BLOCKCHAIN INSPIRED PRODUCT AUTHENTICATION FOR SUPPLY CHAIN SECURITY

By

Fnu Nitya Nitya Kriti

A THESIS

Submitted to
Michigan State University
in partial fulfillment of the requirements
for the degree of

Electrical Engineering – Master of Science

2019

ABSTRACT

BLOCKCHAIN INSPIRED PRODUCT AUTHENTICATION
FOR SUPPLY CHAIN SECURITY

By

Fnu Nitya Nitya Kriti

In today's technologically advanced world, the prevalence of counterfeit products in the market is a major challenge. In every industry from pharmaceutical to the food industry, counterfeit products have a destructive impact on the health of the consumers as well as loss of jobs and lives of millions across the globe. This calls for a better system of product traceability to impede the introduction of counterfeit products in the market. This work proposes a method in which a blockchain inspired system is implemented with the combination of the digital chain of information to the physical tag on the products. The physical tag has DNA of a known source to be privy to only select nodes and connected to the central database. The proposed method includes the use of magnetic stripe cards as product labels. This label is made to contain digital information, which is then coupled with the modified blockchain system. Pertaining to the high information density property of the magnetic stripe cards, partial DNA sequence information can be easily concatenated with the serial number of the product. This can also be re-programmed to track the route of the product along the supply chain. The main feature of the proposed method is the coupling of the re-programmability of the magnetic card labels with the physical DNA tag information contained on the label. The tag can be easily verified even after the product leaves the digital chain. Whilst, within the network coverage, the blockchain inspired tracking system can help track the route taken by the product. This mechanism of merging the physical information with the Internet of Things (IOT) shall address the situation of counterfeit products to an advanced degree of accuracy and reliability.

ACKNOWLEDGEMENTS

I would first like to thank my thesis advisor Dr. Prem Chahal and co-advisor, Dr. Evangelyn Alocilja, for their vital suggestions. They always promoted me to make this thesis my own work and steered me in the right direction whenever I needed it.

I would also like to thank Mr. Saad Sharief from the department of Biosystems Engineering, Michigan State University for his constant help and advice and for constantly working alongside me. I would like to extend my gratitude for the members of Electromagnetics Research Groups (EMRG) for their constant support and guidance. Special thanks to the AXIA Institute for partially funding the project.

I would also like to acknowledge Dr. Tim Hogan from the department of Electrical and Computer Engineering, Michigan State University as the second reader of the thesis and am grateful for his valuable suggestion for the thesis.

I would like to acknowledge Mr. Sovit Kumar Agarwal from the department of Computer Science Engineering, Technische Universität Berlin, Germany for his invaluable help with the development of the blockchain system. Finally, I would like to express gratitude to family and friends for being supportive and encouraging throughout the period of this study.

TABLE OF CONTENTS

LIST OF TABLES

LIST OF FIGURES

1. INTRODUCTION

1.1 SUPPLY CHAIN SECURITY

According to the World Health Organization (WHO), one in 10 drugs sold in developing countries is fake or substandard, leading to tens of thousands of deaths [1]. The WHO estimates that fake drug trade costs the pharmaceutical industry US $75 billion worldwide. This not only affects the economy but also hurts the end consumers, especially with billions of dollars' worth of fake drugs. There is an imminent need to increase security and traceability along the supply chain and not only for pharmaceutical products but for almost all the products across the globe.

As an example, according to research studies by SAFEMEDICINES.org. in 2017 [1] Americans in 30 states across the US have died from counterfeit prescription drugs made with lethal doses of Fentanyl over a course of only 24 months. The problem is far from solved. We need a mechanism if not a whole system to identify not only the fake products but also to identify the points or locations where they are inserted in the supply chain. This study focuses on one such method and aims to provide a more secure way to trace products within the supply chain. A methodology to verify the authenticity of products that cannot be traced by simple digital techniques have been proposed in the study. The method developed is summarized in the Figure 1.1 below.

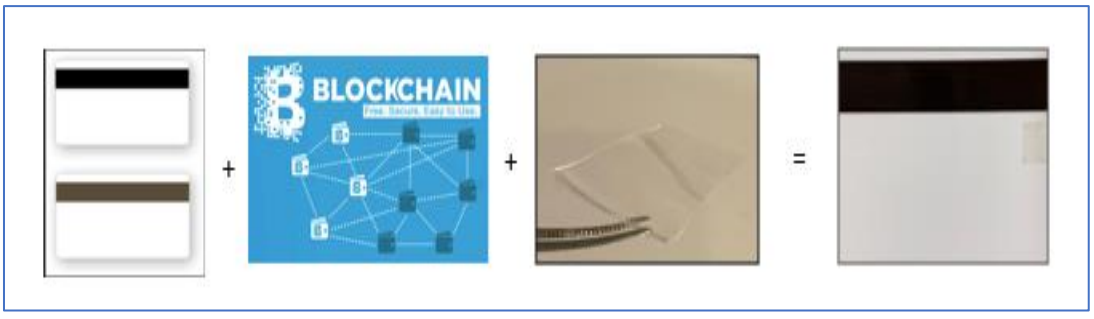


Figure 1.1 The proposed method

This method proposed makes the use of magnetic stripe cards as labels and combines the digital and physical means of authenticating the product. The aim of the study is to establish a method which proves to be cost effective when compared to the already existing and approaches. This study also proves the ease of implementation of the mode of verification processes. Both the digital information and physical DNA information are paired together to give a robust and most secure means of storing product information and product traceability.

1.2 COMBIINING DIGITAL AND PHYSICAL MEANS OF SECURITY

It is important to note that in any industry, be it pharmaceutical, food supply, consumer products, automobile or the defense; all are heavily globalized. Different components usually come from different sources, and all the sources need to be accounted [2]. Also, products from these industries directly impact the economy of the country and more importantly address basic and important consumer needs.

Amongst the various anti-counterfeiting methods currently employed includes holograms, QR codes, and Bar Codes [3], which can still be replicated with relative ease. The problem with multiple anti-counterfeiting measures is also that no uniform method to address the problem has been proposed. We propose one such method so as to make the supply chain mechanism more uniform. This is intended to create an Internet of Things (IoT) imbibing in itself a piece of physical information carried on the packages/products.

Serialization is another measure that can tackle the problem of counterfeiting. Like others, the serialized code can be copied and in future, puts a constraint on the number of characters to be used on smaller products. In addition to these limitations, there are huge database maintenance requirements [4]. Although these methods are user-friendly and easily verifiable, that makes them

all the easier to be replicated. This calls for an approach to integrate different methodologies so as to incorporate the benefits of the various approaches minimizing the disadvantages of various methods. The proposed solution, which can be used in association with any of the above-mentioned technologies providing more levels of security throughout the supply chain.

The method proposed here uses blockchain as a main component of the supply chain system to track and verify the authenticity of the products. The proposed solution uses magnetic ink along with a DNA infused patch on the label providing a verifiable physical entity. Connecting all the nodes present in the network for any product does tracking via a blockchain. Any foreign nodes to that network shall not have any access to the product movement and the information contained on the magnetic stripe.

1.3 CONVENTIONAL BLOCKCHAIN: EXPLAINED

Blockchain was developed by a person (or a group of people) using the pseudonym Satoshi Nakamoto in 2008 [5] mainly for the cryptocurrency Bitcoin. Since then, a number of cryptocurrencies have come up. The various uses of blockchain apart from the digital currency application have been identified [6]. Satoshi Nakamoto proposed that owners of digital coins (currency) transfer the coins to the next owner by digitally signing a hash of the previous transaction and the public key and adding these to the end of the coin [5]. This aims to create a peer-to-peer network for the development of a decentralized ledger for the movement of products (digital currencies in this case). Now, in the absence of verifying institutes such as a financial bank, there is a need to verify the authenticity of the transactions. Also, there is a need for a unique identification label for each transaction being carried out. In a conventional blockchain, a

decentralized, distributed ledger is created, which is, in fact, the blockchain. This ledger is governed by a prescribed set of rules for verification and addition of new information to the chain. The most popular use of blockchain in today's existing technology is for cryptocurrencies like the Bitcoin or the Ethereum[5, 7]. A blockchain can be taken as a list of blocks containing the desired information, which can be either transaction amount as is in case of cryptocurrencies or can be any type of information depending on the application. These blocks are governed by the same set of rules and are all linked to each other by a "hash." The hash is a unique identifier generated for each block using a hash function. A hash function gives an output of a fixed length for any given length of the input. For example, the function SHA256[5] gives an output of 256-bit hash (encrypted) term for any given input. This output is known as a digest and is always of fixed length.

The next step after deciding on the hash function is to define the structure of the blocks. All the blocks in that particular chain should comply with the specified structure[8]. This structure defines the type format and amount of data to be allowed to pass through each block. Generally, we have the following data within each block

- The index of the block with 0 being the initial index. The consecutive blocks then have indices 1, 2 and so on in that order.
- The timestamp of the block. This indicates the time at which the block was created and added to the chain. It can be in any format and up to the required degree of precision. This timestamp is taken from the machine being used to add the block to the chain.
- The next line of information contained within the block is the actual transaction amount (in case of cryptocurrencies) or any other information required to be passed along the nodes in the network. This information can be of any data type and length.

- Each block also has the hash of the current block as well as the previous block's hash.
- It should be noted here that the hash is a combination of all the information contained in the block plus the hash of the previous block. For the hashing algorithm or the encryption algorithm, the index, timestamp, desired transaction information and the hash of the preceding block act as the input to give a 256-bit encrypted output. This output is the hash of the current block. If any of these data points are changed, then the whole output of the hashing algorithm is changed, hence making this method extremely resilient to being replicated.

When the blockchain is initiated, in case that there is no preceding block, the hash of the initial block with index 0 is assigned a random hash or the algorithm automatically generates a hash for the first block. This first block is called as the "genesis" block. Figure 1.1 describes the creation of the genesis block and then the addition of the subsequent blocks. The data displayed can be customized as per requirement.

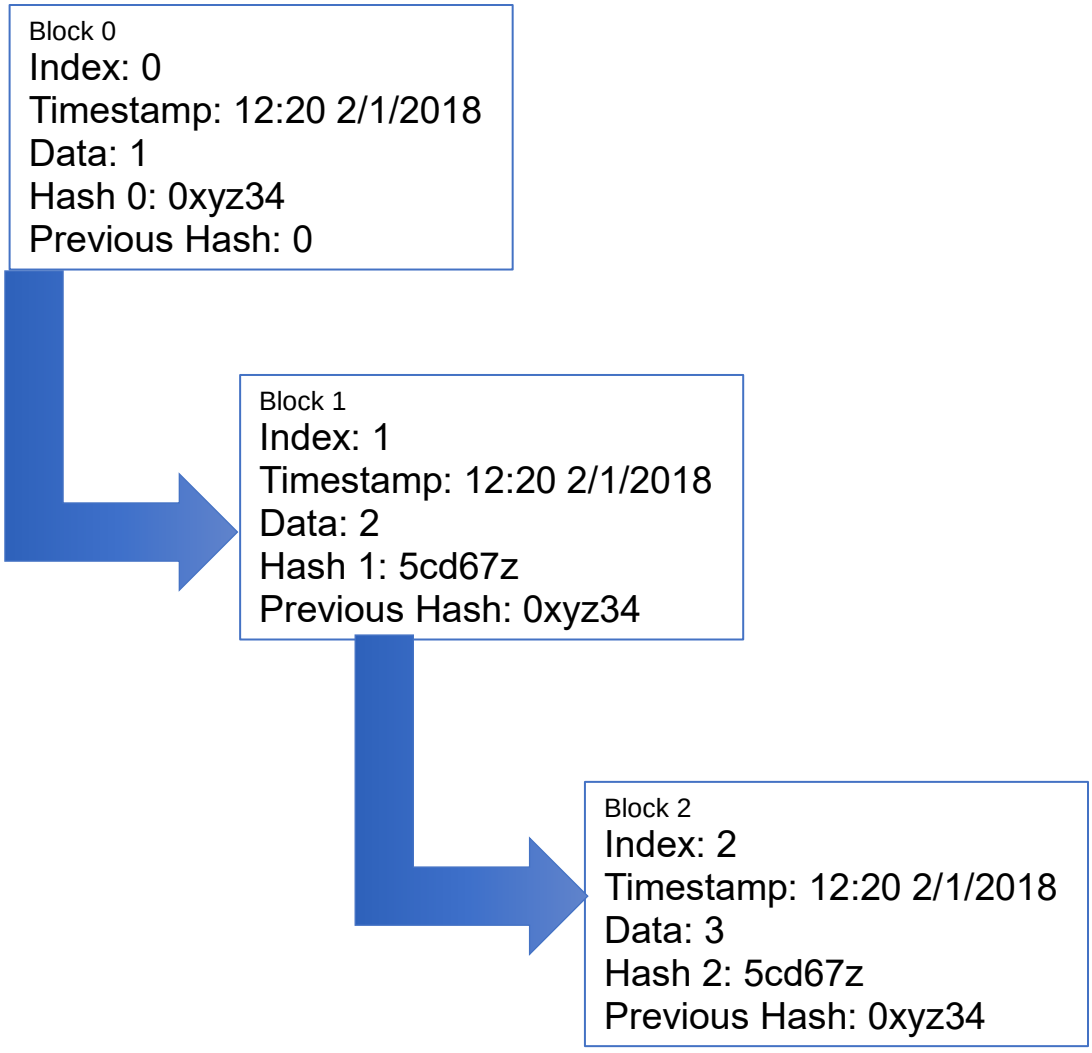


Figure 1.2 A simple depiction of basic Blockchain

Figure 1.2 depicts a basic blockchain with different lines of data sets contained within each block. We should keep in mind that Hash 1 is the output for the timestamp, index 0 data (1) and hash 1 taken together. This hash being generated is extremely difficult to decode and hence, to get the information contained in the current block, all the previous blocks' hash needs to be decrypted which is extremely difficult.

In all the applications of blockchain till date, the Datapoint in the blocks has been virtual information [5]. This makes the data tracking a little bit easier as compared to when the data points

being moved along the nodes are physical entities. Also, changing a single bit of input for the hashing algorithm changes the output hash completely. From this property of the encryption algorithm used, we can differentiate between two blocks containing the same information but create at two different time instances. Due to the timestamps being different, the hash generated for the two blocks will be different.

Now, we ask the question that if the point of differentiation between the two blocks is only the time stamp, then how do we decide which block is to be added amongst the two.

For this purpose, the blockchain mechanism uses a consensus algorithm [9] to elect a leader who will decide the next block be added. Satoshi Nakamoto introduced the concept of Proof-of-Work (POW) in his paper to implement this method [5].

The consensus algorithm is established for user security and to maintain ledger consistency [9]. In other words, the consensus algorithm validates any new transactions before broadcasting new blocks to the blockchain. Now, while figuring out the algorithm and working backward to the desired block is not impossible, it is extremely difficult and requires high mental acuity and knowledge [10]. The above features make the blockchain mechanism a highly desirable method for financial and non-financial applications.

1.4 CURRENT APPROACHES: AN OVERVIEW

It may be possible to combine any detection method with the blockchain technology. However, though many such methods have been suggested [11], each method comes with certain limitations, which needs to be addressed. A few such methods are briefly discussed below.

A very popular method for product verification and authentication is the bar code. The basic concept behind the barcode technology is symbology, which determines the mapping and

interpretation of the encoded interpretation of data [12]. Barcodes are recognized as an array of parallel lines with black and white lines alternating with each other. It was first invented in the year 1974, interestingly, first installed at Marsh's supermarket in Troy, Ohio. Since its inception, it has been put to use for supply chain visibility and tracking for a diverse range of products in almost all the industries across the globe.

As mentioned above, the mapping for a barcode can be done in several different ways. The method of mapping depends on the application for which the barcode technology is being used. While some use multiple width lines and some technologies use two widths to determine the characters [13, 14]. There are linear (1D) and 2D barcodes. While the linear or 1D barcodes use the alternating black and white lines for product labeling, 2D barcodes make the use of more complex dot matrix or in some cases, dataglyphs to achieve more complex encoding and store more characters.

In the case of barcodes, we have alternating black and white lines. The black lines absorb, and the white lines or spaces reflect light. The reflection pattern is what the scanner reads[15]. This needs to be scanned by a laser for further interpretation. The information in the barcode in meant to be encoded in a fashion such that the abrupt transitions of pixel intensities are measurable [14]. This calls for a need for edge detection technology and image processing to go hand in hand to interpret the intensity gradient.

Though barcodes have been a huge success in product authentication, they come with certain limitations. First, 1D barcodes hold less than 100 characters, hence limiting the amount of information that can be saved in the code. Second, this technology depends on scanning on alternating black and white bars, which can easily be distorted. Third, the 1D barcode scanners work in a unidirectional manner, so the angle of the scan line plays a crucial role. If the scan angle does not fit within the range, then the data cannot be read correctly [16]. 1D barcode has limitations

where we do not have access to a database, as this requires additional database management. Fourth, the barcodes are relatively easier to get copied on to fake products.

To overcome some of these limitations, we make use of 2D barcodes [16], which emphasize more on product descriptions as opposed to 1D barcodes, which emphasize on product identification. These are relatively harder to read compared to 1D barcodes. These include codes such as the QR codes, PDF417, and the Data Matrix, to name a few [17].

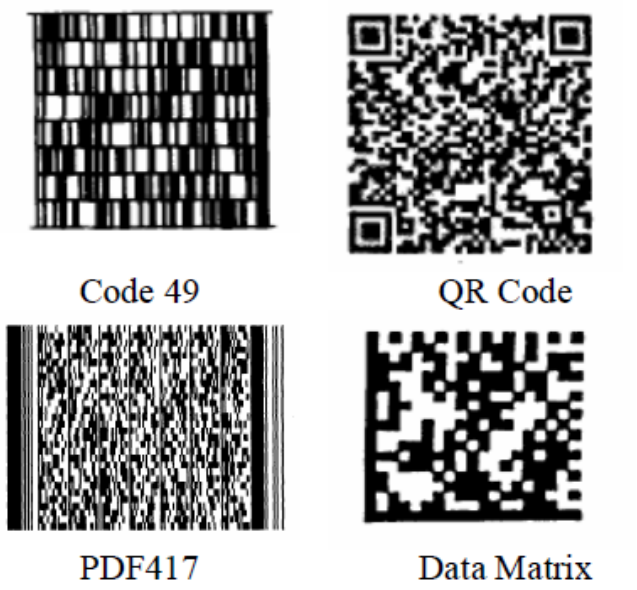


Figure 1.3 Some of the 2D barcodes used today [17]

The Quick Response (QR) code, developed by the Japanese company, Denson-Wave in 1994 is a kind of 2D barcode. Basically, a QR code is a matrix bar code. The black modules in the code are on a white background in a definite pattern defined by the industrial standard ISO/IEC18004: 2006 (Standardization, 2006) [18]. It has been proposed that QR codes can be used for food traceability system as they can contain information about any particular product [18]. It mainly contains a finding pattern, timing pattern, format information, alignment pattern, and data cell [19]. Users

may want a more interactive method for product authentication, which calls for evolving marketing characteristics [3].

Both the 1D and 2D barcodes are non-reprogrammable and can be reproduced with increasing technological advancements. The functioning of the QR codes shall be discussed in chapter 2 in greater detail.

Another approach that can address a number of limitations proposed by the 1D and 2D barcodes is the use of RFID (Radio-Frequency Identification) [19], which enables identification from a distance without the necessary line of sight. Also, with this technology, without human assistance, the system can discern different tags that can be stored in the same location. Also, the amount of data that can be stored on RFID tags is considerably more than the barcode technology. These can also be reprogrammed so that the same tag can be reused for multiple products, thus enabling reusability. We shall discuss the RFID technology along with magnetic cards in detail in chapter 3.

Now, all of the approaches mentioned above can be used in harmony with the blockchain technology. The question now is how to make the whole process as resistant to counterfeiting as possible with the least amount of distress to the end consumers. It can be noted at the end of this study that both RFID technology and the magnetic card can play a better role on this front as compared to the existing barcode technology. In the end, we shall study the cost-effectiveness of the technologies studied and proposed. Balancing the security issues in the supply chain with the cost-effectiveness of the methods shall give us an optimum solution in the ongoing research for the solutions.

1.5 DIFFERENCE BETWEEN PROPOSED APPROACH AND CURRENT APPROACHES

The description in section 1.3 of a conventional blockchain works perfectly as long as the information being exchanged is of digital nature. We are faced with devising a method based on the conventional blockchain using physical tagging of the products also. The proposed implementation of the blockchain system works very similarly to that of a conventional blockchain. But, in the case of a physical entity being the primary source of information, the process of mining is rendered purposeless. Now, the idea behind the implantation of the POW concept is just to decide the longest chain available and not also the decryption of a particular hash in order to confirm the present state of the chain. The below process describes how our proposed method of blockchain differs from the conventional concept.

- For our consideration, we use DNA stamped patch on the label. The label also contains the magnetic ink stripe that actually contains the data to be scanned. The information on the magnetic card can be encrypted as well and can include serial numbers so as to facilitate serialization of the products along with labeling. The information encoded on the magnetic stripe can be designed to be linked to the DNA patch used on the label.
- Now, as the product is scanned or the magnetic card is read, the information is stored on to the magnetic card (the physical information), is saved on to the machine in a user-friendly format. This is the information that needs to be moved along the supply chain or the network of the nodes concerned.
- This information is saved in digital format. This data acts as the “transaction” amount to generate the first or the genesis block.

- The data along with the timestamp of magnetic card scanning are the inputs for the hashing algorithm, SHA256.
- Along with all these data lines, we have added a row for node identifier, which is unique for different nodes and does not change with new blocks being added to the chain.
- In our implementation of the blockchain, we do not require an extra verification process to establish the current state of affairs. In order to verify the current status of the products, it will be easier as the blockchain will give us the location of the nodes and the data is linked to the physical data on the labels of the products.
- Also, magnetic stripes can be reprogrammed. The magnetic cards can also be recycled once the labeled products reach their endpoints. Also, different nodes can add their information onto the magnetic card as per requirement.

1.6 NEED FOR DNA AS AN IDENTIFIER

From the above discussion, it can be noted that that the blockchain technology works in accordance with the information encoding technologies that have been implemented as well as those that are under current research. It should be noted that all these require a system for database management and a connected network through which all the parties in the supply chain are connected. The blockchain system shall work fine only as long as there is substantial network coverage for all the nodes concerned in the supply chain.

Also, the know-how to operate the system is required which in turn means that there needs to be an investment in educating the members included in the system. After the product authentication and verification is done, there is still a possibility that the original product can be replaced with the fake product. In case the blockchain system fails to identify the presence of a non-authentic product whilst in the supply chain, the fake product can reach the end consumer and defy the whole

process for product security. This calls for a physical means of identification, which should be present on the label. We propose the use of a DNA imbued patch on the label along with the magnetic ink stripe.

This solution goes hand in hand with the blockchain technology. These two have been studied to address the problem for product verification when one or the other fails.

It should be noted here that another limitation of any tracking technology is the amount of verifiable unique information that can be stored within a certain limited boundary. Barcodes have limited characters that may not be enough to contain the complete information needed to identify the location, source and the general description of the product. 2D barcodes or QR codes though contain more information than 1d codes, they still are limited within a space and cannot be re-configured. The labels can be copied on to the fake products with much ease. [18]

Now, RFID tags and magnetic cards, though programmable and can contain a high amount of data, they still shall fail to provide sufficient means of authentication once the product moves out of the network coverage where access to the digital technology is limited.

The solution proposed in this study aims to address this very problem. Now, once the product moves outside the conventional observable supply chain, for instance, when the product moves from hand-to-hand, then the digital data cannot be read. This creates opportunities for the introduction of fake products in the system. But, if we have verifiable data, which is unique to the manufacturer, present on the label, then we can ascertain with high confidence that the product is authentic.

In cases where the packaging is done with components from multiple sources, there are multiple nodes for the introduction of fake parts and products in the supply chain. For instance, in the pharmaceutical supply chain, we can have the packages intact, but the actual medicine might have

been replaced with counterfeit medicine. To label, the product then does not simply solve our problem. With the information in the form of DNA patch placed, let us say on the blister packs, will make it extremely difficult to replace the actual pills inside the packages, if not completely eliminate it. The surface area required to contain unique information is considerably less if we take a unique, undisclosed DNA strand as a physical identifier. When we combine this method with the tracking property contributed by the blockchain technology, we can track the product as far as any mobile device can go and even after that product verification is possible with a high level of confidence. If the counterfeit product reaches the end customer, the physical DNA tag on the label can be used for easy product authentication. In any case, we can locate the point of entry of the counterfeit products in the system and then verify if actually the product is authentic.

