



**IJIRCCCE**

e-ISSN: 2320-9801 | p-ISSN: 2320-9798



# INTERNATIONAL JOURNAL OF INNOVATIVE RESEARCH


IN COMPUTER & COMMUNICATION ENGINEERING

Volume 12, Issue 4, April 2024

**ISSN** INTERNATIONAL  
STANDARD  
SERIAL  
NUMBER  
INDIA

**Impact Factor: 8.379**

 9940 572 462

 6381 907 438

 [ijircce@gmail.com](mailto:ijircce@gmail.com)

 [www.ijircce.com](http://www.ijircce.com)

# Product Authentication and Counterfeit Elimination Using Blockchain Technology

K Vijay Simha, R Chandra Vikas, T Sai Kumar, Dr B V V Siva Prasad

UG Student, Dept. of CSE, Anurag University, Hyderabad, India

UG Student, Dept. of CSE, Anurag University, Hyderabad, India

UG Student, Dept. of CSE, Anurag University, Hyderabad, India

Associate professor, Dept. of CSE, Anurag University, Hyderabad, India

**ABSTRACT:** Blockchain technologies have gained interest over the last years. While the most explored use case is financial transactions, it has the capability to agitate other markets. Blockchain removes the need for trusted intermediaries, can facilitate faster transactions and add more transparency. This paper explores the possibility to deflate counterfeit using blockchain technology. This paper provides an overview of different solutions in the anti-counterfeit area, different blockchain technologies and what characteristics make blockchain especially interesting for the use case. We have developed three different concepts, and the expansion of an existing system concept is being pursued further. It is shown that reducing counterfeits cannot be achieved by using technological means only. Increasing awareness, fighting counterfeiters on a legal level, a good alert system, and having tamper-proof packaging are all important aspects. These factors combined with blockchain technology can lead to an efficient and comprehensive approach to reduce counterfeiting.

**KEYWORDS:** Authentication, Blockchain, Encryption.

## I. INTRODUCTION

Although it may seem like a far-off idea, we are surrounded by a lot of counterfeits. From fashion and retail products to software, digital media, electronics, piracy, and intellectual property, reports put the cost of counterfeiting somewhere around \$600bn a year in the US alone. In fact, the International Chamber of Commerce predicts that the negative impacts of counterfeiting and piracy are projected to drain US\$4.2 trillion (about \$13,000 per person in the US) from the global economy and put 5.4 million legitimate jobs at risk by 2022. In Pharmaceuticals, the counterfeit medicine market is now responsible for around 1 million deaths per year, in an industry estimated to be worth \$75bn annually. In fact, the counterfeit medicine industry is estimated to be growing at twice the rate of legitimate pharmaceuticals, making it up to 25 times more lucrative than the global narcotics trade. Trust is a central element in all transactions. No matter if sending money or exchanging goods, it becomes difficult if there is no trust between the entities involved. It becomes even more difficult, as with many transactions, third parties are involved, such as banks. Often, not only one third-party is involved in a transaction, but multiple. An international money transfer does not only include the bank of the sender, the bank of the receiver, but also multiple intermediary entities such as clearing houses. The entities involved in the transaction do not only have to trust each other, but also the third parties. Removing these third parties can decrease transaction costs, facilitate faster transactions and add more transparency. Bitcoin has successfully shown that removing such third parties is possible. The cryptocurrency permits direct sending of coins to a transaction partner, without the need to use banks and clearing houses. The assets are directly transferred from one account to another. There are no intermediaries and thereby no need to trust third parties. In addition, the question if a transaction is valid is not answered by an institution, but by algorithms used. Therefore, it completely removes the need to trust any third party. The technology behind Bitcoin, the blockchain, can however not only be used for financial transactions and crypto currencies in general. Technology has potential to redefine the digital economy because it allows immutable transactions, which can be always checked by everyone. This is because the information is publicly available and distributed globally. It is chronologically updated and cryptographically sealed. The full range of applicable use cases for this technology must be seen, but tracking ownership and history of a product is surely one of them. The possibility to reduce counterfeit using blockchain technology. Authentication, the act of establishing or confirming something as genuine. Authentication is of utmost importance because the use of counterfeit medicines can be harmful to the health and wellbeing of the patients. Their use may result in treatment failure or even death. Authentication is generally done through the overt or covert features of the product. We now have more fakes than real drugs in the market. Christophe

Zimmermann, the anti-counterfeiting and piracy coordinator of the World Customs Organization. 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. Block-supply chain replaces the centralized supply chain design and utilizes a new proposed consensus protocol that is, unlike existing protocols, fully decentralized and balances between efficiency and security. Our simulations show that the proposed protocol offers remarkable performance with a satisfactory level of security compared to the state-of-the-art consensus protocol.

