IARJSET ISSN (O) 2393-8021, ISSN (P) 2394-1588

International Advanced Research Journal in Science, Engineering and Technology

Impact Factor 8.311 ⁜ Peer-reviewed & Refereed journal ⁜ Vol. 12, Issue 7, July 2025

DOI: 10.17148/IARJSET.2025.12745

Blockchain-Based Counterfeit Product Detection

Chaitra M. Kulkarni[1], Neha S. Naik[2], Hrishikesh Mogare[3]

MCA Student, Department of Computer Applications, Gogte Institute of Technology, Belagavi, India[1]

MCA Student, Department of Computer Applications, Gogte Institute of Technology, Belagavi, India[2]

Assistant Professor, Department of Computer Applications, Gogte Institute of Technology, Belagavi, India[3]

Abstract: Fake products are sold as original products at a slightly cheaper rate. These fake products are usually sold to make good money by selling counterfeit products using brand logos or names, but in reality they are a cheap quality product. Such fake products attract only using brand names, but are a growing scam. These products are designed to look almost similar to original ones. These types of products are termed as Second copy. These fake products not only damage brand value and economic systems but also pose significant threats to consumer health and safety. Traditional technologies for product verification, such as holograms, RFID, and barcodes, are increasingly being defeated by counterfeiters. Blockchain plays an important role in detecting fake products using various approaches. The approaches discussed range from Ethereum-based smart contracts to Hyperledger Fabric systems and advanced QR code encryption techniques. These systems ensure data integrity, enhance product traceability, and minimize reliance on centralized intermediaries. Additional layers like protected QR codes and AES encryption further bolster security against cloning and tampering.

Keywords: Blockchain, Counterfeit Detection, Smart Contracts, Product Traceability, QR Code Encryption, Ethereum, Hyperledger.

I. INTRODUCTION

The growth of fake goods is a growing risk that affects many consumer-facing industries. These counterfeit products sometimes seem to be from real sellers or brands, are sold by slightly altering brand logos and fool people into purchasing unsafe items. Examples: fake clothes, medical and beauty goods. The scale of the problem is massive. According to the OECD, counterfeit goods make up over 3% of global trade.

Consumers, enticed by lower prices, frequently fall prey to these deceptive products. In doing so, they compromise quality, after sale service as well that come with original products. However, such purchases harm the reputation of firms and give motivation to carry out illegal selling of goods. The situation is growing faster in industries like healthcare, where fake drugs can result in life danger situations. Traditional anti-counterfeiting mechanisms, including barcodes, holograms, and RFID tags, offer some level of protection but are ultimately centralized and vulnerable to replication. These tools depend on human verification, which can be fake or modified. This can raise fake trust based on altered data.

Blockchain technology introduces a paradigm shift in addressing these challenges. Built on decentralized and cryptographically secure principles, blockchain allows for the creation of tamper-proof transaction records. This data can be used to check the full cycle of a good from production to sale. Using this technology of smart contract is helpful in proving the originality. Along with this, identifiers like QR code or NFC chips can help buyers to know information about real goods using mobile or scan apps. This approach offers both digital and physical security, establishing a more robust framework for counterfeit detection.

Furthermore, smart contracts, programs that run on the blockchain, enable automated authenticity checks. With encrypted QR codes and dual-layer frameworks, blockchain-based systems provide physical and digital protection. This paper reviews key developments in the domain and outlines both the capabilities and constraints of using blockchain for counterfeit product detection.

II. RELATED WORK

As fake goods become more common in global supply chains, more complex technology solutions are needed. QR codes, barcodes, and RFID tags are some of the most common ways to stop counterfeiting, but they have certain problems. For example, they can be copied, data is stored in one place, and they aren't very clear. Blockchain technology has become a promising alternative since it is unchangeable, decentralized, and open.

IARJSET ISSN (O) 2393-8021, ISSN (P) 2394-1588

International Advanced Research Journal in Science, Engineering and Technology

Impact Factor 8.311 ⁜ Peer-reviewed & Refereed journal ⁜ Vol. 12, Issue 7, July 2025

DOI: 10.17148/IARJSET.2025.12745

A. Blockchain for Keeping the Supply Chain Safe

The use of blockchain in the supply of goods has gotten a lot of importance recently because it makes things more transparent and easier. One of the early studies by Tian in 2016 talked about mixing blockchain with IoT sensors to build a full system for tracking food from source to sale. With this setup, every single transaction or movement of goods gets recorded right away, which means you can track the product through its entire journey. This increases trust in the good and reduces the need for manual checking.

Later on, in 2017, Toyoda and others took this further by showing how blockchain could be useful in logistics too. They explained how the data that proves a product's origin—also called provenance—could be stored on a blockchain and accessed by many different people, like manufacturers, delivery partners, and even the end customers. And the best part? You don't have to depend on one central authority anymore to tell you whether something's real or not.