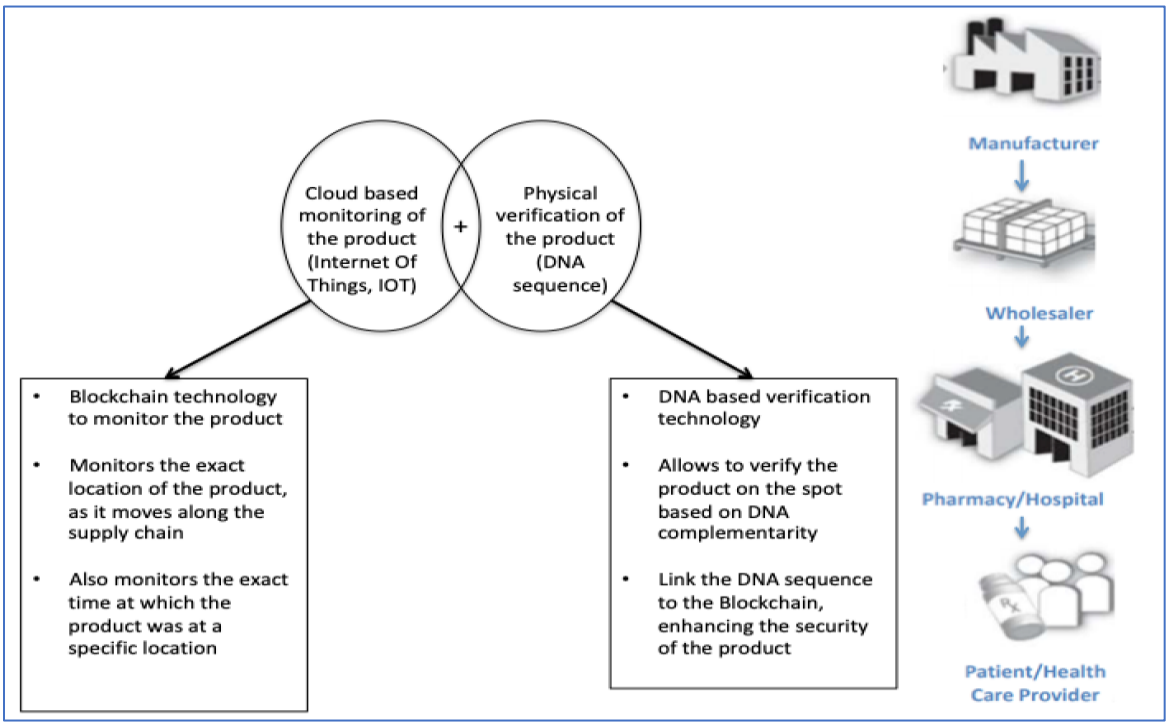


Figure 1.4 Merging Physical and Digital verification for better product traceability

1.7 ADVANTAGES OF THE PROPOSED SOLUTION

- In the case of a conventional blockchain for cryptocurrencies, the data points are the transactions being done. Hence there is no way of verifying the current state of affairs other than the consensus algorithm. In our implementations, we have based the code inspired by the conventional blockchain but without the requirement of verifying through the consensus algorithm. The verification beyond the coverage of blockchain can be easily done with the verification of the physical label containing the DNA patch.
- Also, unlike the current methods for anti-counterfeiting like QR code, Bar Code and Holograms, the magnetic card can be reprogrammed in case the data has to be modified or in case the chain ends.
- We can also use RFIDs for the same functionalities as the magnetic card, but RFIDs prove to be more expensive as compared to the magnetic cards.
- Also, the proposed method uses magnetic cards on the labels, so the product shall not interfere with the functioning of the digital tag, which is not so in the case of RFIDs as product tags.

The programmable and non-programmable methods have been discussed in the next two chapters. It should be kept in mind that there can be many possible solutions to the problem of supply chain traceability and security, but more research needs to be done in this aspect. Blockchain alone shall not be sufficient enough to address all the problems, hence we propose it be merged with a physical entity, which is unique, verifiable and capable of containing high-density information, the DNA patch. We need both, the digital and physical means of verification for added security levels. So as to make the counterfeiting process as tedious as possible. The image below, shows how multiple

DNA tags can be used to secure more than one type of product in a given supply chain. The use of the DNA sequence in the physical tag can depend on the product priority and demand.

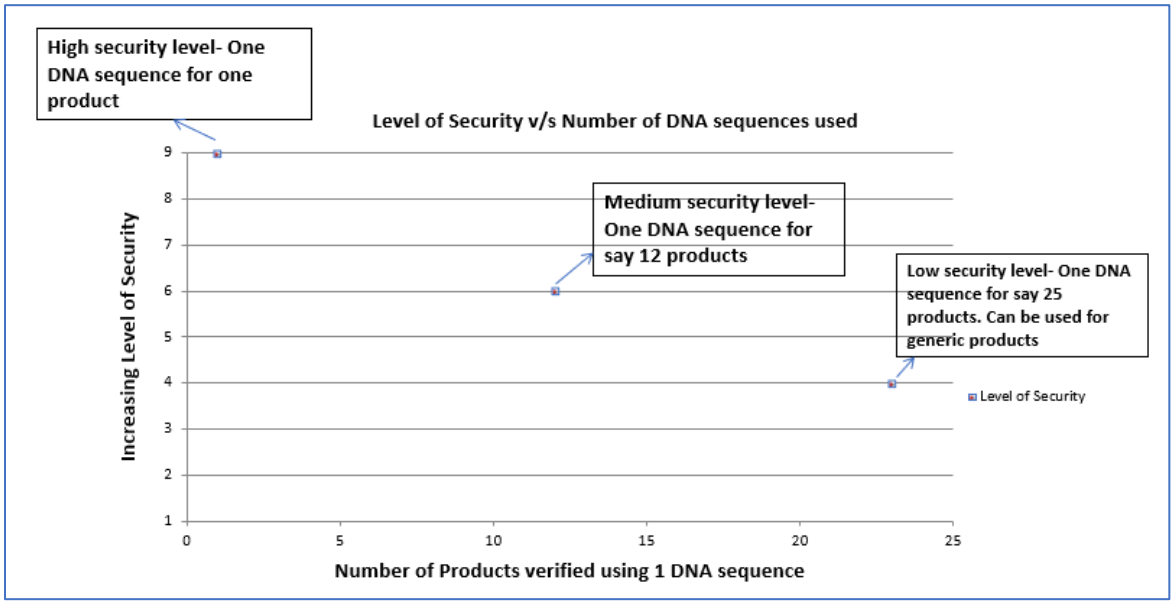


Figure 1.5 DNA Verification: Levels of Security

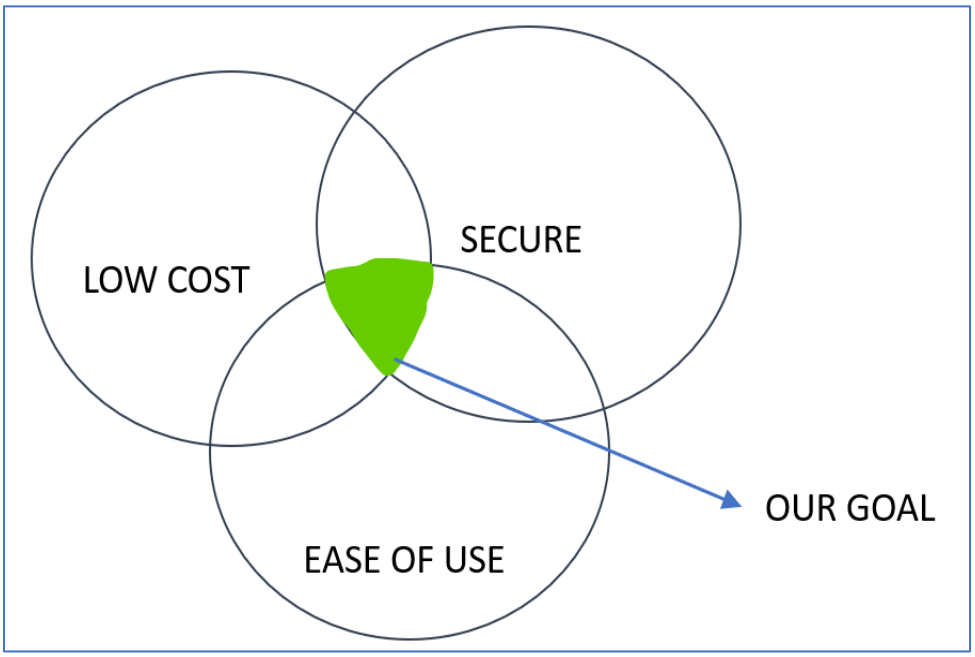


Figure 1.6 Aim of the Study

The final aim of this study is to devise a method for anti-counterfeiting that is easy to use/implement, is cost effective and at the same time as secure as possible. Ease of use is also important, as the steps towards anti-counterfeiting and traceability of products, should be compatible with the existing and proposed technologies. Taking all these three points of consideration, an optimum solution has been suggested. Parametric comparison of the current and the proposed methods have been done to establish the commercial applicability of the proposed method.

2. NON-PROGRAMMABLE APPROACHES

2.1 BACKGROUND

As discussed in the previous chapter, we now know of many methods that can be used for product traceability. We have studied the various methods such as the Barcode technology and the 2-D barcode and the QR code technology [20]. These are efficient methods to address the problem of counterfeit products. However, they have certain drawbacks, which is discussed in this chapter. To address their drawbacks. new methods have been designed some of are discussed in the next chapter. We have focused our review on 1-D and 2-D barcodes and QR codes. These have been extensively utilized in supply chain of various industries. Let us study them in brief to establish a background for out proposed work.

2.2 LINEAR BARCODE TECHNOLOGY

A barcode is basically a real-time application of symbology [10]. As mentioned earlier, symbology defines or maps and interprets the encoded information in the 1-D or linear barcode. Any barcode technology system uses a centralized database is maintained with the records which track the products, prices, and the stock levels or nay other information required to be encoded as required. A barcode is an optical machine-readable representation of the information about the product with which the code is related [12]. It was invented by Norman Joseph Woodland and Bernard Silver and patented in the USA in 1952 (US Patent 2,612,994). Originally based on the Morse code, it was extended to include thin and thick lines to represent characters. Later they were designed in two dimensions, which include a variety of symbols. An optical scanning device or a barcode scanner reads the lines on the barcodes with varying widths. The most widely used and visually

recognizable barcode is the Universal Product Code (UPC), which is a linear barcode and is made up of two parts: the actual visual barcode and the 12-digit UPC number. These 12 digits contain the manufacturer's identification number as the first six digits, the item's number as the subsequent five digits and the last digit is the check digit enabling the scanner to determine if the barcode was read correctly. This is only one way of arranging the data in the form of a barcode. There are many ways to arrange the barcode [21]. Barcodes work through the combination of symbology and a scanner to convert them to user-friendly information about the product on which the barcode is present. The below section explains how barcodes are used to represent digits 0 through 9. The encoding technique gives the same amount of horizontal space: 7 units to each digit. So, in order to differentiate between the digits, the 7 units are color coded with different patterns of black and white stripes. This is shown in figure below, here the thickness of the black and white stripes represents different digits [12].

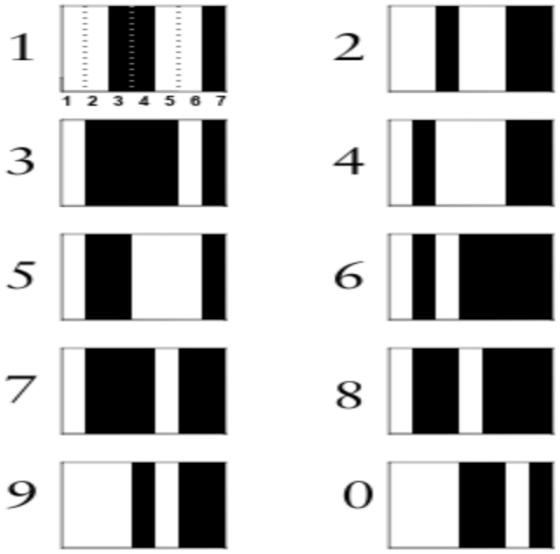


Figure 2.1 Digits 0-9 using Barcode

As mentioned above about the UPC barcode, one can manually key in the product number if the barcode is damaged or incorrectly printed in any way so as to make it unreadable for a barcode scanner. This leads us to study the structure of the barcode and in the manner in which the scanner uses it to read out the information.

2.2.1 Barcode Structure

Figure 2.2 General EAN13 barcode

- The **start character** indicated the beginning of the barcode consists of special barcode characters. These are not transmitted to the host.
- The **stop character** is at the end of the information sequence. Like the start character, these are not transmitted to the host.
- Preceding the start character, we have a **Quiet Zone,** which is at least ten times the width of the narrowest element in the barcode or 0.25 inch [21]. This is also known as the Clear Area. This space is the minimum space required for successful bar-scan ability.
- As mentioned above the **check digit** though not always present, is used to verify the accuracy of other barcode elements. It is usually added at the end of the data, but only as a means of verification or accuracy.

- The rest of the visual code is the actual barcode, which is transmitted to the host and is connected to the central database.

2.2.3 SYMBOLOGIES AND BARCODE FONTS

As mentioned above, the barcode encoding technique uses different types of barcode symbologies [14], as mentioned below

- *2/5 or two of five Unidirectional*
- *2/5 or two of five Bidirectional*
- *Interleaved 2/5*
- *Code 3 of 9 (code 39)*

All the mentioned above are just different patterns or arrangements of the black and white stripes [22]. These can be and are used to give us different sets of barcode protocols. One such example is the UPC. There are many such codes available today that are being used for different purposes across the globe. It should be kept in mind that, even though the barcode encoding method is currently an efficient means of tracking products and has come to mean a dependable means of accuracy measurements for product verifiability, it has its own demerits. Different methods for increasing robustness have been studied [22].

1D BARCODE FONT	DETAILS
 Uniform Product Code (UPC)	Retail stores for sales checkout; inventory, etc.
 Code 39 (Code 3 of 9)	Identification, inventory, and tracking shipments
 POSTNET	Encoding zip codes on U.S. mail
 Bookland	Based on ISBN numbers and used on book covers
 Code 128	Used in preference to Code 39 because it is more compact
 Interleaved 2 of 5	Used in the shipping and warehouse industries
 Codabar	Used by Federal Express, in libraries, and blood banks

Figure 2.3 Different barcode fonts and their uses [14]

2.2.4 BENEFITS OF LINEAR BARCODES

- As opposed to previous non-digital tracking methods, this relatively lowers the possibility of human error.
- It is fast and reliable and takes relatively very low time as compared to the manual method of verification.
- This can be considered as the beginning of supply chain security digitization method.
- This method does not require nay extensive employee training hence reduces the time spent on employee training also making it less expensive.
- These can be applied to most products in circulation for a variety of applications.
- The linear decoding is easier to done, hence to heavy equipment is required

2.2.5 DRAWBACKS OF LINEAR BARCODE

- The amount of data that can be stored is relatively less than other encoding techniques available today.
- In order to store more data, the area required is more, hence this method is extremely limited when the product surface area gets smaller and smaller.
- Once, the code is distorted or damaged in any form or shape, decoding and reading out the information is difficult. This makes product verification more difficult.

2.3 2-D BARCODES AND QR CODE

In contrast to linear barcodes, a 2-D barcode is more complex and can include more information in the same given area. The types of data that can be encoded include web addresses and images as sell in addition to the data stored using linear barcodes[19].

The scanners used to read 2-D barcodes are different than that used for linear barcodes. In this case we require an image scanner for reading the data encoded in the 2-D barcode. These were primarily designed to accommodate encoding of letters along with numbers and punctuation marks. Because of its higher data capacity as compared to linear barcodes, these became widely popular and are still used extensively almost in every industrial supply chain across the globe.

Some examples of 2-D barcodes include a) stacked 2-D barcode, Code 49, b) stacked code, PDF417, c) Data Matrix d) QR Code and Maxicode as shown in Figure 2.4 [13]

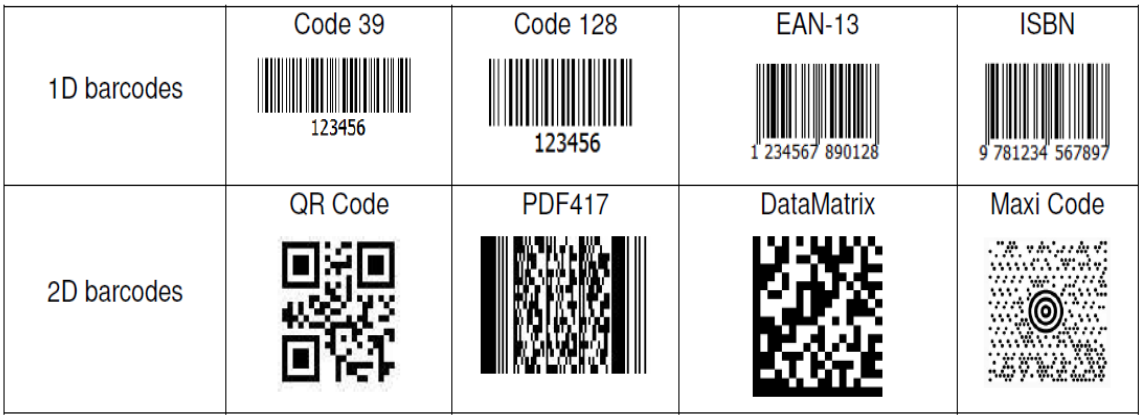


Figure 2.4 Some examples of linear and 2-D Barcodes

It should be noted that the encoding and decoding as well as the scanning programs for a selected 2-D barcode technology can be installed and used on mobile devices along with the dedicated scanners. This shall enable the use and implementation of the 2-D barcode technology for mobile

commerce [19], especially with the supply chain moving more and more toward wireless technology.

2.3.1 QR Code Technology

One of the most popular 2-D barcodes is the QR code (Quick Response code), which is a type of matrix 2-D code that can be read by smartphones. The data to be encoded can be in form of a text or an URL or any other type of data[23] . It was initially used for the purpose of vehicle tracking and is now being used throughout all industries as a better way of product verification as compared to the linear barcode.

Denso Wave originally developed the QR code in 1994, designed particularly for high-speed and omnidirectional reading. One of the exciting aspects of the technology in producing QR codes is its low cost of production and detection. Also, the data is contained in both the *x* and *y* directions as opposed to the linear barcodes, where the data is stored only in one direction. Now, the amount of data that can be stored in the QR code actually depends on the version and the error correction level along with the character set. QR codes are commonly used in the field of cryptographic currencies, particularly those based and including Bitcoin.

As seen in Figure 2.4, the three edge markers, which is used by the processor to locate the corners of the QR code image. The small dots in the code are converted to binary numbers and verified with an error-correcting algorithm. Data storage, error correction, encoding and code decoding are the main steps in the code employment and reading process [24].

Storing data is based on the data type, which is the input character set, and has version from 1 through 40 with increasing complexity with each index. The maximum storage capacities are enabled for version 40 [21]. Error correction is an important part of any encoding technique

especially in this case where the codes are likely to be damaged while in the supply chain. The QR code mechanism relies in the Reed-Solomon error correction algorithm, which has four correction levels as follows

- Level L (Low): 07% restoration of code possible
- Level M (Medium): 15% restoration of code possible
- Level Q (Quartile): 25% restoration of code possible
- Level H (High): 30% restoration of code possible

For version 40, as mentioned above, the highest data storage is possible for correction level L and is denoted by 40-L. However, since the encoding scheme uses 8-bit code words, an individual code block cannot contain more than 255 code words in length. That shall pose a limitation when the requirement of the amount of information to be stored increases. Also, the information density cannot exceed the limit. Due to the error correction capability, we can create more graphic QR code to incorporate colors, and varied graphics as per the need and desire of the manufacturers. We can also manipulate the underlying mathematical constructs to include such designs without compromising the error correction capacity of the said code.

Encoding modes such as alphanumeric encoding, byte encoding or Kanji encoding to name a few, can be mixed as needed within a QR symbol. For example, a URL with a string of alphanumeric characters can be mixed or interleaved, however, the number of bits in the length field depends in the encoding and the symbol version as well [13].

The key features of a QR code are discussed below in the Figure 2.5.

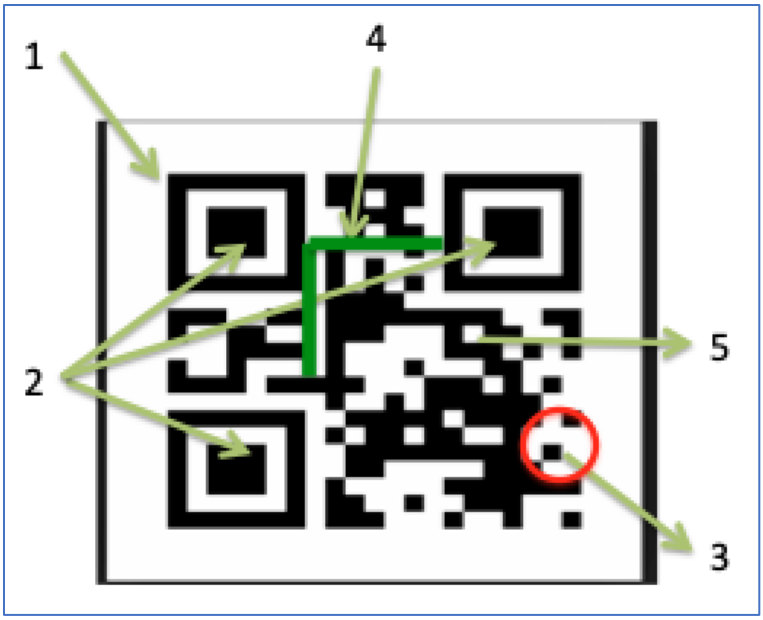


Figure 2.5 Key features of QR code

- The **Quiet Zone**, marked by 1, is the white border, which isolates the code from other printed information.
- The three squares at the three edges, marked by 2, are the **Finding Patterns**, which confirm that it is a QR code. Also, as there are three of these, it can be easily analyzed to see which direction is upward. However, this can be difficult to determine if the code is damaged in those areas.
- The mark 3 denotes the **alignment pattern,** which help us to decipher the code in case of distortion, or when the code is printed on a curved surface.
- The mark 4 denotes the **timing pattern**, which runs horizontally and vertically between the three finder patterns. This is to make it easy to identify single data cells within the QR code especially in case of distortion or damage.
- The **data cells** are marked by 5 and follow the set pattern adhering to any of the encoding protocols.

It should be kept in mind that while QR codes are highly efficient, it is relatively easy to copy them to be used on counterfeit products.

2.3.2 ADVANTAGES OF 2-D BARCODE/QR CODE

- As compared linear barcodes, 2-D barcodes can contain very high amount of data and that too in both the vertical and horizontal directions.
- 2-D barcodes can include a variety of data types to include web addresses and alphanumeric characters.
- Cost of production of QR codes is relatively lower as compared to re-programmable methods
- Also, one can download code readers at low cost.
- The QR codes can be read from any angle and the error correction codes enable us to read the codes and restore the data even if the label has been distorted.
- Systems for payments enabled by 2-D barcodes have been studied [17].
- These can be used with RFID tags or magnetic cards so as to optimize the product tracking process.
- In addition to this, any 2-D barcode is easier to transmit and can be sent over a simple text message to be sued for scanning purposes.
- Since the data capacity and the storage techniques are more complex, hence, 2-D barcodes are more secure then linear barcodes.
- Like linear barcode, the training time required for employees in the supply chain is very less; hence it is very easy to be implemented.
- One of the main advantages is the versatility of QR codes.

2.3.3 DISADVANTAGES OF 2-D BARCODE/QR CODE

- The use of smart device is a mandatory requirement for utilizing this method. In case a product goes beyond the digital coverage area, there is no way of verifying the truth for the product.
- Also, a viable Internet connection is required, without which, again product verification is impossible.
- QR codes can be abused to gather information on users. Some negative elements in the society can use QR codes to retrieve user data before redirecting the user to the desired website.
- Some codes can be used to spread malware into the users' systems; hence knowledge about the proper use of QR code is essential.
- Even if the data storage capacity is very high, there is still a minimum area requirement for the use of QR codes. Hence, as the product surface area reduces, the effectiveness of this method decreases.

Some of the commonly used 2-d barcodes are mentioned below in the Figure 2.6 with their respective uses. It should be kept in mind that any of these approaches can be combined with the blockchain technology to store digital information.

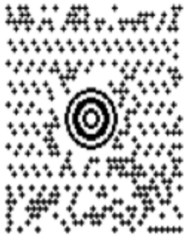
2D BARCODE FONT	DETAILS
 PDF417	Large amounts of text and data can be stored because it can be compressed. Used to print postage accepted by the UPSP. It is also used by airlines on boarding passes.
 Maxicode	MaxiCode symbols can encode two messages; a primary and a secondary message. Used by the United Parcel Service.
 Data Matrix	Ideal for marking small items due to it's ability to encode 50 characters in an extremely small size. Popular in healthcare and electronic components industry.
 QR Code	Common in advertising because it provides a way to access a brand's website quickly. Easily read by smartphones.

