Enhanced Drug Anti-Counterfeiting and Verification System for the Pharmaceutical Drug Supply Chain using Blockchain

Eseosa Ehioghae
Department of Software Engineering, School of Computing and Engineering Sciences, Babcock University, Ilishan-Remo, Ogun State, Nigeria

Sunday Idowu
Department of Software Engineering, School of Computing and Engineering Sciences, Babcock University, Ilishan-Remo, Ogun State, Nigeria

Oluwaseun Ebiesuwa
Department of Computer Science, School of Computing and Engineering Sciences, Babcock University, Ilishan-Remo, Ogun State, Nigeria

ABSTRACT
The safety of the pharmaceutical drug supply chain is a major concern for global public health as the plague of drug counterfeiting along the supply chain is an increasing threat to the health of everyone. Various solutions have been proposed to solve the problem, yet, the problem is still rife, as estimates reveal that between 10% – 30% of drugs in the developed and developing countries respectively are counterfeit. This research proposes an enhanced drug anti-counterfeiting and verification system, using blockchain, to counter the plague of drug counterfeiting along the supply chain, while providing a suitable means of verifying such drugs. Two germane smart contracts – *shipDrug* and *receiveDrug* – were defined to serve as a means of safely moving drugs from one supply chain actor to the other, to secure the drug supply chain from the infiltration of counterfeit drugs. The system was implemented on the Hyperledger Fabric. The implemented system effectively secured the supply chain by allowing only the valid supply chain actors to execute the defined smart contracts. Final consumers were able to verify a drug by using a unique identifier associated with that drug to query the transaction history from the blockchain ledger. Hyperledger Caliper was used to evaluate the proposed system where it was revealed that an optimal throughput of 46 drug verifications per second was obtained, with less utilization of CPU and memory resources. The health ramifications of drug counterfeiting and the findings from this research make it imperative to consider the proposed system as an effective drug anti-counterfeiting system. Finally, it was recommended that the global health authority could implement the system on a global scale, after a smaller scale implementation, such as within countries, to determine its effectiveness in securing the drug supply chain within such jurisdictions.

Keywords
Verification, Anti-counterfeiting, Drugs, Hyperledger Fabric, Supply chain, Counterfeits, Pharmaceutical.

1. INTRODUCTION
Drugs bought and used to treat ailments are expected to bring about positive outcomes. It is however sometimes the case that such ailments could persist or even worsen as a result of the unauthenticity of such drugs. This has always been a serious global scourge, and in more recent times it has posed huge challenges in the pharmaceutical drug supply chain and overall healthcare ecosystem. Newton, Green, and Fernández [1] identified these drugs as poor-quality drugs and the World Health Organization (WHO) further classified them under the terminology SSFFC, which means substandard, spurious, falsely labeled, falsified, and counterfeit drugs [2] [3]. The term 'counterfeit' is an umbrella word used to denote "drugs that have been deliberately and fraudulently mislabeled with respect to identity and/or source and including drugs with incorrect ingredients, without active ingredients, with insufficient active ingredient, or with fake packaging" [2]. This also represents falsely labeled, falsified, and spurious drugs, with spurious being more popularized in India [4]. 'Substandard' drugs however are drugs that fail to meet the quality specification set for them, due to unintentional or negligent errors [2] [3] [4].

The negative impacts of these poor-quality drugs on patients' health and safety are unimaginable, where at best, these drugs are sub-therapeutic (implying that patients taking these compromised drugs get no form of relief from their symptoms) and at worst, these compromised drugs could kill the patients [4] [5]. Some other negative effects include the development of antimicrobial resistance by patients and adverse drug reaction [5]. All these damaging effects eventually diminish confidence in the public health system and increase economic losses for legitimate drug manufacturers [5].

While it is difficult to put an exact value to the prevalence of the problem of drug counterfeiting, published estimates of the problem reveal a global prevalence of about 10%, with these estimates reaching about 50% in some developing countries [6]. Given that billions of drugs are produced by the pharmaceutical industry and eventually consumed every year, even a 1% prevalence is enough to cause death to millions of people. Furthermore, some other estimates suggest that about 169,000 children die from pneumonia while about another 158,000 children die from malaria each year as a result of consuming counterfeit drugs for the respective illnesses [7].

