



# JOURNAL OF EMERGING TECHNOLOGIES AND INNOVATIVE RESEARCH (JETIR)

An International Scholarly Open Access, Peer-reviewed, Refereed Journal

## Blake Blockchain Based E-Commerce Solution for Fake Product Detection

Eram Zafar<sup>1</sup>, Ramesh Kumar<sup>2</sup>

<sup>1</sup> M.Tech Scholar, <sup>2</sup>Assistant Professor (HOD)

<sup>1,2</sup> Department of Computer Science and Engineering, K. K. University Nalanda (Bihar)

**Abstract :** Ecommerce is the fastest growing part of retail, but is plagued by counterfeiters and duplicates. It takes time and money to register a trademark, but it's worth it in the long run. If a company isn't vigilant about their trademarks, they can lose control of their brand and ruin this sheen that they've worked so hard to establish. Sometimes, it is difficult to spot the difference between real and fake. So if you're not an expert, you might mistake a fake for the real one. With a QR code linked to a Blockchain, you can tell whether the product is a fake. Because everything about this product is recorded in the Blockchain once it's made, we can use blockchain technology to detect whether it is genuine or not. The QR code will be checked against information in the blockchain database to see if it is original. It will also alert customers if the product is a fake. We generated the hash using blake-2b.

**IndexTerms – Blockchain, E-Commerce , Fake Products, QR Code, Blake.**

### I. INTRODUCTION

Digital channels for selling and purchasing consumer goods has helped to fuel a rapid increase in fake products being sold around the world. The OECD report indicates that 3.3% of global trade is now counterfeit products which is an increase from years ago.[1]

Online shoppers are mostly unprepared for the counterfeit products being touted on Amazon; Amazon third party sellers are often not what they seem. [1] However, it seems that the problem has gone unnoticed by many people. Most of the items on Amazon are actually from third-party sellers, and not from Amazon themselves.[1]

Products, which are inauthentic and unsafe to consumers, are not just a threat to the business; they're also a health and safety issue. [2] Counterfeit goods are a health and safety risk for consumers because they often contain low-quality and hazardous materials. Counterfeit goods also contribute to the economic growth of legitimate businesses by reducing sales, profit, and competitive advantage. [2]

Blockchain can be used for detecting the fake products. Blockchain is a digital ledger of transactions copied across many different PC networks. Blockchain serves as a digital ledger of transactions that can't be tampered with. Every computer on the blockchain copies these transactions and distributes them to stay current and secure. [3] Blockchain is a database with a distributed set of ledgers, which makes it nearly impossible to mess with the data. The data and transactions in the blockchain can only be modified by changing it in all versions of the ledger at once. [3]

With the blockchain, thousands of computers are able to verify transactions and mistakes are less likely to happen because it would need 51% of the computers to make an error for it to be validated on the rest of the chain. Blockchain allows users to avoid third parties interfering with their transactions. The cost of these third parties is eliminated because the blockchain verifies the transaction with no reason to use an outside source. [4]

The blockchain, is a securely distributed ledger of digital transactions and can be programmed to contain financial information as well as information on things that are valuable. It is updated by tamper-proof Distributed ledger technology. [4] You should avoid traditional banks if you're doing business internationally because it takes 24/7 and 10 minutes to settle your transactions. With traditional banks, the process can take up to a few days.[5]

Blockchain networks are decentralized meaning anyone with an internet connection can view a list of the data stored. Users are unable to access identifying information because Blockchain is not anonymous, it is confidential. [6] Blockchain is the public ledger of transactions that is not linked to any personal information, but only to the name of the account holder. [6]

A blockchain is a chain of data blocks connected by cryptography. Once the blocks are confirmed, that chain includes hashes to verify any future changes on the blockchain. [7]