Figure 2.6 Different 2-D barcodes currently in use

Due to the disadvantages of the above-mentioned methods, studies are being done to use these methods in addition to new technologies, which can help effectively control, the problem of counterfeit products in the various supply chains[11]. The main drawback of these methods is that once they have been printed, or encoded, they cannot be re-programmed to accommodate new data. In cases when the product reaches its destination or the supply chain has run in to an end, the label cannot be recycled. The non-programmability of such methods is limiting their effectiveness as intuitive measures to address the problem of fake products in the market.

In the proposed work, use of a system that is inspired by the blockchain technology has been studied and uses the re-programmable property of a magnetic card, which can be attached to the product label. RFID tags are also extremely conducive for this purpose.

We shall discuss the reprogrammable approaches in the next section and try to establish the main purpose of this study is to innovate a model technique for product tracking.

Approach	Cost	Resilience to damage	Information density	Re-programmable	Ease of Printability
Linear barcode	Low	Low	Lowest	No	High
2-D barcodes/QR codes	Low	Relatively high	High	No	High

Table 2.1 Parametric comparison of the two approaches

As mentioned earlier, the method, to be used should be easy to implement and cost effective. As is clear from the table above, linear and 2-D barcodes are easy to use and are cost effective too, but the information density of the two is low (shall be seen later, as compared to the other methods). Another highlight of the table is that none of the two methods, is re-programmable. Hence, for our purpose, they are limited as the information cannot be changed to mark the critical points in the route of the products. For this purpose, we look at the programmable approaches.

3. PROGRAMMABLE APPROACHES FOR DATA AUTHENTICATION

3.1 INTRODUCTION

The previous chapter discussed some of the most common techniques employed today for product tracking. However, it is known that counterfeit products are prevalent today in almost all type of industries. The main drawback of the current methods such as the barcodes and the QR codes is that once they are printed on to the label or attached to the product, the information contained in them cannot be changed. Also, once the label is damaged, it becomes highly difficult to retrieve the information with precision. This calls for better ways in which the product can be tracked. It is also of importance, to note here, that re-programmable approaches are also required throughout the supply chain so as to add or change the information carried on by the label to denote route. In such cases, previous methods discussed, cannot serve the purpose completely. We shall discuss the other approaches, focusing on magnetic cards and RFID (Radio Frequency Identification) tags in this chapter.

3.2 MAGNETIC STRIPE CARD TECHNOLOGY

3.2.1 BACKGROUND

We have used magnetic cards for the purpose of our study to get the solutions for data encoding and storage for label marking on the products. The main advantage of using a magnetic stripe reader system for information encryption and data storage is that data reprogramming is possible at a lower cost compared to barcodes and data capacity is much more than the previously discussed methods. The magnetic stripe is also called magstripe or swipe card that is read by swiping past a magnetic reading head. They may also contain a transponder, an RFID tag or along with these, a

microchip. These are mostly used for business purposes for access controls and payment methods currently [11, 25, 26].

These, as is in case of access controls, can be used to store data of the products instead of employees and can then be used to track the products depending upon the number of scans or swipes. These are extremely popular to design access cards for buildings with restricted access and in hotel room access. It should be noted that the size and the non-symmetrical function of magstripes makes it challenging to manipulate [27, 28].

3.2.2 MAGSTRIPES: STRUCTURE

The magstripe is made up of tiny bar magnets contained in a plastic-like film. The data is stored on the magnetic stripe by modifying the magnetism of tiny iron-based magnetic particles in the stripe [29]. This method was first developed by IBM in 1960s to develop a better way of securing magnetic stripes to plastic cards. The magnetic stripe on the cards is for storing and reading electronic data.

In the figure below, we have the first magnetic stripe plastic card. Figure 3.1(a) shows the front of the magnetic card [27], where the magnetic stripe is on the front of the card. Figure 3.1(b) shows the back of the same card. Figure 3.1(c) shows an early magnetic card with the stripe at the center of the card, which was applied using magnetic slurry paint.

(a) Card (front)

(b) Card (back)

(c) Card Reader

Figure 3.1 (a), (b) Front and Back of magnetic stripe card
(c) magnetic stripe card reader/writer

Current versions of magnetic stripe cards print the stripe on the back of the card with other information printed on the front as per requirement. There are many ways of encoding data onto the magnetic stripes [27]. Usually, the data written on the magnetic stripe is done so in three tracks. Generally, the three tracks have the densities at 210, 75 and 210 bits/in (1kbit/in^2). The density can be increased through different coding techniques including Bayesian blind inverse filter [24].

The information contained on the tracks must follow certain guidelines so as to be read from the card readers. ISO (International Standard Organization) sets the protocols for the structure of the

data to be stored on the tracks on the magnetic stripes [25]. They are internationally standardized at ISO 7811. The following data can be saved on three tracks:

- Track 1: 79 alpha numeric characters
- Track 2: 40 numeric characters
- Track 3: 107 numeric characters

3.2.3 MAGNETIC CARD TYPES

Magnetic cards are widely used in almost all the industries, mostly for access controls and data verification [30]. A general term associated with the magnetic swipe cards is the 'coercivity' of the cards. There are two popular types of magnetic striped cards

- High Coercivity (HiCo)
- Low Coercivity (LoCo)

The same amount of data can be stored on both HiCo and LoCo cards. The difference lies in the strength of the magnetic field used to write data on the cards. In other words, we can say that coercivity is the values of the coercive force for a substance that is magnetized to saturation or the magnetic force required to change the orientation of the magnetic material. HiCo cards have almost 13 times higher coercivity than LoCo cards and hence, are used for purposes which require high security measures. HiCo cards higher more unlikely to be erased by simple magnets and are more difficult to get corrupted or erased.

Standard cards or LoCo cards use 300 Oersted magnetic tape and are generally brown in color while HiCo cards use about 4000 Oersted magnetic tape and are usually black in color [31]. It should be mentioned here that Oersted or Oe is a unit of field strength of an electro-magnetic field where 1 Oe = $10^3/4\pi$ Am^{-1}. Usually, iron oxide or barium ferrite is ground into a powder and is then combined with a plastic-type material in liquid consistency. This solution is then allowed to

cool and then stamped onto a card. Low coercivity cards are usually made of iron oxide. The stronger magnetic field makes HiCo cards makes them more durable as the data encoded on the stripe is less likely to be erased when exposed to an external magnetic field. This also enables them to have a higher life and more secure information. Hence, these are more commonly used in banking systems like credit cards and as employee identity cards [31]. LoCo cards are used for short-term reasons such as hotel access key cards. LoCo cards are easier to encode information [32].

Figure 3.2 HiCo and LoCo Magnetic cards

In the above figure, the difference between the appearance of HiCo and LoCo cards can be seen. The table below describes the difference between HiCo and LoCo cards. The differences between their appearances and their coercivity, make them suitable for different purposes. The Table 3.1 lists the differences between HiCo and LoCo magnetic cards. These differences make them suitable for different purposes. The uses of the cards are also mentioned in the Table 3.1.

HIGH COERCIVITY MAGNETIC SWIPE CARDS	LOW COERCIVITY MAGNETIC SWIPE CARDS
The magnetic stripe is black in color	The magnetic stripe is brown in color
It is subjected to stronger magnetic field for data writing up to 4000 Oe	Relatively weaker magnetic field is applied, up to 300 Oe.
Resistant to most magnetic fields, hence more difficult to get corrupted	Relatively more susceptible to data corruption and damage.
Mostly used for reasons requiring higher life like credit cards	Commonly used for short-term use like access key cards in hotels.

Table 3.1 Difference between HiCo and LoCo magnetic stripe cards

3.2.4 MAGNETIC CARD DATA LAYOUT

As mentioned above, the magnetic stripes have from two to three separate tracks. Currently, the three tracks are approximately 0.11 inches broad. Usually, all the three tracks can be used to store data, sometimes, only two tracks are used while the third is left for use as per requirement. Let us now see how the data is stored and read from the magnetic stripes. It should be noted here that the information stored on the tracks, can be changed with the help of some available software or through nay code using any language available to the user. The data, however, should be connected to the database, which then verifies the information stored on the card.

We can consider the magnetic stripe to act like a bar magnet with the two ends acting as the north and the south poles respectively. Also, we can take the tiny magnetic particles to act like tiny bar magnets aligned in the N-S (North-South) direction.

Encoding the information means changing the alignment of tiny magnetic particles on the stripe. When the magnetic stripe is placed under very strong magnetic field such that the polarity of the particles on the stripe is flipped, then the flipping of the magnetic field on the stripe is the act of encoding the information stored on the magnetic stripes. This process of encoding is achieved by a solenoid, which acts as a magnet when carrying electric current. So, now, if the current is in one direction, it creates magnetic alignment on the stripe. In order to store any type of data on the magnetic stripe, we need a quick varying current so as to get opposing varying opposite magnetic field alignments created in a very small area in very short amounts of time. So, where we initially had no data, now, we have (due to the solenoid that creates a difference in the magnetic alignment), particles that are aligned as say, N-N-S-S-N-N. the N-S poles of the particles in the magnetic stripe are reversed. Hence, this enables us to store data in the form of 1's and 0's, like in a binary format, which can then be read by any digitally equipped reader.

In this manner, the different characters can be written on the three tracks of information.

Track 1 usually starts with the % sign and is then followed up with the alphanumeric characters, which make up the information as per the requirement. In applications such as banking, this track usually contains the personal information of the account holder. This track has the capacity to hold 79 alphanumeric characters.

Track 2 begins with ';' worth 1byte. In the example of a banking application, this track usually contains the account number with the verification number and maybe the social security number of the account holder. This is the information, when, combined with the first track, gives us a unique combination of data, unique to an individual cardholder and is verified from the central database of the organization. The second track data is compressed at 75 bits per inch.

The third track, though not usually used in banking applications, can be used for other purposes. Track 3 is encoded with a data density of 210 bits per inch and 5 bits per character, with a total of 107 numeric characters.

Though the magnetic stripe data is meant as read-only for applications such as banking and security clearance. Data on the card can be modified so as to accommodate any changes (not for banks or financial institutions) [29].

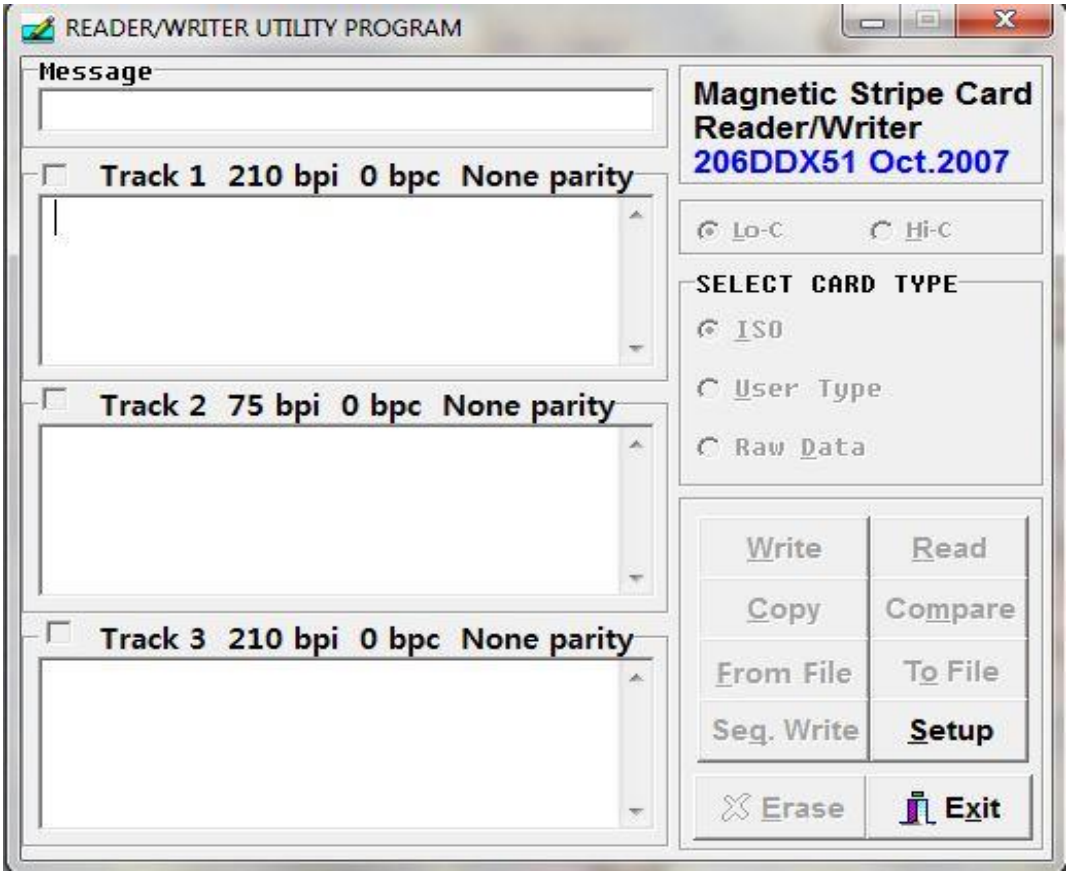


Figure 3.3 Magnetic Card Reader/Writer software for MSR206U (used)

The data on the card can be read as well as new data can be added or re-written on the card. The various magnetic card reader/writer software programs allow easy access to the technology. The same operation can be performed by the use of programming languages such as PYTHON or

MATLAB (or any programming language of choice) tools so as to access the input/output devices connected to the machine. It is now known how data on the magnetic card is stored on the magnetic stripes.

We should also keep in mind that writing the data in the form of three tracks is another way of encoding data on the magnetic stripe. Data can also be written on the card not necessarily in three different tracks. The dedicated card reader shall be able to read the data on the card in both cases. The image below shows the reading capability of the magnetic card reader/writer. The write/erase functions can also be performed. The graphic user interface (GUI) is also password protected.

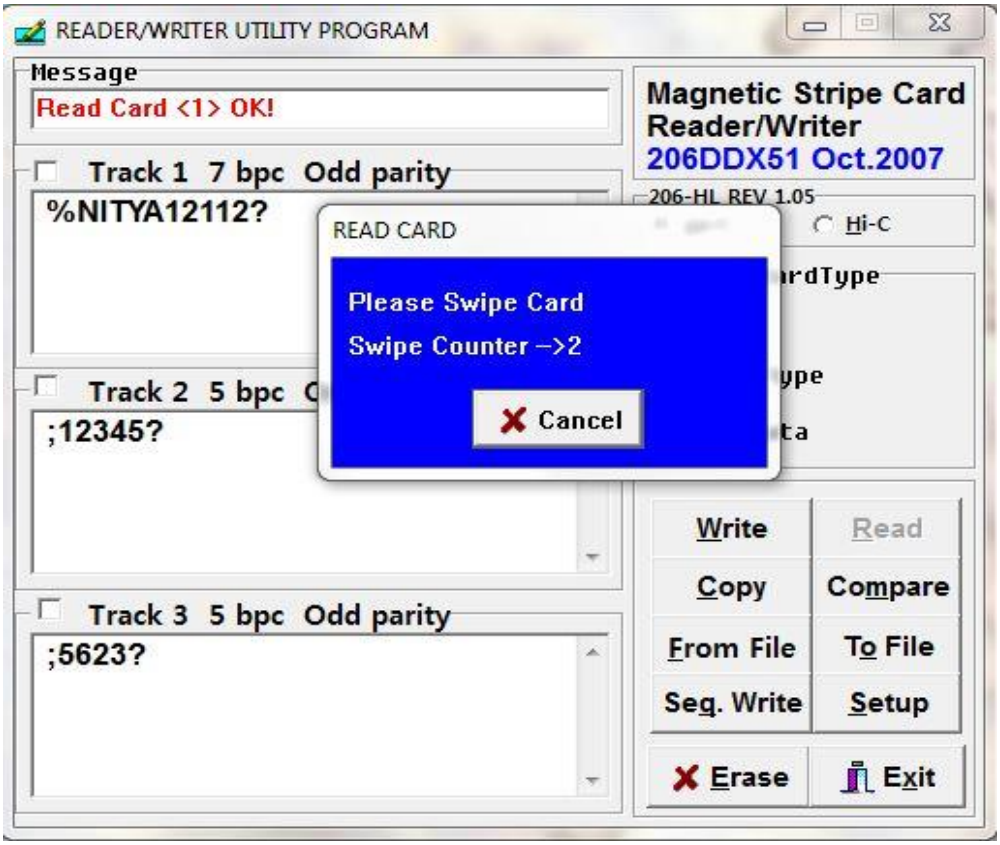


Figure 3.4 Data from the magnetic card is read and displayed on the GUI

The issuer of the card chooses the data to be encoded upon it. We can choose to write data in only alphanumeric characters in a single track throughout the supply chain to enable readability throughout.

In the above figure, it should be noted that one has the option to write data on the card as well. Now, this is only one of many ways to write data onto the card. The reading/writing operation can also be done via means of another programming language to act as an interface between the user and the application.

3.2.5 MAGNETIC CARD READERS AND SCANNERS

It is essential that we have the required technology, not only to encode the data onto the magnetic stripes but also the technology to read and modify (if required) the data with equal ease and precision. In order to read and/or write/erase the data on the magnetic cards so as to increase the usability of the cards, we require the hardware devices that make such operations possible. For this purpose, we have card readers and scanners available. This has an advantage that new investment in designing such equipment is not required.

Let us look at some common reading/writing technology available today that equip us to use the magnetic card data.

In our study, we have used the basic MSR206U magnetic card reader writer so as to minimize the cost of the process [33]. It should be noted, that this only provides us with the user interface between the user and the data. The know-how of such technology is still required throughout the supply chain where we intend to be put it to use. The readers and scanners can be both contact and contactless, depending upon the requirement and the application.

A magnetic card reader is microcontroller-based hardware equipment configured to a particular application for reading the data. Since the data encode follows a set of protocols as specified by the ISO, the reader also, follows the same rules in order to decode the data in a reader-friendly format. The reader/scanner can be connected to the localhost, which can be a personal computer as well through the USB or RS232 cable. The system recognizes both the connections and then the data can be viewed as is stored on the card. As explained earlier, the data is written on the magnetic stripes by changing the magnetic field alignment of the tiny magnetic particles on the stripe. In the same manner, the reader comprehends the changes in the magnetic field caused by the flux reversals on the magnetic stripe to give the output as the actual data that was written on to the card [32].

All magnetic card readers use, what is called as the read head to read the data. As we know, that for encoding data, two-frequency, coherent phase recording is used, which is also known as F/2F sample encoding. Self-clocking is achieved by using data and clock bits. So, to decode the information or the data, the magnetic read heads contain an in-built F/2F bit recovery circuit [66] along with the interface with the host machine [34]. The recovery section of the card reader recovers data bits form the data stream by locking on to the data rate. Hence, it is important for the reader to successfully decode the data that the data encoding is done in a specified manner (e.g. ISO protocols).

The data contained on the card is saved in a central database, which is verified while reading the data and only on successful verification does the reader allow for the transaction to take place (in case of banking or financial transactions).

3.2.6 ADVANTAGES OF MAGNETIC STRIPE CARD TECHNOLOGY

- Since its invention, magnetic swipe technology is still prevalent today and is used across the globe in a number of industries as a reliable means of product verification.
- As opposed to previous methods discussed in chapter 2, these can contain much more data types
- The amount of information stored in the magnetic stripe cards is much more than a simple linear barcode or 2-D barcodes.
- These can be reprogrammed along the supply chain to adjust for new data or erase previously stored data as the product moves along the supply chain.
- The data stored on the magnetic stripe cards is less susceptible to get copied as compared to the 1-D and 2-D barcodes
- These are also more resilient towards damage and the data is less likely to get corrupted.
- Since the data can be modified, these can be reused several times to be used with products that continuously depend on varying data
- The modified data can also be used to denote the different node activities for any product.
- Magnetic swipe cards are far more secure than barcodes and QR codes. In order to manipulate the data, the know-how of the card functions and the database link are required, making it more difficult to get cloned [25].
- When compared to chip readers and RFID tags, these prove to be less expensive to implement and read.

3.3 RFID TAGS FOR PRODUCT TRACEABILITY

Radio Frequency Identification or RFID is a new technology with promising benefits especially in supply chain management [20] [35]. In this method, the digital data is encoded in RFID tags, also called smart labels, similar to the magnetic card digital encoding. This is envisioned to increase productivity and convenience and can be put to use for thousands of applications [36]. As in case if the magnetic cards, the data storage devices, and the readers/scanners are connected to a database through a host computer or a network. Also, similar to the magnetic cards, the RFID tags have read-write capabilities. The data can be re-written, modified and locked [37]. These, hence, provide a better way of tracking products if the proper infrastructure is established.

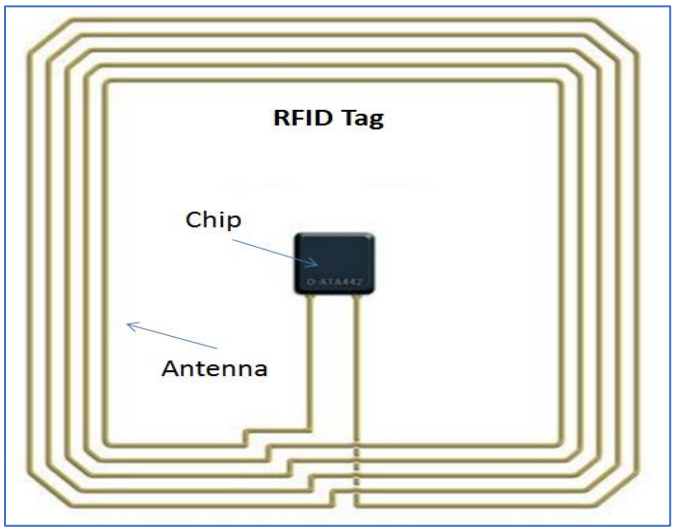


Figure 3.5 A basic RFID tag image

The initial RFID tags were known as inductively coupled RFID tags and were powered by a magnetic field that was generated by the reader. Next came the capacitively coupled tags. This was done to lower the cost of manufacturing and implementation. These could store about 2kB of data stored on a microchip [38].

RFID circuitry gain power from the radio waves emitted by the readers in their vicinity [39]. The data on the microchip on the RFID tag contains information such as the serial number of the product and/or other useful information used to identify the product. This microchip is connected to the antenna. The whole setup is then referred to as the RFID tag [40]. The antenna communicates with the reader present in the vicinity of that particular tag. The reader uses this information by converting it to digital information so as to pass it on to the main database frame for that product or set of products. The technology can be enhanced by equipping the tags with location information [39].

Currently, RFID based communication is useful for short-range radio technology. This is mainly used to send/receive digital data between two moving objects or a moving object and a stationary object. This is achieved by the employment of a simple device, which is the tag or the transponder and linking it with a complex back-end device. Currently, RFID industry includes active, semi-active, and also passive RFID transponders or tags. The antenna on the tag receives electromagnetic energy from the RFID reader's antenna[38]. The reader then interprets the tag's radio waves and the frequencies as useful data.

The above-mentioned inductively and capacitively coupled RFID tags are bulky and expensive, hence now active, semi-passive, and passive RFID transponders help make the technology more useful and accessible [41]. We can see the basic block diagram of an RFID transponder in the figure below.

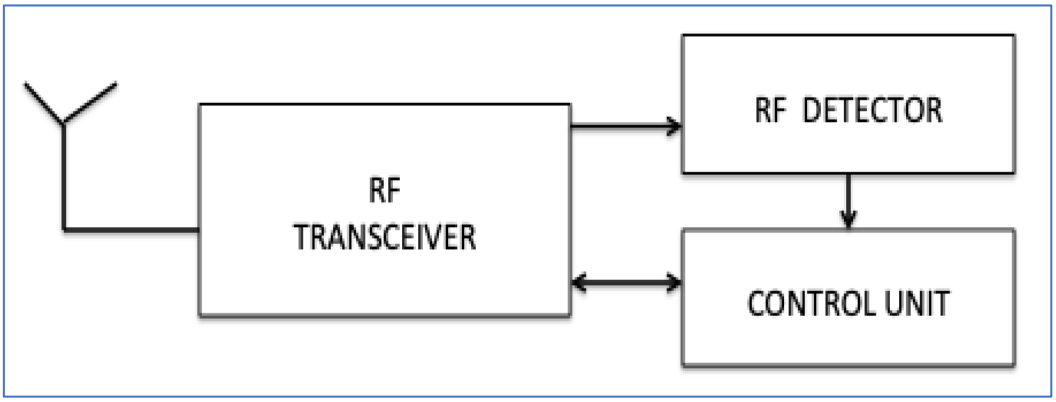


Figure 3.6 Basic block diagram of an RFID transponder [42]

The power supply is one of the main criteria used today to classify RFID tags based on their power requirements. Active tags use internal batteries to power their circuit as well as to broadcast information to the reader. Semi-passive tags use batteries to power their circuit but rely on the reader for power supply for broadcasting purposes. These operate at frequencies of about 850-900 MHz and can be used for larger distances of up to 30 meters or more. Additional batteries can be used to increase the distance at which the tags can be read. These methods are useful for expensive products [42].