B. Using Smart Contracts to Verify Products

Smart contracts are kind of like automated rules or scripts that run on blockchain. In the case of detecting fake products, they help by doing the verification steps automatically. For example, on Ethereum, developers can create smart contracts that store key product info—things like batch number, who made it, when it was made, and who currently owns it.

Some popular platforms like VeChain and OriginTrail already use this method. They let users scan QR codes or tags that connect to a smart contract, which then checks if everything is legit. Since these checks are automatic, there's less chance of human mistakes, and it's a lot quicker, especially if you're dealing with thousands of items.

C. Tokenization to Stop Counterfeiting

Another cool idea is tokenization. This is where every real product gets its own unique digital twin on the blockchain, usually in the form of an NFT or a token. Bae and his team explored this concept in 2020 for high-end luxury items. Their system gave each item a digital ID, like a fingerprint, that lives on the blockchain. That way, anyone with access—like a buyer or seller—can look it up and confirm if it's the real deal.

And if the item doesn't have a matching token? Well, it might be fake. This way not only helps know counterfeits but also provides extra features like generating digital warranty.

D. Connecting with IoT and Frontend Devices

Lots of modern anti-counterfeit systems are combining blockchain with things like QR code readers, mobile apps, or smart sensors. This makes it easier for regular users—not just tech people—to check if what they're buying is real. Big names like IBM's Food Trust or Everledger are already doing this for things like wine, diamonds, and even electronics. By scanning a code on your phone, you can instantly get the full background of a product. And with IoT devices in the mix, companies can also keep tabs on stuff like temperature, humidity, or rough handling—things that matter a lot for sensitive goods.

E. Limitations and Next Steps

Now, even though blockchain sounds like the perfect solution, it's not all smooth sailing. One major issue is scalability. On public blockchains, every transaction takes time and costs money (thanks to gas fees), which can be a pain if you need to do a lot of them quickly.

Another big problem is the data that gets entered in the first place. If someone adds wrong info at the beginning, the blockchain will lock it in forever—even if it's incorrect. That kind of defeats the point of having a tamper-proof system, right?

To fix these, researchers are looking into new solutions. Things like AI to double-check data before it's recorded, systems that let different blockchains talk to each other, and better rules for working across borders. Some suggest using a mix of public and private blockchains, so you get both openness and control depending on the need.

III. METHODOLOGY

A. Ethereum-Based Smart Contract Systems

One of the most common blockchain platforms used for counterfeit detection is Ethereum. The big reason is that it supports smart contracts really well. In some of the research, like what Gupta did, Ethereum's test network—called Goerli—was used to create and test smart contracts that check whether a product is real or not. These contracts are tied to QR codes that get scanned by the user.

IARJSET ISSN (O) 2393-8021, ISSN (P) 2394-1588

International Advanced Research Journal in Science, Engineering and Technology

Impact Factor 8.311 ⁜ Peer-reviewed & Refereed journal ⁜ Vol. 12, Issue 7, July 2025

DOI: 10.17148/IARJSET.2025.12745

So here's how it works: let's say a customer buys a product and scans the QR code with their phone. That QR code is linked to a contract already on the blockchain. The contract then automatically checks if the QR data matches what's stored on the blockchain. If everything matches, the product is genuine; if not, the system flags it. MetaMask, which is a browser-based wallet, is often used to interact with these contracts easily.

This setup helps users validate product authenticity in a way that's fast and doesn't require them to contact the brand or seller. And since the data is already locked on-chain, no one can go back and edit it.

B. Hyperledger Fabric and Encrypted Frameworks

Ethereum is good for open networks, but when companies need more privacy and control, they often go for something like Hyperledger Fabric. One example is the FPISMF model, which uses Fabric to store product data that's been encrypted using AES (Advanced Encryption Standard).

What's special here is that the QR codes themselves are a bit smarter. If the scan is blurry or something is off, the system can correct the error because it uses error-correcting codes. Also, the code is only readable by systems that have the proper key or authorization. That adds another layer of safety.

And since Hyperledger is permissioned, only authorized members like manufacturers or regulators can write data to the blockchain. This avoids unnecessary traffic and helps maintain performance even when supply chains are large and complex.

C. Multi-Layer QR Code Protection Systems

Some researchers have gone a step further by creating QR codes that are unreadable by regular scanners. For example, Aulia et al. developed a method where only the brand manufacturer's system can read and decode the QR code because the metadata is stored in a special encrypted format.

This is especially useful in sectors like pharmaceuticals, where fake pills or medical devices can be a matter of life and death. By having QR codes that can't be cloned or interpreted without special software, counterfeiters are blocked right at the packaging level.

D. Blockchain Frameworks with Two Layers

There are also solutions that use a two-layer blockchain structure. A study by Ding et al. proposed a system where there's one blockchain that everyone can see—the public facing layer—and another private blockchain that stores sensitive company data.

So the consumer can still scan a code and check product authenticity on the public blockchain, while regulators or trusted entities can access deeper information through the private layer. This structure keeps everything efficient and secure, and only the right people get access to the right data.