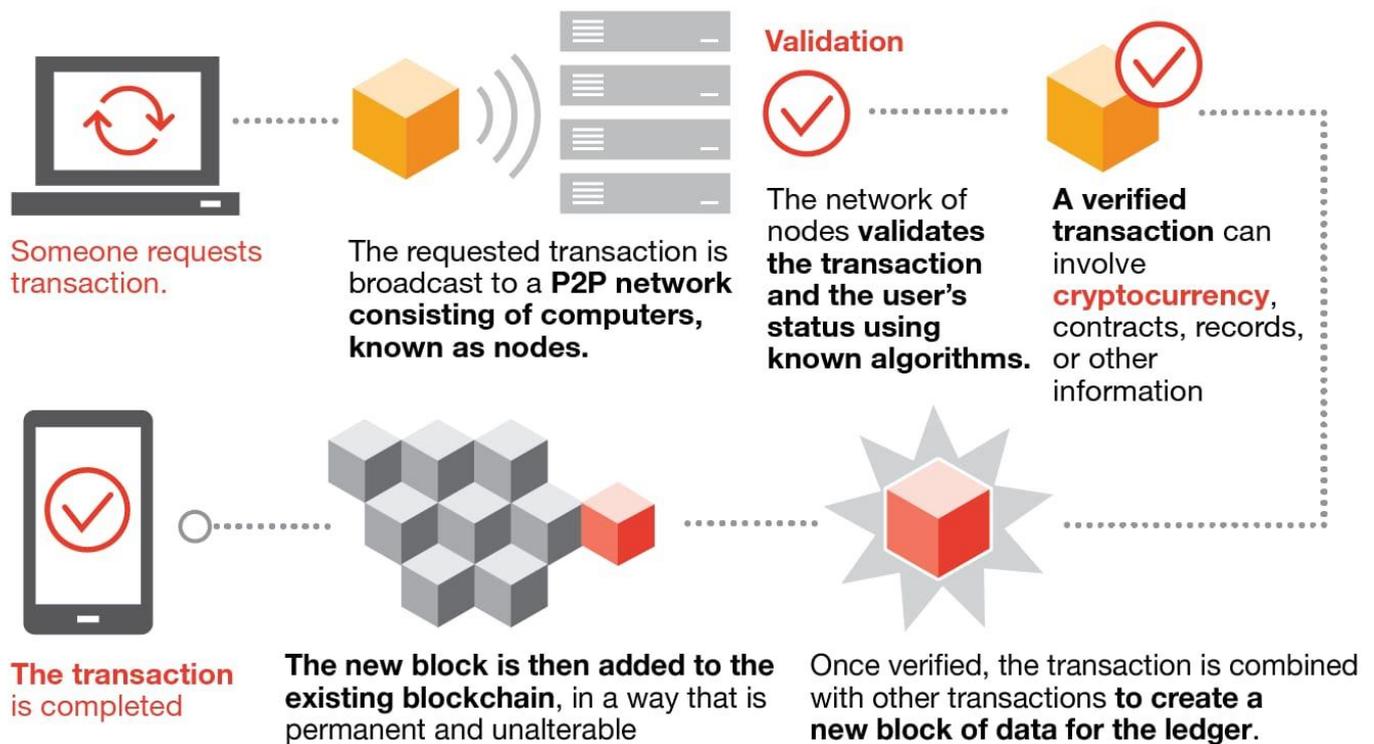


Fig 1. Block Chain Concept

## II. LITERATURE REVIEW

Shevchuk, R. et al. (2020) There is a growing awareness of the risks associated with social media, but many users are still not aware of what security settings provide. Researchers developed software for automatic estimating security settings of Facebook and Instagram social media accounts, in order to provide tailored recommendations for improvement. [8]

Lai, J. (2019) article talks about the logistics system in cross-border e-commerce and how a decentralizing block chain can be applied to enhance its efficiency. Part of this article talks about how cross-border logistics is hard because there are many variables that have to come together successfully, but with block chain technology, these logistics can become much more feasible. [9]

Cui, X. (2019) social media is an unorganized organization. In the era of big data, the analysis results based on social media data lead to the leakage of personal information. The Prism event rang the awakening of the world. Water army and social robots based on artificial intelligence appeared. Rumors and fake news exploded. Events such as the Twitter Revolution that caused national turmoil. Ensuring the secure transmission, storage, use and authenticity of personal information is a serious task. [10]

