

ARTICLE

A Holistic Anti-Counterfeiting Platform Using NFC and Blockchain Technologies

Rajendren Subramaniam¹, Saaidal Razalli Azzuhri^{2,*}, Teh Ying Wah¹, Atif Mahmood³ and Vimala Balakrishnan¹

¹Department of Information System, Faculty of Computer Science & Information Technology, Universiti Malaya, Kuala Lumpur, 50603, Malaysia

²Department of Computer System & Technology, Faculty of Computer Science & Information Technology, Universiti Malaya, Kuala Lumpur, 50603, Malaysia

³Faculty of Data Science and Information Technology, INTI International University, Nilai, 71800, Malaysia

*Corresponding Author: Saaidal Razalli Azzuhri. Email: saaidal@um.edu.my

Received: 27 November 2024; Accepted: 18 March 2025; Published: 19 May 2025

ABSTRACT: Counterfeiting is still a pervasive global issue, affecting multiple industries and hindering industrial innovation, while causing substantial financial losses, reputational damage, and risks to consumer safety. From luxury goods and pharmaceuticals to electronics and automotive parts, counterfeit products infiltrate supply chains, leading to a loss of revenue for legitimate businesses and undermining consumer trust. Traditional anti-counterfeiting measures, such as holograms, serial numbers, and barcodes, have proven to be insufficient as counterfeiters continuously develop more sophisticated replication techniques. As a result, there is a growing need for more advanced, secure, and reliable methods to prevent counterfeiting. This paper presents a novel, holistic anti-counterfeiting platform that integrates Near Field Communication (NFC)-enabled mobile applications with blockchain technology to provide an innovative, secure, and consumer-friendly authentication mechanism. Our approach addresses key gaps in existing solutions by incorporating dynamic product identifiers, which make replication significantly more difficult. The system enables consumers to verify the authenticity of products instantly using their smartphones, enhancing transparency and trust in the supply chain. Blockchain technology plays a crucial role in our proposed solution by providing an immutable, decentralized ledger that records product authentication data. This ensures that product verification records cannot be tampered with or altered, adding a layer of security that is absent in conventional systems. Additionally, NFC technology enhances security by offering unique identification capabilities, enabling real-time product verification. To validate the effectiveness of the proposed system, real-world testing was conducted across different industries. The results demonstrated the platform's ability to significantly reduce counterfeit products in the supply chain, offering businesses and consumers a more robust and reliable authentication method. By leveraging the combined strengths of blockchain and NFC, this solution represents a significant advancement in the fight against counterfeiting, ensuring enhanced security, transparency, and consumer trust.

KEYWORDS: Blockchain; near field communication (NFC); anti-counterfeiting

1 Introduction

Counterfeiting refers to the production and sale of products by a third party under an original brand name without the authorization of the brand owner. The presence of counterfeit products in the market causes significant financial losses to industries, consumers, and governments. Consumers are often deceived



into purchasing fake products, believing them to be genuine. The global value of counterfeit goods has reached 1.6 trillion US dollars [1], making it the largest criminal enterprise in the world. Over the past two decades, counterfeiting has grown by more than 10,000%, affecting various industries, including food, beverages, footwear, apparel, electronics, auto parts, accessories, pharmaceuticals, toys, cosmetics, and currency [2]. Despite continuous efforts by industries, universities, and governments to combat counterfeiting, the problem remains unresolved and continues to escalate [3]. This persistence indicates that no concrete solution or holistic system has yet been developed to effectively eliminate counterfeit products from the market.

While numerous research efforts, including those involving Near Field Communication (NFC) technology and Blockchain technology, claim to address counterfeiting, few attempts have been made to combine both technologies to enhance effectiveness [4]. In this research, we investigate the integration of NFC and Blockchain technology to tackle the counterfeiting problem. Through a comprehensive literature review of previous studies, we examine existing anti-counterfeiting platforms (ACPs) and propose a remodeled holistic ACP to address the limitations of current platforms. The key components in designing the new ACP include NFC technology [5], Blockchain technology, and Mobile Computing. Besides the original product manufacturers, consumers play a crucial role in a holistic ACP (HACP). Therefore, we developed an effective HACP that combines these components to mitigate counterfeiting.

Based on our literature review, we identified three major gaps in previous studies. The first gap is the failure to address the counterfeiting problem holistically [6]. Previous research did not consider the complete supply chain management processes across the lifecycle of a product in the fight against counterfeiting [7]. Additionally, the role of consumers as a key component in this battle has been largely neglected.

The second gap concerns product identity encoding and authentication, specifically the issue of static product identities. Since static identities are easily cloned, this vulnerability should have been highlighted in prior research. However, static product identities remain widely accepted. We approach this problem from a different perspective by adopting the concept of dynamic product identity [8,9]. In the authentication process, encoding is typically performed by original product manufacturers, while authentication is carried out by consumers. Traditionally, these processes operate independently. However, we propose a novel technique, Blockchained Dynamic Encoding within the Authentication process (AuthentiCoding), which represents a key contribution of this research. Blockchained AuthentiCoding ensures that product identities remain dynamic, effectively neutralizing any compromised identities.

The third gap in previous research is the lack of emphasis on a holistic “proof of concept.” Researchers have often focused on micro aspects of anti-counterfeiting efforts, with insufficient attention given to how their findings fit into a broader, real-world context [10]. As a result, it has been difficult to determine the practical effectiveness of their solutions. To address this, we evaluated our HACP in a real-world environment using a working prototype with potential live clients.

We aim for our new HACP to establish a benchmark in holistic counterfeiting prevention. Beyond benefiting original product manufacturers, the outcomes of this research will also serve the public and governments. Additionally, this study lays the foundation for future academic researchers seeking to tackle the global counterfeiting problem effectively.

2 The Concept

In this research, we propose a Holistic Anti-Counterfeiting Platform (HACP) to combat counterfeiting by utilizing a Near Field Communication (NFC)-enabled mobile application integrated with Blockchain technology. The proposed HACP will enable buyers to verify whether a product is original or counterfeit at

the point of purchase. This system includes an NFC-enabled mobile app that interacts with a backend server connected to a blockchain engine. NFC chips will be encoded and tagged on products at the manufacturing stage by the original manufacturers. We propose an NFC tag serialization and encoding algorithm that leverages blockchain technology. Additionally, we introduce our AuthentiCoding algorithm, which keeps the NFC tag ID dynamic, thereby mitigating risks associated with compromised NFC tags.

Our work includes an evaluation of various encoding systems, encompassing algorithms, tools, and techniques. Encoded NFC chips will be tagged on products throughout the supply chain until they reach the storefront. Consumers will use an NFC-enabled mobile app to authenticate NFC tags via our AuthentiCoding algorithm before making a purchase. The key research components include: (i) NFC Tag Encoding and (ii) NFC Tag AuthentiCoding. Our contribution involves assessing different encoding and AuthentiCoding systems, including their algorithms, tools, and techniques. The new HACP builds upon past research while introducing additional features to enhance the system's effectiveness.

This research employs the block-supply chain concept, a decentralized supply chain mechanism designed to detect counterfeiting attacks using blockchain and NFC technologies [11]. The block-supply chain replaces traditional centralized supply chain models and implements a newly proposed consensus protocol that, unlike existing protocols, is fully decentralized and optimizes both efficiency and security. Simulations demonstrate that the proposed protocol delivers remarkable performance while maintaining a satisfactory level of security compared to the state-of-the-art Tendering consensus protocol.

We adopt the Tag Reapplication Detection (TRD) approach as a key strategy for detecting reapplication attacks [12]. This method employs low-cost NFC tags and public-key cryptography. The use of NFC enhances user-friendliness, as many modern smartphones support NFC functionality. TRD detects reapplication attacks by tracking the number of times a tag has been scanned throughout the supply chain using an online AuthentiCoding protocol. By integrating Alzahrani's lightweight authentication protocol with the block-supply chain and our AuthentiCoding method, we aim to enhance security and combat counterfeiting more efficiently and accurately.

Table 1 provides a summarized overview of selected prior research efforts addressing counterfeiting. It highlights the approaches, methodologies, and technologies utilized in these studies, along with the specific challenges or shortcomings identified in each. This table serves as a foundational reference for understanding the existing landscape of anti-counterfeiting strategies and identifying gaps that future research and interventions can address.

Table 1: Sample glance of previous studies on addressing counterfeiting problem with their respective limitations

Reference	Summary	Comments/limitation
[13]	This article proposed blockchain technology in India's entire drug supply chain to address the lack of adequate audibility and clarity of the initial source of drugs.	Utilised blockchain technology to address counterfeiting but no significant evidence that the proposed idea is feasible.