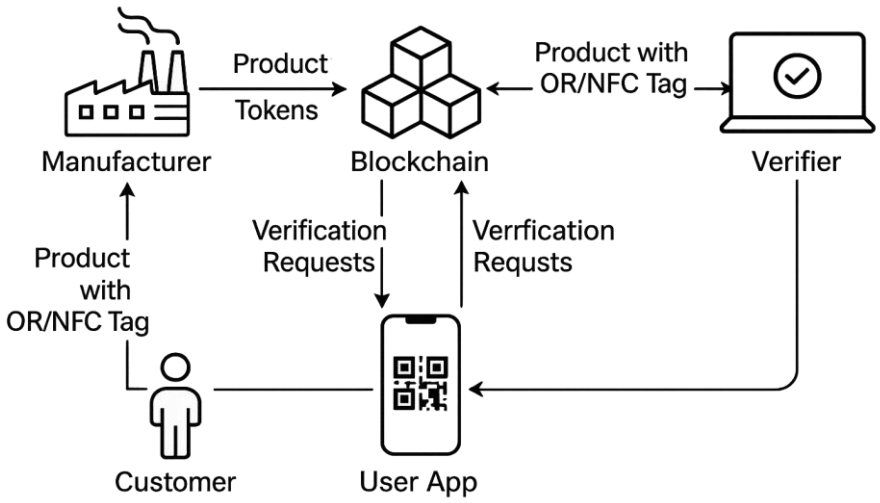

Fig. 1 Overall System Architecture

IARJSET ISSN (O) 2393-8021, ISSN (P) 2394-1588

International Advanced Research Journal in Science, Engineering and Technology

Impact Factor 8.311 ⁜ Peer-reviewed & Refereed journal ⁜ Vol. 12, Issue 7, July 2025

DOI: 10.17148/IARJSET.2025.12745

The Overall System Architecture Diagram presents a high-level view of how a blockchain-based counterfeit product detection system functions. It showcases the interaction between major entities: manufacturers, blockchain networks, verifiers, user applications, and customers.

The process begins at the manufacturer's end, where a unique digital identity (via token or QR/NFC) is assigned to a product and registered on the blockchain. Once the product enters the supply chain, end-users can scan the code using a mobile application, which sends a verification request to the blockchain.

The blockchain then interacts with a verifier module, which cross-validates the data. The verified result is transmitted back to the user, confirming whether the product is genuine. This architectural flow establishes a decentralized trust mechanism, ensuring tamper-proof authenticity checks across the lifecycle.

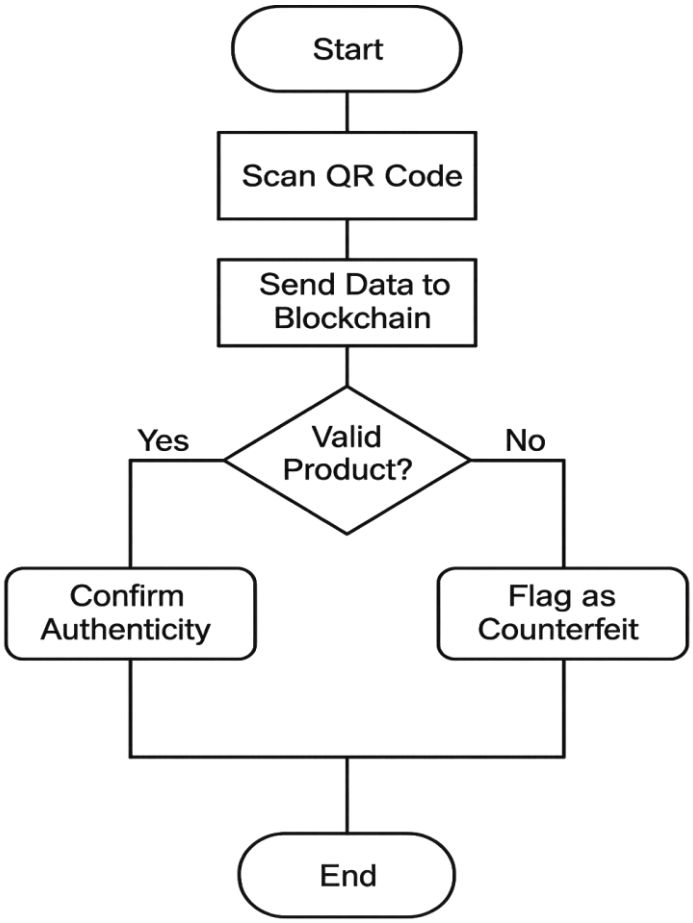

Fig. 2 Activity Diagram

The Activity Diagram illustrates the sequential steps involved in verifying a product's authenticity using blockchain-based systems. The process initiates when a customer scans a product's QR code. This scan activates a smart contract on the blockchain that cross-checks the product's metadata.