Madhu, et al. (2020) To fight overpopulation, the agricultural sector needs to grow more food. From farmers to logistics and consumers, many businesses are now looking into using a combination of IoT and Blockchain technologies. Using these tools, we have developed a farm robot and an application for growers that promises reduced environmental footprints, increased customer satisfaction, and improved transparency throughout the supply chain. [11]

Sanjay Kumar .et. al (2020) propose an advanced security architecture for user identification which makes use of two factor authentication with AES-based file encryption and decryption of data uploaded to the cloud. [12]

**III. PROPOSED CONCEPT**

- Digital Identity of Product → Product ID
- Batch Number
- Location of Manufacturing (Plant Details)

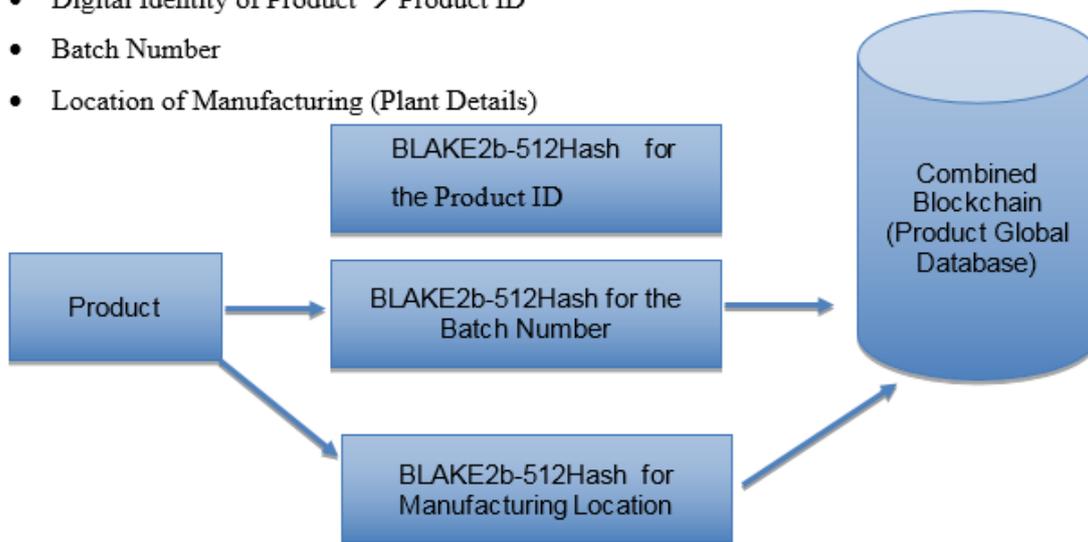


Fig 2. Blockchain Generation Process

**Product Validation**

Now, at the time of the validation

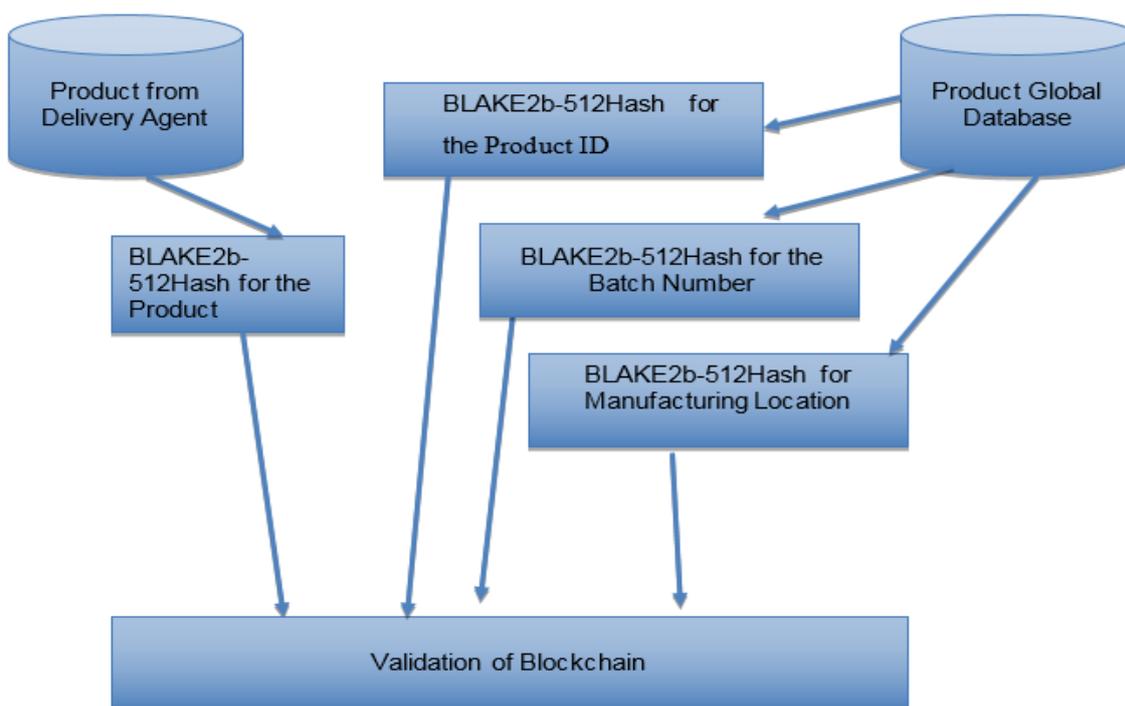


Fig 3. Product Blockchain Verification

**IV. IMPLEMENTATION AND RESULT ANALYSIS**

For the implementation of the fake product detection we will simulate the model via an online application (web application), which can be implemented in Web technologies like .Net

The blockchain generated in the process can be test tested for attacks like dictionary attacks, brute force attacks using the tools which check for the number of years involved in breaking the password or tools which evaluate on the basis of the entropy.