## **II.LITERATURE REVIEW**

Research on product anticounterfeiting traceability systems based on blockchain. International Journal of Advanced Manufacturing Technology

Authors: Zhang, Y., Wang, Y., & Zhang, L.

The author analyzed the performance of their system with a traditional traceability system and found that the blockchain-based system was more effective in terms of anti-counterfeiting and traceability. Traceability has emerged as a prime requirement for a multi-tier and multi-site production. It enables visibility and caters to the consumer requirements of transparency and quality assurance. The proposed system can build a technology-based trust among the supply chain partners, where the distributed ledger can be used to store and authenticate supply chain transactions.

A blockchain-based application system for product anti-counterfeiting.

Authors: J. Ma, S.-Y. Lin, X. Chen, H.-M. Sun, Y.-C.Chen, and H. Wang

The paper proposed a decentralized Blockchain technology approach to ensure that consumers do not fully rely on the merchants to determine if products are genuine. manufacturers can use this system to provide genuine products without having to manage direct-operated stores, reducing the cost of product quality assurance. Blockchain has received increasing attention and numerous applications have emerged from this technology. A renowned Blockchain application is the cryptocurrency Bitcoin, that has not only been effectively solving the double-spending problem but also it can confirm the legitimacy of transactional records without relying on a centralized system to do so.

Therefore, any application using Blockchain technology as the base architecture ensures that the contents of its data are tamper-proof.

Blockchain Beyond Bitcoin, in Communications of the ACM.

Authors: S. Underwood

Blockchain Technology has attracted attention as the basis of cryptocurrencies such as Bitcoin, but its capabilities extend far beyond that, enabling existing technology applications to be vastly improved and new applications never previously practical to be deployed. Also known as distributed ledger 7 Blockchain technology, blockchain is expected to revolutionize industry and commerce and drive economic change on a global scale because it is immutable, transparent, and redefines trust, enabling secure, fast, trustworthy, and transparent solutions that can be public or private. It could empower people in developing countries with recognized identity, asset ownership, and financial inclusion.

ETHEREUM: A secure decentralized generalized transaction ledger.

Authors: DR. Gavin Wood

Ethereum is a project which attempts to build the generalized technology; technology on which all transaction-based state machine concepts may be built. Moreover, it aims to provide to the end developer a tightly integrated end-to-end system for building software on a hitherto unexplored compute paradigm in the mainstream: a trustful object messaging compute framework.

Understanding and fighting the medicine counterfeit marketl, in Journal of Pharmaceutical and Biomedical Analysis.

Authors: K. D'égardin, Y. Roggo and P. Margot.

Medicine counterfeiting is a serious worldwide issue, involving networks of manufacture and distribution that are an integral part of industrialized organized crime. Despite the potentially devastating health repercussions involved, legal sanctions are often inappropriate or simply not applied. The difficulty in agreeing on a definition of counterfeiting, the huge profits made by the counterfeiters and the complexity of the market are the other main reasons for the extent of the phenomenon.

Technology designed to combat fakes in the global supply chain, in Business Horizons.

Authors: L. Li

This article discusses the growing issue of counterfeit products in the global market due to increased globalization and online shopping. It presents various technologies used in the supply chain to combat counterfeiting, focusing on both product authentication and product tracing and tracking. The article also examines the pros and cons of these technological solutions and highlights success stories in the fight against counterfeits. Additionally, it addresses challenges such as rising anti-counterfeiting costs, collaborative efforts to combat fakes, and the exploration of a comprehensive strategy to tackle the issue.

### III. EXISTING SYSTEM

#### Existing System with Disadvantages:

Blockchain technology to authenticate supply chain products as this product may be supplied from multiple third-party distributors and this distributor can make clone/fake/counterfeits of this product BAR CODE and then manufacture fake products and add this counterfeit label to fake product and this fake product can cause huge loss of financial and lives if fake medicine manufacture. Many businesses rely on third-party vendors. The outsourced supplier has access to all the original assets, there is a risk that will not only make legitimate products, but also counterfeits. Not only supply chain, any other online transaction requires a third party to complete the transaction and people must trust on third parties to complete their transaction and sometimes this third party can make fraud transactions or misuse user data. There are many chances of cloning the product. Even now there are more fakes than real drugs in the market. Features expected to assist the users to confirm the genuineness of a pack. Such features will be significantly visible, and complex or expensive to reproduce.