Following this, the smart contract performs an authenticity check. If the product's digital record matches a valid entry on the blockchain, the system emits a confirmation event. Conversely, if no match is found, the item is flagged as counterfeit. The customer is then notified of the result, concluding the verification process.

This diagram offers a clear visual representation of how blockchain, smart contracts, and QR verification come together to enable real-time counterfeit detection.

IARJSET ISSN (O) 2393-8021, ISSN (P) 2394-1588

International Advanced Research Journal in Science, Engineering and Technology

Impact Factor 8.311 ⁜ Peer-reviewed & Refereed journal ⁜ Vol. 12, Issue 7, July 2025

DOI: 10.17148/IARJSET.2025.12745

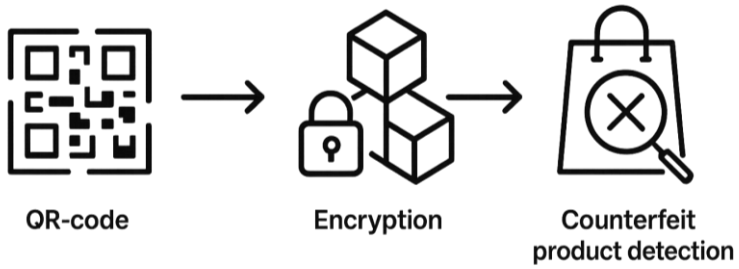

Fig. 3 QR Flow

The Smart Contract Workflow Diagram outlines the automated process of validating a product's authenticity using smart contracts on a blockchain platform like Ethereum.

The flow begins with the deployment of a smart contract on either a testnet (e.g., Goerli) or the Ethereum main net. Each product is associated with a unique QR code that encodes critical metadata such as product ID, batch number, and manufacturing timestamp.

When a consumer or stakeholder scans the QR code using a verification application, the encoded data is extracted and sent to the smart contract. The contract then cross-verifies this information with its on-chain records.

If the input data matches a valid, non-expired, and unaltered entry within the smart contract, the system emits a success event confirming the product's authenticity. Conversely, if there is a mismatch or the product record is absent, the contract halts the process and flags the product as potentially counterfeit.

This entire workflow leverages blockchain's inherent properties—immutability, transparency, and automation—to ensure secure, real-time, and tamper-proof product validation without requiring centralized manual intervention.

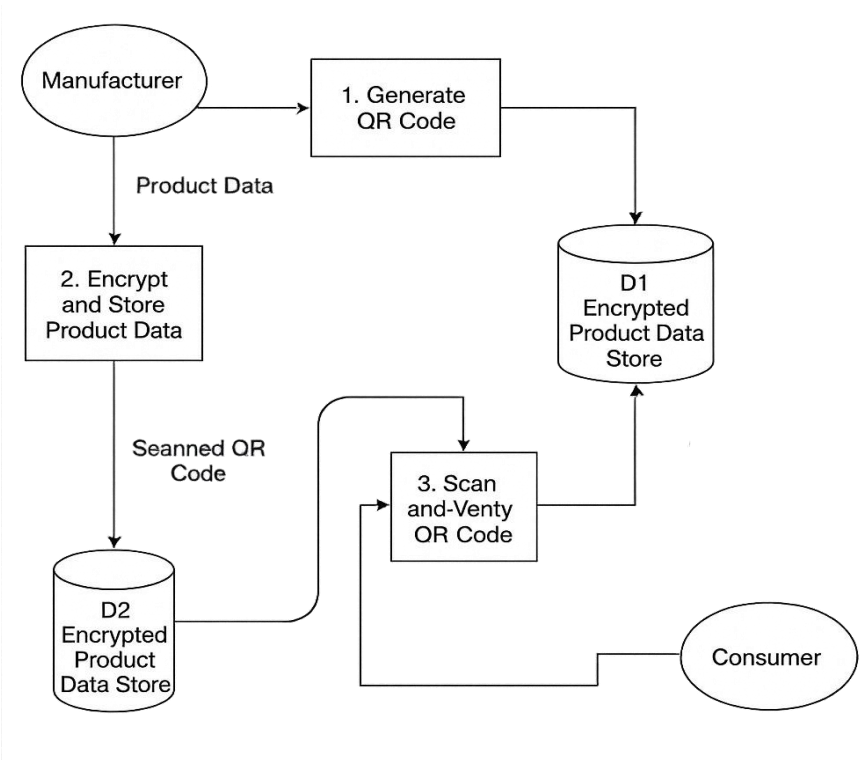

Fig. 4 Data Flow Diagram

The Activity Diagram illustrates the sequential steps involved in verifying a product's authenticity using blockchain-based systems. The process begins when a customer scans a product's QR code, initiating the verification workflow.