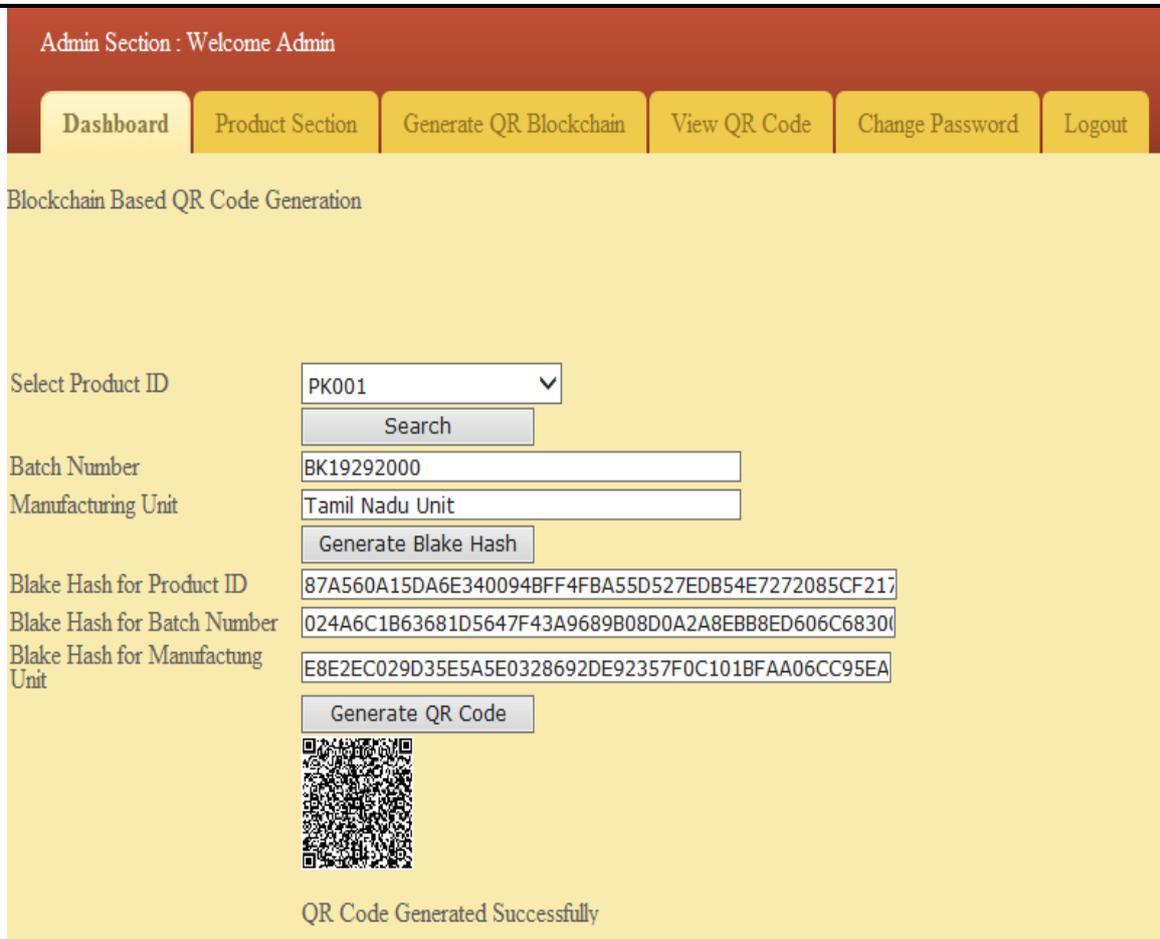


Fig 4. QR Code Generation

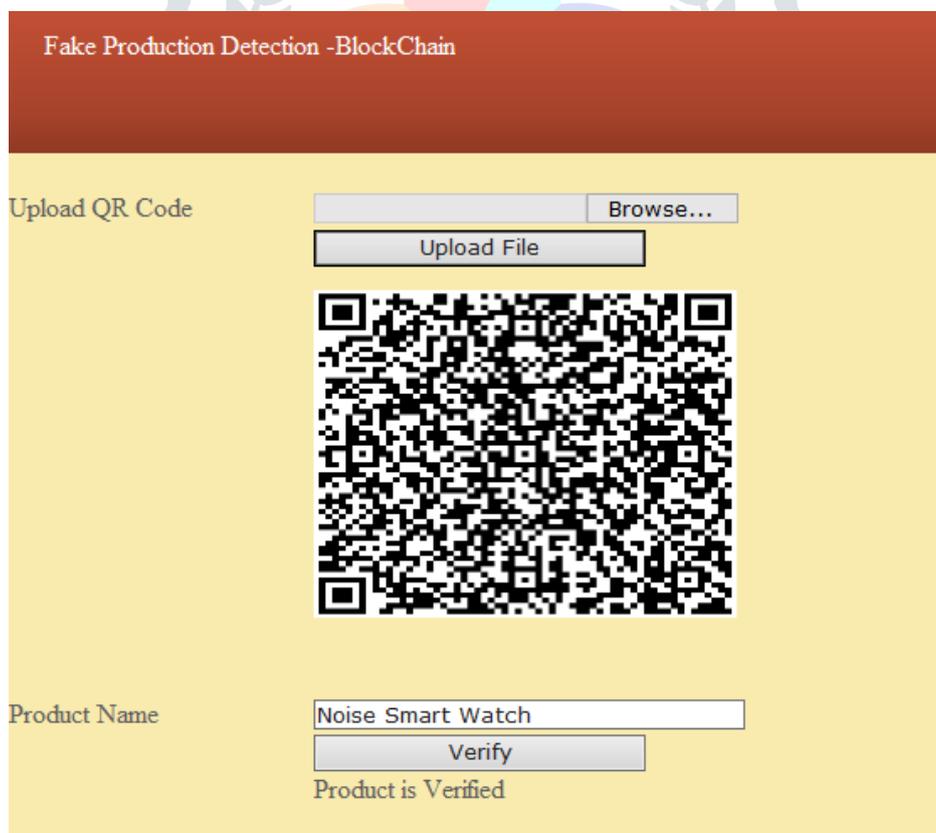


Fig 5. Product Verification

Base Paper ,Sankaj Kumar , et.al 2020 [10] used AES 10 round key e.g. 18FFFEF86DA4245ADCC1A4FE3B356F26

### Result Analysis using Password.blue Test

18FFFEF86DA4245ADCC1A4FE3B356F26

Show



Fig 6. Base Key Test on Password.blue

87A560A15DA6E340094BFF4FBA55D527EDB54E72\_024A6C1B63681D5647F43A9689B08D0A2A8EBB8E\_E8E2EC029D35E5A5E0328692DE92357F0C101BFA

Show



Fig 7. Proposed Results from Password.Blue Test

### Result Analysis using Rumkin Test

Enter your password or passphrase here:

**Length:** 32  
**Strength:** **Strong** - This password is typically good enough to safely guard sensitive information like financial records.  
**Entropy:** 127.6 bits  
**Charset Size:** 36 characters

Fig 8. Base Results from Rumkin Test

Enter your password or passphrase here:

.....