#### Disadvantages:

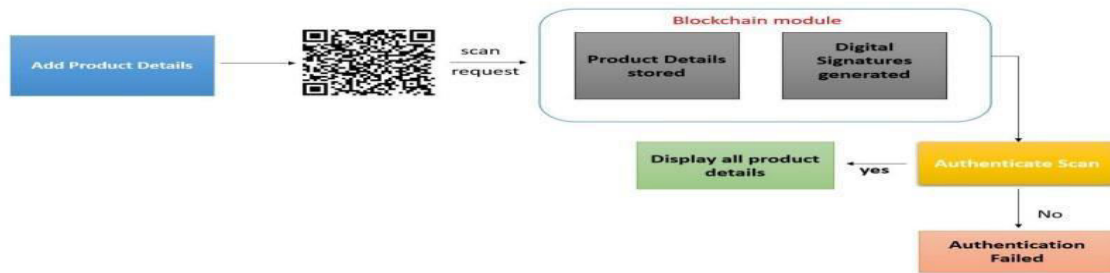
1. One of the challenging issues is privacy and data protection. In case of any other online transaction to complete the transactions, they must trust these third parties. However, these third parties can sometimes misuse the customer data or commit fraud.
2. Outsourced supplier has access to all the original assets, there is a risk that they can clone the products.
3. There will be huge financial and human losses if fake medicine is manufactured in the market.
4. Ensuring widespread adoption of technology. For the system to be effective, all parties involved in the supply chain, including manufacturers, retailers, and consumers, must use the technology. Achieving this level of adoption can be difficult, especially in industries with many different stakeholders and competing interests.

### IV. PROPOSED METHOD

Proposed System with features: Blockchain technology which does not require any third party and verification will be done by software algorithm itself without involvement of any third party. In this to avoid forge counterfeit we are converting all products details/barcode into digital signatures and this digital signature will be stored in Blockchain server as this Blockchain server support tamper proof data storage and nobody can hack or alter its data and if by a chance if its data alter then verification get failed at next block storage and user may get intimation about data alter. In Blockchain technology the same transaction data is stored at multiple servers with hash code verification and if data alter at one server, then it will be detected from other server as for same data hash code will get different. For example, in Blockchain technology data will be stored at multiple servers and if malicious users alter data at one server, then its hash code will get changed in one server and other servers left unchanged and this changed hash code will be detected at verification time and future malicious user changes can be prevented. In the supply chain all products barcode digital Blockchain signatures will be stored and if any third -party distributor makes a clone of

barcode then its signature will be mismatch and counterfeit will be detected. In Blockchain each data will be stored by verifying old hash codes and if old hash codes remain unchanged then data will be considered, as original and unchanged and then new transaction data will be appended to Blockchain as new block. For each new data storage all block hashcodes will be verified.

### Proposed System Architecture



### Advantages:

- In the supply chain also, all products barcode digital Blockchain signatures will be stored and if any third-party distributor makes a clone of the barcode, then its signature will be mismatched and counterfeit will be detected.
- In blockchain Server once the product is stored cannot be modified.
- Data protection and privacy are maintained. If there is any data alter the user will get intimated and verification fails at the next block.