(Continued)

Table 1 (continued)

Reference	Summary	Comments/limitation
[14]	This article proposed an anti-counterfeit model via NFC technology using a lightweight cryptographic algorithm on the NFC.	The setback of this model is on the secret information to be stored on the NFC for it to work offline. The NFC has limited storage space and is unable to store a large amount of data for it to work offline. A significant working prototype would be good as POC.
[15]	This paper proposed packaging-related anti-counterfeit methods that can be utilized within a broader anti-counterfeit strategy.	The exact packaging measurement proposal is vaguely defined. However, any packaging is easily duplicable.
[16]	This research proposes a new split production-based pill-level unduplicatable chipless RFID tag that inherently produces a random unique ID from numerous sources.	The proposed a reliable unclonable solution but needs a special device to detect if the item is original or fake. Consumers are not roaming around with those gadgets to detect if the pill-level UCR is genuine.
[17]	The counterfeit problems were addressed using RFID technology.	RFIDs are easily duplicable. Hence, this approach will not be a completely proven anti-counterfeit solution.

2.1 More on Technology

Recent advancements in Radio Frequency Identification (RFID) and Near Field Communication (NFC) technology have encouraged original product manufacturers to explore ways to replace traditional product identification methods such as barcodes, QR codes, and holograms. NFCs are a type of RFID. These RFID/NFC tags are cost-effective labels that facilitate real-time tracking and tracing. Additionally, these tags enable retailers to provide a more intelligent shopping experience, allowing customers to purchase items through smart retail systems equipped with RFID-enabled shopping carts.

Subramaniam et al. [14] stated that, to combat counterfeiting, researchers have designed solutions based on the Internet of Things (IoT), incorporating barcodes, RFID, and QR codes for authentication and authorization. However, RFID technology requires a physical RFID reader device, which is not yet widely accessible or affordable for general consumers. Compared to QR codes, RFID tags and labels are slightly more expensive as they are designed for both reading and writing. These tags can only be read using an RFID reader, meaning that anyone with an RFID reader can access and potentially clone the code [18].

The proliferation of counterfeit products has plagued various industries for decades, making the fight against counterfeiting a persistent challenge. Existing anti-counterfeit solutions are generally centralized. To address this limitation, Alzahrani et al. [19] proposed the Block-Supply concept, a decentralized anti-counterfeiting supply chain that integrates NFC-enabled mobile computing with blockchain technology. Unlike most existing protocols, this approach introduces a truly decentralized consensus protocol that does not require Proof of Work (PoW) [19].

In another study, Alzahrani et al. [5] introduced an authentication protocol based on the Internet of Things (IoT) to help validate unit drug dosages in anti-counterfeit pharmaceutical systems. This protocol utilizes NFC technology, which is particularly convenient for mobile environments. Their test results indicate

that the proposed system effectively mitigates common vulnerabilities while enhancing computational efficiency and security.

Further proposals suggest the use of NFC chips in banknotes to prevent counterfeit currency [20]. A smart-banknote system was developed and evaluated using fault tree analysis and flow model analysis. Additionally, research has explored electrode signal transformation into a 105.9-kb/s Manchester-encoded serial bit stream transmitted via NFC, reinforcing the potential adoption of NFC chips in anti-counterfeiting platforms [21].

A survey conducted in Indonesia demonstrated that NFC-based mobile payment systems have been well received [22]. Beyond financial transactions, NFC technology has also become a promising tool for healthcare and wellness monitoring. Research has demonstrated the feasibility of embedding temperature and sweat sensors into smart textiles using NFC antenna technology [23]. This proven concept could be adapted for anti-counterfeiting applications.

India has been one of the earliest adopters of NFC technology in the pharmaceutical industry [24]. The proposal involved embedding NFC tags into pharmaceutical packaging to improve drug authentication and traceability. However, the research did not propose a comprehensive end-to-end solution to evaluate the feasibility of implementing this system in real-world environments.

3 Literature Review

Over the past two decades, counterfeiting has increased by over 10,000% [25], spreading across various industry segments, including food, beverages, footwear, apparel, electronics, auto parts, accessories, pharmaceuticals, toys, cosmetics, and currency [25]. Vendors of counterfeit goods often infringe upon a brand proprietor's trademark, design, or copyright, falsely passing off their products as genuine. Counterfeiting has become a serious issue in modern commerce, with an estimated global value of 1.6 trillion U.S. dollars [26]. Brand owners collectively spend up to 204 billion dollars annually to combat this growing problem. In 2013, counterfeit goods accounted for 5%–7% of global trade, and by 2014, counterfeiting had led to an estimated loss of 2.5 million jobs worldwide, including 750,000 jobs lost in the United States. Furthermore, the Organisation for Economic Co-operation and Development (OECD) reported that in 2013, nearly 5% of products imported into the European Union were counterfeit.

Over the past few decades, numerous efforts have been made to combat counterfeiting. It is estimated that approximately 1347 anti-counterfeiting tactics are currently being used [27]. Technology has played a significant role in these efforts. However, despite technological advancements, counterfeiting has not declined, raising concerns about the effectiveness of current solutions.

One widely adopted method is QR code authentication using smartphones [28]. Technology vendors provide QR code-based labels or stickers that allow consumers to verify a product's authenticity by scanning the QR code at the point of purchase. Users are then redirected to an application programming interface (API) [29] or a centralized database [30] for verification. This method offers convenience; however, QR codes are easily replicable, allowing counterfeiters to duplicate them and place them on fake products. Since the validation check relies solely on scanning, a copied QR code cannot reliably indicate whether a product is counterfeit. As a result, QR code-based track-and-trace systems are ineffective in combating counterfeiting.

Researchers have also explored machine learning and the Internet of Things (IoT) for counterfeiting detection in e-commerce. A prediction model has been proposed to analyze consumer purchasing patterns and detect potential counterfeit product sellers [31]. Additionally, a universal forgery detection system based on cloud computing has been proposed as a theoretical framework. While empirical evidence supports the

feasibility of this method, it has a significant drawback-counterfeit detection occurs only after fraudulent transactions have already taken place [32].

By the time counterfeit products are detected, fraudulent manufacturers may have already altered or discontinued their fake products. Typically, counterfeit manufacturers operate with short-term objectives, aiming to maximize quick profits before shifting to new counterfeit products. As a result, a universal cloud-based forgery system is ineffective as a long-term anti-counterfeiting solution.

4 Methodology

We began by reviewing the strengths and weaknesses of existing anti-counterfeiting solutions through an extensive literature review. Based on this review, we analyzed a range of Anti-Counterfeiting Platforms (ACPs), examining the advantages and disadvantages of each. Following this analysis, we proceeded to investigate the remodeling of ACPs, considering the technologies utilized, tools employed, methodologies, algorithms, and approaches.

The key components in designing the new Holistic Anti-Counterfeiting Platform (HACP) include Near Field Communication (NFC), Blockchain, and Mobile Application technology. An effective HACP to combat counterfeit products will be developed using a combination of these components and factors. The remodeling of the HACP consists of two main phases: “Encoding” and “AuthentiCoding.”

The first phase, “Encoding,” encompasses various processes such as serialization, metadata construction, data hashing, blockchain notation, and digital signatures, among others. In this phase, we employ Alzahrani’s protocol to enhance security and data integrity. The second phase, “AuthentiCoding,” involves data decryption and authentication. Fig. 1 illustrates the evolution of the HACP, from HACP1 to HACP5, demonstrating the progressive improvements in its design and functionality.

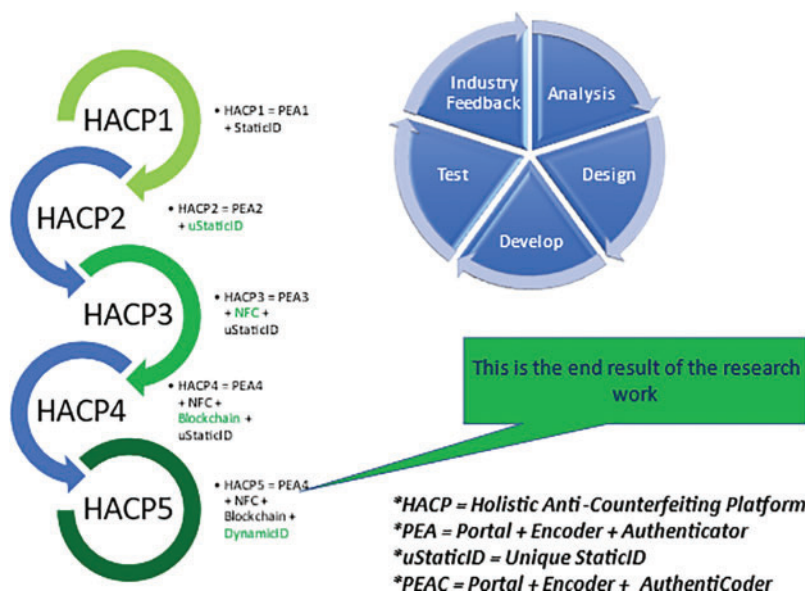


Figure 1: The journey of remodeling HACP

HACP1 = PEA1 + QR Codes

HACP1 is the initial HACP model derived from a preliminary literature review. This model establishes the starting benchmark for the research work. It incorporates key technological components, including

the manufacturer portal, encoder application, authenticator mobile application, and a backend processing system that integrates with the blockchain network. This set of components closely represents current anti-counterfeiting practices in the industry. The manufacturer portal allows original product manufacturers to independently create product brands and production batches with Security IDs, ensuring that no third party is involved in generating the Product ID.