One of the key reasons for the infiltration of counterfeit drugs into mainstream pharmacies and hospitals, as identified by Liu and Lundin [8], is the vulnerability of the supply chain, which gives ample opportunities for criminally-minded entities to commit heinous crimes within the drug supply chain, to benefit their selfish interest or for some other nefarious purposes. They can get along with this crime most times mainly because of the intrinsic complexity of the pharmaceutical drug supply chain, having lots of interacting stakeholders from different countries across the world [9] [10].

To combat this problem of drug counterfeiting within the

supply chain, researchers in the literature proposed various technological solutions based on technologies such as barcodes [11], Radio Frequency Identification (RFID) [12], data matrix [13], Near Field Communication (NFC) [14] for the protection of this compromised drug supply chain. While most of these solutions were able to temper the problem, most of them had inadequate security features and hence they could easily be gamed by determined counterfeiters, while some others lacked a concrete practicable implementation due to one constraint or the other, which precluded further investigation of their system. Also, they were all based on a centralized client-server architecture, which presented a single point of failure and ran the risk of tampering.

More recently, blockchain technology, a secure distributed digital ledger that gained popularity from the decentralized cryptocurrency of Bitcoin [15], has gained increasing popularity in other industry verticals, particularly in healthcare [16] [17]. Blockchain technology presents certain characteristics such as decentralization, cryptographic security, immutability, transparency, smart contract execution, which have made blockchain a plausible choice of technology in situations where extensive reputational issues are associated with a final product – essentially, where the integrity of such a product must be ensured [16]. This precisely describes the current pharmaceutical drug supply chain which is largely devoid of trust and integrity.

In this paper, we design and implement an enhanced drug anti-counterfeiting and verification system for the pharmaceutical drug supply using blockchain. We achieve this by implementing a decentralized ledger system that records the movement of only genuine drugs across the supply chain as drug transactions on the decentralized ledger, to secure the supply chain through which drugs pass through, from the nefarious activity of drug counterfeiting. Also, the decentralized ledger system enables final consumers to be able to trace the drugs purchased back to the original manufacturers, to verify and establish the genuineness of such drugs. The system was implemented on Hyperledger Fabric and further evaluated on Hyperledger Caliper.

The paper has been organized in the following way: section 2 gives a review of similar systems, section 3 gives a detailed description of the methods employed in this paper, section 4 discusses the implementation of the system, section 5 discusses the results of the implementation of the system, section 6 evaluates the system based on certain key metrics, section 7 concludes the entire paper, section 8 provides some recommendations.

2. RELATED WORKS

For a long time, RFID and barcode were the standard means of ensuring anti-counterfeiting of products generally, including drugs, along the supply chain. However, with the advent of blockchain technology, some anti-counterfeiting systems have been proposed based on blockchain technology. Hence, we reviewed two categories of anti-counterfeiting systems, one was based on the older RFID and barcode technology, while the other was based on the more nascent blockchain technology.

Choi and Poon [12] proposed an anti-counterfeiting system based on RFID, for providing a product pedigree, which was the record of transactions of an item since it was manufactured up to the current time when the transaction was taking place. The supply chain actors and end-consumers could both access this product pedigree, to determine the genuineness of the product in question. Verification of the product was done by using a phone which had an RFID reader embedded into it, to view a complete pedigree of the product, to establish its genuineness. Phones with RFID readers were not in existence at the time they carried out the research, which had the potential of making their system unusable pending when mobile phones with RFID readers were publicly made available.