## V. INPUT AND OUTPUT DESIGN

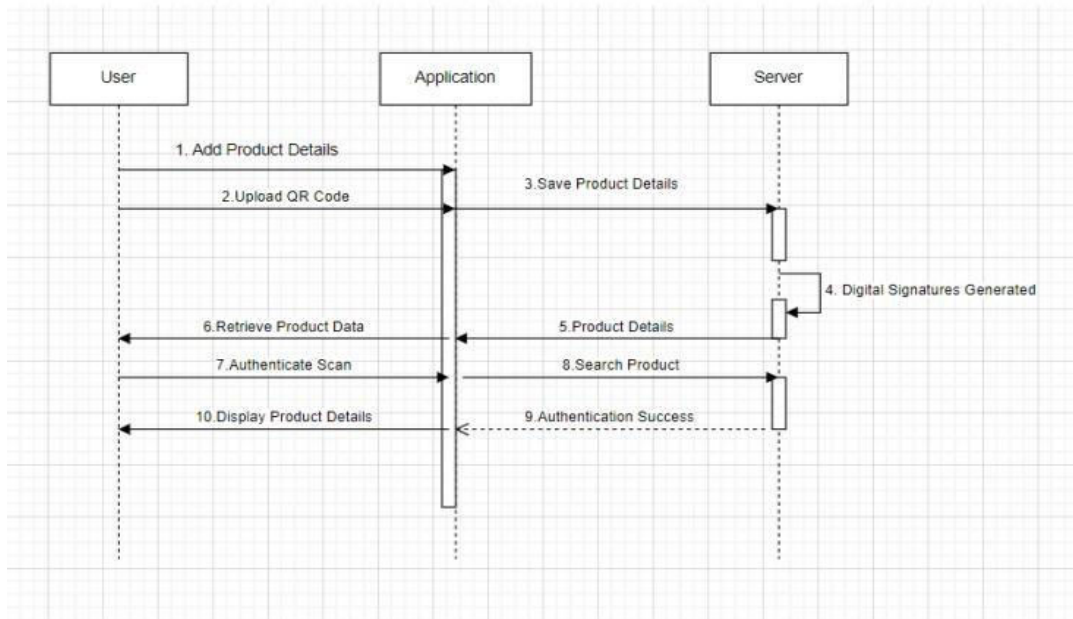
The input design is the link between the information system and the user. It comprises the developing specification and procedures for data preparation and those steps necessary to put transaction data into a usable form for processing can be achieved by inspecting the computer to read data from a written or printed document or it can occur by having people keying the data directly into the system. The design of input focuses on controlling the amount of input required, controlling the errors, avoiding delay, avoiding extra steps and keeping the process simple. The input is designed in such a way that it provides security and ease of use while retaining privacy.

Input Design considered the following things:

- What data should be given as input?
- How the data should be arranged or coded?
- The dialog to guide the operating personnel in providing input.
- Methods for preparing input validations and steps to follow when error occur.

## VI. SEQUENCE DIAGRAM

A sequence diagram shows object interactions arranged in time sequence. It depicts the objects involved in the scenario and the sequence of messages exchanged between the objects needed to carry out the functionality of the scenario. Sequence diagrams are typically associated with use case realizations in the Logical View of the system under development. Sequence diagrams are sometimes called event diagrams or event scenarios.



### VII.OUTPUT DESIGN

A quality output is one which meets the requirements of the end user and presents the information clearly. In any system results of processing are communicated to the users and to other systems through outputs. In output design it is determined how the information is to be displaced for immediate need and the hard copy output. It is the most important and direct source of information to the user. Efficient and intelligent output design improves the system’s relationship to help user decision-making.

1. Designing computer output should proceed in an organized, well thought out manner; the right output must be developed while ensuring that each output element is designed so that people will find the system can be used easily and effectively. When analysis design computer output, they should Identify the specific output that is needed to meet the requirements.
- 2.Select methods for presenting information.
- 3.Create documents, reports, or other formats that contain information produced by the system. The output form of an information system should accomplish one or more of the following objectives.
- 4.Convey information about past activities, status or projections of the Future.
- 5.Signal important events, opportunities, problems, or warnings
- 6.Save Product with Blockchain Entry:

In this module the user will enter product details and then upload product bar code images and then digital signatures will be generated on uploaded barcodes and then these transaction details will be stored in Blockchain. Before storing transaction Blockchain will verify all old transaction and upon successful verification new transaction block will be store

Retrieve Product Data:

Using this module, users can search existing product details by entering product id.

Authenticate Scan:

Here in this module, we don’t have any scanner so we are uploading original or fake bar code images and then Blockchain will verify digital signature of uploaded bar code with already stored barcodes and if a match is found then Blockchain will extract all details and display to user else authentication will be failed.

### VIII.RESULTS

#### Blockchain Advantages for Authentication and Counterfeit Prevention:

Transparency and Security: Blockchain technology provides transparency in product sales by storing details as digital signatures, ensuring authenticity and preventing data tampering.

Tamper-Proof Data Storage: The tamper-proof nature of Blockchain servers prevents data alteration, enhancing security and trust in product verification processes.