The encoder mobile application is used by manufacturers to encode product information, followed by consumers utilizing the mobile authenticator application to verify the Product ID at the point of purchase. The Product ID is a common static identifier used across all products, a standard practice among industry practitioners. This complete solution was demonstrated to respondents to gather their feedback. However, initial industry feedback indicated that this model is susceptible to duplication, similar to existing anti-counterfeiting systems. Security IDs can be replicated across counterfeit products, making duplication relatively easy. Once an ID is duplicated, it can be copied across an unlimited number of counterfeit products.

HACP2 = PEA2 + Unique QR Codes

The limitations of HACP1 led to the development of HACP2, where we introduced a Unique Security ID for each product. Every Product ID is uniquely assigned. Consequently, to produce n counterfeit products, counterfeiters would need to acquire n original products to duplicate n Security IDs. While this model partially mitigates the counterfeiting problem, industry feedback indicated that further improvements were necessary.

HACP3 = PEA3 + NFC

To enhance HACP2, we developed HACP3, incorporating NFC chips known for their resistance to duplication. We designed, developed, and introduced an NFC-enabled mobile encoder application for encoding NFC chips. While this model improved security compared to HACP2, industry feedback suggested the need for further refinements.

HACP4 = PEA4 + NFC + Blockchain

Our literature review on blockchain research highlighted its adoption across the downstream supply chain ecosystem. As a result, HACP4 was introduced to leverage blockchain technology. Our backend system was redesigned to accommodate blockchain integration, and we implemented the Ethereum blockchain in this research. However, further industry feedback necessitated continued improvements to the model.

HACP5 = PEAC + NFC + Blockchain + DynamicID

Finally, we further enhanced HACP by introducing DynamicID. All previous security measures relied on static IDs. Recognizing the vulnerabilities of static identification, we leveraged NFC chips' read-and-write capabilities to implement DynamicIDs as product identifiers.

To facilitate authentication and encoding, we replaced the traditional authenticator mobile application with the AuthentiCoding mobile application, which integrates the newly introduced DynamicID system. This transition enables seamless authentication and encoding, significantly strengthening HACP5's security framework.

By combining Near Field Communication (NFC), blockchain technology, and DynamicID, we developed a novel system that enhances security against counterfeiting threats. Previous security protocols relied primarily on static IDs, making them vulnerable to attacks. The introduction of DynamicID adds a dynamic element to product authentication, making it more resilient to security breaches.

The AuthentiCoding mobile application functions as an efficient platform for authentication and encoding tasks, further strengthening the security measures of HACP5. By incorporating DynamicID alongside NFC and blockchain technology, our research significantly improves the overall security framework, offering

a more comprehensive solution to address evolving challenges in secure identification and authentication protocols. We utilized Alzahrani's [5] lightweight authentication protocol. The second part of the system involves data decryption and AuthentiCoding.

4.1 More on Methodology

To further enhance security, we propose the use of dynamic product IDs embedded within NFC chips, leveraging blockchain technology. Unlike static identification systems, our proposed product IDs are dynamic. Our product authentication algorithm includes an encoding algorithm that ensures the product ID remains dynamic.

Addressing the counterfeiting ecosystem requires multi-stakeholder involvement across the product supply chain. Therefore, utilizing NFC-based dynamic product IDs in conjunction with blockchain technology will significantly enhance security in a holistic manner. The desired processes and parameters for constructing an optimized, remodeled ACP are illustrated in Fig. 2.

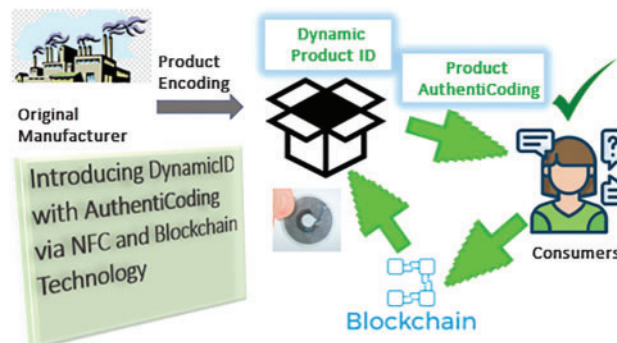


Figure 2: Introducing AuthentiCoding

Thus, as shown in Fig. 3, even if a counterfeit manufacturer successfully duplicates the product ID and places it on a fake product, the authentication will fail due to the duplicate entry.

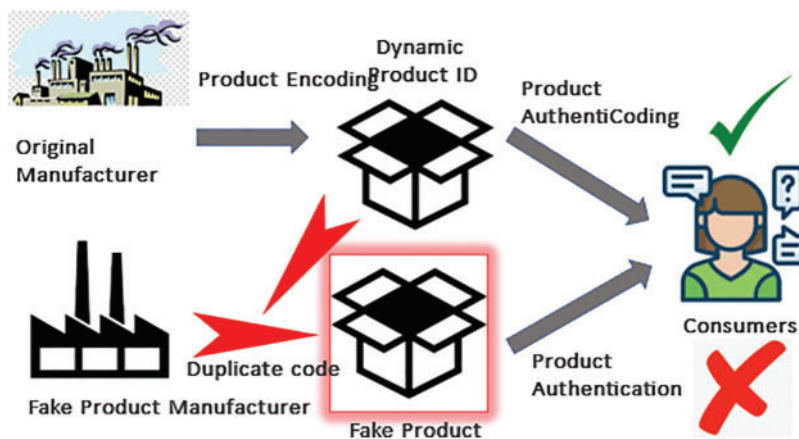


Figure 3: Proposing dynamic product AuthentiCoding

After we finalised the remodelled ACP, the next step was the design and development of a prototype to validate the desired ACP. Based on the literature review, one of the major gaps in previous studies is, missing proof of concept or missing working system to prove the proposed system works or not. Past research was focused on individual components of an anti-counterfeiting platform. Hence, they are unable to perform a complete end to end test to address the counterfeiting problem holistically. Thus, in our research, we are serious about closing this gap. Hence, we see designing and developing an ACP prototype as the critical success factor of this research. The product originator module shall be made available for the original product manufacturer to configure and encode the NFC tags into their original products. On the other side, a mobile app shall be made available for the public to authenticate the NFC tags. The encoding process and AuthentiCoding process are two separate processes to be developed independently. The challenge here is to ensure the AuthentiCoding function will be able to verify the authenticity of the encoded NFC tags.

Finally, our research findings will be evaluated with the industry [33,34]. We have selected manufacturers of original products who are committed to protecting their products from counterfeiting. We will provide training to help them utilize our prototype system and allow their products to circulate in the market. Consumers will then use our mobile authenticator application to verify the authenticity of these products before purchasing them. We also challenge the original product manufacturers to attempt to duplicate the product ID. Feedback from these manufacturers will be obtained to assess the reliability of our proposed methods and solutions, validating that our research findings work as expected. Industry feedback is a key factor in determining whether we succeed in the battle against counterfeiting. Unlike other research methodologies where evaluation occurs at the end, our evaluation process is continuous and integrated into the research journey.

5 The Holistic Anti-Counterfeiting Platform (HACP)

We need both hands to clap. Most of the anticounterfeiting efforts were centralised on the suppliers as the key stakeholder in the framework but the role of consumers are often neglected when considering an HACP. The role of consumers plays vital role in perfecting an anticounterfeiting framework.

As depicted in Fig. 4, we identified there are four major components that would form a successful HACP.

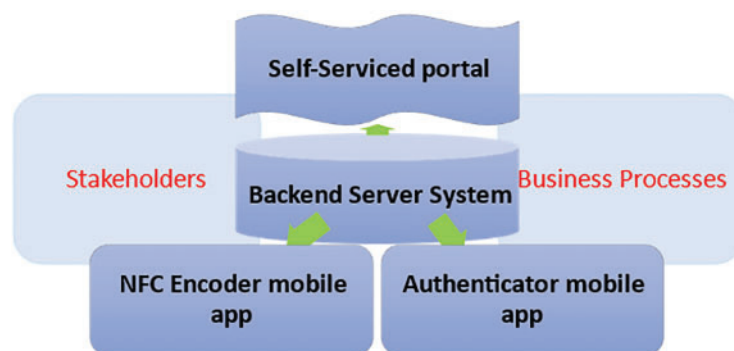


Figure 4: A holistic anti-counterfeiting platform

- Backend Server System that facilitates Administration, Blockchain operation, authentication, Encoding Algorithm
- A portal for the original product manufacturers
- Mobile application for NFC encoding for the original product manufacturers
- Mobile application for NFC authentication for consumers (public)

5.1 Backend Server System

The backend server system is hosted on cloud which keeps the records of original product manufacturers and their respective products and transaction. This server also will facilitate the blockchain integration. We utilize off-chain concept [35,36]. Off-chain transactions can be better understood when compared to on-chain transactions. An on-chain transaction, simply called a transaction, occurs, and is considered valid when the blockchain is modified to reflect the transaction on the public ledger [37]. It involves the transaction being validated and authenticated by a suitable number of participants, recording the details of the transaction on the suitable block, and broadcasting the necessary information to the whole blockchain network, which makes it irreversible.