**Length:** 128  
**Strength:** Very Strong - More often than not, this level of security is overkill.  
**Entropy:** 499.9 bits  
**Charset Size:** 36 characters

Fig 9. Proposed Results from Rumkin Test

## V. CONCLUSION

Transactions can be made digitally with blockchain technologies by developing a decentralized e-commerce platform. With this, transactions are recorded on a database and sent out across many computers rather than one central authority. Sometimes, it is difficult to spot the difference between real and fake. So, if you're not an expert, you might mistake a fake for the real one. With a QR code linked to a Blockchain, you can tell whether the product is a fake. Because everything about this product is recorded in the Blockchain once it's made, we can use blockchain technology to detect whether it is genuine or not. The QR code will be checked against information in the blockchain database to see if it is original. It will also alert customers if the product is a fake. We generated the hash using blake-2b.

## REFERENCES

1. Chattopadhyay, A. et al. (2018) "A middle-school case study: Piloting A novel visual privacy themed module for teaching societal and human security topics using social media apps," in 2018 IEEE Frontiers in Education Conference (FIE). IEEE, pp. 1–8.
2. Chung, W., Mustaine, E. and Zeng, D. (2017) "Criminal intelligence surveillance and monitoring on social media: Cases of cyber-trafficking," in 2017 IEEE International Conference on Intelligence and Security Informatics (ISI). IEEE, pp. 191–193.
3. Colbaugh, R. and Glass, K. (2013) "Analyzing social media content for security informatics," in 2013 European Intelligence and Security Informatics Conference. IEEE, pp. 45–51.
4. Ekwunife, N. (2020) "National security intelligence through social network data mining," in 2020 IEEE International Conference on Big Data (Big Data). IEEE, pp. 2270–2273.
5. Guidi, B. and Michienzi, A. (2020) "Users and Bots behaviour analysis in Blockchain Social Media," in 2020 Seventh International Conference on Social Networks Analysis, Management and Security (SNAMS). IEEE, pp. 1–8.
6. Gupta, S. S., Thakral, A. and Choudhury, T. (2018) "Social media security analysis of threats and security measures," in 2018 International Conference on Advances in Computing and Communication Engineering (ICACCE). IEEE, pp. 115–120.
7. Giraldo, F. D., Milton C., B. and Gamboa, C. E. (2020) "Electronic voting using blockchain and smart contracts: Proof of concept," IEEE Latin America Transactions, 18(10), pp. 1743–1751.
8. Shevchuk, R. et al. (2020) "Software for automatic estimating security settings of social media accounts," in 2020 10th International Conference on Advanced Computer Information Technologies (ACIT). IEEE, pp. 769–773.
9. Lai, J. (2019) "Research on cross-border E-commerce logistics supply under block chain," in 2019 International Conference on Computer Network, Electronic and Automation (ICCNEA). IEEE.
10. Cui, Z. et al. (2020) "A hybrid BlockChain-based identity authentication scheme for multi-WSN," IEEE transactions on services computing, 13(2), pp. 1–1.
11. A. Madhu, K. Archana, D. H. Kulal, R. Sunitha and P. B. Honnavalli, "Smart Bot and E-commerce Approach based on Internet of Things and Block-chain Technology," 2020 4th International Conference on Electronics, Communication and Aerospace Technology (ICECA), 2020, pp. 629-634.
12. Sanjay Kumar, Syed Akbar Abbas Jafri, NishitArun Nigam, Nakshatra Gupta, Gagan Gupta1 and S K Singh,"A New User Identity Based Authentication, Using Security and Distributed for Cloud Computing",IOP Conf. Ser.: Mater. Sci. Eng. ,2020.