



QR Code Based Product Validation for Counterfeit Product Detection

¹ Anju, ²Dr. Sudhir rathi

¹M.Tech Research Scholar, ²Professor¹Name of Department of 1st Author,

¹Department of Computer Science , Sobhasaria group of Institutions, Sikar

Abstract: Blockchain can help address counterfeiting, because it ensures the origins of products. Blockchain offers a secure and trusted system for tracking materials from the beginning of the manufacturing process to your doorstep. Blockchain essentially helps identify where items come from, so with this technology law enforcement can more easily establish if products are counterfeit, as well as companies can better protect their intellectual property. QR codes can be scanned to view the block on the blockchain that contains the product information. If you scan the QR code on a product using your smartphone, it will search for matches in the Blockchain database. If there is a match, it will let you know whether or not the product is authentic. For privacy reasons, there is no information storage outside of the Blockchain database.

Index Terms – Blockchain, Data Security, Data Validation, Hashing, Product Validation

I. INTRODUCTION

India is experiencing a significant growth of its e-commerce market. The Indian e-commerce market is expected to grow to US\$200 billion by 2026 from US\$ 48.5billion in 2018. This growth has been triggered by increased internet and smartphone penetration. India, who already has the highest amount of internet users compared to other countries, is going through an increase in all online developments. More and more Indians are buying online, which will contribute to a drastic increase in India's total internet user base by 2021. In India, growing online retail sales are contributed mainly by Flipkart, Amazon India and Paytm Mall. [1]

With a share of approximately 48%, electronic is the biggest category of items sold, followed closely by apparel at 29%. American brands can now reach Indian customers in more eCommerce platforms. There has been an increase in the cross-border trade of goods and services, with eCommerce emerging as a rapidly growing trade channel. [1]

There is growing demand for international, quality products among digitally connected Indian consumers. Most categories, such as lifestyle goods and clothing, are seeing higher sales through e-commerce. There are four main types of eCommerce in India. They are domestic, cross-border, B2B and B2C, and marketplace. [2]

The e-commerce industry in India has seen rapid growth with the assistance of modern technology, such as digital payments, hyperlocal logistics, and customer engagement. Digital India, Skill India, Startup India and Make in India have contributed to the expansion of the e-Commerce industry. [2]

E-commerce has a lot of advantages over traditional physical shopping. The most important thing is that you don't need to physically go anywhere, which means you can buy anything anytime. Consumers are going online more often, so brands have created a presence on sites like Amazon and Alibaba in order to meet this demand. [3]

Selling on e-marketplaces has increased in recent years, but so have counterfeit products. This problem is widespread and growing steadily. About 7-8% of the world's trade every year is counterfeit goods. This percentage is according to FBI, Interpol, the World Customs Organization, and the International Chamber of Commerce. [3]

Counterfeiting not only damages brands through the risk of trademark infringement, decreasing brand value, and damaging goodwill but also harms consumers by increasing the risk they'll receive low quality products that may impact their health. [4]