Decentralized Verification: Verification done by software algorithms within the Blockchain system eliminates the need for third-party involvement, ensuring robust and efficient product authentication.

Multiple Server Redundancy: Storing transaction data at multiple servers ensures integrity, using hash code verification to detect alterations and enhance data trustworthiness.

#### **Blockchain Implementation and Python Utilization:**

Trustworthiness: Blockchain technology and Python programming enhance the trustworthiness and security of products, enabling consumers to verify authenticity and prevent counterfeit product infiltration.

Cost-Effective Solutions: The integration of Blockchain and Python offers cost-effective measures for authenticating products, reducing financial losses, and ensuring customer safety.

Accessibility: Python's widespread usage, along with Blockchain technology, provides accessible solutions to combat counterfeiting challenges across various industries. These results underline the significant advancements and benefits derived from utilizing Blockchain technology for product authentication and leveraging Python's advantages for effective counterfeit prevention methods.

### **IX.MATHEMATICAL ANALYSIS**

#### **Mathematical Analysis of Blockchain Technology and Python's Role in Counterfeit Prevention**

1. Trustworthiness (T): Formula:  $T = (\text{Number of valid transactions} / \text{Total transactions}) * 100\%$

Analysis: This metric indicates the percentage of valid transactions, ensuring data integrity and trust in the blockchain system.

2. Transparency (Tr): Formula:  $Tr = (\text{Number of transparent transactions} / \text{Total transactions}) * 100\%$

Analysis: Transparency in transactions can be measured to evaluate the effectiveness of blockchain in providing visibility across the network.

3. Data Integrity (DI): Formula:  $DI = (\text{Number of unaltered data records} / \text{Total records}) * 100\%$

Analysis: Data Integrity metric shows the percentage of unaltered data records, indicating the resistance of the blockchain system to unauthorized modifications.

4. Productivity (P): Formula:  $P = (\text{Lines of code written per hour} / \text{Complexity of implementation})$

Analysis: Productivity measurement assesses the efficiency in implementing counterfeit prevention methods using Python's libraries and features.

5. Innovation Index (I): Formula:  $I = (\text{Number of innovative features} / \text{Total features}) * 100\%$

Analysis: Innovation Index quantifies the level of creativity and uniqueness in developing counterfeit prevention strategies using Python's capabilities.

6. User Satisfaction (US): Formula:  $US = (\text{Number of positive user feedback} / \text{Total user feedback}) * 100\%$

Analysis: User Satisfaction metric indicates the percentage of users satisfied with the user-friendly interfaces developed using Python.

7. Effectiveness Score: Combination of Blockchain Trustworthiness, Data Integrity, and Python Productivity scores to assess the efficacy of the system in combating counterfeiting.

Innovation Impact: The Innovation Index and Transparency metrics demonstrate the innovative approach and transparency maintained in the system.

User Experience: User Satisfaction and Transparency results reflect the user-centric design and transparent transactions facilitated by the system.

By conducting a mathematical analysis of these metrics, a comprehensive evaluation of the blockchain technology and Python's role in counterfeit prevention methods can be achieved, providing quantitative insights into the effectiveness and efficiency of the proposed system.



X. SAMPLE TEST CASE

Step	Test Case	Test Data	Expected Result	Actual Result	Status (Pass/Fail)
------	-----------	-----------	-----------------	---------------	--------------------

	Details	Product Name: Mobile Company Name: iPhone Location: Hyderabad Upload QR Code	Details stored on the server.	Details Stored in Server.	
--	---------	--	-------------------------------	---------------------------	--

Step	Test Case	Test Data	Expected Result	Actual Result	Status (Pass/Fail)
2.	Retrieve Product Data	Product ID:1	Details of the product displayed.	Details of the product displayed.	Pass

Step	Test Case	Test Data	Expected Result	Actual Result	Status (Pass/Fail)
3.	Authenticate Scan	Fake QR Code	Authentication Failed	Authentication Failed	Pass

XI.CONCLUSION

The system provides that the product's journey from manufacturing to customer can be recorded, and the customer is assured that the scans were faked. Manufacturers can prove their product is authentic and is also able to track their product pathway. The setup is easy to implement and requires less operation cost. Manufacturers can also adopt RFID or NFC tokens instead of QR codes to further strengthen their system.