The backend module of our simulation project is implemented using Flask for the backend, SQLite for the database, and a simulated blockchain for hash storage. Here are some key points about the backend module:

1. **API Endpoints:** The backend includes several API endpoints to handle various functionalities. For example, the /api/nfc-authenticate endpoint handles NFC tag reading and authentication.
2. **Database Integration:** The backend uses SQLite for database integration. The database stores product details such as productId, productDesc, productPrice, timestamp, and hash.
3. **Blockchain Integration:** The backend includes a simulated blockchain to store hash values. The blockchain is used to verify the authenticity of products by checking the hash values.
4. **NFC Functionality:** The backend includes functions to read from and write to NFC tags. For example, the read_from_nfc function reads the hash value stored on an NFC tag, and the write_to_nfc function writes the updated hash value to an NFC tag.
5. **Hash Generation:** The backend includes a function to generate hash values using the SHA256 algorithm.
6. **Threading:** NFC writing is triggered in a separate thread to ensure the API response is not delayed.

The blockchain module is implemented using a simulated blockchain for hash storage. Here are the key points:

1. **Blockchain Class:** The Blockchain class is defined in the blockchain.py file. It includes methods to initialize the blockchain, add a block, and verify a block.
2. **Initialization:** The blockchain is initialized with an empty chain when an instance of the Blockchain class is created.
3. **Adding Blocks:** The add_block method appends a new hash value to the blockchain.
4. **Verifying Blocks:** The verify_block method checks if a given hash value exists in the blockchain item.
5. **Integration with Backend:** The blockchain is integrated with the backend module implemented using Flask. The backend includes API endpoints to handle product registration and authentication, which involve adding and verifying hash values on the blockchain.
6. **Hash Generation:** Hash values are generated using the SHA256 algorithm and are used to ensure the authenticity of products.
6. **NFC Integration:** The backend also includes functions to read from and write to NFC tags, which involve interacting with the blockchain to verify and update hash values.

5.2 Self-Serviced Portal for Original Manufacturers

We proposed a portal for original product manufacturers to configure their company, products, and brand details so that they can encode the NFC tags in batches. This dedicated portal for the original manufacturers is necessary due to the privacy and security of the original product information. The original manufacturers must be independent in providing their product details. This is to avoid any third-party

involvement that might lead to potential fraudulences. Hence, the portal would be able to ensure the objective is achieved to upkeep this security measurement. Past research neglected this component as their focus was not on a holistic platform to address counterfeiting problem.

Figs. 5 and 6 illustrate an admin portal in our proposed HACP for the original product manufacturers to do initial registration and the setup of their products. The first step is for the manufacturers to register themselves and provide their business details. This first step is only required only once before setting up anything else. Normally to be done by the system admin. A centralized authentication team is required to verify the authenticity of the manufacturer. Once the manufacturer was verified, they are allowed to proceed to login into the portal and setup products.

The second step, shown in Fig. 7, involves manufacturers setting up their product brands in the system. The system supports multiple brands per manufacturer, allowing users to add brand details such as descriptions and logo images. For our research evaluation, configuring just one brand is sufficient.

Admin Portal v2.0.5 Account : MAXXIMA

Home Business Setup Brands Content Editor Tag Batch (QRcode/NFC) Token Purchase Transaction History Technical Support

Business Setup

Enter the details about your organization here

Organization Name: MAXXIMA RESOURCES (M) SDN BHD

Description: Drawing more experiences, charting excellent scientific innovation, offering up-to date lifestyle products, streamlining solid values and standardising high quality control, MAXXIMA continues to pave new pathways for people to lead healthier and wealthier lives - and the numbers are increasing every day.

Logo: Recommended Resolution : 100px X 50px. MAXXIMA. Upload Image

Organization Type: Private Limited

Operation Type: Product Manufacturer/Assembler Nature Of Business

Registration Number: A123456789 Official Registration number of this Business/Organization

Country: Malaysia

Address: Micom Glenmarle Industrial Park, Section U1, 40150 Shah Alam, Selangor Darul Ehsan.

Website: https://maxxima.my/

Tel: 1 800 18 7996

Email: maxxima@orygene.uk

Verified Status: Apply for Verified Status

Save

Figure 5: Admin portal for original product manufacturers steps

Admin Portal v2.0.5 Account : MAXXIMA

Home Business Setup Brands Content Editor Tag Batch (QRcode/NFC) Token Purchase Transaction History Technical Support

Manage Brand

Edit the record details here. If your brand requires verified status, click 'Apply for Verified Status' button

Brand Name: AFX

Organization's Role: Manufacturer

Logo: Recommended Resolution : 200px X 50px

Upload Logo

Description: AFX adalah makanan tambahan dalam bentuk kapsul yang meningkatkan sistem imuniti dan mengecas tubuh anda dengan pelbagai jenis khasiat dari ekstrak AFA. Campuran unik makanan tambahan ini juga mampu meningkatkan tenaga, bertindak sebagai antioksidan dan menaikkan mood anda.

Verified Status: Apply for Verified Status

Save Delete

Record Saved
The record has been saved
OK

Figure 6: Admin portal for original product manufacturers to manage their brands

Admin Portal v2.0.5 Account : MAXXIMA

Home Business Setup Brands Content Editor Tag Batch (QRcode/NFC) Token Purchase Transaction History Technical Support

Edit Content

Compose your Content here. This content will be displayed to user when the tags is scanned with Authenticator app.

Upload Image

Content Name: AFX-Ver 2021

Brand: AFX

Content Type: Static

Content Editor Script

Kenapa AFX?

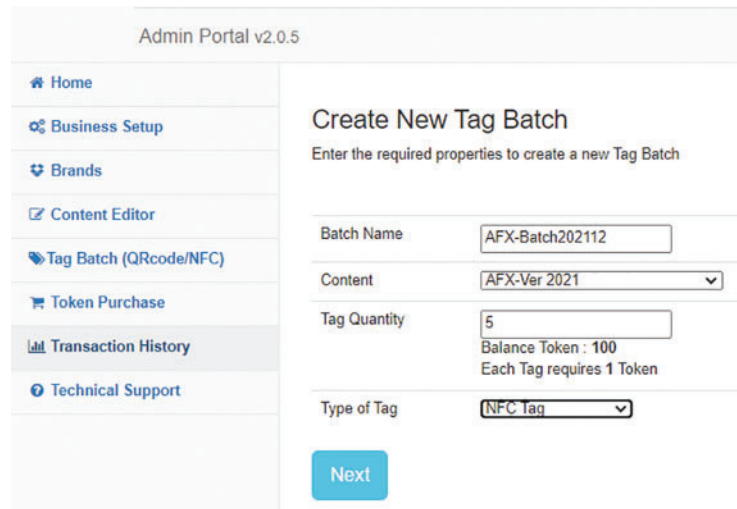
AFX mampu meningkatkan tenaga dan menyumbang kepada kesihatan yang lebih baik untuk anda dan keluarga. Makanan tambahan ini menggunakan teknologi moden untuk melindungi khasiatnya yang sensitif terhadap haba dan menghalang oksidasi berlaku sepanjang proses rhyah-kimia produk ini. Selain itu, kelebihan utama AFX adalah kemampuannya dalam meningkatkan kesihatan tubuh anda untuk menjaga dan memulih sel-sel baharu dengan menyokong sel-sel sihat didalam tubuh anda. 1 botol mengandungi 45 kapsul.

Save Delete

Figure 7: Admin portal for original product manufacturer to manage the contents of their brands

Once the product brand and contents were configured, the fourth step is to create production batches as illustrated in Fig. 8. Each batch consist of the batch ID, quantity, creation date, expiry date and other relevant fields. Though we provide both options of NFC tags and QR codes, this step is required to generate unique identifications which will be encoded into the NFC tags. It is necessary to have the batches as the products

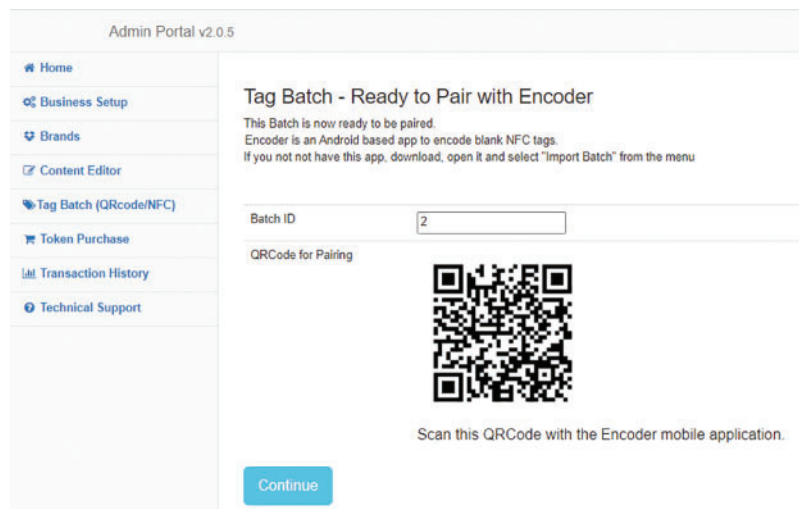
are produced in batches and each batch has its own properties like the manufacturing dates, expiry dates etc. The batches are associated with the brand and their respective contents. It is also required to specify the quantity for each batch. The quantity is the control for the number of NFC tags to be issued for the batch. Our research considers all aspect of business requirements which is in line with the production operation.