IARJSET ISSN (O) 2393-8021, ISSN (P) 2394-1588

International Advanced Research Journal in Science, Engineering and Technology

Impact Factor 8.311 ⁜ Peer-reviewed & Refereed journal ⁜ Vol. 12, Issue 7, July 2025

DOI: 10.17148/IARJSET.2025.12745

Once the scan is completed, a smart contract associated with the QR code is triggered on the blockchain network. This smart contract fetches and evaluates the corresponding product metadata, comparing it with the blockchain ledger's stored records.

If the retrieved data matches a legitimate, registered product entry, the contract emits a confirmation event indicating successful authentication. Otherwise, if no valid match is found or if the record has been tampered with, the contract flags the product as counterfeit.

Finally, the system notifies the customer of the verification result—whether the product is authentic or counterfeit—thus completing the validation process. This flow highlights how blockchain, smart contracts, and QR verification work in tandem to enable secure, automated, and real-time counterfeit detection.

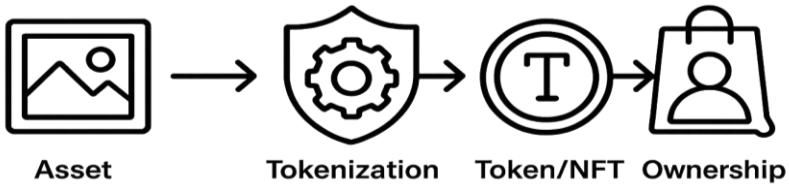

Fig. 5 Tokenization Flow for NFT-Based Ownership

The Tokenization Flow diagram illustrates the step-by-step process of converting real-world or digital assets into tokens or NFTs on a blockchain network. The process begins with an Asset, which can be a physical or digital item such as artwork, certificates, or documents. This asset is then subjected to tokenization, where a unique digital representation of the asset is created using blockchain-compatible technologies and smart contract logic.

Once tokenized, the result is a Token or NFT (Non-Fungible Token), which securely and immutably represents the asset on the blockchain. This token is then associated with an individual or entity, marking the final stage as Ownership. Ownership of the NFT allows for verifiable, transferable rights over the asset, enabling traceability and security within decentralized ecosystems.

Technology Security Level Limitations Barcodes/Holograms Low Easy to replicate RFID Tags Medium Expensive for mass use Blockchain (Public) High Gas fees, slower speed Hyperledger (Private) High Less transparent, more complex Tokenization (NFT) Very High Needs wallet integration.

TABLE I: Comparison of Counterfeit Detection Technologies

Technology	**Security Level**	**Limitations**
Barcodes/Holograms	Low	Easy to replicate
RFID Tags	Medium	Expensive for mass use
Blockchain (Public)	High	Gas fees, slower speed
Hyperledger (Private)	High	Less transparent, more complex
Tokenization (NFT)	Very High	Needs wallet integration

IV. OUTCOMES

A. Stronger Verification of Product Authenticity

All these systems had one big thing in common: they made it easier to track a product and prove it was real. Because blockchain records can't be changed after they're written, no one can go back and fake a product's history. This gives a solid base for authenticity, even if the product moves through many hands.

IARJSET ISSN (O) 2393-8021, ISSN (P) 2394-1588

International Advanced Research Journal in Science, Engineering and Technology

Impact Factor 8.311 ⁜ Peer-reviewed & Refereed journal ⁜ Vol. 12, Issue 7, July 2025

DOI: 10.17148/IARJSET.2025.12745

It also helps manufacturers monitor their own supply chain. They can see exactly when and where their products are being sold, and if something fishy is going on—like sales happening in unauthorized regions—they'll know right away.

B. Reduced Counterfeit Risks

By connecting each product to a digital identity on the blockchain, it becomes way harder to fake it. If someone tries to sell a copy, and that copy's QR code or token doesn't match what's on the blockchain, it gets caught immediately.

This kind of system discourages counterfeiters because the moment something doesn't check out, users and regulators are alerted. Plus, even if someone copies a QR code, the system can flag duplicates or invalid scans.

C. Higher Trust and Transparency

Consumers these days care a lot about where their products come from. Whether it's a designer bag, a smart phone, or even groceries—people want to know the origin. With blockchain, they can scan a product and get instant access to its background.

Retailers and sellers also benefit. They can prove to customers that their goods are legitimate, which builds brand trust. And from the manufacturer's side, transparency helps detect leaks in the distribution network or unauthorized sellers.

D. Easy Integration with Mobile and Web

Another good outcome was that most of these blockchain systems worked well with mobile apps or web interfaces. So even users who aren't very technical can just scan a code and get the info they need.

This also allows for extra features like warranty registration, customer feedback, or loyalty programs—making the system more useful for both buyers and sellers.

E. Future Scalability and Customization

Most of the models studied were designed in a way that they could grow. That means the core system could work in different industries—like food, electronics, or cosmetics—and new tech like AI or IoT sensors could be added later.

So while the current solutions focus on product authenticity, there's room to make them smarter. For example, adding an AI-based fraud detection layer or letting two different blockchains talk to each other through bridges.

