and economic stability. This study presents a new blockchain-based approach for dealing with counterfeiting by creating a safe and transparent product authentication platform. Each product is assigned a unique digital identifier that links to detailed information safely recorded on an immutable blockchain ledger. Smart contracts simplify authentication processes, allowing users to verify in real time using mobile apps or web interfaces. This enables consumers to make more informed purchasing decisions and builds trust in the supply chain. Furthermore, the system includes the Practical Byzantine Fault Tolerance (PBFT) consensus mechanism, which ensures secure and efficient network agreement. This improves system dependability and fault tolerance, giving stakeholders greater confidence in the inviolability of blockchain-recorded data.**

***Keywords*— Counterfeiting, blockchain-based approach, product authentication, transparency, smart contracts, Practical Byzantine Fault Tolerance (PBFT), supply chain trust.**

I. INTRODUCTION

The global market for counterfeit goods is a broad and pernicious phenomena, estimated to be worth $4.6 trillion. These imitations not only reduce real brand income, but also endanger consumer safety and public health. From fake pharmaceuticals with potentially life-threatening side effects to substandard electronics that risk fire hazards, counterfeits undermine consumer trust and disrupt healthy competition within the marketplace.
Traditional methods of tackling counterfeiting frequently rely on centralised verification processes and physical security measures. However, these options are limited. Centralised methods are subject to tampering and fraud, whereas physical precautions such as holograms or distinctive packaging can be copied with greater complexity. Furthermore, following a product's intricate route through traditional supply chains can be difficult, enabling opportunities for counterfeit products to enter the market unnoticed. In recent years, a groundbreaking technology called blockchain has developed with the potential
to change the fight against counterfeiting. Blockchain technology supports cryptocurrencies such as Bitcoin, but its possibilities go far beyond the financial realm. Blockchain is based on a distributed ledger system, which is essentially a digital record of transactions copied and securely stored across a network of computers. This scattered nature provides several major benefits:

- Immutability: Once data has been stored on the blockchain, it cannot be changed or erased without disrupting the entire network, making it very resistant to tampering and fraud.
- Transparency: All network members have access to the entire transaction ledger, which ensures a clear audit trail and fosters trust in the system.
- Security: Cryptographic hashing and consensus procedures safeguard the integrity and validity of data recorded on blockchains.

This study presents a revolutionary blockchain-based method for combating counterfeiting by providing a safe and transparent platform for product authentication. Our system uses blockchain technology's basic qualities - immutability, transparency, and security - to produce a decentralised and tamper-proof record of product information. To improve security and fault tolerance, our system includes the Practical Byzantine Fault Tolerance (PBFT) consensus mechanism. PBFT guarantees secure and efficient agreement across network nodes, even in the face of hostile actors, increasing faith in the immutability of blockchain-recorded data.

II. RELATED WORK

[1] APPB is characterized by offering dual advantages,

by utilizing the immutability of blockchain and keeping the privacy of product selling information and business relationship. Both security analysis and experimental results are conducted, and the results indicate that APPB can achieve privacy protection and anti-counterfeiting with acceptable efficiency. [2] We suggest a decentralised Blockchain system to stop the fabrication of fake products so that both the supplier and the consumer may use it to trade real goods without having to supervise directly owned stores, which can significantly reduce the cost of product quality assurance. In this project, Quick Response (QR) codes offer a powerful method to tackle the practice of product counterfeiting thanks to new developments in wireless and mobile technologies. [3] This paper uses blockchain technology to combat the sale of counterfeit products. We use blockchain to allow manufacturers to add authentic product serial numbers onto the ledger; consumers can then use the serial number to verify the authenticity of a product before purchasing it [4] We employ a data-driven content analysis approach to examine previous research on blockchain technology in operations management and supply chain management. We investigate the extent to which blockchain technology was considered in scholarly works, structure the research efforts, and identify trends, interrelated themes, and promising research opportunities. Quantitative and qualitative content analysis is conducted on an extensive literature sample of 410 articles. [5] This study aims to explore the current status, potential applications, and future directions of blockchain technology in supply chain management. A literature survey, along with an analytical review, of blockchain-based supply chain research was conducted to better understand the trajectory of related research and shed light on the benefits, issues, and challenges in the blockchain-supply-chain paradigm. [6] Since Bitcoin's debut in 2008, blockchain, the technology behind the cryptocurrency, has been gaining increasing scientific and industrial interest. Due to the technology's innate distributed and immutable features, the adoption of blockchains on supply chains is one of the most promising recent applications. [7] With the proposed POMS, a customer can reject the purchase of counterfeits even with genuine RFID tag information, if the seller does not possess their ownership. We have implemented a proof-of-concept experimental system employing a blockchain-based decentralized application platform, Ethereum, and evaluated its cost performance. [8] Current anti-counterfeiting supply chains rely on a centralized authority to combat counterfeit products. This architecture results in issues such as single point processing, storage, and failure. Blockchain technology has emerged to provide a promising solution for such issues. In this paper, we propose the block-supply chain, a new decentralized supply chain that detects counterfeiting attacks using blockchain and Near Field Communication (NFC) technologies.