REFERENCES

[1] Satoshi Nakamoto, —Bitcoin: A Peer-to-Peer Electronic Cash Systeml, 2008

[2] Hyperledger, —Hyperledger Blockchain Performance Metricsl, V1.01, October 2018

[3] R.C. Merkle, "Protocols for public key cryptosystems," In Proc. 1980 Symposium on Security and Privacy, IEEE Computer Society, pages 122-133, April 1980.

[4] Armin Ronacher, —Flask Docsl, <http://flask.pocoo.org/docs>

[5] G. Wood, \_\_Ethereum: A secure decentralised generalized transaction ledger Tech. Rep., 2014.

[6] OECD (2016), Illicit Trade: Converging Criminal Networks, OECD Reviews of Risk Management Policies, OECD Publishing, Paris, <https://doi.org/10.1787/9789264251847-en>.

[7] M. Castro and B. Liskov, \_\_Practical byzantine fault tolerance and proactive recovery."ACM Trans. Comput. Syst., vol. 20, no. 4, pp. 398–461, Nov. 2002.

[8] Clement, E. Wong, L. Alvisi, M. Dahlin, and M. Marchetti, \_\_Making byzantine fault tolerant systems tolerate byzantine faults, in Proc. 6th USENIX Symp. Netw. Syst. Design Implement., 2009, pp. 153–168.

[9] Cachin, \_\_Architecture of the hyperledger blockchain fabric "Tech. Rep., Jul. 2016...

[10] S. Underwood, —Blockchain Beyond Bitcoinl, in Communications of the ACM, vol. 59, no. 11, p. 15-17, 2016.

[11] Deloitte, Israel: A Hotspot for Blockchain Innovation, 2016. [Online]. Available: [https://www2.deloitte.com/content/dam/Deloitte/il/Documents/financialservices/israel\\_a\\_hotspot\\_for\\_blockchain\\_innovation\\_feb2016\\_1.1.pdf](https://www2.deloitte.com/content/dam/Deloitte/il/Documents/financialservices/israel_a_hotspot_for_blockchain_innovation_feb2016_1.1.pdf). [Accessed: 2.11.2016].

[12] G. Greenspan and M. Zehavi, Will Provenance Be the Blockchain Break Out Use Case in 2016, 7.1.2016. [Online]. Available: <http://www.coindesk.com/provenance-blockchain-tech-app/>. [Accessed: 12.12.2016].

[13] Counterfeit medicines. QA counterfeit. World Health Organization (WHO) 2009. Available from:<http://www.who.int/medicines/services/counterfeit/QACounterfeit-october2009.pdf> [last cited on 2010 Jun 12].





- [14] An ICC initiative Business Action to Stop Counterfeiting and Piracy (BASCAP). Brand protection directory. The World Business Organization. Available from: <http://www.iccwbo.org/bascap> [last cited on 2010 Jun 10].
- [15] L. Li, —Technology designed to combat fakes in the global supply chain, in *Business Horizons*, vol. 56, no. 2, p. 167-177, 2013. 45
- [16] White paper. Dhar R. Anti counterfeit packaging technologies. A strategic need for the Indian industry. Confederation of Indian Industry 2009:1-47. Available from:[http://www.bilcare.com/pdf/CII\\_anti\\_counterfeit\\_pkg\\_technologies\\_report.pdf](http://www.bilcare.com/pdf/CII_anti_counterfeit_pkg_technologies_report.pdf) [last cited on 2010 Oct 29].
- [17] Berman, —Strategies to detect and reduce counterfeiting activity, in *Business Horizons*, vol. 51, no. 3, p. 191-199, 2008.
- [18] K. D'egardin, Y. Roggo and P. Margot. —Understanding and fighting the medicine counterfeit market, in *Journal of Pharmaceutical and Biomedical Analysis*, vol. 87, p. 167-175, 2013
- [19] R. C. Merkle, —A digital signature based on a conventional encryption function, “in *Proc. Conf. Theory Appl. Cryptogr. Techn.*, 1987, pp. 369–37



INTERNATIONAL  
STANDARD  
SERIAL  
NUMBER  
INDIA



# INTERNATIONAL JOURNAL OF INNOVATIVE RESEARCH

IN COMPUTER & COMMUNICATION ENGINEERING

 9940 572 462  6381 907 438  [ijircce@gmail.com](mailto:ijircce@gmail.com)



[www.ijircce.com](http://www.ijircce.com)

Scan to save the contact details