The screenshot shows the 'Admin Portal v2.0.5' interface. On the left is a sidebar menu with options: Home, Business Setup, Brands, Content Editor, Tag Batch (QRcode/NFC), Token Purchase, Transaction History, and Technical Support. The main area is titled 'Create New Tag Batch' with the instruction 'Enter the required properties to create a new Tag Batch'. The form contains the following fields: 'Batch Name' with the value 'AFX-Batch202112', 'Content' with a dropdown menu showing 'AFX-Ver 2021', 'Tag Quantity' with a value of '5' and a note 'Balance Token : 100 Each Tag requires 1 Token', and 'Type of Tag' with a dropdown menu showing 'NFC Tag'. A blue 'Next' button is at the bottom.

Figure 8: Admin portal for original product manufacturer to create production batches

The fifth step, as illustrated in Fig. 9, is to generate a QR code for the batch for pairing with the NFC encoder mobile application. This QR code is the key to bridge the product profile to be transferred into the NFC encoder mobile application. This step describes to role of the mobile encoder application starting from importing the desired profile from our backend server before enabling NFC tag encoding.



The screenshot shows the 'Admin Portal v2.0.5' interface. The sidebar menu is the same as in Figure 8. The main area is titled 'Tag Batch - Ready to Pair with Encoder' with the instruction 'This Batch is now ready to be paired. Encoder is an Android based app to encode blank NFC tags. If you not not have this app, download, open it and select "Import Batch" from the menu'. The form contains the following fields: 'Batch ID' with a value of '2', and a 'QRCode for Pairing' section displaying a QR code. Below the QR code is the text 'Scan this QRCode with the Encoder mobile application.' and a blue 'Continue' button.

Figure 9: Admin portal for original product manufacturer to pairing tag batches

5.3 Mobile Application for NFC Encoding

The 3rd technology component of our HACP is a mobile application for NFC encoding, which has been designed and developed to encode the NFC tags. Also referred as the NFC Encoder. As illustrated in Fig. 10, this step describes to role of the mobile encoder starting from importing the desired profile from our backend server before enabling NFC encoding.

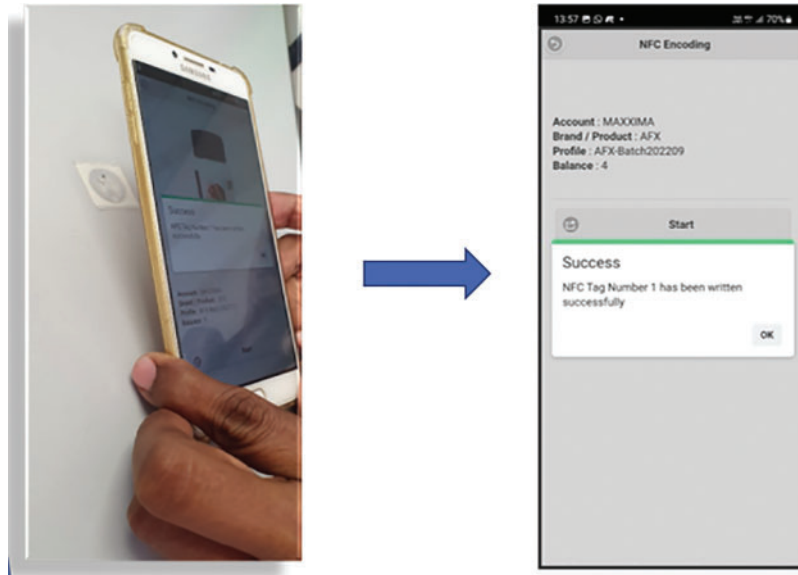


Figure 10: Encode NFC tags step 3

The first step from the mobile encoder is the pairing process where the encoder application is required to scan the QR code generated by the batch process in the web portal. A mobile application for NFC encoding has been designed and developed to encode the NFC tags. Also referred as the NFC Encoder. The first step is to scan the QR code generated by the batch process mentioned above.

Once the QR code is scanned as shown in Fig. 9, the NFC Encoder will download the NFC encoding details of the desired products from the backend server and prepared for encoding the NFC tags. A confirmation popup is displayed upon successful pairing of the product details into the NFC encoder application.

We just need to tap on the NFC tags one by one. The mobile apps will display successful results on screen as shown in Fig. 10. These steps mentioned above, completes a full cycle of product encoding from the original product manufacturers, which is the first part of a complete anti-counterfeiting platform. Meanwhile, the user can also opt to use multiple NFC Encoders to encode the same batch. This encoding process also can be automated for large quantities. Once the NFC Tags has been encoded, the NFC Tags must be attached on the respective products. Normally it will be attached on the product packaging. NFC encoding success will be displayed to the users to confirm that the NFC tag has been encoded successfully. Along the process, our backend server will keep track of the encoding quantities.

Fig. 11 illustrates the tracking of the NFC tags that has been encoded and used on the field. We keep track the frequency of the tag verified via our NFC authenticator mobile application. We are also able activate or deactivate and NFC tag if there is any suspicion of the NFC tags being compromised. This is the management console to manage the tags that has been generated. We may click the refresh button to load newly generated tags. Once tags are listed in the table, we may click on the individual row to preview the tag and make any

changes if required. Once the NFC Tags has been encoded, the NFC Tags must be placed on the respective products. Normally it will be placed on the product packaging.

Batch Name

Glenfiddich202012

Batch Number

162

Content

Glenfiddich 18 Year Old Sr

Tag Type

QR Code

Show 10 entries

Tag Number	Tag ID	Usage	Status
1	DwpoRLFOaSazn6	0	Active
2	yPnzKgFR7TMzWe	0	Active
3	rZxGmVFL7CPzp2	0	Active
4	Eqaz5ZF74CBJ76	0	Active
5	5xwJYWF69UkGBY	0	Active
6	xXR0qVFrVINGZw	0	Active
7	6R4z21FgYSqG23	0	Active
8	EN3zaJFDKt8JdL	0	Active
9	TV5G02Fj8hNo0a	0	Active
10	7B3GBQFbAIXoXZ	0	Active

Showing 1 to 10 of 10 entries

Previous

1

Next

Export to CSV

Refresh

Preview QR Codes

Figure 11: Logs of encoded NFC tags

5.4 Mobile Application for NFC Authentication

The second part of the anti-counterfeiting platform is the role of the consumers. This role is a critical factor in an anti-counterfeiting eco-system. This component is often overlooked in previous research evaluation [38]. A mobile application for the NFC authentication has been designed and developed and made available for the public [39]. We expect the consumer to scan the NFC Tags using the NFC Authenticator application, which will cross check the validity of the NFC Tags with our server [40]. With the start-up screen displayed as illustrated on Fig. 12, a touch on the product with the NFC tag, shall read the SecurityID of the NFC tag and cross check for the authenticity with our backend server. If the NFC tag do not have any contents, nothing will be displayed on the screen. If an invalid NFC were detected, an error message will be displayed. If a valid NFC tag were detected, the application will fetch the NFC Tag details from our server as per configured at setup stage by the original manufacturer.

During authentication, the AuthentiCoding process will take place. This step will be the climax of the cycle of the proposed anti-counterfeiting eco-system where the system will regenerate the blockchain product identifier and recode it back on the NFC chips. Hence, this will keep the product identifier dynamic, which eliminates static identifiers that prone to duplication. The DynamicID defuses any attempt of duplication. With this process it completes an end-to-end anti-counterfeiting eco-system. These steps completes showcase of one full cycle of NFC tag encoding and authentication.