III. METHODOLOGY

A. Product Registration and Unique Digital Identity:

The first phase in our blockchain-based anti-counterfeiting system is to register products and assign unique digital identities (UDIs) to them using QR codes. Manufacturers or authorized distributors register products by providing detailed information, such as product characteristics, production specifics, and safety certifications, to a specified blockchain platform. This process makes use of the accessibility and data capacity of QR codes. Following registration, each product is given a permanent and unique UDI, which can be an alphanumeric string or a hashed identification that is encoded into a QR code. Optional extra product data, such images, manufacturing dates, or regional variations, can also be included. Encryption and digital signature are two examples of security techniques used to guarantee the secrecy and integrity of the encoded data. In order to strengthen authenticity verification and discourage tampering, QR codes are strategically positioned on packaging or integrated directly into items. The incorporation of UDIs into blockchain technology guarantees a transparent and safe record of product validity, making it simple for customers to verify using mobile applications or online interfaces.

B. Secure Data Storage and Transparency:

Our suggested blockchain-based anti-counterfeiting system's transparent management and safe storage of product data are its main components. This section explores the complex balance that exists between protecting sensitive data secrecy and encouraging transparency about important product features. Product specifics including batch numbers, origin, materials, and production information are securely connected to the individual digital identification (UDI) that is assigned to every product in order to combat counterfeiting. The actual thing and its digital representation on the

blockchain are clearly linked by this interconnection.

Although establishing trust in the system requires transparency, some product information may need to be kept private. This might consist of:

- Formulas that are proprietary: For goods that have special formulations or trade secrets, the particulars of these formulas can be kept private while other data points are used to confirm the product's legitimacy.
- Supplier information: Certain manufacturing locations or the identity of raw material suppliers may be deemed commercially sensitive and kept private from the general public.
- Personally Identifiable Information (PII): Strict compliance with data privacy laws is essential when the product contains user data (such as linked devices). The blockchain should only contain aggregated or anonymized data that is necessary for the identification of counterfeiting.

Our system may make use of multiple strategies to allow for the transparent and selective exchange of product information:

- Access Control Lists (ACLs): ACLs specify on the blockchain who is allowed access to what data. Authorized users can be given access to private information while keeping public access to critical authenticating data, such as regulators, brand owners, or authorized verification authorities.
- Off-chain Storage: With a reference hash connecting it to the UDI on the blockchain, extremely private data can be safely stored off-chain. This guarantees the existence of the data without disclosing the details.
- Zero-Knowledge Proofs (ZKPs): ZKPs are cryptographic methods that enable users to demonstrate that they are in possession of particular data without actually disclosing that data. Without disclosing the precise source of the materials used in the manufacturing process, a ZKP could be used to prove that a product was made using those resources.

Transparency is given priority by the system, which provides users with a mobile app or web interface to obtain critical product information such as specifications, manufacturing details, and sustainability data. By offering details about a product's lifecycle, the use of recycled content, or fair trade methods, this openness promotes confidence and empowers customers to make informed decisions. It also appeals to environmentally conscious consumers. The solution guarantees improved protection against unauthorized access and manipulation when combined with secure data storage via blockchain technology. Additionally, selective sharing procedures maintain confidentiality for important information. In the end, this fusion of security and openness improves supply chain visibility and brand reputation by strengthening consumer trust and brand accountability.