Unlike the other two, passive tags do not have an internal battery to supply power. Hence, they need the power to be supplied as power emitted from the reader. This power can be used for data processing and transmission as well, although, not all passive RFID tags are capable of performing data processing. This makes passive tags less expensive and easier to design and implement [41]. Active tags engage in transponder driven communication. This is because a reader's presence is not mandatory to maintain the continuous flow of data. These can store more data as compared to the passive tags as they have internal batteries for power supply. These can save their power by not being active or transmitting data when they do not sense the presence of a reader. Active tags

can also be reprogrammed, hence can be very useful in tracking products across the supply chain in almost all the industries, just like the magnetic cards.

3.3.1 KEY FACTORS AFFECTING THE IMPLEMENTATION OF RFID TECHNOLOGY

The RFID technology is still more expensive than other programmable approaches for storing data for the purpose of product traceability. This means that the implementation of such technology calls for heavy investment and is hence affected by organizational factors [43] for implementation and maintenance. In this case, the organizational size, top-management investment, and availability of IT support are among the most important factors that should be present for the successful implementation of a verification system based on RFID technology.

The cost of production affects the implementation time and scope of the use of the technology. Data storage type influences the cost of RFID tags. The storage types are read-write (R/W), read-only and the WORM (Write Once, Read Many). R/W cards can have much more use as the data can be written and overwritten. The data on the tag can include the serial number for the products as well making it easier to set a protocol for the data storage system [44]. Active and semi-passive tags are more expensive than their passive counterparts. The range requirements, data storage capacity directly affects the implementation of the technology [45].

Along with data storage capacity, the required volume of data affects the cost of production of RFID tags. It is also imperative that the industry in which the technology needs to be implemented is not too complex. The standards are to be set in order to maintain compatibility with the current practices of data verification in a uniform manner along the supply chain. For magnetic cards, the ISO sets protocols for data storage and density of data to be stored on the magnetic strip making it

more compatible with the supply chains across the globe. RFID technology also calls for such rules or standards to make the technology more accessible and readable throughout the supply chain. [43]

The main challenge for this technology is bringing down the cost of production and implementation for industrial use. Also, distinguishing original tags form their fake counterparts. Strong authentication protocols such as the ISO/IEC 978-2 standard [46], which can provide proof for identity. It is also important to address the problem of multiple readings at once, which happens if the reader picks up the signal from multiple tags at the same instant. Readers also need to be separated as they might interfere with each other's signals. Though there are some challenges, RFID tags have some significant advantages over the other current practices for product traceability and verification.

3.3.2 ADVANTAGES OF RFID TECHNOLOGY

- High data storage as compared to the current methods like the barcode and 2-D barcode technology
- The time required for product verification is significantly lower than the actual scanning of the products.
- RFID tags are the way forward to implement the Internet of Things (IoT) a possibility as the supply chain moves forward to getting more and more digital every day.
- Scanning of devices is simples and does not require a particular line of sight as opposed to the barcode technology [46].
- Know-how to duplicate the tags is much more difficult than any current practices today.

- As opposed to linear and 2-D barcodes, these can be re-programmed and, hence can be used several times with data being added/modified as per requirement.
- Human involvement in product verification is minimal as compared to other methods, hence speeding up the verification process as the scans take milliseconds and work automatically [47].
- RFID tags can be used not only to track products but can also be used to track wildlife for monitoring and research purposes [37].
- These are being investigated to be used in the health care industry also [48]

The RFID technology is still an emerging technology and more advances are yet to be made in the implementation of the RFID system. These can be used for a myriad of applications [40, 49, 50] More research needs to be done for use in the medical industry and for tagging animals. Better transponders need to be designed to bring down the cost of the technology [42, 43].

3.4 SMART CARDS – OTHER PROGRAMMABLE APPROACHES FOR PRODUCT TRACEABILITY

3.4.1 BACKGROUND

Smart cards are like magnetic stripe cards, but instead of the magnetic stripe, these have an embedded microprocessor. These have become increasingly popular for banking purposes. The microprocessor chip enhances security for the data stored on the chip. Like magnetic stripes, the information on the cards can be encoded are portable and hence, are becoming increasingly popular. Different types of modulation techniques, such as amplitude and frequency modulation or binary phase shift keying. Designing methods also include code division multiple access to

result in more secure communication, though, has higher power requirements [51]. The smart card system consists of the microchip-enabled card, the readers and the centralized database background system. These have the ability to store large amounts of data along with encryption and mutual authentication [76]. Smart cards are of two types based on their method of operation, namely, contact smart cards and contactless smart cards [52].

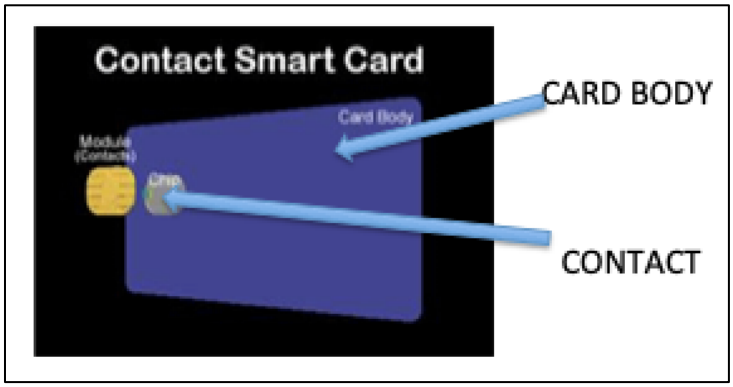


Figure 3.7 Contact smart card

In case of a contact card, the card is inserted into the smart card reader. The surface of the card is generally gold plated and comes in direct contact with the reader.it is then that the transmission of data and verification takes place. Transmission of card status and data communication takes place through contact points [53]. These are extensively used in credit and debit cards. Commands to the chip in the smart card can be sent by one of the contacts called the I/Os. The protocols used for this purpose are defined in the ISO/IEC 7816-3.

Contactless cards have an embedded microchip along with internal memory with a small antenna that communicates with the reader through the RF (Radio Frequency) interface. These are most useful for fast transactions and are mostly used for government security cards and documents such as electronic passports and visas [76]. Unlike contact cards, the chip on the contactless cards, the chip is embedded within the plastic body of the card and not exposed. In the case of contactless

cards, the electromagnetic field provided by the reader plays the role of the communication channel and also powers the card.

There are also hybrid cards, which contain two chips, one with a contact interface and one with a contactless interface. The main advantages of smart card technology is that the memory chip on the card is a highly secure method of storing data and provides for better verification of data. These are also compatible with the current system available and can be supported by a USB enabled machine. Data on the cards are much more difficult to get copied and less prone to damage by external factors [54].

The main disadvantage of smart card technology is the cost of operation and implementation. Because of the higher cost, these are limited to be applied for high-end applications such as banking. There is a challenge to make the information more secure as these cards carry more sensitive data.

The design process of the smart cards is also more tedious as compared to the magnetic stripes card. The above-mentioned methods for reprogrammable approaches for product traceability are still under investigation. There is scope for improvement, and these can be incorporated to create an Internet of Things (IoT) so as to make communication between digital devices smooth and secure. There is a need to attempt to establish one such method using magnetic stripe cards and create the digital link via a blockchain-inspired mechanism and combine it with a physical entity to be placed on the products.

Approach	Cost	Resilience to damage	Information density	Re-programmable	Ease of Printability
Linear barcode	Low	Low	Lowest	No	High
2-D barcodes/QR codes	Low	Relatively high	High	No	High
Smart Cards	High	High	High	Yes	Low
RFID	High	Low	Very high	Yes	Low
Magnetic stripe cards	Low	High	Very high	Yes	High

Table 3.2 Analysis of the current and proposed approaches

As is seen from the table above, RFID technology and the magnetic card technology are both useful in the sense that, they both have high information density and are re-programmable. Amongst the two, we should note that the RFID technology has higher cost of infrastructure and is not as easy to implement as the magnetic stripe cards. For the countries or the supply chain networks, it is imperative, that the method used to track the products, should be easily adaptable. In addition to this, the RFIDs are to be made specific to the product being used and this adds to the cost of production. In contrast, the same magnetic stripe card labels can be used for multiple products and can be then easily recycled as well. The analysis is concluded in table 3.3. magnetic stripe card labels, then prove to be the optimum solution for tracking products and storing

information about the products. It should be kept in mind that all of these approaches can be combined with the blockchain technology to complete the digital aspect of supply chain traceability.

Approach	Information Density	Resilience to damage	Cost of infrastructure	Re-programmable	Ease of Printability
RFID	High	Low	Very high	Yes	Low
Magnetic stripe cards	High	High	Low	Yes	High

Table 3.3 Parametric Comparison of RFID and Magnetic stripe cards

As is clear from the above table, when all the parameters are taken into consideration, magnetic stripe cards have a few advantages over the RFID technology. Hence, this study proposes the use of magnetic cards on the labels of the products. The label can be printed on any product. the label is made to contain the digital and the physical tag for the information. The Figure 3.8 shows, how the magnetic card label shall be placed on the product. it can be made flexible to be placed on a curved surface as well.

Figure 3.8 The label placed on smaller products

Figure 3.8 shows the placement of the digital and physical tags on the product. The label can be easily read by a proximity magnetic stripe reader. The technology can also be combined with part magnetic stripe card label and barcodes too to accommodate for smooth transition and application in the existing supply chain. The study uses the MSR206 U card reader /writer for editing/reading the information on the magnetic card. The same can be done with the help of any programming languages to account for data modification. As the technology and the infrastructure improves, the readers and the system can be made to go wireless. It should be kept in mind that this technology can be easily coupled with the blockchain system and the information is linked to the physical tag (containing the DNA information). Any magnetic proximity card reader can be used to decipher the information and perform the same functions as any other reader/writer.

4. BLOCKCHAIN INSPIRED IOT FOR PRODUCT TRACEABILITY

4.1 BACKGROUND

In the previous chapters, we discussed the current methods and technologies present to track the products in the supply chain. Supply chain traceability is one of the major challenges across the world [2, 55]. Counterfeit products are prevalent in almost all industries, especially in the pharmaceutical industry. According to the International Chamber of Commerce, the economic impacts are major and are estimated to drain US$ 4.2 trillion from the global economy and may cause 5.4 million legitimate job losses by the year 2022 [56].

In 2016, the historic Declaration of Internet (DOI) was signed by many brand owners and representatives from the international shipping industry to prevent the maritime transport of counterfeiting products. the main purpose of this agreement was to address the challenge of increasing supply chain integrity and to increase awareness and training in the process of tackling counterfeit and mislabeled products. This also calls for better means of sharing the data about the products [56].

Over the past few decades, globalization has changed the meaning and now a traditional supply chain may include multiple countries with products crossing borders several times before actually reaching the intended customer. BASCAP or the Business Action to Stop Counterfeiting and Piracy paper [56] aims at studying the steps needed to be taken by the intermediaries in any supply chain so as to eliminate global supply chain susceptibilities and minimize if not stop counterfeit and pirated products.

The problem is complicated by the complexity of the health care system, which may not be uniform across the globe. The WHO (World Health Organization) estimates that about 5% to 8% of the

worldwide trade in pharmaceuticals is counterfeit [1]. There are many factors that make it more and more difficult to tackle the problem of counterfeit products [55]. There are many intermediaries and small businesses selling pharmaceutical products to areas where there is no digital coverage. In the regions where adequate digital coverage is available, it is still becoming extremely difficult to track fake products as well as ascertain the source of such products. These situations call for measures so as to track the products in real-time along with determining the sources of such damaging products [2]. In all industries, primarily food, pharmaceuticals, medical devices, consumer products, and automobiles, have been recognized as primary industries due to their global presence and outsourcing process that take place in several countries. This gives a chance for counterfeiters to introduce fake parts of the products, which is even more difficult to trace. In this study, proposed is a method to combine digital tracking with the option of physical verification of the product. This is done by incorporating a blockchain-based backend system for verification and tracking products in real-time. The physical verification of the product uses a tag containing DNA sequence which plays the role of a physical entity unique to the company or the product and that can be verified in case the digital network for verification fails or is limited. The digital backend of the proposed solution includes the scanning of the magnetic card information and then using blockchain-based chain to then track the labeled product in real-time

4.2 SUPPLY CHAIN AND THE CONCEPT OF BLOCKCHAIN

Our proposed work relies extensively on the system established and supported by the blockchain technology [5]. The blockchain technology helps us establish a secure network for better product safety and security and increased transparency.

The best-known example of the blockchain technology is the Bitcoin, which is the most popular cryptocurrency. In this study, the system used is inspired by the concept of blockchain. We concentrate on the use of blockchain specifically from the perspective of supply chain requirements and challenges. The following flow diagram depicts a simple supply chain with the minimum require ed a number of nodes. All the participating points, like the manufacturer, the distribution unit, the wholesale and the retail distributors are nodes in the network similar to the nodes in case of cryptocurrencies. In our study, the information exchange or the transactions taking place are not only of virtual nature but carry physical information as well in the form of a DNA patch. The transactions, in our use of blockchain, mean the transport of tangible products, which are linked to the virtual data as well.

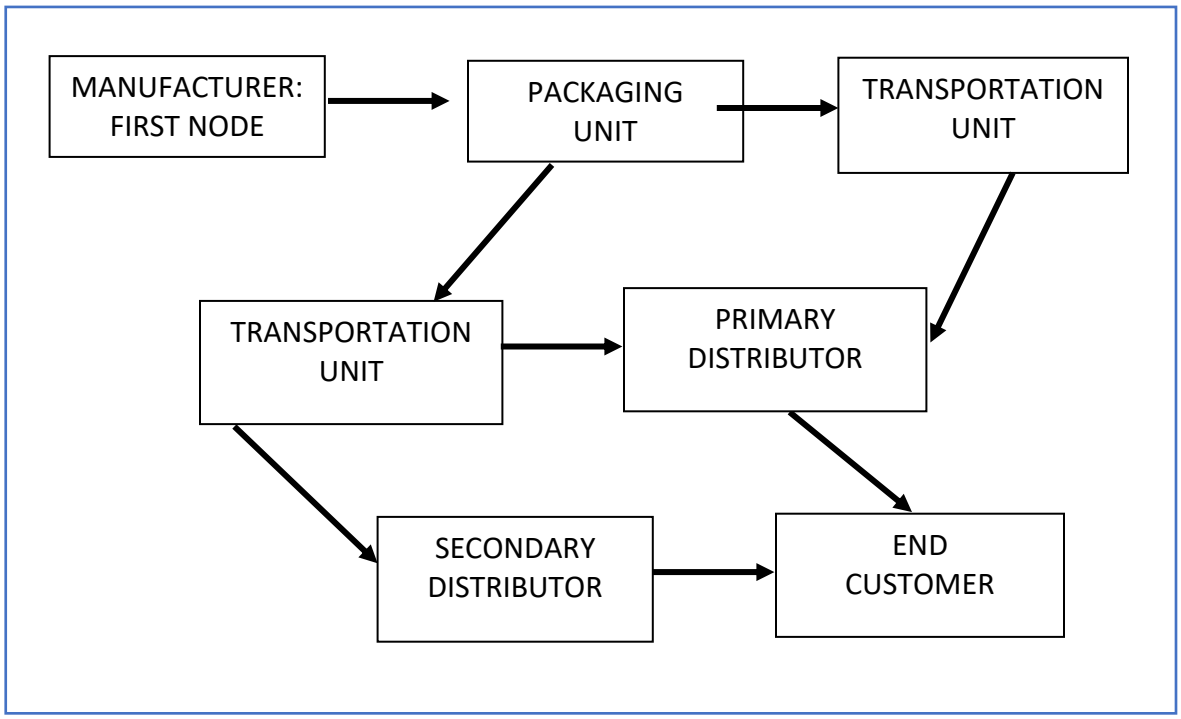


Figure 4.1 A basic pharmaceutical supply chain from manufacturer to customer

As the product moves along the supply chain, illegitimate sources have the opportunity to introduce counterfeit products at any point without detection.

For the purpose of our study, we call each of the participants name, the manufacturer, the packager, assembly unit, transportation unit, the primary distributor, the secondary distributor and finally the end customer, as the nodes in the network. As discussed in the first chapter, the purpose of the blockchain is to increase transparency and security along the supply chain [57].

Basically, blockchain technology serves as a distributed ledger or a peer-to-peer network. Unlike the concept of cryptocurrency, in our study, one "transaction" is equivalent to the scanning of labels on the products [11]. Once the label is scanned, the information is stored on the machine and is then used as the source of data by the blockchain code.

4.3 BLOCKCHAIN INSPIRED NETWORK BUILDING

As mentioned earlier, a blockchain is a system of the distributed database or a public ledger, with the digital list of transactions being shared by all the participating parties or nodes. Data can be added to the chain in a chronological order where the digital signature includes the timestamp of the transaction being recorded. The information can include any data type. The most important point to be noted about the blockchain system is the concept of consensus, where the participating nodes agree on the longest existing chain and then the new block is added on to the chain [58].

In our study, we have the data to be read, the index of the current block, and the hash of the previous block to be taken as the input and then generate the current hash of the block [10].

The hashing algorithm used is SHA256, which is the Secure Hash Algorithm [5, 59]. The SHA256 is one of the many available hashing algorithms and is considered as one of the strongest encryption algorithms currently. A hashing algorithm is not exactly encryption as the hash

generated cannot be decrypted. It works as a one-way encryption program. The input can be any number of bytes long and the output is always a 256-bit long encrypted code called the hash [59]. If any of the input bits is changed, then the output or the hash is completely different, hence any generated hash cannot be repeated, making it extremely difficult to get copied or duplicated. In this manner, the trust of the parties is maintained without the use of the trust-in-third party [10]. Therefore, despite it being an open system (anyone with access can verify the data), blockchain is extremely secure. Each modification to the already existing data creates a whole new block. Hence, tampering with the data without creating or adding another block to the chain is nearly impossible. As explained in chapter 1, each block is linked to its predecessor through the hash of the previous block. If any product or label is added in the middle of the supply chain through outside factors, it shall not be added to the existing chain. Either it shall be rejected, or it will start a new chain. In either case it can be differentiated from the original product and can be traced to its point of entry into the supply chain. The figure below depicts the supply chain for generic products using blockchain.

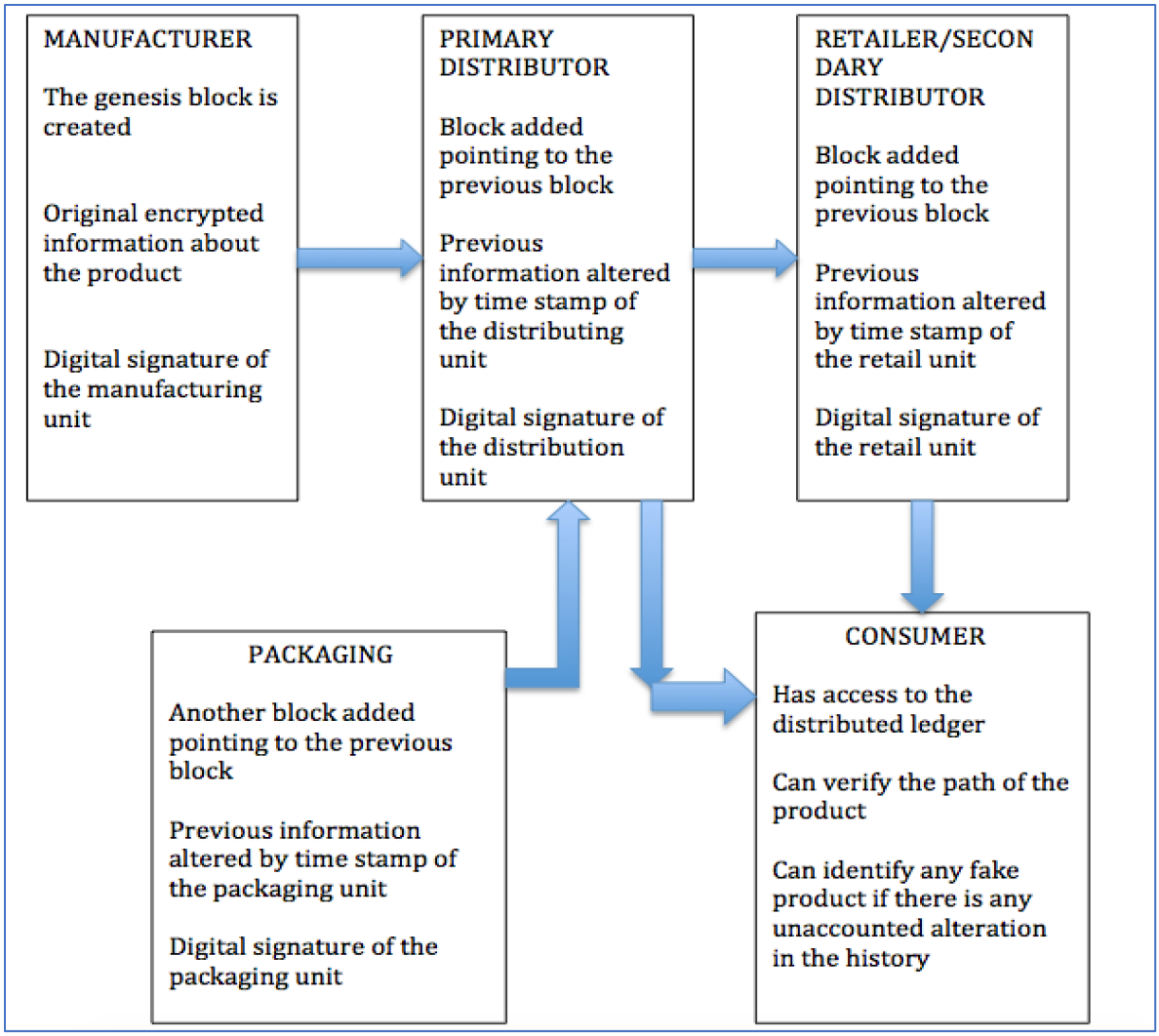


Figure 4.2 Basic supply chain depicted using blockchain technology

The data or the label (in this case) is stored in the magnetic card. The information is encoded on the magnetic stripe and can be in any form.

According to the DSCSA (Drug Supply Chain Security Act) manufacturers are required to include serial numbers or track numbers on the products all along the supply chain in addition to verification for recalls, resales return to ensure only safe drugs reach the end customer [60].

4.4 BUILDING INTERNET OF THINGS IN THE PHARMACEUTICAL SUPPLY CHAIN

At the manufacturer's end, the information (on the magnetic stripe label) is read by the reader/scanner. This information includes DNA sequence data is used as the data for the first block, or the genesis block. This starts the blockchain for that product or the batch of products. The digital technology is being studied to build an IoT [61].

While creating the first block, no previous hash exists, so the algorithm assigns a random hash. This hash will change if the scan time-stamp changes. This means that a single product can be scanned only once.

The product moves along the supply chain, the next unit is usually the packaging and/or the assembly unit. The label is read/scanned with the help of magnetic card readers or proximity scanners. This in turn, adds another block to the previously created block using its hash as the prior reference. This starts the chain where the nodes are linked to the previous nodes through the hash of the precious block digitally. Subsequently, as the product moves and is scanned by the distribution unit (primary and secondary), blocks are consecutively added to the chain.

In case the participating node needs to verify the course of any given product, they access the local network hosting the chain and can see the details of the nodes with the node identifier and the timestamp on the displayed data.

To modify the hash of any one block, all the previous hashes need to be determined, which requires extensive technological prowess and system. This makes it extremely difficult, if not entirely impossible to tamper with any existing chain [57]. This will be displayed on the common host network where all the nodes can verify the data.

This system also ensures that no centralized database needs to be maintained as the peers in the network act as distributed networks for all the transactions taking place. As opposed to the previous

methods [11], where the label can be tampered with and the information once stored cannot be changed, the proposed method makes use of programmable labels (magnetic stripes). This shall enable the nodes (access as per security, safety, and privacy requirements) to add their own identification information as the product moves along the supply chain in concern.

The above-described process can point to the source and time of the introduction of fake or sub-par products. it should be noted here that for this system to work unscrupulously digital access to the blockchain system is essential. Also, it is highly required that all the participating nodes in the network have the technical know-how to read the data displayed when accessing the blockchain network.