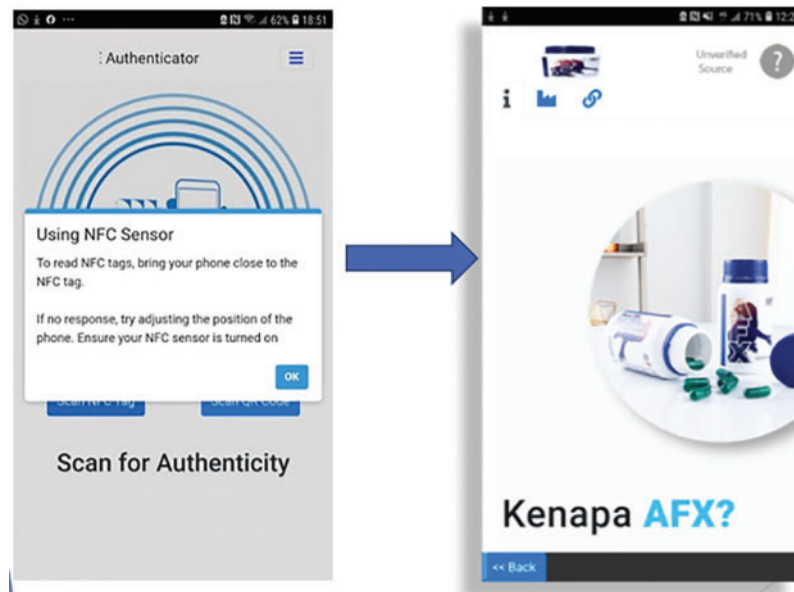


Figure 12: NFC authentication

6 AuthentiCoding

Common anti-counterfeiting solutions have two main components, that is Encoding and Authentication. Encoding is the process from the original product manufacturer to generate product codes that will be attached along with the products. A simplified version of encoding pseudocode is shown on [Fig. 13](#).

```
Encoding(newCode){
  try {
    const ndef = new NDEFReader();
    await ndef.write(newCode);
    log("NFC encoding success");
    blockchainProcess(sendData);
    log("Blockchain process success");
  } catch (error) {
    log("Encoding fail" + error);
  }
}
```

Figure 13: Encoding pseudocode

The second component is the Authentication process to authenticate the product codes. The common practice is for these product codes to remain static across the lifespan of the product. However, in our research, we are introducing the AuthentiCoding process instead of Authentication process. A simplified AuthentiCoding pseudocode is shown in [Fig. 14](#). The NFC encoding function is being called within the Authentication function.

```

AuthentiCoding(){
  try {
    const ndef = new NDEFReader();
    await ndef.scan();
    log("> Scan started");

    ndef.addEventListener("readingerror", () => {
      log("NFC Not Valid, Suspected duplicate product");
    });

    ndef.addEventListener("reading", ({ TagData, serialNumber }) => {
      validatedNFC(${serialNumber},${TagData});
      if validationSuccess(){
        displayMessage("Original Product :"+
          extractProductDetails (${serialNumber},${TagData}));
      }
      Encoding(generateNewCode());
    });
  } catch (error) {
    log("Read Error " + error);
  }
}

```

Figure 14: AuthentiCoding pseudocode

7 Evaluation

7.1 Research Evaluation Participants

One of our sponsoring companies, Global Vision Research Sdn Bhd (GVR), facilitates the engagement of the research participants. GVR has more than 25 years of experience in the research business, has been supporting this research project since the introduction of HACCP. A total of 400 invitations were sent to various industry experts from multiple countries. We shortlisted forty (40) industrial experts based on their seniority, position and industrial experience to assist us in the evaluation by providing industrial feedback on our research findings. These industrial experts include original product manufacturers that have concern on their products being imitated by the counterfeiters. GVR has carefully identified respondents by circulating invitations to four hundred (400) randomly selected industrial experts. From the responses, forty industrial experts were shortlisted to participate in this research. The average industrial experience of these participants is 28 years.

With reference to [Table 2](#), 26% of the research participants are from Fast Moving Consumer Goods (FMCG) sectors while another 26% from pharmaceutical sector. These two industries are among the industries that are extensively affected by counterfeiting. The respondents from these 2 industries includes manufacturers and retailers. The remaining research participants of 48% are from the Technology sector who are involved or interested in developing anti-counterfeiting solutions.

[Table 3](#) refers to the positions of the research participants. Only respondents with senior positions are considered for the research, where 19% of the research participants comprises of Chief Executive Officers (CEO), 40% are Chief Information Officers (CIO), 17% are Chief Operating Officers (COO) and the remaining 24% are other Senior Managers.

Table 2: Industry sectors of the research participants

Industry sector	Ratio
FMCG	26%
Technology	48%
Pharma	26%
Total	100%

Table 3: Positions of the research participants

Positions	Ratio
CEO	19%
CIO	40%
COO	17%
SM	24%
Total	100%

Table 4 shows the origin country of the research participants. Based on the seniority qualification and the industrial sector, the filtered research participants come from various countries. The largest number of research participants are from Malaysia, with 31% of them. Number of the research participants from Italy is the second largest with 24%. The remaining 45% of the research participants comes from United Arab Emirates, Germany, Brazil, United States, Greece, Canada, Qatar and Saudi Arabia.

Table 4: Origins of the research participants

Countries	Ratio
Brazil	5%
Canada	2%
Germany	7%
Italy	24%
Malaysia	31%
New Zealand	5%
Qatar	2%
Saudi Arabia	2%
United Arab Emirates	12%
United States	5%
Greece	5%
Total	100%

7.2 The Research Evaluation Process

After the initial literature review and industry exploration, we introduced our first HACP. We identified there are four major components in the HACP that comprises of (1) a backend server system, (2) a self-serviced portal, (3) encoder application and (4) an authenticator mobile application. These 4 components are

required to form a complete anticounterfeiting solution. This is mandatory to evaluate our research findings. The backend server system is required to process all requests from the web portal, encoder application and the authenticator mobile application. Apart from that, the backend server system also processes communication between blockchain networks. The self-service portal is required for the manufacturers to establish their presence as the original product manufacturer, create their product branding and production batches. This is followed by the use of encoding mobile application that acquires the product batch details to create the product identification with cryptographically generated product codes. That completes the first three components of HACP that catered for the original product manufacturers. The other side of the coin is the authentication process. An authenticator mobile application was developed and provided for the key players of HACP, consumers. Consumers play a vital role in combating counterfeiting. The authenticator mobile application was provided to consumers to authenticate the product at the point of purchase. Apart from the consumers, all parties across the downstream supply chain can also utilize the authenticator application to authenticate the products at the entire logistic process.

HACP1 (as per Table 5), was the first release introduced, which utilizes static identification as the product identification. This first release of HACP will be the benchmark to further evaluate our research findings. Hence, we imitated the most common anti counterfeiting measurements that are being practiced in the industry. HACP1 is the control measurement for our next phases of research and for the future releases of HACP. HACP1 utilizes static identifications (StaticID) as the product identifications. With the initial forty respondents, the entire platform works as expected. The self serviced portal enables original manufacturers creation. They were able to continue to create their product brands by themselves and followed by their production batches for their respective SKUs. Once the production batches are created, they proceed with the product encoding application. For this test, we utilized QR codes. They were able to successfully generate QR codes with the respective brand and batches. Then the QR codes were placed on the original products. The final step is to utilize the mobile authenticator application to scan the QR codes where our backend server will facilitate authentication of the QR codes. If it is a valid QR code, the product details will be fetched from our database and displayed on the users mobile screen. If the QR code is not valid, the system will respond as invalid identification. This completes the full cycle of product encoding and authentication. Almost 100% of the feedback obtained from the respondents is about the vulnerability of static identification which is prone to duplication. Apart from that, the counterfeiters just need to use one original ID to duplicate unlimited multiple IDs. Hence, there is a huge gap in addressing counterfeiting problem.

Table 5: Survey summary-acceptance levels of security measurements incorporated into HACP

	HACPv1	HACPv2	HACPv3	HACPv4	HACPv5
Very low	76%	2%	0%	0%	0%
Low	24%	12%	0%	0%	0%
Medium	0%	38%	7%	0%	0%
High	0%	38%	24%	5%	2%
Very high	0%	10%	69%	95%	98%

Considering the feedback on HACP1 about the vulnerability of the static identification that is prone for duplication, and after further literature review, we introduced HACP2. This is our second release of HACP, where we introduced unique IDs. Despite being a static ID, made it a unique static ID. For example, in HACP1, if the manufacturer wants to produce 1000 products, he just needs to use the same product IDs

for all the 1000 products. Currently, this is the common practice among most manufacturers. In HACP2 (as per Table 5), we introduced unique IDs for each product. Our authentication system was also reviewed and redeveloped to detect similar product IDs being scanned repeatedly from multiple geographic locations. Geolocations has been incorporated into the authenticator application. This method is able to detect the presence of duplicate products because the same product cannot be presence at multiple locations within a short time frame. The current algorithm will take into account the timing and travel distance of multiple locations of the same product. Our application will trigger an alarm to the original product manufacturer and prompt to block the suspected duplicated identification. The system also allows blocking of the suspected identification, where the authenticator application will notify the consumer about the suspected duplication. Hence, if the original manufacturer were to produce 1000 products, he needs to have 1000 unique IDs for each product. So, if the counterfeiter were to clone 1000 duplicate products, he must purchase 1000 original products to achieve his objective. But this action may not be feasible as it defeats their objective of counterfeiting. The redeveloped HACP2 was presented to the research participants again. They went through the same process of creating product batches and generate new product identifications with unique IDs for each product. The research participants we requested to scan the IDs using the mobile authenticator from various geographical locations to witness the duplication alerts. We obtained feedback from the respondents and noted the confidential level improved where 38% of them have a high level of satisfaction and 10% of them very high level of satisfaction with HACP2. But we still have 52% of the research evaluation participants not reached high level of acceptance level. The feedback was that there is still room for possibilities of duplication and the battle on counterfeiting is not fully addressed. Hence, we proceed with further literature review to try to close the gap.