C. Smart Contract Automation:

Self-executing programs that are kept on the blockchain are known as smart contracts. They specify a set of guidelines and requirements that are automatically activated upon the fulfillment of particular requirements. Smart contracts manage the essential functions of product authentication in our system.

The Workflow for Product Authentication:

Consumer Initiation: Users engage with the blockchain and the smart contract through a mobile application or online interface that is tailored to their needs.

UDI Input: Customers can start the authentication process in one of two ways:

- QR Code Scanning: A built-in QR code scanner may be included in the mobile app. Customers only need to scan the QR code linked to the UDI that is either embedded in the goods or on the box.
- Manual UDI Entry: Users have the option to manually input the UDI into the web interface or app.

Smart Contract Interaction: The blockchain's deployed smart contract communicates with the application or web interface. It sends the scanned or input UDI to the smart contract as input data.

Blockchain Data Retrieval: From the safe storage on the blockchain ledger, the smart contract retrieves the product details associated with the received UDI. Details like as origin, materials, manufacturing data, and batch numbers may be included in this information.

Execution of Authentication Logic: Using the acquired product data and the UDI itself as inputs, the smart contract carries out pre-established authentication logic. This reasoning could include:

- UDI Validation: The smart contract checks the UDI's validity and format to make sure it hasn't been altered.

- Data matching involves comparing the product information that was retrieved with a predetermined set of criteria that were recorded on the blockchain. Owners of brands may set these requirements, which could include information on anticipated manufacturing locations, material composition, or batch number ranges.

Authentication Outcome: When the authentication logic is executed, the smart contract produces an output that indicates if the product is considered valid or fake.
Customer Notification: The consumer is presented with the authentication result in an easy-to-understand style via the mobile app or web interface. A straightforward "Genuine" or "Counterfeit" notification may be included, coupled with more information for transparency (such as the cause of the authentication failure).

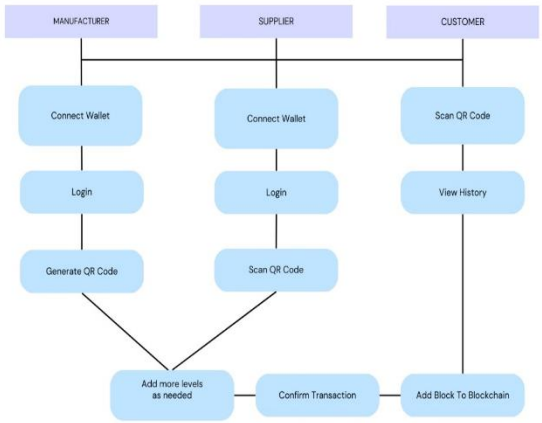

Fig 1: Workflow

D. Secure Consensus with PBFT:
Our blockchain-based anti-counterfeiting system's ability to successfully store product information depends on it. This section explores how the blockchain's data integrity and immutability are guaranteed via the Practical Byzantine Fault Tolerance (PBFT) consensus method. Byzantine failures are a common problem for traditional distributed systems. These failures extend beyond straightforward node crashes and include instances in which nodes behave maliciously, giving false or contradictory information. Within our system, the integrity of the entire system could be compromised by a Byzantine malfunctioning node trying to change product information that is kept on the blockchain.

A key component of our system is the Practical Byzantine Fault Tolerance (PBFT) consensus algorithm. It offers a reliable method of reaching consensus across nodes in a distributed setting, even when Byzantine faults occur. A multi-phase communication mechanism underpins PBFT's operations, guaranteeing agreement on the blockchain's current state. The protocol proceeds through the prepare, commit, and decision phases after starting with the pre-prepare phase, in which a primary node suggests improvements to the blockchain. Replica nodes verify proposals, send out agreement messages, and complete modifications during these phases, guaranteeing data consistency throughout the network. Because of PBFT's multi-phase strategy, our system is resilient and can survive hostile situations while preserving the blockchain ledger's integrity.