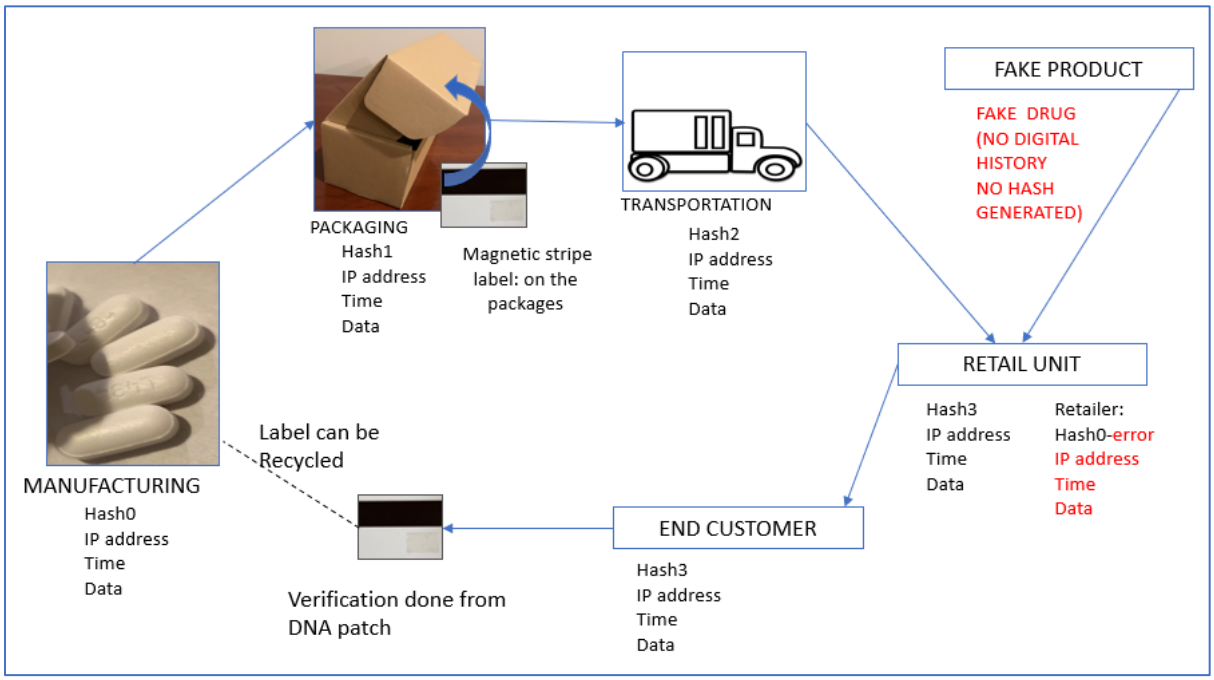


Figure 4.3 Building the digital supply chain with physical tags

The above figure shows the flow of products within a given supply chain. The blockchain system helps us to identify the weak points/nodes responsible for the introduction of counterfeit products in a supply chain. Also, since, the magnetic cards are re-programmable, the information o them can be changed and can be recycled for another product easily.

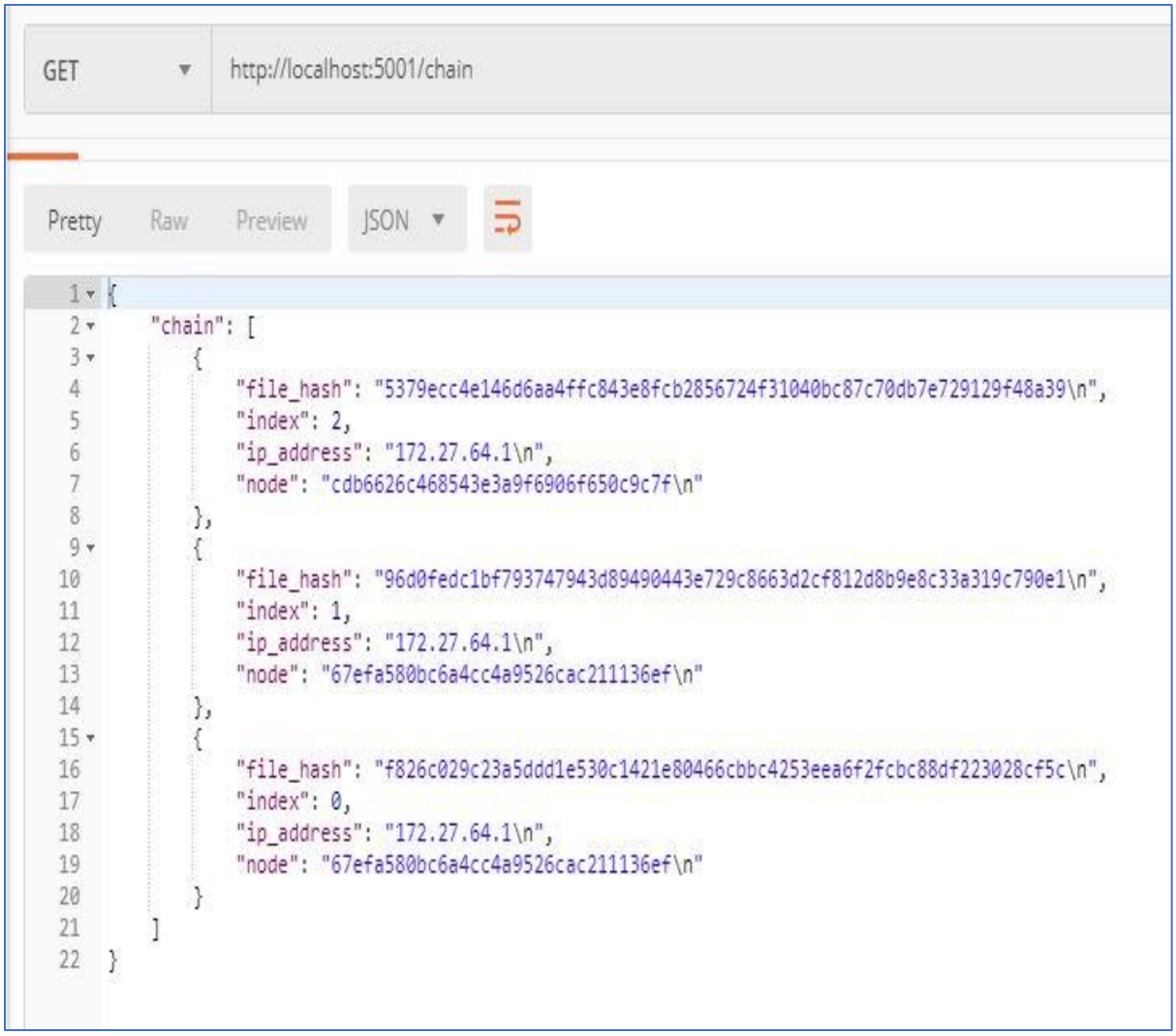


Figure 4.4 Blockchain with multiple nodes with their node identifiers

The above figure shows what a basic blockchain might look like with multiple nodes participating with the same information (the product) being read by the different nodes. Now, at any point in the supply chain if any new data is to be added to the magnetic card label, then the new information is added, and the block is added to the current existing chain.

It might be possible that more than one product is being scanned at the same time. In that case, the concept of consensus [14] is used. In such cases of conflict, the algorithm verifies the longest existing chain and then that chain is selected, and the new block is added to the selected chain.

Subsequent blocks follow the same protocol. This also gives the nodes the freedom to the users to decide the other nodes in the network to be trustworthy [62].

This system creates a small network for the physical entities and connects that entity to the digital cloud. Each node has the freedom to verify the information at any point that is enabled with access to and capacity to maintain the digital network [63]. RFID tags can also be used to create the Internet of Things (IoT) in the same manner [50, 59] to increase product visibility and trust throughout the market.

4.5 LIMITATIONS OF THE DIGITAL METHOD

- As discussed earlier, the IoT established by the help of the magnetic card, readers and the blockchain system addresses the problem of identifying counterfeit products so long as the digital network covers the area.
- Many high-end pharmaceutical products do not follow the traditional supply chain with the same number of nodes or the end customer. In many cases, such drugs for cancer, are often directly delivered to the hospital administering them. in such scenarios, we need a system to verify the product when the product has already exited the digital cloud.
- In many developing and under-developed countries, there is no system to scan the labels and training the nodes to participate in the blockchain network. Most of the pharmaceutical products reaching such countries often originate in places where digital coverage is viable. But, when the product can no longer be tracked through, the nodes in the blockchain, we need a physical means of verifying the labels. Also, the information stored on the magnetic card labels can be associated tithe the physical means of verification.

- To increase the coverage and efficiency of the method, it is essential to not only make the labels reprogrammable but to also have the labeled information directly linked to the physical information being carried on the label.
- Current approaches of linear barcodes, 2-D barcodes, magnetic cards, RFID tags, can only function up to their optimum efficiency if the digital data that they contain is linked with a physical entity that we propose to be placed on the label [50].
- Also, as the surface area of the actual product, at the unit level gets smaller, it shall get more and more difficult to label more information using traditional methods. The parent package can still be authentic, while the child package can be tampered with.
- With parallel trading being an immediate challenge, there is a need to go beyond blockchain and merge both the digital and physical means of product traceability.

Subsequently, when the blockchain becomes an inherent part of supply chains, it shall become pertinent to add the DNA patch at the unit level. This can be achieved keeping in mind that with DNA patch as the identifier, we can increase the information density for any product.

In our work, we employ the use of DNA patch on the label along with re-programmable magnetic cards. The data stored on the label can be in any form, as discussed earlier. The system can be designed in such a way that the information carried with the digitally encoded magnetic stripe is related to the DNA patch. For example, the DNA sequence being used can be stored on the magnetic stripe. Since the information density for magnetic stripe cards is high, we can accommodate additional information. The following use-cases are some of the scenarios where both, the digital and the physical product tags are essential for product traceability and supply chain security.

4.6 USE CASE EXAMPLES

USE CASE 1: COUNTERFEIT PRODUCT IS INTRODUCED IN THE SYSTEM

Most counterfeit products enter the supply chain before they reach the end customer, especially in the pharmaceutical supply chain [55]. This case arises when the authentic products are removed from the original supply chain and are replaced by a counterfeit product with the same label. Since, all products, right from the manufacturing unit, have a digital footprint in from of the blockchain, the route of all the products can be verified by any participating node. When the new product is introduced and scanned, the hash for the corresponding block shall not be created as there is no preceding hash for that. In that case, the product can be identified as a foreign product. Since the blockchain is time-stamped, the exact time and the location of the node involved in the introduction of the counterfeit product can be determined within seconds. The block diagram in figure 4.5 and 4.6 represent the first use case.

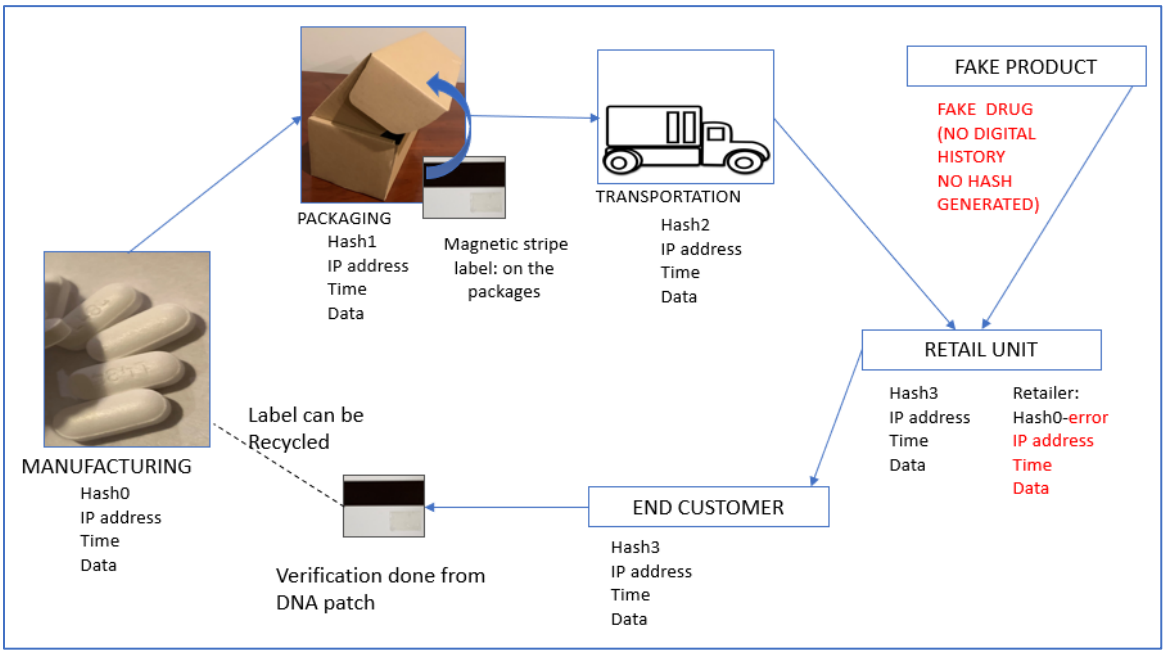


Figure 4.5 Use Case 1: Entry of fake product at any node

USE CASE 2: A COUNTERFEIT PRODUCT IS INTRODUCED AT GENESIS BLOCK

In the previous case, it is relatively easier to ascertain the location of the introduction of illegitimate products. This becomes more difficult when the false information is used to create the genesis block, thereby starting a new chain. Any subsequent node shall scan the label and add corresponding blocks to the chain without any alert messages. It is only at the end of the chain when the product reaches the end customer where it can be validated as a fake or genuine product. The digital data on the product needs to be verified. But the authenticity of the actual product shall still remain questionable. In this case, the digital traceability of the product does not guarantee the legitimacy of the product. This is where the physical DNA tag helps as the actual physical information that can provide a higher sigma level of accuracy for determining the validity of the product.

The block diagram below depicts this scenario. Each time the label is scanned, a new block is added, as the previous hash for each block exists and hence no red flags are raised. Especially in case of pharmaceutical product, this could lead to loss of life and reduce the trust of the customer in the supply chain management system.

This process is represented by the block diagram in Figure 4.7.

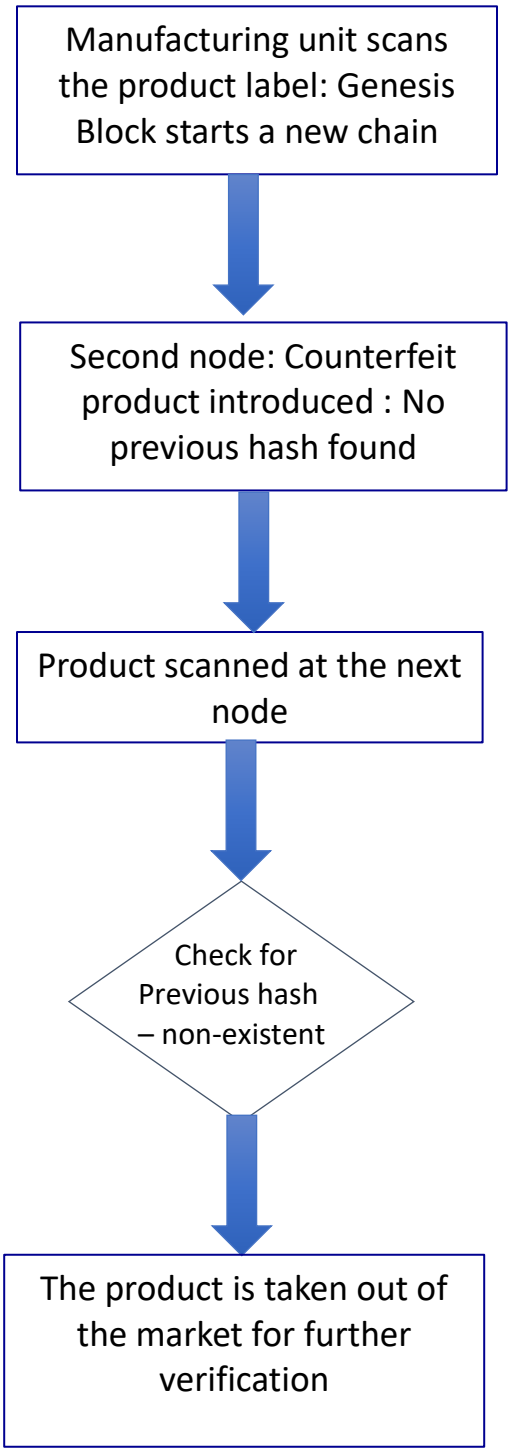


Figure 4.6 Block diagram for Use case 1

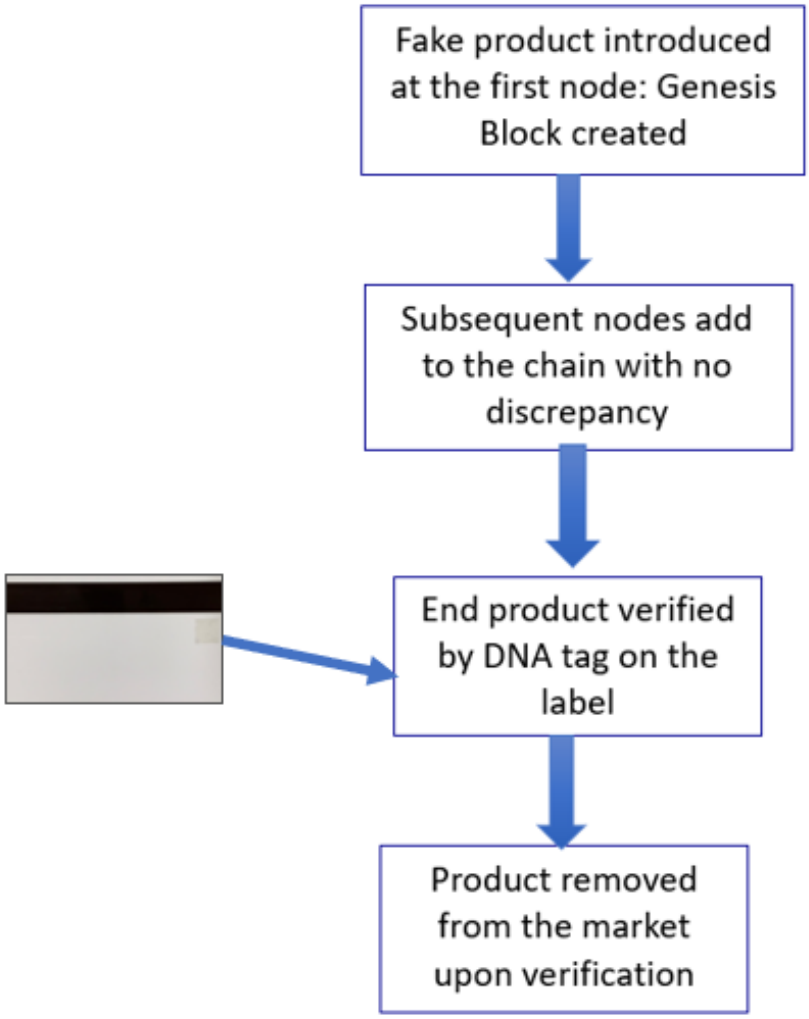


Figure 4.7 Block diagram for Use case 2

4.6.3 USE CASE 3: PARALLEL TRADING

Another major challenge the industries facing today is the problem of parallel trading [64]. Parallel trading is a term used to refer to the practice of the cross-border sale of goods outside the intended manufacturer's distribution system without the manufacturer's consent. This is especially prevalent in the pharmaceutical supply chain. Through the digital label and the blockchain system, the route of each package being moved can be traced in real-time. Here, we can make use of the

re-programmability of the labels. Systems can be put into place to add identifiers to the label as the goods cross borders. Then the blockchain traces the package. In case the package is replaced with the one, not in the system, or a mislabeled package, the subsequent node scanning the data shall not be able to add new block similar to use case 1. In the scenario that the label is read successfully, and the nodes are unable to trace the mislabeled products, the physical data on the package can be verified, similar to use case 2. The DNA tag on the package should match that of the manufacturer's to be stored in a central database. If the physical tag also matches, then the extensive investigation is required. But if the physical and the digital entries do not match the manufacturer's or the parent company's database, the product shall be recalled. In this manner, the digital tracking system along with the physical tag on the label give a higher sense of product authenticity and safety. Figure 4.8 shows the process of parallel trading/retail arbitrage. The block diagram in figure 4.9 explains how the proposed method shall help to limit the practice of parallel trading.

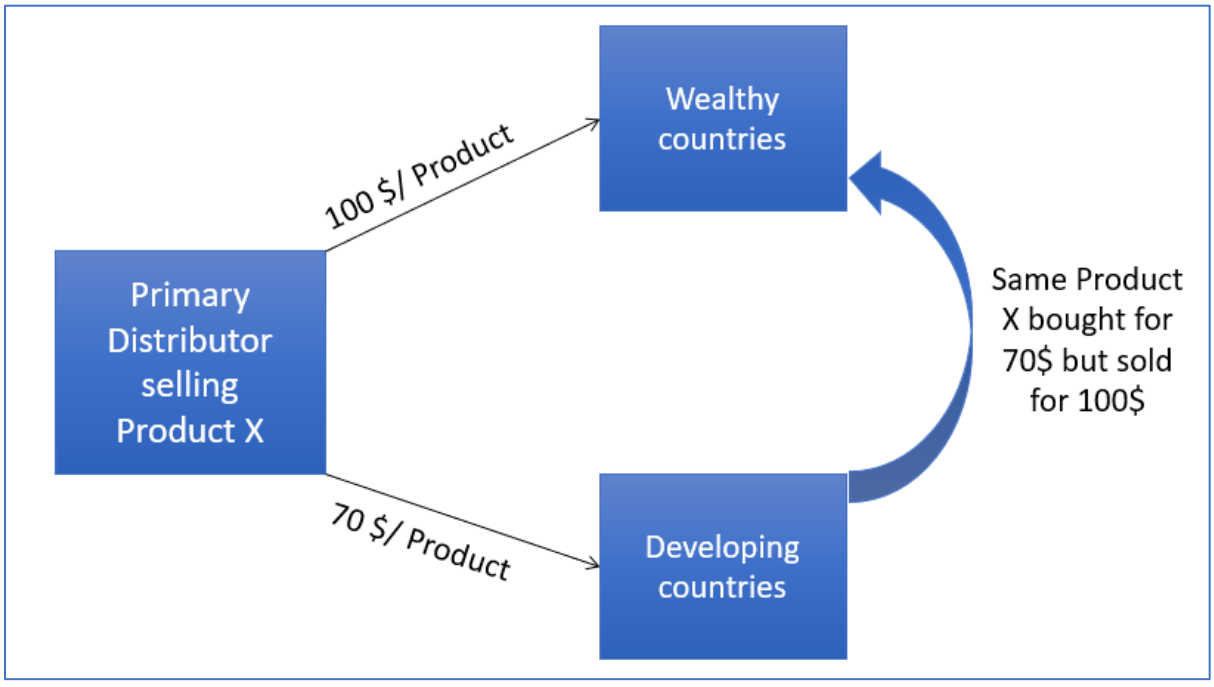


Figure 4.8 Retail arbitrage/Parallel trading in effect

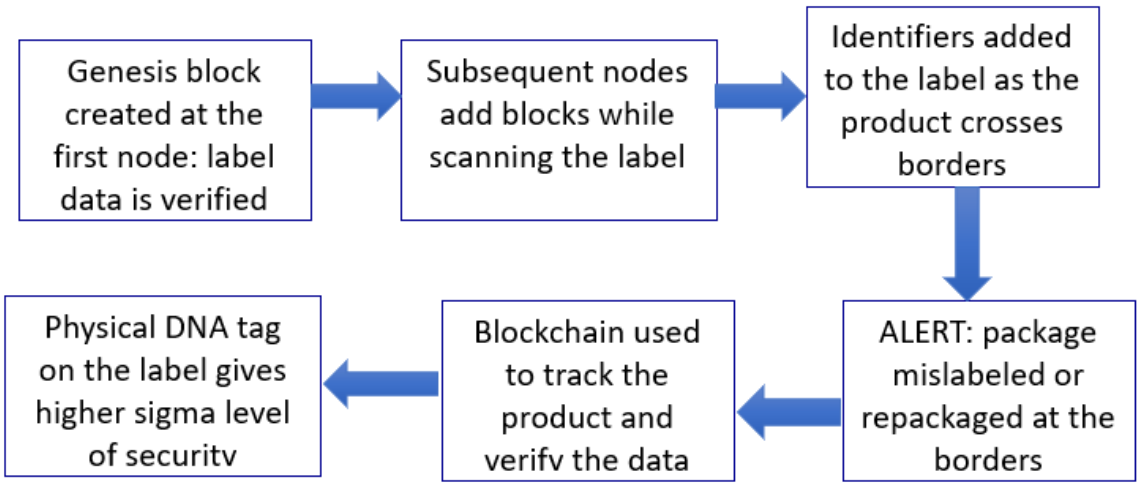


Figure 4.9 Digital plus the physical means of verification to counter parallel trading

In these cases, the re-programmability of the magnetic stripe card labels become extremely crucial. Within a supply chain (network), crucial nodes shall be identified, for example border patrol units. These nodes should be given the authority to change the information on the magnetic label. As mentioned above, the information is linked to the DNA sequence used in the physical tag (say ACTGACTG). Coded information can be added before or after this number to mark the entry/exit of the products. Different border patrols can be encoded and only those data points need to be saved into the central database. This method, being easy, also may then be extremely helpful in tracking the products even after they leave the country of production.