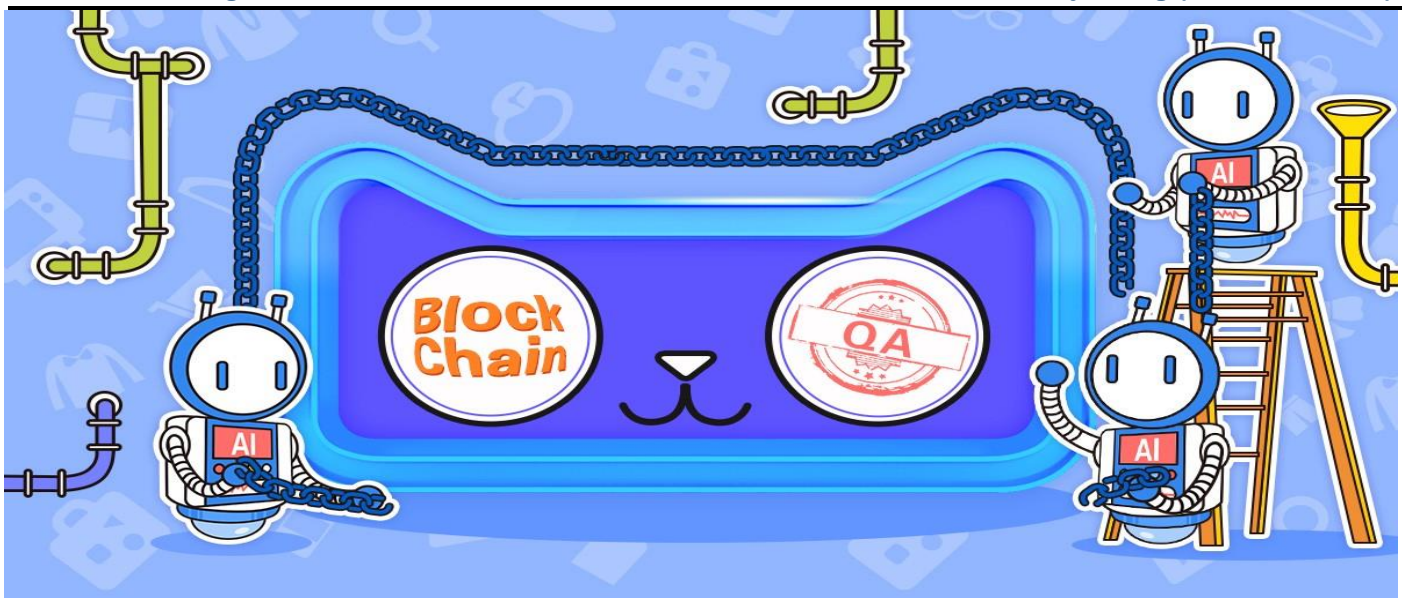


Fig 1. Blockchain v/s Fake Products

Counterfeit products affect more than just the luxury goods market, they can also include automobiles, aircraft, computers and medicines. Due to the rise of e-commerce, counterfeiters have also switched to this format and have counterfeited goods specifically for that site. [4]

You can find a wider selection, better availability, and more competitive prices in an e-marketplace. This is because there are multiple suppliers from which to choose, rather than just one vendor. Counterfeiters have also started creating fake websites that mimic the look and feel of a genuine brand's website. [5]

Scammers use fake websites in order to force consumers to pay money for goods that never arrive and to steal their credit card and bank information. These sites look very convincing so it can be difficult to tell them apart from the original website. [5]

II. BLOCKCHAIN AND PRODUCT VALIDATION

Blockchain is a digital ledger of transactions that are immutable and cannot be changed. This new technology allows for distributed digital information to be recorded but not edited. The shared ledger is an important component of the blockchain that fosters inclusion and accuracy. It uses technology to establish trust among a group of parties that don't need a central authority. Blockchain is a technology that documents the entire supply chain. Blockchain can transparently track food from farm to fork and increase a company's brand credibility. [6]

III. LITERATURE SURVEY

Mu and Yao (2018) proposed a new way to create graphical passwords. They do so by creating a grid of numbers and assigning specific characters as the numbers that are placed on the grid. Authors recommend switching to text-based passwords, which are much more secure than Hanzi-gpws. To create a text based password, you can use one of the systems we present in this article. In addition, new graphs are being developed that teach people how to create and break down new passwords. [8]

B. Bilgi and B. Tugrul, 2018, Graphical passwords have emerged as a way to combat the growing hacking problem, updating traditional text-based passwords with one simple graphical interface. Though people may be tempted to forgo the security of GTU for convenience, these passwords are more secure and quality-tested than their text-based counterparts. As the number of "shoulder surfing" incidents has increased, people have had a tendency to include their passwords in simple-to-spot places like public transportation, diners, and classrooms. To help mitigate this problem, we have developed graphical authentication for users of our site that would be impervious to attacks using blended images. Our technique is distinctive from other graphical and text-based approaches as we streamline security and accommodation. [9]

D. Gupta, et.al 2017 Obviously there are risks of risking security with passwords and relative mix-ups which may need to be corrected. However, general users do have problems remembering all their passwords and may not be aware of the dangers of using an oblivious mix. With this tool, you can pick your own graphical advancements for the articles that you see in virtual environment before generating a password. [10]