A variety of fault tolerance techniques are incorporated into PBFT in order to successfully handle Byzantine failures. Robust leader elections are essential to its resilience because they guarantee that a certain primary node coordinates every consensus round. We periodically rotate this leadership role to reduce the possibility of manipulation. Moreover, before approving an update, PBFT requires consent from the majority of trustworthy nodes (usually two-thirds), preventing the disproportionate influence of a single bad node. To ensure the stability and integrity of the system, PBFT utilizes a view change protocol to remove a node that exhibits suspicious activity and elect a new leader. Together, these fault tolerance techniques strengthen our system's defenses against Byzantine failures and increase its dependability in hostile circumstances.

By guaranteeing consensus in spite of any Byzantine failures, PBFT greatly strengthens the security of our system and fortifies the blockchain's integrity. The authenticity of product information stored on the blockchain is efficiently protected by PBFT's multi-phase communication method, which maintains data immutability by requiring agreement from a majority of honest nodes before confirming revisions. Moreover, PBFT improves fault tolerance, allowing the system to continue functioning and being dependable even when certain nodes are compromised. But large-scale network scalability is still a problem, which is why researchers are continuously looking on optimizations and different consensus methods to solve this issue for more

widespread blockchain applications. The robustness of our system is greatly enhanced by PBFT's contributions to fault tolerance, data integrity, and security, even in spite of scaling concerns.

IV. CONCLUSION

By giving customers real-time verification capabilities at the point of sale, the suggested blockchain-based anti-counterfeiting system reduces the possibility that they may unintentionally acquire counterfeit goods. Having access to comprehensive product details, such as materials, origin, sustainability practices, and safety certifications, helps customers make well-informed decisions and encourages them to take an active role in the fight against counterfeiting by quickly reporting any suspected fakes. Effective anti-counterfeiting measures improve brand reputation; the immutability of the blockchain ledger improves brand protection; consumer trust in the authenticity of products drives sales and customer loyalty; and streamlined authentication procedures improve operational efficiency for brand owners. The system's verifiable and secure features improve supply chain traceability by making it possible to identify vulnerabilities and the source of counterfeit goods. Accountability among all parties involved promotes ethical sourcing and quality control procedures, and the lower risk of fraud reduces supply chain fraud. Blockchain technology facilitates cooperation amongst brand owners, producers, distributors, and retailers in the fight against counterfeiting. Metrics such as lower counterfeit detection rates, higher consumer verification activity, better brand reputation, and higher supply chain efficiency can be used to assess the system's efficacy. In order to maximize the system's impact in creating a more secure and trustworthy marketplace for all participants, future considerations include raising consumer awareness, promoting industry-wide standards and interoperability between various anti-counterfeiting blockchain platforms, and seamlessly integrating the system with existing infrastructure.

REFERENCES

[1] “APPB: anti-counterfeiting and privacy-preserving blockchain-based vehicle supply chains” Can Zhang , Liehuang Zhu, Chang Xu , Kashif Sharif , Rongxing Lu , and Yupeng Chen

[2] “Fake product identification system using blockchain” Mallegowda M, Anita Kanavalli, M.N. Thippeswamy, Kushagra Gupta, Lakshya Khandelwal, Vishal Bhattad

[3] “A blockchain-based fake product identification system” Yasmeen Dabbagh, Reem Khoja, Leena AlZahrani, Ghada AlShowaier, Nidal Nasser

[4] “Blockchain technology in operations & supply chain management: a content analysis” Jacob Lohmer, Elias Ribeiro da Silva, Rainer Lasch

[5] “When blockchain meets supply chain: a systematic literature review on current development and potential applications” Shuchih E. Chang, Yichian Chen

[6] “A novel blockchain-based product ownership management system (poms) for anti-counterfeits in the post supply chain” Kentaroh Toyoda, P. Takis Mathiopoulos, Iwao Sasase, Tomoaki Ohtsuki

[7] “Blockchain implementations and use cases for supply chains-a survey” Peter Gonczol, Panagiota Katsikouli, Lasse Herskind, Nicola Dragoni