4.7 MATERIALS AND METHODS

1. The card printer: In our work, for experimental purposes, we used the Zebra ZC100 model of magnetic card printers. The information can easily be written on to the card enabling encoding as well. This also allows us to create the database as the records are added and new cards are printed. The advanced versions of the printer can also be used which allow the user the option of using MS Excel for database management.

2. The magnetic stripe cards and readers: For the purpose of our study, we used the magnetic card reader, MSR206U [33]. The cards used were both high coercivity cards and low coercivity cards. The user interface application for the magnetic card reader can be used to read, write and/or erase the data from the magnetic stripe. This can also be done by the means of any programming language like C++ and Python (few among many). The reader can be connected to any personal computer via the USB or the RS232 cable. The data read is stored on the computer.

Figure 4.10 The magnetic card reader, MSR206U

3. The Blockchain algorithm: Saving the data on to the machine follows the magnetic stripe label read from the above-mentioned reader. The scope of the study can be extended to design machines dedicated for this purpose. This information is then used as the basis or the source of information for the first/genesis block of the intended blockchain. Subsequent readings of the label follow the same procedure to add blocks to the existing chain. Any added block has the information about the node in the form of the node identifier, which is unique for any given node and does not change if the same node adds multiple times.

The nodes all agree on the Proof of Work, which is the consensus algorithm in any blockchain network. The consensus is required to determine the valid chain when multiple nodes are functioning at the same time. In a conventional blockchain network, the Proof of Work (PoW) [8] is required for mining purposes, which is a means of establishing the current state of affairs. But this is a requirement where the whole system is virtual, as is in case of cryptocurrencies [7]. To access the blockchain, the participating node has to access the localhost through which all the nodes are connected. Any nodes can then, view the existing chain or add to the chain.

Figure 4.11 Example of what the actual blockchain looks like

4. The DNA label: The label in our study is the magnetic card with the encoded information on it. The DNA sequence or part of it cannot be duplicated. A known DNA standard from Salmon testes (Sodium salt) was used. It should be kept in mind that this DNA was used because of the ease of access in the lab environment. For the purpose of mass production

for labeling products, DNA from any other source can be used. This shall especially be helpful in situations where accessing the product route through the virtual cloud is not possible.

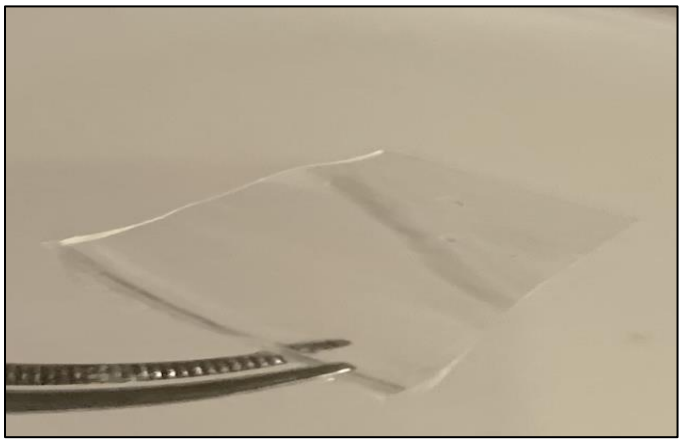


Figure 4.12 The DNA patch to be placed on the label

The DNA patch was synthesized by using Poly Vinyl Alcohol. Briefly, 7 grams of PVA was dissolved in 100 ml of water and mixed on a magnetic stirrer for 3 hours. Following this, 100 microliters of DNA (1800 nanograms/microliter) was added and stirred for 4 hours. The mixture was then cast on a Petri dish and frozen at -20 degree C for 12 hours after which it was placed at room temperature for 12 hours. The freezing and room temperature storage of the film was repeated for 2 more cycles [65].

DNA Extraction from the film:

To extract the DNA, a small piece of the film was cut and placed in a microcentrifuge tube filled with 1ml DI water. After approximately 2 hours of incubation, 500 microliters from the sample was purified using a purification kit (Qiagen). The sample was run on a 1% agarose gel and run at 120V for 20 minutes. The gel was visualized by exciting at a UV source of 365 nm (Axygem Imaging Station). The Figure 4.14 shows the placement of the DNA patch synthesized on to the

magnetic stripe card labels. The labels shall then be placed on the product packages as per the requirement.

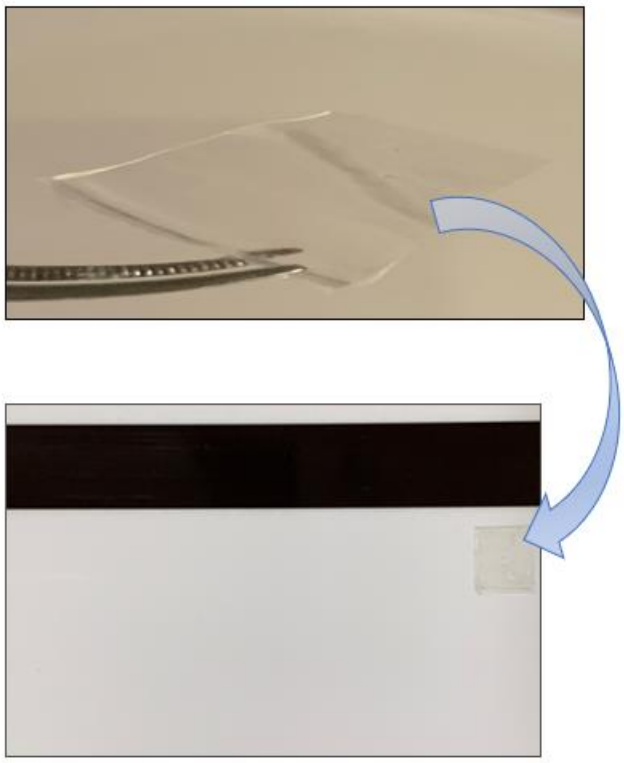


Figure 4.13 The DNA patch as shown on the label

4.8 EXPERIMENTAL RESULTS

The magnetic cards were printed on with the magnetic stripe using the Zebra ZC100 magnetic card printer. The DNA patch was placed under the magnetic stripe so that one does not interfere or damage the other. The magnetic stripe can be read, and the information encoded on it can be modified, or new information can be added on to it as per requirement. The magnetic stripe card with the magnetic stripe and the DNA patch is shown in Figure 4.14.

Figure 4.14 The magnetic stripe card with the DNA patch below it.

The data on the magnetic stripe can be read, and new data can be written on the stripe as per requirement. Figure 4.15 shows the information from the magnetic card being read. Figure 4.16 shows, the writing operation is done on the same card. The supply chain can be designed in such a manner that certain important nodes are identified and have the authority to alter the information contained on the card. The idea behind this is to use the property of re-programmability of magnetic stripes to identify critical points in the supply chain and take preemptive measures against the introduction of counterfeit products.

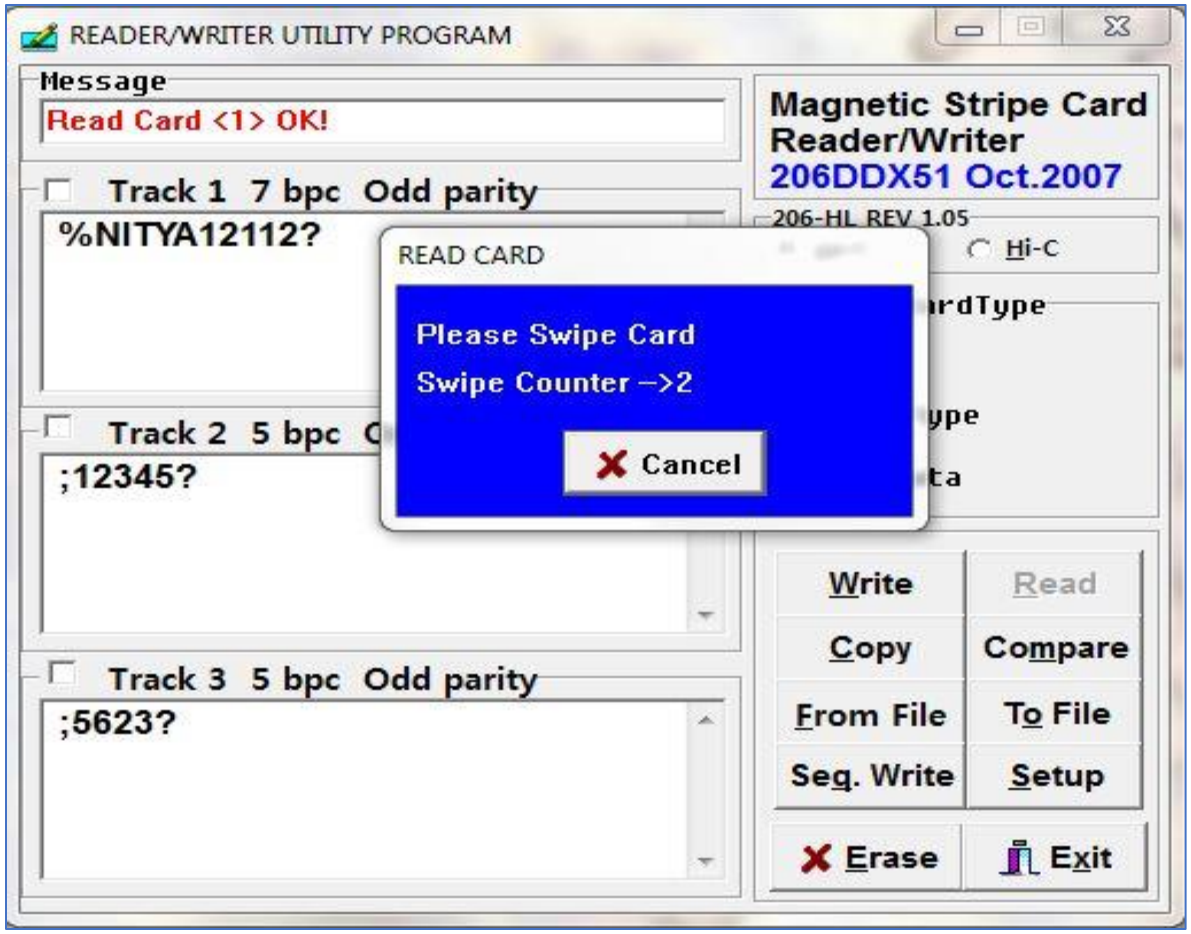


Figure 4.15 Reading the data on the card

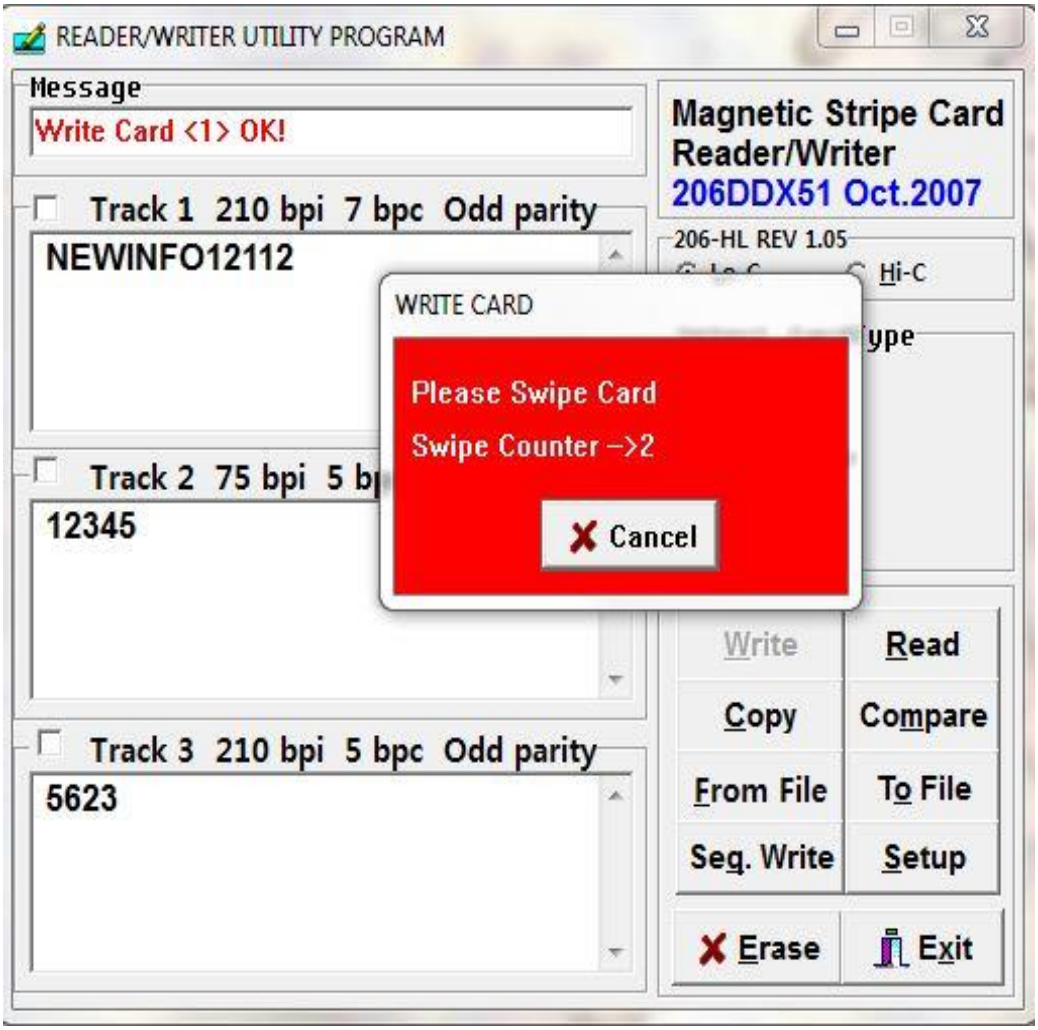


Figure 4.16 The data on the magnetic card can be modified

The data on the magnetic card can be saved in the form of a text file. The python code then takes the text file to add the next block. In this manner, a new text file is saved on to the computer scanning the magnetic stripe. The aim of adding the text file is that the data being read can be saved on the machine for swift verification. The idea is to track the product via the blockchain, verify the data on the machine in case of dispute and then to resolve the dispute with the verification of the physical DNA tag present on the label. These three points of verification give a better level of security and traceability throughout the supply chain. Before the card is scanned to

execute the blockchain code, no genesis block exists to start the blockchain. When the localhost is accessed, no block is displayed, and a blank chain is displayed. This is shown in Figure 4.17.

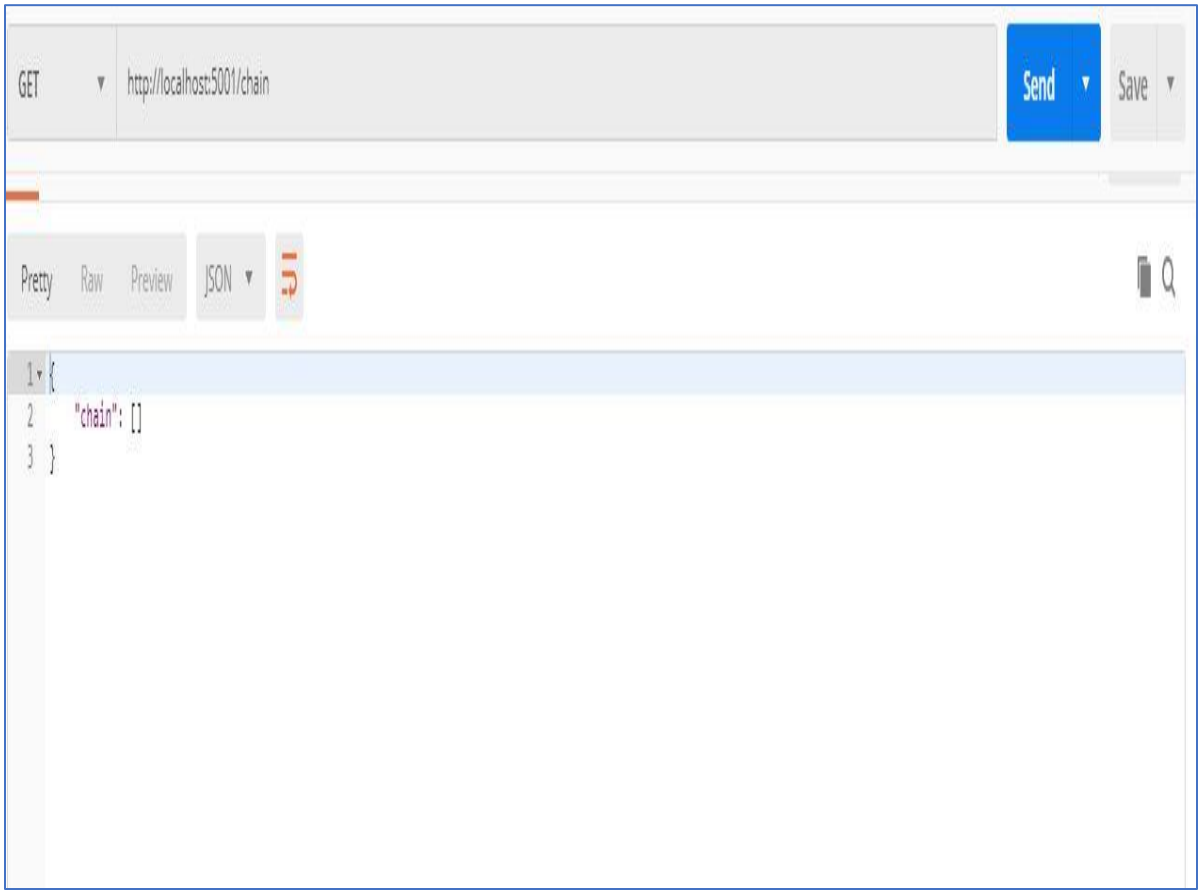


Figure 4.17 The blockchain with no blocks added: broadcast from a localhost

The data on the card is modified to represent the DNA sequence and the serial number of the product. One such text file is shown in Figure 4.18. This text file can then be used for creating the genesis block for the blockchain. The data in the text file should match the serial number from the database. When the same label is scanned at another node, the data is again saved in the form of the text file. This becomes the basis for the next block and so on. One such text file with the possible information to be saved is shown in Figure 4.19

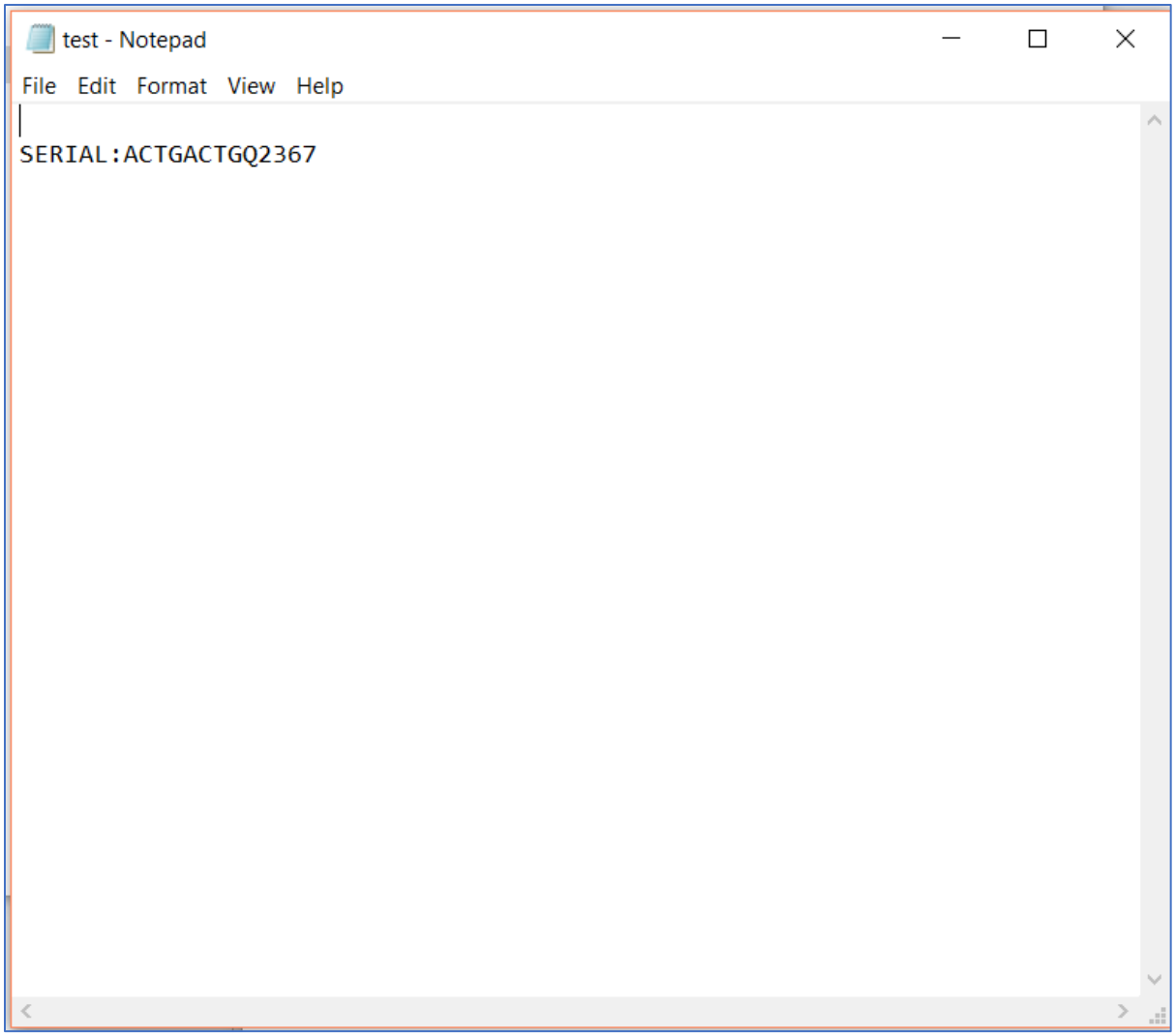


Figure 4.18 The stored text file for the blockchain system with the product's serial number along with the DNA sequence used in the patch.

After the first scanning of the card, the genesis block is created and the text file for this block is saved on the machine. This text file contains the hash generated along with the information in the previous block, the IP address of the machine and the node identifier. This information can further be verified from the data in the blockchain. Hence, there are two points of verification for the node identifiers with the time stamp. This is represented in Figure 4.16.

```
{
  "chain": [
    {
      "file_hash": "9fd6484cc85553d0c8e2b744b33358cebf1504eeaf608cd22e6f1d0f3170a597\n",
      "index": 0,
      "ip_address": "10.0.0.135\n",
      "node": "3f8d8e7acd9e40b8b998a5ae1490357b\n"
    }
  ]
}
```


```
9fd6484cc85553d0c8e2b744b33358cebf1504eeaf608cd22e6f1d0f3170a597
10.0.0.135
2019-08-07 08:41:36.695796
SERIAL:ACTGACTGQ2367

3f8d8e7acd9e40b8b998a5ae1490357b
```

Figure 4.19 The text file corresponding to the genesis block

Figure 4.19 shows the blockchain display after the first node adds the genesis block. This block can be accessed for reading function by all the nodes/ports in the network, that is the intended supply chain. For different products, different supply chains can be followed.

```
{
  "chain": [
    {
      "file_hash": "9fd6484cc85553d0c8e2b744b33358cebf1504eeaf608cd22e6f1d0f3170a597\n",
      "index": 0,
      "ip_address": "10.0.0.135\n",
      "node": "3f8d8e7acd9e40b8b998a5ae1490357b\n"
    }
  ]
}
```


Figure 4.20 The first block added. Note the node identifier is mentioned

Figure 4.21 displays the blockchain when the same node creates the second block. The block identifier remains the same, as does the IP address. The hash changes. This is because the time instant for the addition of the block to the chain is different for the two blocks even though the same node adds them. The node identifier remains the same. If the IP address of the machine seems to be insufficient data to determine the addition of the block to the chain, the node identifier adds to the authenticity of the node. In this manner, not only the products can be tracked, but also, the actions of the nodes are accounted for.