Paik, et al. [18] proposed SmartTrack, which was focused on using a smart tag based on RFID for tracking the flow of the Anti-RetroViral (ARV) drugs used in Highly Active Anti-Retroviral Therapy (HAART) programs for HIV/AIDS patients, across the supply chain. The RFID tags affixed on the ARV drug package allowed the supply chain actor to use an RFID-enabled phone to capture the tag information, to ensure counterfeits were not introduced into the supply chain. They provided three distinct ways of verifying the authenticity of a drug. The first being that the tags could be scanned and immediately uploaded to a central server for instant verification. Second, all the valid tags could have at a previous time been gotten from the central server, stored locally on the phone, and then verified locally when there was a drug at hand that needed verification. Third, multiple tags could be scanned at once and then uploaded later for verification in a bulk manner. Their system also relied on cellphones being able to read RFID tags, which were not in mainstream circulation at the time of the writing of their paper. More so, two of the options used for verifying the genuineness of drugs relied on storing information on the cellphone used by the supply chain actors for verification as identified above. What was not consider was that if anything happened to that phone used for the verification (for example, it was damaged or stolen), then such drugs ran the risk of being unable to be verified for genuineness by the supply chain actors.

Paik, Chen, and Subramanian [11] proposed Epothecary, which leveraged camera-equipped mobile phones and 2D barcodes to provide a drug pedigree and tracking system for the supply chain. They proposed two protocols as the underlying principles on which their system ran on. The first was between the supply chain actors, and it ensured only genuine drugs moved from one actor to the other, which it did by the scanning of the 2D barcodes on the drugs' package and verification of such drugs as it moved from one actor to the other. The verification was achieved via SMS. The second protocol was between the retailers and the end-users, such that the retailers generated an 8-digit reference number by scanning the drug package, then consumers could send the 8-digit reference number to a verification server to verify such a drug. Their system required a lot of SMS-based communication between the central server and the supply chain actors during the process of moving drugs across the supply chain. There could be latency between the sending and receiving of each SMS, or worse, the SMS could fail to deliver, which could seriously impede verification and further progress of drugs along the supply chain.

Huang, Wu, and Long [19] proposed a drug traceability system called Drugledger, which leveraged blockchain technology to provide a drug traceability and regulation system. Their system was heavily premised on a flaw they identified from current client-server based anti-counterfeiting systems. This was that current client-server based anti-counterfeiting systems did not separate between the logic of the core anti-counterfeiting system (that is, the logic behind how a counterfeit is detected), and the logic of the administrator of the system, whose primary role was more

administrative, which included functions such as viewing logs and the overall setup of the entire system. Hence, they proposed Drugledger, which separated the entire system logic into three independent service providers, working together to ensure authenticity and privacy of traceability data, while ensuring a stable blockchain storage by pruning the blockchain ledger, based on the expiry date of the drugs. There was no concrete way to practically evaluate how their system solved the problems it claimed to solve, as they affirmed that they were still building a prototype.

Toyoda, Mathiopoulos, Sasase, and Ohtsuki [20] proposed a blockchain-based product ownership management system for detecting counterfeits in the post-supply chain. Their premise was that current research efforts in product anti-counterfeiting had majorly been within the supply chain, while little or no attention had been paid to products beyond the end of the supply chain – the post-supply chain. Hence, they proposed a proof of possession of product protocol, where supply chain actors had to prove "the possession of a product" so that the next supply chain actor and the final consumers could reject a product even with a genuine tag if the current owner of the product could not prove that he was the owner of such a product. This was made possible by a smart contract they proposed, which could only be executed by the current actor in possession of the product. It should be noted that while their work addressed a genuine problem, the World Health Organization advises that drugs should not be purchased from unauthorized sources such as drug peddlers and hawkers in the first place, which most times are post supply chain sources [2].

Sylim, Liu, Marcelo, and Fontelo [21] proposed a system based on blockchain technology for the detection of substandard and falsified drugs within the supply chain. They proposed a Distributed Application (DApp) running on smart contracts with the backend based on a Distributed File System (DFS) called Swarm, which was used for storing the DApp, the smart contracts, and the entire blockchain records. They proposed an instance of the DApp on Ethereum blockchain, which is one of the largest public blockchain networks. This one used a proof-of-work consensus algorithm called Ethash. They also proposed a future deployment of the same solution on Hyperledger Fabric, which they said was more ideal for the pharma industry as it is a private consortium blockchain. Their proposed system did not provide any practical working system or algorithm that we could evaluate, as they affirmed that the entire system was developed and tested in a simulated network.