V. USE CASE SCENARIO: VERIFYING LUXURY GOODS

To demonstrate the practicality of our proposed system, consider a scenario in the luxury goods industry, where counterfeit handbags often flood the market. A manufacturer embeds an encrypted QR code tied to a unique token stored on a blockchain. When a customer purchases the product, they scan the QR code using a mobile app.

This scan triggers a smart contract on the Ethereum blockchain, which verifies the token's authenticity. If the token exists and is valid, the application confirms that the product is genuine. If not, the system alerts the user that the product may be counterfeit. This real-time validation not only assures customers but also helps brands maintain their market credibility and reduce post-sale verification costs.

VI. CHALLENGES AND FUTURE WORK

A. Challenges

- Data Entry Integrity: One of the biggest challenges is making sure that the data entered into the blockchain is accurate in the first place. Since blockchain records are immutable, any mistake or tampered entry becomes permanent, leading to unreliable verification results.
- Scalability and Transaction Costs: As blockchain networks grow, especially public ones like Ethereum, the cost (gas fees) and time to validate transactions can become a bottleneck. This can be a serious issue in large-scale real-time systems like global supply chains.
- Privacy Concerns: Public blockchains are transparent by nature, which could lead to sensitive business data being exposed. Without privacy-preserving techniques or permissioned chains, companies may hesitate to adopt blockchain solutions.
- Technology Adoption: In many regions, especially developing countries, the infrastructure to support blockchain systems may be lacking. This includes everything from internet access to technical skills and awareness, which slows down adoption.

IARJSET ISSN (O) 2393-8021, ISSN (P) 2394-1588

International Advanced Research Journal in Science, Engineering and Technology

Impact Factor 8.311 ⁜ Peer-reviewed & Refereed journal ⁜ Vol. 12, Issue 7, July 2025

DOI: 10.17148/IARJSET.2025.12745

- Integration with Legacy Systems: Most enterprises still operate on traditional centralized IT systems. Connecting these older infrastructures with decentralized blockchain networks is not straightforward and often requires custom middleware or APIs.

B. Future Work

- AI-Based Data Validation: Machine learning can be used to validate incoming data before it is recorded on the blockchain. AI can flag anomalies or inconsistencies in product metadata to reduce human errors and fraud.
- IoT Integration: Using smart sensors, RFID tags, and GPS trackers can help automate data collection in real-time. These IoT devices can send verified updates to the blockchain, improving data quality and reducing manual inputs.
- Cross-Blockchain Communication: There is increasing interest in enabling different blockchain platforms, such as Ethereum and Hyperledger, to work together. Bridges and interoperability protocols can unify systems, allowing more seamless and scalable verification.
- Legal Smart Contracts: Future systems could include legally enforceable smart contracts that comply with regulations and provide stronger guarantees for dispute resolution across borders and jurisdictions.
- User Experience Enhancements: Simplifying mobile interfaces, supporting multiple languages, and designing intuitive user flows will be essential for getting widespread user adoption, especially by non-technical stakeholders like everyday consumers and small retailers.

VII. FUTURE ENHANCEMENTS

As the landscape of blockchain technology continues to evolve, several enhancements can be integrated into counterfeit detection systems to improve performance, scalability, and user adoption. These future enhancements aim to bridge the gap between technological innovation and practical deployment across various industries.

- Decentralized Identity (DID): Incorporating de-centralized identity frameworks will allow manufacturers, distributors, and consumers to authenticate themselves without relying on centralized authorities. This enhances trust and accountability across the supply chain.
- Integration with Zero-Knowledge Proofs (ZKPs): Zero-Knowledge Proofs can be used to validate product authenticity without revealing sensitive metadata on public chains. This preserves privacy while ensuring tamper-proof verification.
- Digital Watermarking with Blockchain Anchoring: Embedding invisible digital watermarks in product packaging or labels and anchoring the signature on the blockchain can further deter tampering or cloning attempts, especially in luxury goods and pharmaceuticals.
- Multichain Compatibility: Future solutions may benefit from being blockchain-agnostic. Supporting Ethereum, Hyperledger, Polygon, and other networks would enable flexible deployments and better interoperability based on enterprise needs.
- Consumer Incentivization Models: Rewarding consumers with micro-incentives (e.g., tokens or loyalty points) for scanning and verifying products can increase user engagement and early counterfeit detection at the retail level.
- Integration with Legal Enforcement Mechanisms: Systems can be extended to notify regulatory authorities in real-time when a counterfeit product is detected, allowing for swift legal action and stronger deterrence.

VIII. REAL-WORLD APPLICATIONS

Blockchain-based counterfeit detection systems have immense potential across various sectors. By leveraging immutable records, smart contracts, and tokenization, these systems offer robust protection against tampering and fraud.

A. Pharmaceutical Industry

Fake drugs are a major global health risk. Using blockchain, each medicine pack can be assigned a unique, encrypted QR code tied to a smart contract. Pharmacies and patients can instantly verify the drug's authenticity before use. Blockchain ensures full traceability from manufacturer to end-user, significantly reducing counterfeit circulation.