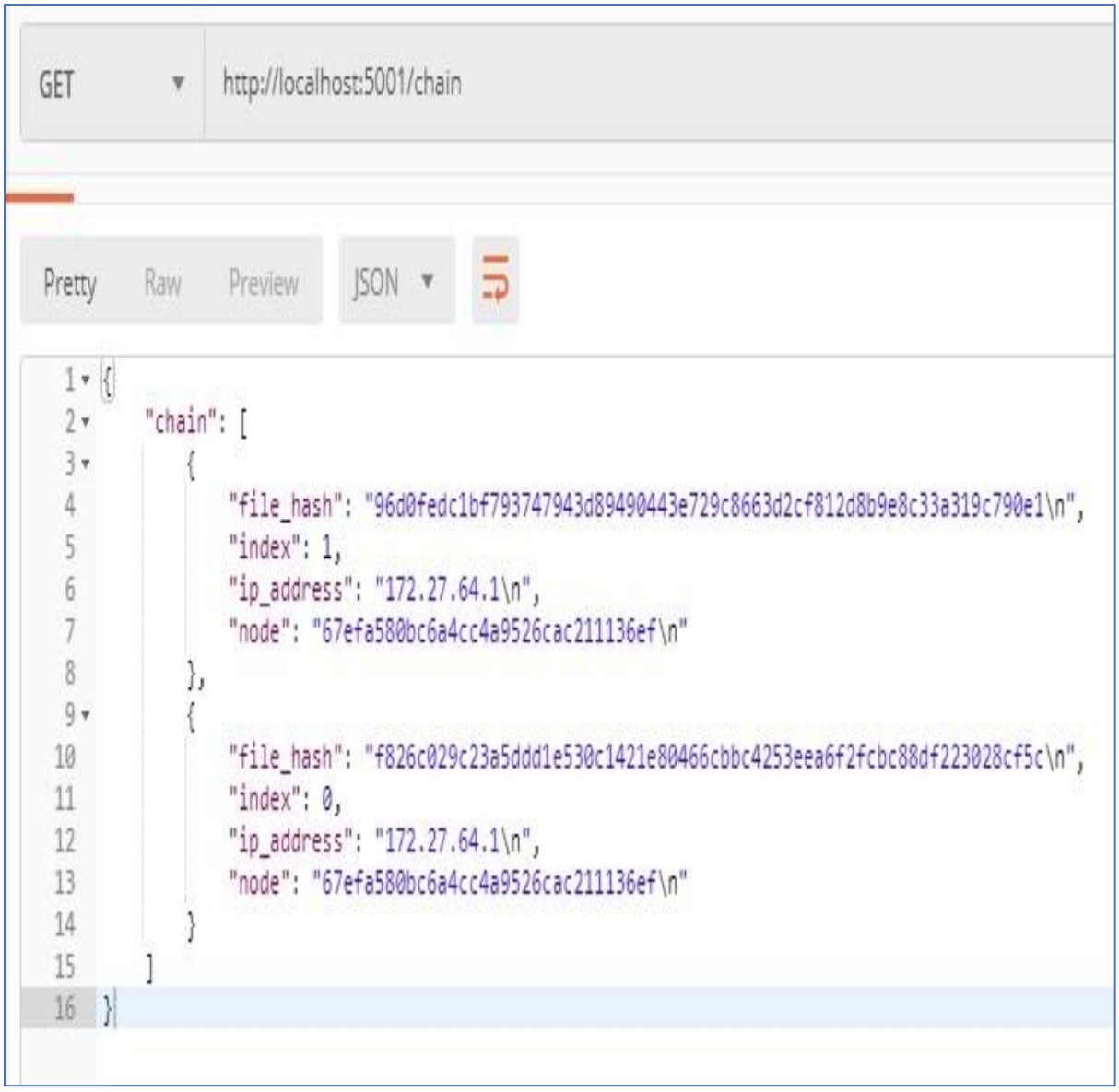


Figure 4.21 Multiple blocks added from the same node

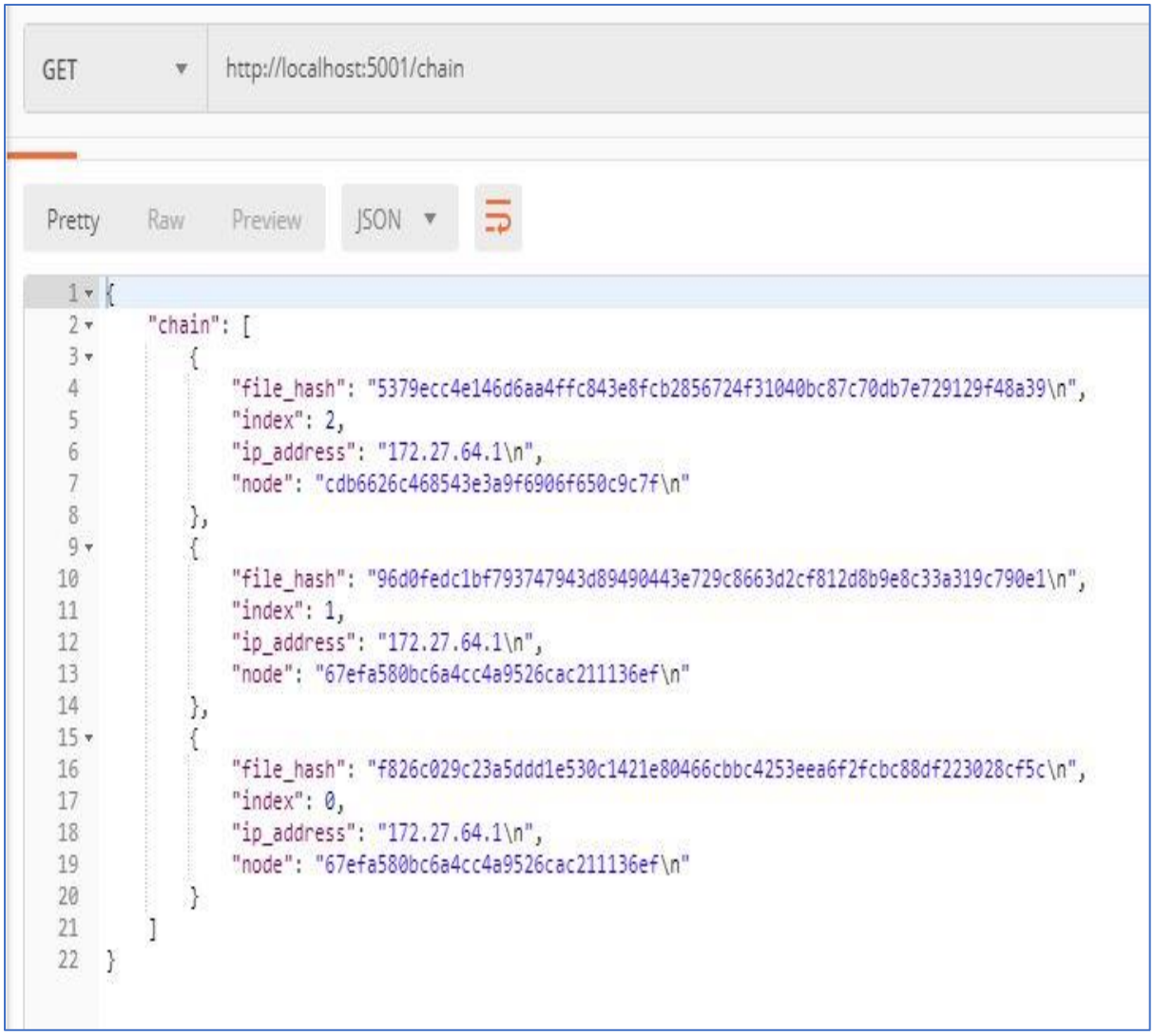


Figure 4.22 Different nodes participating in the blockchain

Figure 4.22 displays the blockchain with two nodes participating in the network. The node identifiers for the different nodes are different and unique. The actual location coordinates can be chosen to be displayed on the screen as well. In this manner, each node is accounted for along with digital product tracking in real-time. The hash generated each time is different. If the same node creates more than 1 block in the chain, then the hash and index of the block will be different, keeping the node identifier and the IP address of the node same.

Figure 4.22 depicts the blocks added to the chain from the same node. Note that the node identifier remains the same as well as the IP address. But since the time instance of the execution of the code is different, a new block is added to the chain with a new hash and incremented the index. In case a separate label is read for which the previous hash does not exist, then that block is not added to the existing chain as shown in Figure 4.23. This will start a new chain. Since this is not added at the manufacturer's IP address, or the node, this product can be tracked by each node instantly. This not only helps us to track the product but also increases transparency in the supply chain. In case this product is introduced at the first legitimate node, the data should be verified with the help of the text file saved and the database information.

Figure 4.23 Block with index 0 created if introduced from outside the supply chain, with no preceding hash present

Now, in case of dispute over the authenticity of the products, the DNA patch on the labels can be verified. The information on the magnetic stripe labels have to be linked to the DNA sequence used to formulate the physical tag. This can be seen in the Figure 4.24.

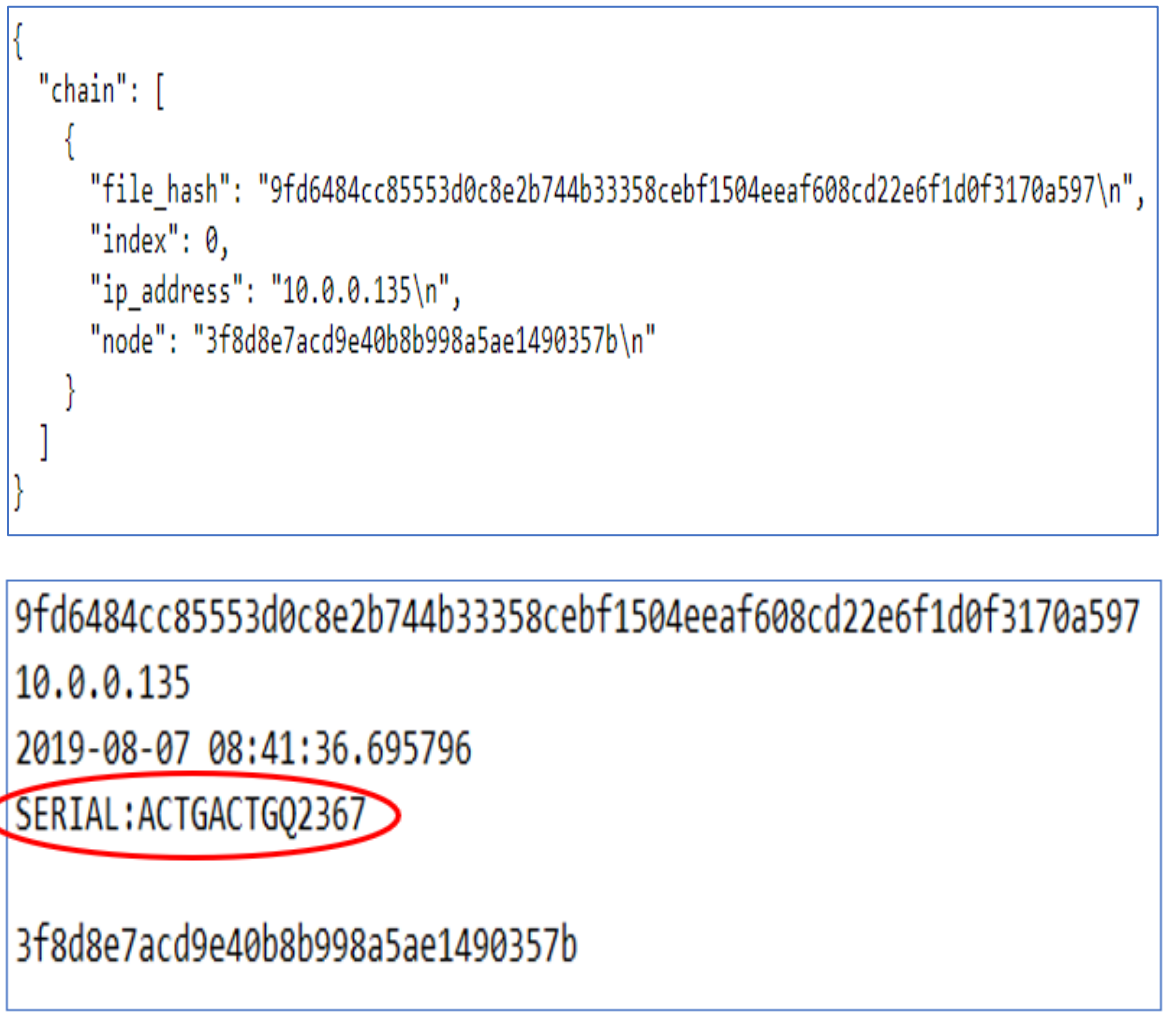


Figure 4.24 The encircled SERIAL number contains the partial DNA sequence

One means of information verification is through the stored data on the magnetic card label. the other ultimate test for authentication is the DNA patch verification for the presence of DNA. This was achieved by the method of gel electrophoresis. The results of the extracted DNA were viewed under the influence of UV light. This is shown in Figure 4.26. Lane 1 consists of a DNA ladder, lane 2 consists of DNA control and lane 3 consists of an extracted DNA sample from the

PVA/DNA film. As a control, pure PVA film without DNA was tested (lane 4). As can be seen, no fluorescence was observed.

Figure 4.25 DNA verification by Gel electrophoresis

The DNA patch is easily verified after the digital footprint is rendered insufficient to maintain the authenticity of the product. Combining both the digital and physical means of verification gives a higher level of authentication and security. The Figures 4.26 and 4.27 re-iterate the importance of DNA tags to enhance the security level for different products. Different DNA sequences may be used to produce different solutions for the PVA film to identify and secure the products more conveniently.

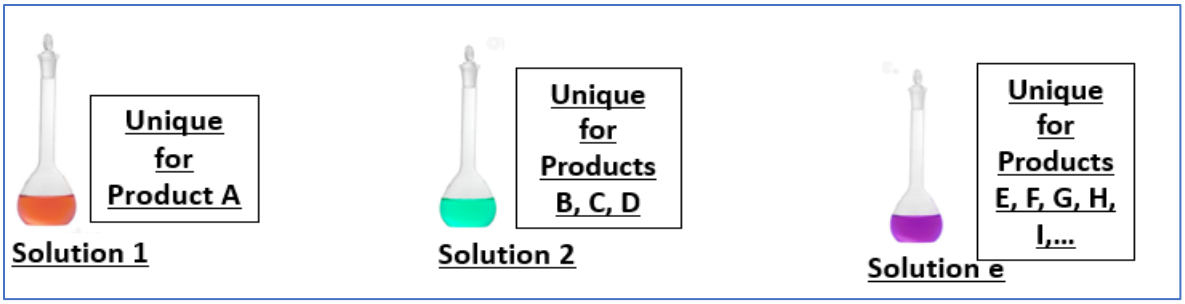


Figure 4.26 DNA patch for enhanced security levels

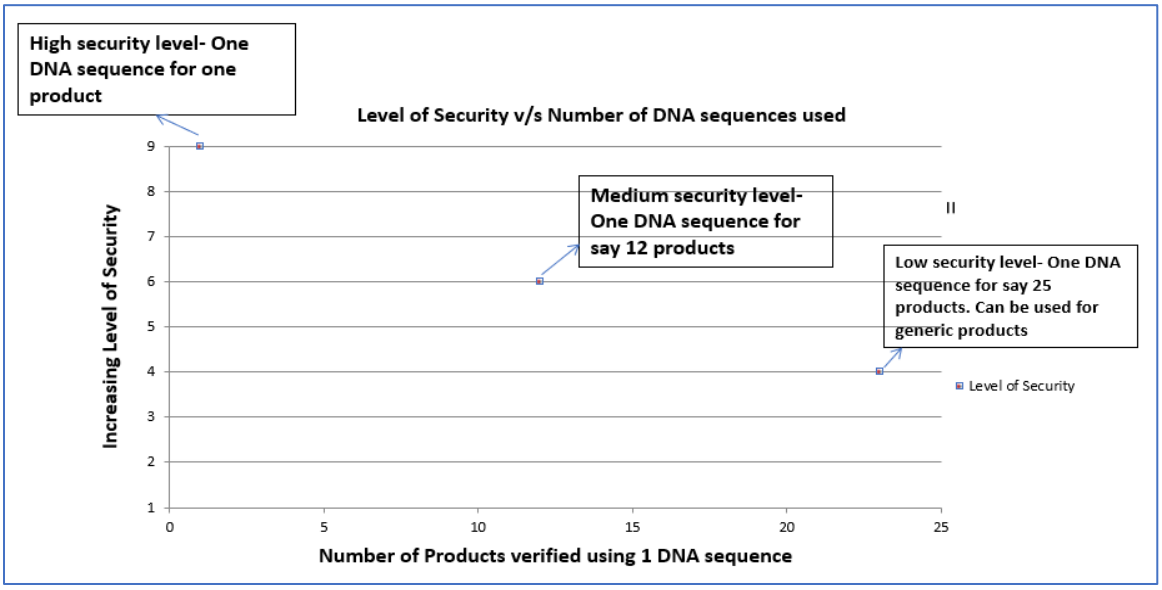


Figure 4.27 Different Security levels for different products

The enhanced security levels for different products can also be applied to different parts of the same product. This method can also be used to differentiate between “assembled in” products and “made in” products. This is because many product parts are made in various countries and then shipped for assembly at a different node possibly in a different country. This method then helps us not only to differentiate the nodes but also do the differentiation based on the action of the node. This is made possible by the physical tag on the product/product part, which can easily be verified by the digital data on the label and blockchain.

5. CONCLUSION AND FUTURE WORK

The objective of this study was to devise a new method to enhance traceability and security of the products in any supply chain. With the re-programmable magnetic cards, we can add/erase/create new sets of information points as per the need of the hour. This cannot be achieved with linear and 2-D barcodes. The DNA patch can be attached to the label, irrespective of the size. The verification of the DNA patch after the nodes have scanned the card, proves that the patch contains DNA whose information can be verified with the help of the central database. The use of magnetic cards is cheaper than the use of RFID tags and smart cards, making it optimal for the use in product tracking. The blockchain-inspired system is almost irrefutable, and the hashes cannot be decrypted in the backward direction. Figure 5.1 shows the proposed magnetic card labels that can be implemented in a supply chain. Here, both the physical and digital tags have been placed on the same label. Packaging labels having magnetic stripes and DNA label can be manufactured using the existing printing technology.

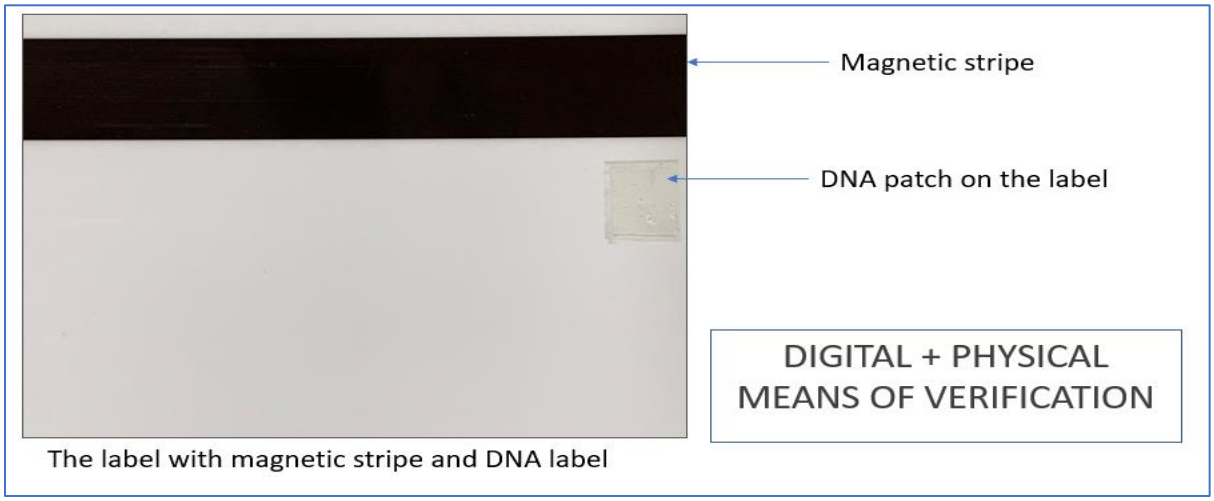


Figure 5.1 Digital and Physical tag to be placed on the same label

Now, in case the surface area of the product decreases, the magnetic label shall get smaller and smaller. Proximity cards can then be used to read the data. In this case, the use of barcodes and QR codes and RFIDs will get very limited. We will need the physical tag to contain more information. This makes the use of DNA patches even more important, as it is unique and has high information density. This can be placed at the unit level, especially for high priority products. Hence, by means of this study, we have established an optimum method to counter the effects of counterfeiting in a given supple chain. It should noted that this method can be used in all the industries for all types of products. Figure 5.2 shows the combination of digital information with blockchain and then combined with the physical tag to give us the proposed magnetic stripe card label.

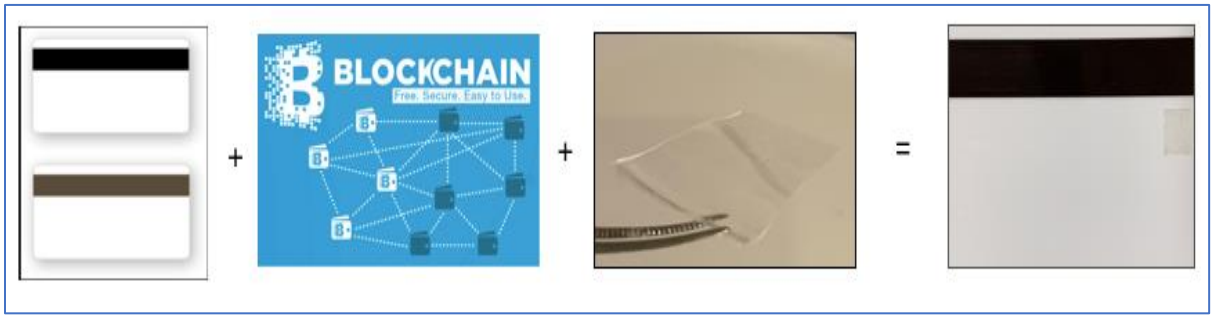


Figure 5.2 Digital information coupled with blockchain and physical tag

This method is both cost effective and easy to implement. These are two of the major criteria which affect the practicality of any method before it can be used for commercial purposes. In addition to this, the proposed method uses blockchain AND DNA patch as the identifier. Both these components are almost impossible to duplicate and are possibly the most secure means of storing information. The information on the physical tag (DNA sequence) can be added to the digital information carried by the magnetic stripes. This is coupled with the blockchain technology, which makes it very secure and transforms this information into hash. Due to this property of the proposed

method, not only are the digital and physical information points linked together, but the information is also encrypted and cannot be seen by anyone outside the network. Figure 5.3 depicts how a product carries the magnetic stripe label which connects the PVA patch containing the DNA information to the blockchain backbone.

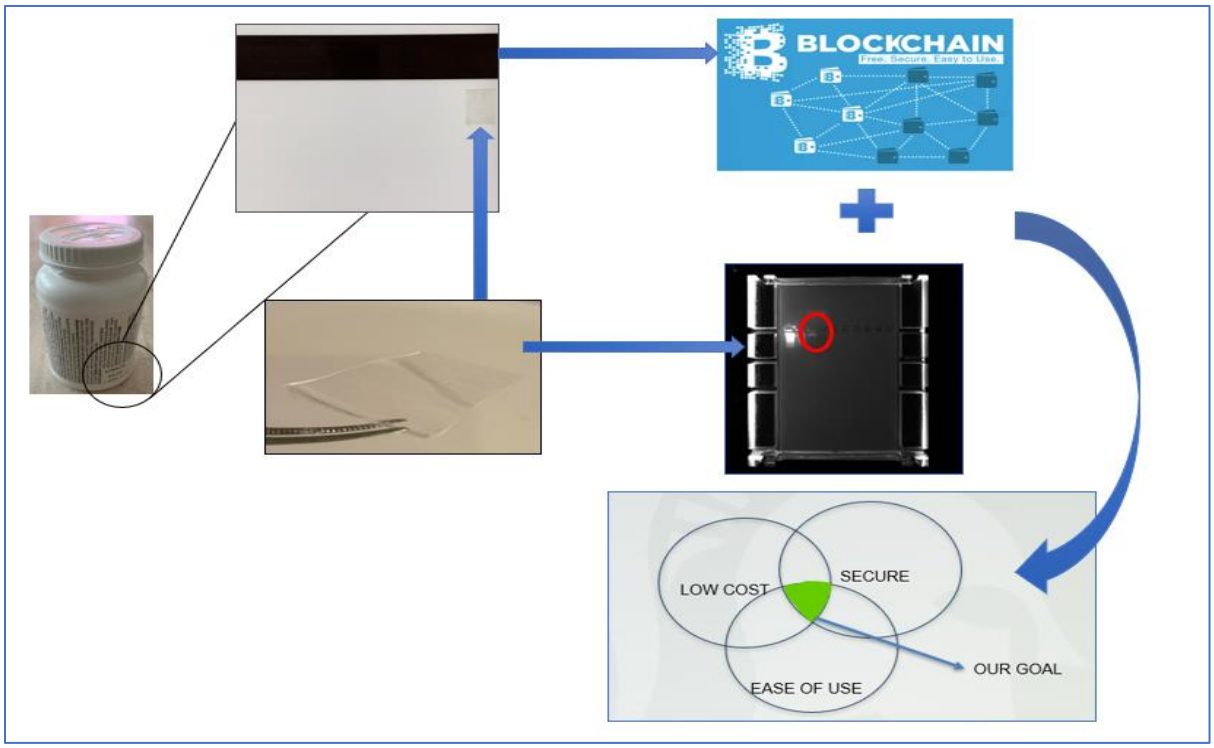


Figure 5.3 The DNA patch and blockchain are coupled with the magnetic stripe label

This means of coupling has not been studied before. The physical tags are resilient to damage and since the DNA is enclosed within the PVA film, it is not exposed to environmental factors that might damage the DNA sequence. Also, while making the PVA film, the DNA concentration is uniform, hence, any part of the film can be taken to verify the presence of DNA. The patch can also be made as transparent and as opaque as per requirement. This study combined the aspects of

cost effectiveness, security and ease of implementation to achieve our goal of better product traceability and security along the supply chain.