J. A. Jaffar and A. M. Zeki, 2020 In security, user authentication is a key component. There are different methods for authentication, for instance alphanumeric usernames and passwords. However, with the limitations of this method, examples based passwords have been proposed as an alternate option. This study contains an extensive investigation at graphical passwords and evaluates all the available plans at two places- accessibility and convenience. Currently, it also answers the question "Are graphical passwords more secure than alphanumeric password?" [11]

S. Yang, et.al 2019 This paper proposes two models in ring network, which are given the concept of odd-easy labellings. The authors want to form two types of Topsnut-gpws for more security and usability for establishing a secure data transmission. [12]

Shen et.al, 2017 showed that "smart" devices like our phones are fundamental for our lives today. A typical password is drawn on the touchscreen or entered into it to open the "screensaver." The basic security system can be an unfortunate tradeoff for having greater security. The users can have access to a scary few of words or data spilled under the severe thought about gamblers. With a few closely connected individuals, they may have chance to listen in on the user's great gadget by hacking it and taking their singular data. [13]

IV. PROPOSED CONCEPT

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

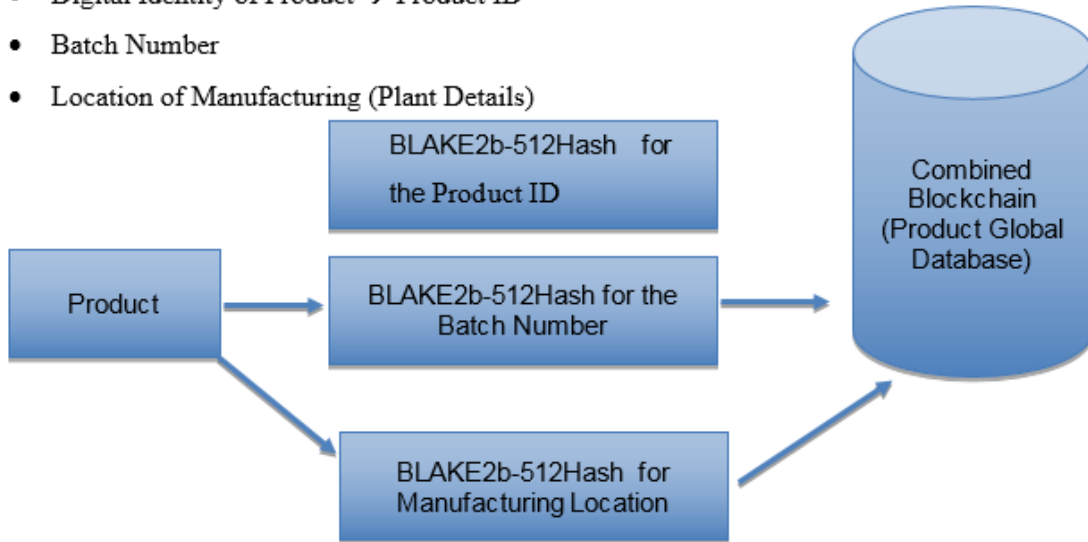


Fig 2. Product Entry Blockchain

Product Validation

Now, at the time of the validation

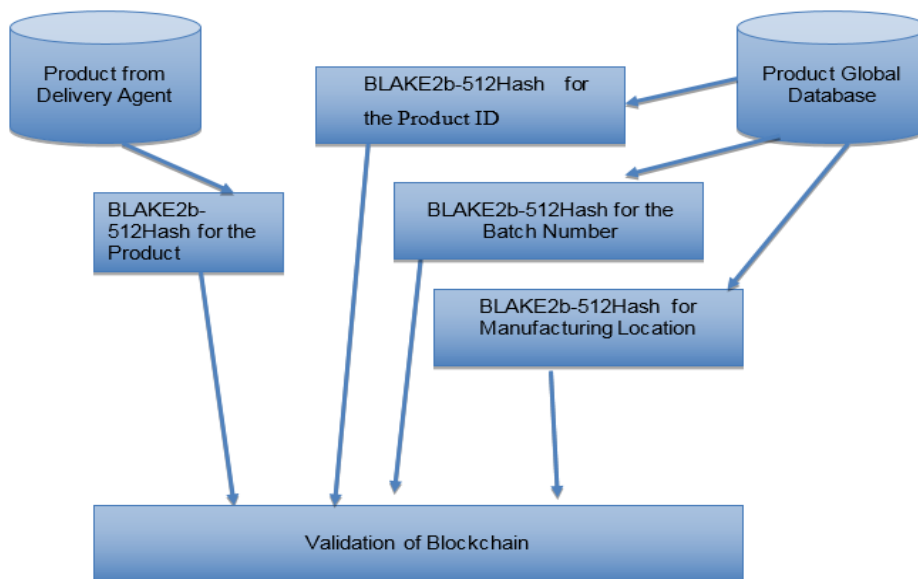


Fig 3. Product Validation Blockchain

V. IMPLEMENTATION AND RESULT ANALYSIS

The simulation website is created in VS 2010 and using database in SQL server 2008