B. Luxury Goods and Fashion

High-end fashion brands often fall victim to second copy or lookalike products. Blockchain-backed digital certificates and NFTs can verify originality, while consumer apps enable easy verification during resale or secondary purchases.

C. Electronics and Hardware

IARJSET ISSN (O) 2393-8021, ISSN (P) 2394-1588

International Advanced Research Journal in Science, Engineering and Technology

Impact Factor 8.311 ⁜ Peer-reviewed & Refereed journal ⁜ Vol. 12, Issue 7, July 2025

DOI: 10.17148/IARJSET.2025.12745

Counterfeit electronic parts are a growing problem, especially in defense and aerospace. Blockchain can log manufacturing origin, part serial numbers, and quality inspection records. Smart contracts can automate warranty validation and flag grey-market devices.

D. Agriculture and Food Supply Chains

Products like organic vegetables, seafood, or halal meat need clear provenance. QR-based blockchain tags ensure authenticity claims (e.g., farm origin, organic certification) are verifiable and transparent.

E. Art and Collectibles

NFT-backed digital ownership for art, sports memorabilia, or collectibles prevents duplication and establishes transparent ownership history. This model also enables fractional ownership and resale authenticity.

TABLE II: Comparison with Traditional Anti-Counterfeiting Techniques

Aspect	**Traditional Methods**	**Blockchain Based Approach**
Data Integrity	Can be manipulated	Immutable and tamper-proof
Verification	Manual, error-prone	Automated with smart contracts
Transparency	Limited visibility	Fully transparent ledger
Scalability	Requires central control	Distributed and scalable
Security	Relatively weak	Strong cryptographic security

Ethical and Legal Considerations: Implementing blockchain for counterfeit detection also raises important questions about data privacy, compliance with international laws, and consumer rights. Solutions must be designed to meet data protection standards such as GDPR. Moreover, legal frameworks for smart contracts are still evolving, and collaboration with regulators will be key for real-world deployment.

IX. CONCLUSION

Counterfeit product detection is no longer just a challenge for brand protection—it has become a global issue that affects consumer safety, market integrity, and the economy as a whole. Traditional mechanisms like holograms, RFID, and barcodes, while useful in the past, are increasingly inadequate against sophisticated counterfeiting methods. Blockchain technology offers a promising alternative by providing transparency, immutability, and decentralization—features that are well-suited for verifying product authenticity throughout complex supply chains.

This paper has explored how blockchain, especially when combined with smart contracts, tokenization, and encrypted QR codes, can create a secure infrastructure for anti-counterfeiting. Various approaches, from Ethereum-based public solutions to Hyperledger-based private frameworks, show that blockchain systems can be tailored to different industries and use cases. Additionally, integrating frontend apps, IoT devices, and multi-layer architectures makes it easier for both businesses and consumers to engage in real-time product verification.

However, the journey toward mass adoption is still in its early stages. Technical hurdles like transaction scalability, data privacy, and system interoperability must be addressed. There are also practical concerns involving legal frameworks, user education, and infrastructure readiness, especially in developing regions.

Future developments should focus on creating more intelligent and scalable ecosystems. AI can assist in validating data inputs, IoT devices can ensure continuous real-world tracking, and cross-chain bridges can unify currently fragmented blockchain platforms. Legal frameworks for smart contracts and enhanced user experiences will also be key to widespread adoption.

In summary, while blockchain is not a silver bullet, it represents a transformative shift in how we approach counterfeit detection. With the right advancements, collaborations, and regulatory support, it has the potential to make global supply chains significantly more secure and trustworthy.

DOI: 10.17148/IARJSET.2025.12745

ACKNOWLEDGMENT

The authors wish to express their heartfelt gratitude to the Department of Computer Applications at KLS Gogte Institute of Technology, Belagavi, for their unwavering support and academic assistance during this research. The insightful guidance from the faculty members significantly influenced the trajectory and quality of this study.