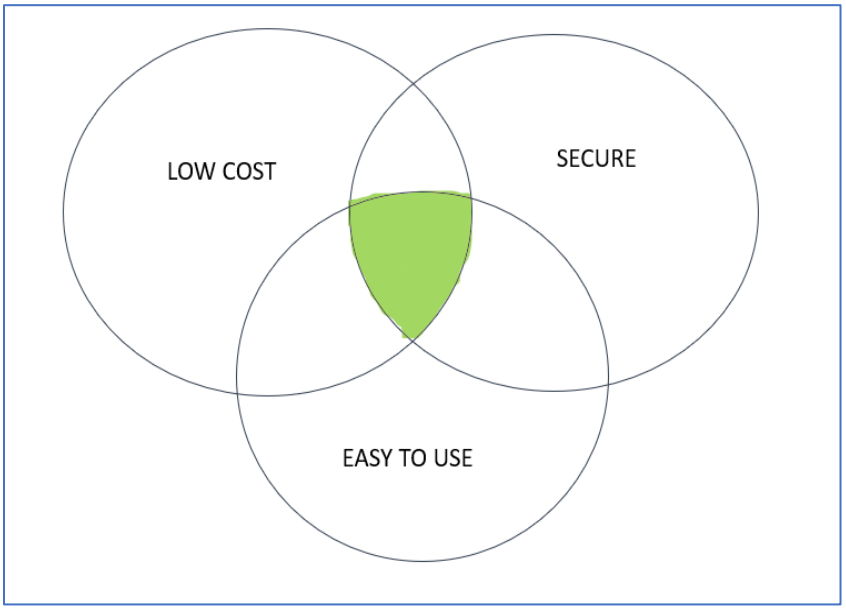


Figure 5.4 Practical, cost-effective, secure method of product authentication

More research needs to be done to prove the viability of the technology at a global level. We have suggested the use of physical tagging of the products along with digital tracking. Especially in the case of pharmaceutical products, the units (the actual drug) can be very small to print tags. The magnetic stripe with the DNA patch shall go hand in hand for complete verification. In cases, where the digital footprint of the product is not available, the physical DNA patch is one of the most reliable means for product validation. Figure 5.1 shows the scope of implementation of the proposed work. This is especially important where the digital monitoring is rendered limited. In any case, the physical tag is additionally helpful to prove the authenticity of the products.

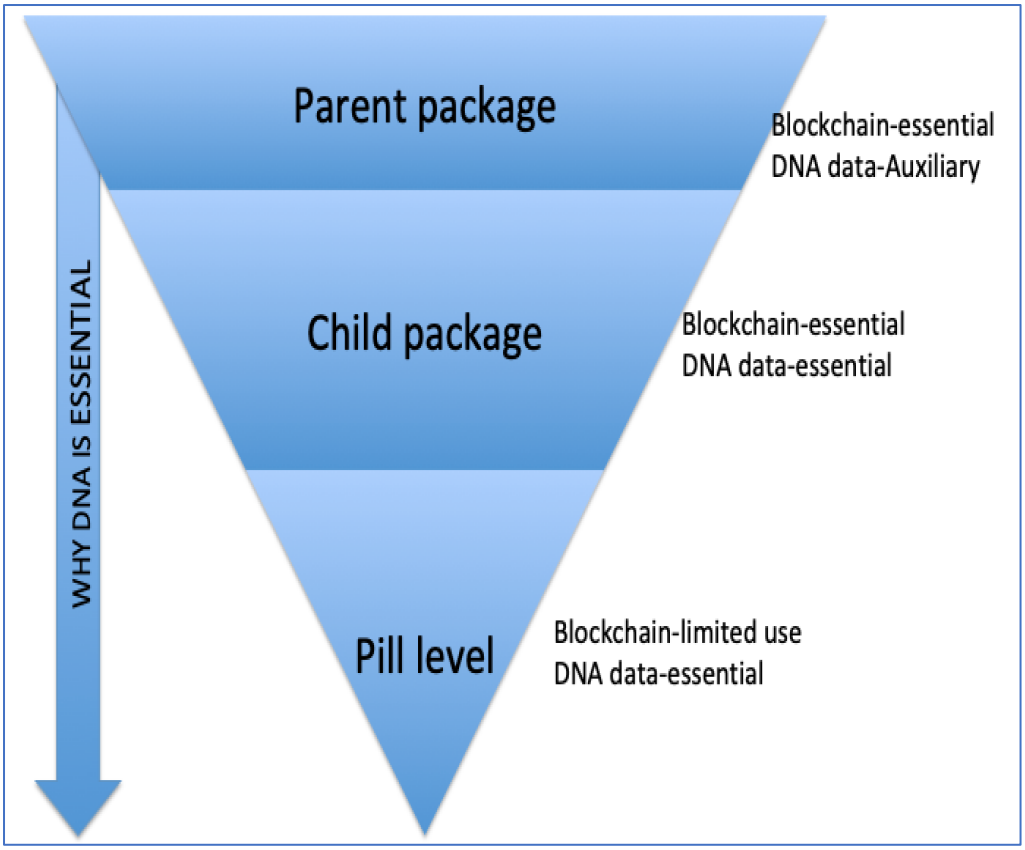


Figure 5.5 Scope of the implementation of the proposed work

The blockchain system can be customized for different products, depending upon their demand and sensitivity. For high-end pharmaceutical products, can be made to carry separate DNA patches than, say, an aspirin. Also, for products catering to the defense industry, follow different nodes and can be made to carry multiple DNA patches for extra levels of security. The access to the text files saved on the machines shall be made limited to only a select group of people. This system can be implemented across the globe to enhance security and liability throughout different supply chains. The same method can be studied further to be used in the health industry to store patient information. In such cases, the magnetic card information can be re-programmed to contain confidential patient information to be read only by designated doctors or medical agencies. Depending on the information stored, i.e. the patient history, a quick response shall be guaranteed.

This shall save crucial seconds and also shall be able to prevent misdiagnoses of patients. Since the information capacity of the magnetic stripe cards is very high, the patient history can be easily encoded and summarized for easy readability. Further research needs to be done to study the commercial practicality of this method. The scope of the application of any technology is immense especially in the era of complex computing, wireless technology and artificial intelligence. There is no limit to how the technology shall be helpful to eradicate the problem of counterfeiting across the globe.

APPENDIX

APPENDIX

PYTHON CODE FOR THE MODIFIED BLOCKCHAIN

```
import socket
from datetime import datetime
import hashlib as hasher
import hashlib
import json
from time import time
from urllib.parse import urlparse
from uuid import uuid4
import os

import requests
from flask import Flask, jsonify

hostname = socket.gethostname()
IPAddr = socket.gethostbyname(hostname)

class Block:
    def __init__(self, index, timestamp, data, previous_hash, node_iden):
        self.index = index
        self.timestamp = timestamp
        self.data = data
        self.previous_hash = previous_hash
        self.hash = self.hash_block()
        self.node = node_iden

    def __str__(self):
        return 'Block #{}'.format(self.index)

    def hash_block(self):
        sha = hasher.sha256()
        seq = (str(x) for x in (
            self.index, self.timestamp, self.data, self.previous_hash))
        sha.update(''.join(seq).encode('utf-8'))
        return sha.hexdigest()


def make_genesis_block():
    """Make the first block in a block-chain."""
```

```
    file_open = open("test.txt", "r")
    fp = read_default_file(file_open)
    block = Block(index=0, timestamp=datetime.now(), data=fp, \
                previous_hash="0", node_iden= node_identifier)
    output_file = open("Block #{}.txt".format(block.index), "w")
    create_text(block, output_file)
    file_open.close()
    output_file.close()

    return block


def next_block(last_block):
    """Return next block in a block chain."""
    data_file = open("Block #{}.txt".format(last_block.index), "r")
    file_open = open("test.txt", "r")
    data_block = read_default_file(file_open)
    idx = last_block.index + 1
    block = Block(index=idx,
                timestamp=datetime.now(),
                data=data_block,
                previous_hash=last_block.hash,
                node_iden=node_identifier)
    output_file = open("Block #{}.txt".format(block.index), "w")
    create_text(block, output_file)
    data_file.close()
    output_file.close()

    return block


def read_default_file(fp):
    line_list = []
    for line in fp:
        line_list.append(line)

    return ''.join(line)


def read_block_file(fp):
    line_list = []
    #for line in fp:
        #line = line.strip('\n')
        #line_list.append(line)
    line_list = [line for line in fp.readlines() if line.strip()]
```

```
    return line_list


def create_text(block, output_file):
    print(block.hash, file=output_file)
    print(IPAddr, file=output_file)
    print(block.timestamp, file=output_file)
    print(block.data, file=output_file)
    print(block.node, file=output_file)


# Instantiate the Node
app = Flask(__name__)

# Generate a globally unique address for this node
node_identifier = str(uuid4()).replace('-', '')

# Instantiate the Blockchain
if(not os.path.exists('Block #0.txt')):
    first_block = make_genesis_block()

#print(first_block.index)

@app.route('/mine', methods=['GET'])
def mine():
    count = 100
    while count >= 0:
        try:
            file_open = open("Block #{}.txt".format(count), "r")
            line_list = read_block_file(file_open)
            data = line_list[-1]
            file_hash = line_list[0]
            prev_block = Block(count, datetime.now(), data, file_hash, node_identifier)
            new_block = next_block(prev_block)
            file_open.close()
            break
        except FileNotFoundError:
            count -= 1
            continue
    else:
        new_block = make_genesis_block()

    response = {
        'index': new_block.index,
        'timestamp': new_block.timestamp,
        'node-identifier': node_identifier,
```

```
    }

    return jsonify(response), 200

@app.route('/chain', methods=['GET'])
def full_chain():
    count = 100
    full_chain = []
    while count >= 0:
        try:
            #print('here')
            file_open = open("Block #{}.txt".format(count), "r")
            line_list = read_block_file(file_open)
            node = line_list[-1]
            file_hash = line_list[0]
            ip_address = line_list[1]
            index = count
            list_of_data = {'index': index, 'node':  node, 'file_hash': file_hash, 'ip_address':
ip_address}
            full_chain.append(list_of_data)
            file_open.close()
            count -= 1
        except FileNotFoundError:
            count -= 1
            continue

    response = {
        'chain': full_chain,
    }
    return jsonify(response), 200


if __name__ == "__main__":

    from argparse import ArgumentParser

    parser = ArgumentParser()
    parser.add_argument('-p', '--port', default=5001, type=int, help='port to listen on')
    args = parser.parse_args()
    port = args.port

    app.run(host='127.0.0.1', port=port)
```

BIBLIOGRAPHY

BIBLIOGRAPHY

[1] A. Drug and A. Symposium, “Counterfeit Medicine In America : 2018 9 th Annual Drug Abuse Symposium,” 2018.

[2] A. Marucheck, N. Greis, C. Mena, and L. Cai, “Product safety and security in the global supply chain: Issues, challenges and research opportunities,” *J. Oper. Manag.*, vol. 29, no. 7–8, pp. 707–720, 2011.

[3] D. H. Shin, J. Jung, and B. H. Chang, “The psychology behind QR codes: User experience perspective,” *Comput. Human Behav.*, vol. 28, no. 4, pp. 1417–1426, 2012.

[4] D. Bansal, S. Malla, K. Gudala, and P. Tiwari, “Anti-counterfeit technologies: A pharmaceutical industry perspective,” *Sci. Pharm.*, vol. 81, no. 1, pp. 1–13, 2013.

[5] Satoshi Nakamato, “Bitcoin: A Peer-toPeer Electronic Cash System,” pp. 1–9, 2013.

[6] F. Tian, “An agri-food supply chain traceability system for China based on RFID & blockchain technology,” *2016 13th Int. Conf. Serv. Syst. Serv. Manag. ICSSSM 2016*, 2016.

[7] G. Wood, “A secure decentralized generalized distributed ledger,” *Ethereum*, 2018.

[8] S. Singh and N. Singh, “Blockchain: Future of financial and cyber security,” *Proc. 2016 2nd Int. Conf. Contemp. Comput. Informatics, IC3I 2016*, pp. 463–467, 2016.

[9] Z. Zheng, S. Xie, H. Dai, X. Chen, and H. Wang, “An Overview of Blockchain Technology: Architecture, Consensus, and Future Trends,” *Proc. - 2017 IEEE 6th Int. Congr. Big Data, BigData Congr. 2017*, pp. 557–564, 2017.

[10] M. Crosby, P. Pattanayak, S. Verma, and V. Kalyanaraman, “Applied Innovation Review,” *Appl. Innov. Rev.*, no. 2, pp. 5–20, 2016.

[11] M. Schöner, D. Kourouklis, P. Sandner, E. Gonzalez, and J. Förster, “Blockchain Technology in the Pharmaceutical Industry,” *FSBC Work. Pap.*, no. July, pp. 1–9, 2017.

[12] C. Woodford, “Barcodes and barcode scanners,” *Explainthatstuff.Com*, pp. 1–11, 2014.

[13] J.-C. Chuang, Y.-C. Hu, and H.-J. Ko, “A Novel Secret Sharing Technique Using QR Code,” *Int. J. Image Process.*, vol. 4, no. 5, pp. 468–475, 2010.

[14] T. Sriram, K. Vishwanatha Rao, S. Biswas, and B. Ahmed, “Applications of barcode technology in automated storage and retrieval systems,” pp. 641–646, 2002.

[15] E. Ohbuchi, H. Hanaizumi, and L. A. Hock, “Barcode readers using the camera device in mobile phones,” *Proc. - 2004 Int. Conf. Cyberworlds, CW 2004*, pp. 260–265, 2004.

[16] D. W. Jackson *et al.*, “+ (,1 2 1/,1(,” vol. 1, 2011.

[17] J. Z. Gao, L. Prakash, and R. Jagatesan, “Understanding 2D-BarCode technology and applications in M-commerce - Design and implementation of A 2D barcode processing solution,” *Proc. - Int. Comput. Softw. Appl. Conf.*, vol. 2, no. Compsac, pp. 49–56, 2007.

[18] L. Tarjan, I. Šenk, S. Tegeltija, S. Stankovski, and G. Ostojic, “A readability analysis for QR code application in a traceability system,” *Comput. Electron. Agric.*, vol. 109, pp. 1–11, 2014.

[19] J. P. Qian, X. T. Yang, X. M. Wu, L. Zhao, B. L. Fan, and B. Xing, “A traceability system incorporating 2D barcode and RFID technology for wheat flour mills,” *Comput. Electron. Agric.*, vol. 89, pp. 76–85, 2012.

[20] A. Musa, A. Gunasekaran, and Y. Yusuf, “Supply chain product visibility: Methods, systems and impacts,” *Expert Syst. Appl.*, vol. 41, no. 1, pp. 176–194, 2014.

[21] N. Sivakami, “Comparative study of Barcode, QR-code and RFID System in Libaray Environment,” *Int. J. Acad. Res. Libr. Inf. Sci.*, vol. 1, no. 1, pp. 1–5, 2018.

[22] R. Muniz, L. Junco, and A. Otero, “A robust software barcode reader using the Hough transform,” *Proc. - 1999 Int. Conf. Inf. Intell. Syst. ICIIS 1999*, pp. 313–319, 1999.

[23] S. Baik, “Rethinking QR code: Analog portal to digital world,” *Multimed. Tools Appl.*, vol. 58, no. 2, pp. 427–434, 2012.

[24] J. Rouillard, “Contextual QR codes,” *Proc. - 3rd Int. Multi-Conf. Comput. Glob. Inf. Technol. ICCGI 2008 Conjunction with ComP2P 2008 1st Int. Work. Comput. P2P Networks Theory Pract.*, pp. 50–55, 2008.

[25] V. Mornar, D. Palavra, and D. Kalpic, “Application of smart cards in distributed information systems,” *Proc. Int. Conf. Inf. Technol. Interfaces, ITI*, 2004.

[26] C.-C. Chen, Y.-L. Chen, and S.-C. Chen, “Application of RFID technology—upper extremity rehabilitation training,” *J. Phys. Ther. Sci.*, vol. 28, no. 2, pp. 519–524, 2016.

[27] V. Sukhoy, V. Georgiev, T. Wegter, R. Sweidan, and A. Stoytchev, “Learning to slide a magnetic card through a card reader,” *Proc. - IEEE Int. Conf. Robot. Autom.*, pp. 2398–2404, 2012.

[28] R. Nechushtai, M. Elit, and S. M. Systems, “(12) United States Patent,” vol. 1, no. 12, 2001.

[29] D. F. Smith, T. Donnelly, and D. J. Mapps, “High density storage on a magnetic stripe card,” *IEEE Trans. Magn.*, vol. 32, no. 5 PART 1, pp. 4025–4027, 1996.

[30] K. Krishnan Nair, “An Approach to Authenticate Magnetic Stripe Bank Card Transactions at POS terminals,” *Int. J. Cyber-Security Digit. Forensics*, vol. 7, no. 3, pp. 248–255, 2018.

[31] K. Michael, M. G. Michael, K. Michael, and M. G. Michael, “Magnetic-Stripe Cards,” *Innov. Autom. Identif. Locat. Serv.*, vol. 44, no. April 1995, pp. 116–153, 2011.

[32] J. Ferrari and R. Mackinnon, “Smart Cards : A Case Study,” *Contract*.

[33] R. Encoder, R. Card, and R. Speed, “MSR206 format,” p. 2009, 2009.

[34] R. Walker, *Clock and data recovery for serial digital communication*, no. February. 2002.

[35] A. Elsherbeni, “Recent Rfid Technology and Applications,” 2006.

[36] M. Tajima, “Strategic value of RFID in supply chain management,” *J. Purch. Supply Manag.*, vol. 13, no. 4, pp. 261–273, 2007.

[37] K. Michael and L. Mccathie, “The pros and cons of RFID,” *Strateg. Dir.*, vol. 21, no. 5, pp. 24–26, 2005.

[38] D. Hahnel, W. Burgard, D. Fox, K. Fishkin, and M. Philipose, “Mapping and localization with RFID technology,” pp. 1015-1020 Vol.1, 2004.

[39] J. Landt, “The history of RFID,” *IEEE Potentials*, vol. 24, no. 4, pp. 8–11, 2005.

[40] “63_02635570710723804.pdf.” .

[41] P. Sorrells, “Passive RFID Basics,” *Microchip Technol. Inc*, pp. 1–7, 2002.

[42] S. Preradovic, N. Karmakar, and I. Balbin, “RFID Transponders,” *IEEE Microw. Mag.*, vol. 9, no. 5, pp. 90–103, 2008.

[43] S. Rahman, S. Khan, S. Waters, and L. Yang, “Factors affecting radio frequency identification technology implementation: A comparative study of australian and chinese supply chains,” *24th Australas. Conf. Inf. Syst. ACIS2013*, pp. 1–12, 2013.

[44] R. Cited and U. S. P. Documents, “United States patent,” *Geothermics*, vol. 14, no. 4, pp. 595–599, 1985.

[45] M. . Paridah, A. Moradbak, A. . Mohamed, F. abdulwahab taiwo Owolabi, M. Asniza, and S. H. . Abdul Khalid, “We are IntechOpen , the world ’ s leading publisher of Open Access books Built by scientists , for scientists TOP 1 %,” *Intech*, vol. i, no. tourism, p. 13, 2016.

[46] M. Aigner and M. Feldhofer, “Secure Symmetric Authentication for RFID Tags,” *Telecommun. Mob. Comput. -- TCMC 2005*, 2005.

[47] S. Preradovic *et al.*, “Multiresonator-Based Chipless RFID System,” *IEEE Trans. Microw. Theory Tech.*, vol. 57, no. 5, pp. 1411–1419, 2009.

[48] W. Yao, C. H. Chu, and Z. Li, “The use of RFID in healthcare: Benefits and barriers,” *Proc. 2010 IEEE Int. Conf. RFID-Technology Appl. RFID-TA 2010*, no. June, pp. 128–134, 2010.

[49] M. Attaran, “RFID: An enabler of supply chain operations,” *Supply Chain Manag.*, vol. 12, no. 4, pp. 249–257, 2007.

[50] E. Lansing, “ro,” 2008.

[51] H. Chien, J. Jan, and Y.-M. Tseng, “Solution to Remote Authentication : Smart Card,” *Comput. Secur.*, vol. 21, no. 4, pp. 372–375, 2002.

[52] O. Linton, “Smart Card,” *Acad. Radiol.*, vol. 17, no. 11, p. 1455, 2010.

[53] X. Leng, “Smart card applications and security,” *Inf. Secur. Tech. Rep.*, vol. 14, no. 2, pp. 36–45, 2009.

[54] L. a Mohammed, A. R. Ramli, and V. Prakash, “Smart Card Technology : Past , Present , and Future,” *Int. J. Comput. Internet Manag.*, vol. Vol. 12, no. 1, pp. 12–22, 2004.

[55] R. Koh, Schuster, Ew Edmund W, I. Chackrabarti, and A. Bellman, “White paper: securing the pharmaceutical supply chain,” *AUTO-ID CENTER, Massachusetts Inst. … …*, 2003.

[56] BASCAP, “Responsibilities of intermediaries: piracy in the supply chain advocacy,” no. Março, pp. 1–108, 2015.

[57] T. Ahram, A. Sargolzaei, S. Sargolzaei, J. Daniels, and B. Amaba, “Blockchain technology innovations,” *2017 IEEE Technol. Eng. Manag. Soc. Conf. TEMSCON 2017*, no. 2016, pp. 137–141, 2017.

[58] L. S. Sankar, M. Sindhu, and M. Sethumadhavan, “Survey of consensus protocols on blockchain applications,” *2017 4th Int. Conf. Adv. Comput. Commun. Syst. ICACCS 2017*, 2017.

[59] A. Gowthaman and M. Sumathi, “Performance study of enhanced SHA-256 algorithm,” *Int. J. Appl. Eng. Res.*, vol. 10, no. 4, pp. 10921–10932, 2015.

[60] Product Identifier Requirements Under the Drug Supply Chain Security Act, “Product Identifier Requirements Under the Drug Supply Chain Security Act –Compliance Policy Guidance for Industry,” no. September, p. Online, 2018.

[61] L. Atzori, A. Iera, and G. Morabito, “The Internet of Things: A survey,” *Comput. Networks*, vol. 54, no. 15, pp. 2787–2805, 2010.

[62] I. Haq and O. Muselemu, “Blockchain Technology in Pharmaceutical Industry to Prevent Counterfeit Drugs,” *Int. J. Comput. Appl.*, vol. 180, no. 25, pp. 8–12, 2018.

[63] S. Cuomo, P. De Michele, A. Galletti, and G. Ponti, “A Numerical Approach for Assigning a Reputation to Users of an IoT Framework,” *Procedia Comput. Sci.*, vol. 98, pp. 455–460, 2016.

[64] P. Kanavos, D. Gross, and D. Taylor, “Parallel trading in medicines: Europe’s experience and its implications for commercial drug importation in the United States,” no. June, 2006.

[65] A. J. M. Valente, S. M. A. Cruz, M. C. Morán, D. B. Murtinho, E. C. Muniz, and M. G. Miguel, “Release of DNA from cryogel PVA-DNA membranes,” *Express Polym. Lett.*, vol. 4, no. 8, pp. 480–487, 2010.