3. METHODOLOGY

3.1 System Model

In this research, the entire drug supply chain was modeled as an interacting set of entities, such that blockchain transactions defined the movement of drugs across the supply chain, where only authorized valid supply chain actors could take part in executing these blockchain transactions. This meant that in the physical world, drugs did not just move from the manufacturer to the distributor and the rest of the actors in the supply chain as is the case in the current drug supply chain systems. Rather, the physical movement of drugs from one supply chain actor to the other in this research was defined as the successful execution of blockchain transactions defined for the actor at that stage in question. This was in a bid to prevent illegal actors from introducing drugs of questionable quality into the supply chain. A valid supply chain actor in this research was an actor who could execute the transactions defined for the supply chain actor at the level in which he operated, by virtue of a previous addition to the network, assignment of appropriate cryptographic identities, and appropriate mapping to pertinent real-world roles on the blockchain network. Hence, the proposed system ensured that if an actor was added as a wholesaler, for example, that same actor was not able to execute transactions belonging to another actor (a retailer for example). This role-based access also underpinned the security of the proposed system.

Finally, consumers were able to verify the genuineness of a drug they wanted to purchase, by sending a unique identifier on the drug package to the blockchain network to query the transaction history of the drug in question. They were able to get a response on the validity of the drug and some other pertinent information, such as the drug's prescription, based on the validity of that drug's transactions while it traversed the supply chain.

The proposed system comprised five actors, namely, Manufacturer, Distributor, Wholesaler, Retailer, and Consumer. These actor types were based on the modeled supply chain proposed by Litke, Anagnostopoulos, and Varvarigou [22].

3.2 System Methodology

The methods employed in developing the system are now explained below.

3.2.1 Blockchain Network Methodology

In this research, two germane smart contracts were defined to update the blockchain ledger with drug transactions. The first smart contract was called *shipDrug*, which was executed by the actor currently in possession of the drug, who wanted to transfer the drug to the next supply chain actor. While the second smart contract was called *receiveDrug*, which was executed by the next supply chain actor after that actor had received the drug from the current actor in possession of the drug. The execution of these smart contracts yielded appropriate writes of drug transactions by the relevant supply chain actors while ensuring that the status of the drug was also appropriately updated on the ledger.

To secure the entire blockchain network, the proposed system presented a Membership Service Provider (MSP), which was responsible for issuing cryptographic identities to the supply chain actors in the relevant stages of the supply chain, which allowed these actors to participate in writing transactions via the issued digital identities. This was a crucial component of the system, as this cryptographically based access was what largely differentiated the system from other systems where access to the ledger was opened to anyone. This thereby secured the entire blockchain network from malicious entities attempting to update the state of the drug transactions on the network.

3.2.2 Drug Authentication Methodology

Furthermore, the drug's Serialized Global Trade Item Number (SGTIN) was encrypted with the Advanced Encryption Standard (AES) encryption algorithm and encoded as a 2D barcode on the drug package based on the Global Standards 1 (GS1) format [23]. The SGTIN is the combination of the Global Trade Item Number (GTIN), which is a unique and internationally accepted identifier for a product, and a serial number, encoded in a specific format, which could be SGTIN-64, SGTIN-96, or SGTIN-198. In this research, the SGTIN-96

was used, which in the binary form is a 96 bits code, consisting of an 8 bits header, 3 bits filter, 3 bits partition, 24 bits company prefix, 20 bits item reference number, and 38 bits serial number which totals 96 bits and hence the name SGTIN-96.