Next, we introduced HACP3 (as per Table 5), with NFC tags as our security measurement key instead of QR codes. Our literature review revealed a huge number of security measurement identifications like QR codes, hologram, security stamps, etc. One of the best security measurements was the NFC tags as it is known for its inability for duplication [41]. The entire HACP has been reviewed, reengineered, and modified accordingly. This modification includes the backend system, encoding mobile application, and the mobile authenticator application. The process of setting up the original product details like the brand and production batches remains the same. The product ID encoding has been shifted from QR code encoding to NFC tags encoding. We continued the unique identification concept introduced in HACP2. We went into phase 3 of our research evaluation. We requested the same respondents to test HACP3. We invested in a good number of NFC tags to facilitate the product encoding process. We obtained further feedback and noted more than 90% of them have a high level of satisfaction with HACP3. 24% of the research evaluation participants recorded high level of satisfaction and 69% of them recorded very high level of satisfaction. Nevertheless, we still have another 7% of them still feel there are room for improvement. Despite obtaining up to 93% of high satisfaction level, we still have about 7% gap. This is due to the nature of NFC tags. Though the NFC tags are known for their inability to be duplicated, but there are still very slim chances for duplication [42]. Hence, we decided to further the research to close this gap too.

Next, we introduced HACP4 (as per Table 5), where we bring blockchain technology into the equation. We proceed with further literature review where we noted that blockchain technology is known for its highly secured database features. We utilized the blockchain technology to record the encoded product identification which captures the timestamp, NFC details, GPS location, etc. At this stage, the backend server system was reviewed, reengineered to cater for blockchain notation and authentication for the new product code. The mobile encoder and mobile authenticator have been revisited to meet this new requirement. There were not major changes in the user interaction perspective as the changes happens at backend processing. The research evaluation participants were presented again with this new version of HACP. Upon evaluation,

we obtained 95% of very high levels of satisfaction and balance 5% is high level of satisfaction. Despite this high level of satisfaction achievement, we still wanted to further the research to obtain 100% of very high level satisfaction.

In HACP5 (as per [Table 5](#)), we introduced DynamicID concept with AuthentiCoding method. Hence, the evaluation focused on the AuthentiCoding component of our HACP, that's on encoding result vs. AuthentiCoding result. Both Encoding process and AuthentiCoding process are 2 separate processes that work independently. The result from the Encoding process must match with the result from the Authorization process. All these processes happen in the background. The users will not be able to see these processes. Nevertheless, with the introduction of this new research findings, the acceptance level of very high level of satisfaction increased to 98% and the remaining 2% of the participants remains at high level of satisfaction.

Based on the survey conducted to assess the acceptance level of various security measures incorporated into a holistic anti-counterfeiting platform (HACP), the results indicated that the acceptance level varied significantly across different versions of the platform. HACPv5, the latest version, demonstrated the highest acceptance level with 98% of the respondents rating it as "Very High." This version incorporated advanced security measures such as NFC (Near Field Communication) and blockchain technology, which likely contributed to its high acceptance level. The NFC-enabled mobile application aspect of HACPv5 appeared to have a significant impact on the respondents' perception of security and trustworthiness.

It is worth little that earlier versions of the HACP, such as HACPv1 and HACPv2, were met with limited acceptance, with only 76% and 10% of respondents rating them as "Very Low" and "Very High," respectively. This indicates that the incorporation of new security measures in subsequent versions, such as the dynamic ID functionality, played a crucial role in improving acceptance levels. The dynamic ID feature likely provided a heightened level of security, enabling the platform to adapt and evolve in response to emerging counterfeiting threats. Overall, the survey results suggest that the integration of NFC, blockchain, and other cutting-edge technologies into a holistic anti-counterfeiting platform can greatly enhance its acceptance and effectiveness in combating counterfeiting activities. With this results, we decided to proceed to the next phase of evaluation.

8 Results and Discussion

One of the major gaps in previous studies is the lack of a concrete evaluation method for their proposed anticounterfeiting solutions. Thus, our proposed HACP evaluation will be on encoding result vs. AuthentiCoding result. Both the encoding process and AuthentiCoding process are 2 separate processes that work independently with various parameters and algorithm. The result from the Encoding process must match with the result from the Authorization process. The ultimate objective of this research is to ensure our proposed ACP will not be compromised. Key research components will be (i) NFC Tag Encoding; and (ii) NFC Tag AuthentiCoding. Our work includes evaluating various encoding and AuthentiCoding systems which include algorithm, tools, and techniques. The new HACP adopted some of past research works while enhancing them with additional features to improve the system. Hence, we evaluated and validated the remodeled the HACP with a prototype using real-life case studies [43]. We found 5 established original product manufacturers to evaluate our system. The research ensures that serialization and encoding algorithms are not possible to be imitated or duplicated. The encoded NFC chips were tagged along with the products across the supply chain until they reached the storefront. An NFC-enabled mobile application was proposed for the consumers. The Mobile application was used to authenticate the NFC tags, which adopted our algorithm for the AuthentiCoding. The consumers used our proposed mobile app to scan the NFC chip that was tagged on the product before buying it. We obtained feedback from the original product manufacturer on the ease of using the platform across the supply chain. We also challenged the manufacturers

to try to duplicate our proposed product ID. We met our aim of ensuring our research findings that our proposed solutions are not prone to be compromised.

9 Conclusions

This research contributes to the ongoing fight against counterfeiting by proposing a holistic platform that integrates NFC and blockchain technologies. The system's validation through real-world application shows its effectiveness in reducing counterfeit goods in the supply chain. Future research should focus on expanding this model to other industries and improving consumer accessibility to authentication tools.

The concept of AuthentiCoding is to keep the product identification dynamic, which defuses any duplicated identification because the duplicated identification will carry an obsolete identification. When the mobile authenticator tries to authenticate the NFC tag with an obsolete identification, The NFC tag will be shown as unauthorized tag. However, there are chances of the original NFC tags also to be shown as duplicated if the duplicated supersedes the AuthentiCoding process. Hence, further research will be required to close this gap. Despite the above stated limitations, we would consider our research outcome as one of the most sophisticated, state of art holistic anti-counterfeiting platform to combat counterfeiting at the moment. Nevertheless, there is always room for improvement.

Acknowledgement: We would like to extend acknowledgment for the support and guidance provided by Soft Solvers Solutions Sdn Bhd, Global Vision Research Sdn Bhd and the University of Malaya to carry out this research successfully.

Funding Statement: The work is supported by Soft Solvers Solutions Sdn Bhd.

Author Contributions: Rajendren Subramaniam served as the primary author of this research. Saaidal Razalli Azzuhri supervised the study, providing expertise in blockchain technology. Teh Ying Wah collaborated with Rajendren Subramaniam on NFC integration and related activities. Vimala Balakrishnan and Atif Mahmood contributed to the overall review of the research, refining the objectives, proposed solutions, and manuscript writing. All authors reviewed the results and approved the final version of the manuscript.

Availability of Data and Materials: The data that support the findings of this study are available from the corresponding author upon reasonable request.

Ethics Approval: Not required.

Conflicts of Interest: The authors declare no conflicts of interest to report regarding the present study.

References

1. Trade I. Trends in trade in counterfeit and pirated goods. Alicante: OECD Publishing, Paris/European Union Intellectual Property Office; 2019.
2. Hoke E, Marada J, Heinzová R. International trade risks. In: MATEC Web of Conferences; 2019; EDP Sciences. Vol. 292.
3. Ranjan T. New age tussle with the legal measures in controlling the counterfeiting practices: a specific study on ip segment. *Int J Soc Sci Econ Res.* 2022;7:4058–90.
4. Wang H, Wang H, Qiao Z. Anti-counterfeiting traceability system for agricultural products based on RFID and blockchain. In: *Proceedings of the 2020 International Conference on Materials, Control, Automation and Electrical Engineering (MCAEE 2020)*; 2020; Shanghai, China. p. 22–3.
5. Alzahrani BA, Mahmood K, Kumari S. Lightweight authentication protocol for NFC based anti-counterfeiting system in IoT infrastructure. *IEEE Access.* 2020;8:76357–67.
6. Dhar R. Anti-counterfeit packaging technologies: a strategic need for the Indian industry. *Confed Indian Ind Gurgaon Confed Indian Ind.* 2009;41–42.