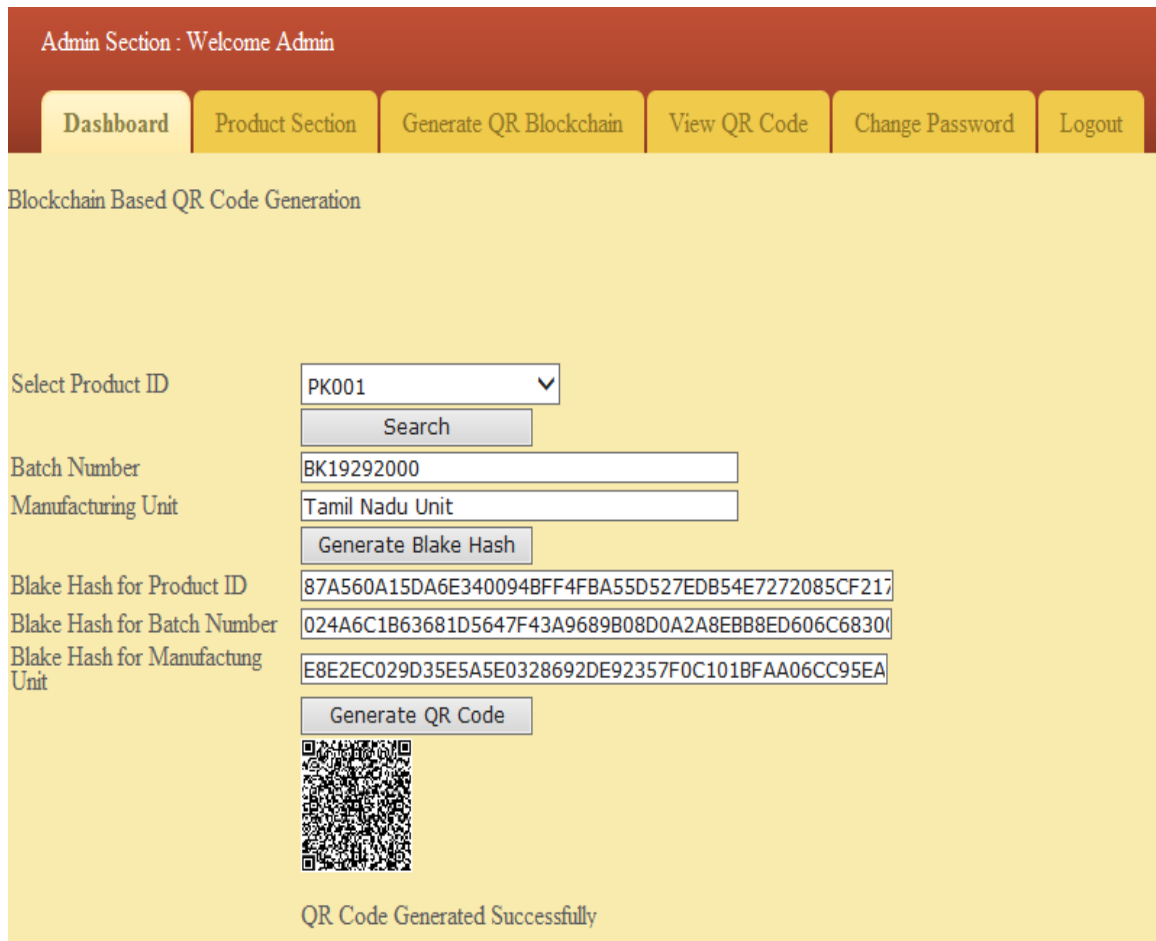


Fig 4. Product Record QR



Fig 5. QR Validation for Product

Result Analysis using Password.blue Test

18FFFEF86DA4245ADCC1A4FE3B356F2d

Show



Fig 6. Test 1 Results base Work

87A560A15DA6E340094BFF4FBA55D527EDB54E72_024A6C1B63681D5647F43A9689B08D0A2A8EBB8E_E8E2EC029D35E5A5E0328692DE92357F0C101BFA

Show



Fig 7. Test 1 Results Proposed Work

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. Test 2 Results Base Work

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. Test 2 Results Proposed

VI. CONCLUSION

With the rise in online sales, there is an increase of counterfeits. When a company is looking to have physical storefronts and items, they need to know how to help protect themselves. It is unwise to use the company's logo on an unlicensed product, as this will cause inconvenience for the customer, and may also degrade your own company's brand. When fake items are cheaper or of lower quality, it is difficult to discern between original product and imitation. Add the QR codes in a manufacturing stage so that the customer can be sure that it is an original product. The concept proposed in the paper is effective in tacking the counterfeits products.

REFERENCES

- 1) Madhu, A. et al. (2020) "Smart bot and E-commerce approach based on internet of things and block-chain technology," in 2020 4th International Conference on Electronics, Communication and Aerospace Technology (ICECA). IEEE
- 2) 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.
- 3) Teja, J. R. (2020) "Proposing method for Public record maintenance using Block chain," in 2020 International Conference on Mainstreaming Block Chain Implementation (ICOMBI). IEEE, pp. 1–5.
- 4) Shree, J. et al. (2020) "To Design Smart and Secure Purchasing System integrated with ERP using Block chain technology," in 2020 IEEE 5th International Conference on Computing Communication and Automation (ICCCA). IEEE.