REFERENCES

[1]. S. Nakamoto, "Bitcoin: A Peer-to-Peer Electronic Cash System," 2008. [Online].
[2]. C. Cachin, "Architecture of the Hyperledger Blockchain Fabric," *Workshop on Distributed Cryptocurrencies and Consensus Ledgers*, 2016.
[3]. M. Crosby et al., "Blockchain Technology: Beyond Bitcoin," *Applied Innovation Review*, vol. 2, pp. 6–10, 2016.
[4]. M. Mettler, "Blockchain Technology in Healthcare: The Revolution Starts Here," *IEEE 18th Int. Conf. on e-Health Networking, Applications and Services (Healthcom)*, Munich, 2016.
[5]. K. Toyoda, P. T. Mathiopoulos, I. Sasase, and T. Ohtsuki, "A Novel Blockchain-Based Product Ownership Management System (BPOMS) for Anti-Counterfeits in the Post Supply Chain," *IEEE Access*, vol. 5, 2017.
[6]. Z. Zheng et al., "An Overview of Blockchain Technology: Architecture, Consensus, and Future Trends," *IEEE Int. Congress on Big Data*, pp. 557–564, 2017.
[7]. Y. Tian, "An agri-food supply chain traceability system for China based on RFID & blockchain technology," *International Journal of Information Management*, vol. 42, pp. 89–98, 2018.
[8]. H. Kim and M. Laskowski, "Toward an Ontology-Driven Blockchain Design for Supply-Chain Provenance," *Intelligent Systems in Accounting, Finance and Management*, vol. 25, no. 1, pp. 18–27, 2018.
[9]. A. Reyna et al., "On Blockchain and Its Integration with IoT. Challenges and Opportunities," *Future Generation Computer Systems*, vol. 88, pp. 173–190, 2018.
[10]. H. Choi, "Combating Counterfeit Drugs: A Blockchain-Enabled Supply Chain Management Framework," *International Journal of Engineering and Technology*, vol. 7, no. 4.5, pp. 138–142, 2018.
[11]. X. Yue, H. Wang, D. Jin, M. Li, and W. Jiang, "Healthcare Data Gateways: Blockchain and Smart Contracts for Medical Data Management," *Computational and Structural Biotechnology Journal*, vol. 17, pp. 1390–1401, 2019.
[12]. R. Casino et al., "Blockchain-Based Applications in the Smart
Grid: A Systematic Review," *Energies*, vol. 12, no. 11, pp. 2140, 2019.
[13]. Q. Ding et al., "Double-Layer Framework for Supply Chain Traceability using Blockchain," *IEEE Access*, vol. 8, pp. 145678–145692, 2020.
[14]. A. Ghaleb, M. Salah, and M. A. Serhani, "AChecker: A Smart Contract Vulnerability Detection Framework," Univ. of British Columbia, 2021.
[15]. IBM Corporation, "IBM Food Trust Blockchain for Food Traceability," *IBM, White Paper*, 2021. [Online].
[16]. VeChain Foundation, "VeChain ToolChain: Blockchain-as-a-Service for Product Lifecycle," *White Paper*, 2022. [Online].
[17]. T. Hewa, M. Ylianttila, and M. Liyanage, "Survey on Blockchain-Based Smart Contracts: Technical Aspects and Future Research," *IEEE Access*, vol. 10, pp. 11728–11760, 2022.
[18]. D. Tapscott and A. Tapscott, *Blockchain Revolution: How the Technology Behind Bitcoin Is Changing Money, Business, and the World*, Penguin, 2016.
[19]. J. Benet, "IPFS - Content Addressed, Versioned, P2P File System," *arXiv:1407.3561*, 2014.
[20]. M. Jalalzai et al., "Fast-HotStuff: A High-Performance BFT Protocol for Blockchain," Univ. of British Columbia, 2022.
[21]. K. Wasnik, P. Patil, and D. Dakhore, "Detection of Counterfeit Products using Blockchain," *Proc. of RAIT*, 2022.
[22]. N. Pulgam and A. Katre, "Fake Product Detection Using Blockchain," *Proc. of RAIT*, 2023.
[23]. OriginTrail, "Decentralized Knowledge Graph for Supply Chain Integrity," *White Paper*, 2022. [Online].
[24]. S. Gupta, "An Ethereum-based Product Identification System for Anti-counterfeits," University of Kentucky, 2023.
[25]. Y. Lei, Z. Wang, and W. Liu, "Effect of counterfeits and fake reviews in credence markets," *Omega*, vol. 108, pp. 102892, 2025.
[26]. S. Gupta, S. Patil, and A. Deshmukh, "FPISMF: Fabric Protected Identification System using Multi-layer Fabrication," *Measurement Sensors*, vol. 32, 2024.
[27]. M. Aulia, L. Rahman, and D. Prasetyo, "Protected QR Code System for Pharma Authentication," *Proc. of MIST Conference*, 2024.
[28]. M. Finke et al., "SPOQchain: A Privacy-Preserving Blockchain for Supply Chain," *arXiv:2408.17049*, 2024.

IARJSET ISSN (O) 2393-8021, ISSN (P) 2394-1588

International Advanced Research Journal in Science, Engineering and Technology

Impact Factor 8.311 ⁜ Peer-reviewed & Refereed journal ⁜ Vol. 12, Issue 7, July 2025

DOI: 10.17148/IARJSET.2025.12745

[29]. R. Ghosh and S. Bhattacharya, "Blockchain for Supply Chain Transparency: A Literature Review," *IEEE Technology and Engineering Management Conference*, 2022.

[30]. H. Pun, Y. Jiang, K. Chan, and Z. Ye, "Application of blockchain in the secondary market with counterfeiting," *Transportation Research Part E: Logistics and Transportation Review*, vol. 164, pp. 102800, 2025.