7. Agarwal U, Rishiwal V, Tanwar S, Chaudhary R, Sharma G, Bokoro PN, et al. Blockchain technology for secure supply chain management: a comprehensive review. *IEEE Access*. 2022;10:85493–517. doi:10.1109/ACCESS.2022.3194319.
8. Sun H, Lee SY, Joo K, Jin H, Lee DH. Catch id if you can: dynamic id virtualization mechanism for the controller area network. *IEEE Access*. 2019;7:158237–49. doi:10.1109/ACCESS.2019.2950373.
9. Do HH, Anke J, Hackenbroich G. Architecture evaluation for distributed auto-ID systems. In: *Proceedings of the 17th International Workshop on Database and Expert Systems Applications (DEX 2006)*; 2006; IEEE. p. 30–4.
10. Tan J, Goyal S, Singh Rajawat A, Jan T, Azizi N, Prasad M. Anti-counterfeiting and traceability consensus algorithm based on weightage to contributors in a food supply chain of Industry 4.0. *Sustainability*. 2023;15(10):7855. doi:10.3390/su15107855.
11. Alzahrani N, Bulusu N. Block-supply chain: a new anti-counterfeiting supply chain using NFC and blockchain. In: *Proceedings of the 1st Workshop on Cryptocurrencies and Blockchains for Distributed Systems*; 2018; Munich, Germany. p. 30–5. doi:10.1145/3211933.3211939.
12. Alzahrani N, Bulusu N. Securing pharmaceutical and high-value products against tag reapplication attacks using nfc tags. In: *2016 IEEE International Conference on Smart Computing (SMARTCOMP)*; 2016; St. Louis, MO, USA. Piscataway, NJ, USA: IEEE Computer Society. p. 1–6.
13. Kumar A, Choudhary D, Raju MS, Chaudhary DK, Sagar RK. Combating counterfeit drugs: a quantitative analysis on cracking down the fake drug industry by using blockchain technology. In: *2019 9th International Conference On Cloud Computing, Data Science & Engineering (Confluence)*; 2019; Noida, India. Piscataway, NJ, USA IEEE Computer Society. p. 174–8.
14. Subramaniam R, Azzuhri DSR, Wah DTY. A review on combating counterfeiting by empowering consumers via nfc enabled mobile computing leveraging on blockchain technology. [cited 2025 Jan 20]. Available from: <https://ssrn.com/abstract=5012178>.
15. Soon JM, Manning L. Developing anti-counterfeiting measures: the role of smart packaging. *Food Res Int*. 2019;123:135–43. doi:10.1016/j.foodres.2019.04.049.
16. Yang K, Botero U, Shen H, Forte D, Tehranipoor M. A split manufacturing approach for unclonable chipless RFIDs for pharmaceutical supply chain security. In: *2017 Asian Hardware Oriented Security and Trust Symposium (AsianHOST)*; 2017; Beijing, China: IEEE p. 61–6.
17. Khalil G, Doss R, Chowdhury M. A new secure RFID anti-counterfeiting and anti-theft scheme for merchandise. *J Sens Actuator Netw*. 2020;9(1):16. doi:10.3390/jsan9010016.
18. Khalil G, Doss R, Chowdhury M. A comparison survey study on RFID based anti-counterfeiting systems. *J Sens Actuator Netw*. 2019;8(3):37. doi:10.3390/jsan8030037.
19. Alzahrani N, Bulusu N. A new product anti-counterfeiting blockchain using a truly decentralized dynamic consensus protocol. *Concurr Comput Pract Exp*. 2020;32(12):e5232. doi:10.1002/cpe.5232.
20. Sakazaki H, Fukuzawa Y. Study on the feasibility of smart-banknotes. *J Inf Process*. 2015;23(5):633–45. doi:10.2197/ipsjjip.23.633.
21. Zulqarnain M, Stanzione S, Rathinavel G, Smout S, Willegems M, Myny K, et al. A flexible ECG patch compatible with NFC RF communication. *npj Flexible Electronics*. 2020;4(1):13.
22. Pitari DF, Gayatri G, Furinto A, Assauri S. Integration of intention and resistance in adopting near field communication-based mobile payment innovation. *Int J Sci Technol Res*. 2020;9(4):857–66.
23. Jiang Y, Pan K, Leng T, Hu Z. Smart textile integrated wireless powered near field communication body temperature and sweat sensing system. *IEEE J Electromagn RF and Microw Med Biol*. 2019;4(3):164–70. doi:10.1109/JERM.2019.2929676.
24. Raja S, Raj S, Babu B, Vardhan G, Reddy K. Innovations in pharmaceutical packaging-an update. *Int J Adv Biomed Pharm Res*. 2012;1(1):29–9.
25. Shankar BP, Jayavadeivel R. A survey of counterfeit product detection. *Int J Sci Technol Res*. 2019;8(12).
26. da Silva PM Medeiros, de Sousa JC, do Vale AF Nery, de Lima Dantas BL, de Araujo FN Moreira. Materialism and luxury goods consumption fake. *Rev Cienc Adm*. 2017;23(3):446–58.

27. Wilson JM, Grammich CA. Protecting brands from counterfeiting risks: tactics of a total business solution. *J Risk Res.* 2021;24(9):1141–60. doi:10.1080/13669877.2020.1806908.
28. Fangfang C, Peng C. Research on dual anti duplication and anti-counterfeiting technology of QR code based on metamerism characteristics. In: 2020 IEEE 5th International Conference on Image, Vision and Computing (ICIVC); Beijing, China: IEEE; 2020. p. 303–6.
29. Abbas K, Afaq M, Ahmed Khan T, Song WC. A blockchain and machine learning-based drug supply chain management and recommendation system for smart pharmaceutical industry. *Electronics.* 2020;9(5):852. doi:10.3390/electronics9050852.
30. Baldini G, Fovino IN, Satta R, Tsois A, Checchi E. Survey of techniques for the fight against counterfeit goods and Intellectual Property Rights (IPR) infringement. In: JRC technical report; 2015. EUR 27688 EN. doi:10.2788/97231.
31. Chin SH, Lu C, Ho PT, Shiao YF, Wu TJ. Commodity anti-counterfeiting decision in e-commerce trade based on machine learning and Internet of Things. *Comput Stand Interf.* 2021;76(1):103504. doi:10.1016/j.csi.2020.103504.
32. Kim K, Lee G, Kim S. A study on the application of blockchain technology in the construction industry. *KSCE J Civ Eng.* 2020;24(9):2561–71. doi:10.1007/s12205-020-0188-x.
33. Jinasena DN, Spanaki K, Papadopoulos T, Balta ME. Success and failure retrospectives of FinTech projects: a case study approach. *Inf Syst Front.* 2023;25(1):259–74. doi:10.1007/s10796-020-10079-4.
34. Stake R, Visse M. Case study research. In: International encyclopedia of education. 4th ed. Amsterdam, Netherlands: Elsevier; 2022. p. 85–91.
35. López-Pimentel JC, Rojas O, Monroy R. Blockchain and off-chain: a solution for audit issues in supply chain systems. In: 2020 IEEE International Conference on Blockchain (Blockchain); 2020; Rhodes, Greece: IEEE. p. 126–33.
36. De Salve A, Franceschi L, Lisi A, Mori P, Ricci L. L2DART: a trust management system integrating blockchain and off-chain computation. *ACM Trans Internet Technol.* 2023;23(1):1–30. doi:10.1145/3561386.
37. Miyachi K, Mackey TK. hOCBS: a privacy-preserving blockchain framework for healthcare data leveraging an on-chain and off-chain system design. *Inf Process Manag.* 2021;58(3):102535. doi:10.1016/j.ipm.2021.102535.
38. Shan J, Jiang L, Cui AP. A double-edged sword: how the dual characteristics of face motivate and prevent counterfeit luxury consumption. *J Bus Res.* 2021;134(2):59–69. doi:10.1016/j.jbusres.2021.05.032.
39. Li D, Zhang L, Jin X. An improvement for PDF417 code authentication on mobile phone terminals based on code feature analysis and watermarking. *Multimed Syst.* 2022;28(5):1585–96. doi:10.1007/s00530-022-00910-0.
40. Yiu N. Toward blockchain-enabled supply chain anti-counterfeiting and traceability. *Future Internet.* 2021;13(4):86. doi:10.3390/fi13040086.
41. Chatzopoulos D, Bermejo C, Kosta S, Hui P. Offloading computations to mobile devices and cloudlets via an upgraded NFC communication protocol. *IEEE Trans Mob Comput.* 2019;19(3):640–53. doi:10.1109/TMC.2019.2899093.
42. Lazaro A, Boada M, Villarino R, Girbau D. Study on the reading of energy-harvested implanted NFC tags using mobile phones. *IEEE Access.* 2019;8:2200–21. doi:10.1109/ACCESS.2019.2962570.
43. Danese P, Mocellin R, Romano P. Designing blockchain systems to prevent counterfeiting in wine supply chains: a multiple-case study. *Int J Oper Prod Manag.* 2021;41(13):1–33. doi:10.1108/IJOPM-12-2019-0781.