- 5) Li, G., Sun, S. and Li, X. (2020) "Block chain digital invoice system risk assessment and system development research," in 2020 International Conference on Intelligent Transportation, Big Data & Smart City (ICITBS). IEEE.
- 6) Rajashekaragouda and Dakshayini, M. (2020) "Block-chain Implementation of Letter of Credit based Trading system in Supply Chain Domain," in 2020 International Conference on Mainstreaming Block Chain Implementation (ICOMBI). IEEE.
- 7) 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.
- 8) Y. Mu and B. YAO, "Construction Of Topological Graphic Passwords By Hanzi-gpws," 2019 IEEE 3rd Information Technology, Networking, Electronic and Automation Control Conference (ITNEC), 2019, pp. 1957-1961.
- 9) B. Bilgi and B. Tugrul, "A Shoulder-Surfing Resistant Graphical Authentication Method," 2018 International Conference on Artificial Intelligence and Data Processing (IDAP), 2018, pp. 1-4.
- 10) D. Gupta, A. P. Singh, V. Goar and S. Mathur, "Combination of textual and graphical based authentication scheme through virtual environment," 2017 3rd International Conference on Advances in Computing, Communication & Automation (ICACCA) (Fall), 2017, pp. 1-4.
- 11) J. A. Jaffar and A. M. Zeki, "Evaluation of Graphical Password Schemes in Terms of Attack Resistance and Usability," 2020 International Conference on Innovation and Intelligence for Informatics, Computing and Technologies (3ICT), 2020, pp. 1-5.

- 12) S. Yang, M. Zhang, B. Yao, J. Guo and Z. Bai, "Topological Graphic Passwords Made By Series Sun-graphs On Odd-graceful Property," *2019 IEEE 8th Joint International Information Technology and Artificial Intelligence Conference (ITAIC)*, 2019, pp. 1617-1621
- 13) S. Shen, T. Kang, S. Lin and W. Chien, "Random graphic user password authentication scheme in mobile devices," *2017 International Conference on Applied System Innovation (ICASI)*, 2017, pp. 1251-1254.