The drug's SGTIN was first encrypted and then encoded on the 2D barcode, rather than the conventional approach of just encoding these values on the 2D barcode. This was done to ensure more security at the drug scanning level. The valid supply chain actors, who after signing in and scanning the encrypted information on the 2D barcode, could now authorize the drug's passage across the supply chain. This was done by using a secret key associated with the encrypted drug information to decrypt the encrypted value, to reveal the original data which contained the drug's SGTIN which was then used to query the blockchain network to call the associated smart contract, to authorize the drug's movement and update the state of the drug transaction on the blockchain network. This ensured more security as not just anyone with access to the 2D barcode could scan it and attempt to authorize such a drug movement, hence ruling out the possibility of malicious entities, who although might have access to the 2D barcode by an illegal means of copying it and using on their counterfeit drug, from being able to authorize counterfeit drugs along the supply chain.

3.2.3 Drug Verification Methodology

Finally, the record of the transactions of a particular drug could be queried from the blockchain network, to ascertain the genuineness of such a drug. This was made possible by leveraging a transaction log of all drug transactions across the system, which was maintained by the nodes within the blockchain network. To achieve this, the current conventional approach of embedding a covert unique ID associated with the drug, which could only be scratched and revealed at purchase, was used to query the transaction log to retrieve the transaction history of the drug from the manufacturer up to the retail point of sale. This was used to verify a drug, as only drugs that had followed the supply chain with valid supply chain actors authenticating their movement could be verified.

3.3 System Architecture

From the proposed architecture shown in figure 1, the Administrator (1), represents a regulatory agency in the country, such as the FDA in the United States and NAFDAC in Nigeria, overseeing health and other related activities in such a country. This Administrator, who although did not take part in writing drug transactions on the blockchain, held a crucial role in ensuring that the supply chain actors being enrolled in the system were valid supply chain actors.

After the successful enrollment of valid supply chain actors by the Administrator, a Membership Service Provider (2) was responsible for assigning a valid cryptographic identity to each of the supply chain actors – the Manufacturers, Distributors, Wholesalers, and the Retailers. The Membership Service Provider guaranteed the security of the system by ensuring that the supply chain actors accessing the ledger to write transactions had valid cryptographic identities previously issued to them by this Membership Service Provider. This, as has already been established, was in a bid to prevent malicious actors from gaining any form of access into the system. Also, role-based access to the ledger was enforced in this research to ensure that an actor type, a manufacturer, for example, could not run drug transactions designated for another actor type, a retailer, for example. This role-based information was encoded in the cryptographic identities issued to the supply chain actors, and it was also validated by the Membership Service Provider, to further ensure the security of the system.

The manufacturer (3) could now subsequently manufacture a drug and then execute the appropriate blockchain transaction to register such a drug on the blockchain ledger as a drug transaction, after which the drug could now be shipped by the manufacturer to the next supply chain actor – the distributor. These two respective activities of the manufacturer manufacturing a drug and shipping it to the distributor yielded two drug transactions (*manufacturerCreateDrug* and *manufacturerShipDrug*), which were written to the ledger to effectively represent the current state of the drug.

As part of the manufacturing process, the conventional approach of encoding the drug information such as the SGTIN as a 2D barcode was implemented to be used to authorize the manufactured drug's movement across the supply chain. However, to ensure more security during the movement, the drug's SGTIN was encrypted with the AES encryption algorithm rather than just encoding the original value on the 2D barcode, to ensure that only valid supply chain actors could scan such a drug and not just anyone, thereby precluding opportunities for counterfeiters to exploit.

Afterwards, the distributor (4) received manufactured drugs from the manufacturer by scanning the 2D barcode attached to the drug package to authorize the receipt of such a drug, which further updated the state of the drug on the blockchain network appropriately. Subsequently, the distributor distributed the drugs to the wholesaler along the supply chain by clicking on the ship drug button on their page of the application. These two respective activities of the distributor receiving manufactured drugs from the manufacturer and shipping them to the wholesaler yielded two drug transactions (*distributorReceiveDrug* and *distributorShipDrug*), which were written to the ledger to effectively represent the current state of the drugs.

The wholesaler (5) received the drugs from the distributor by also scanning the 2D barcode attached to the drug package to authorize the receipt of such a drug, which further updated the state of the drug on the blockchain network appropriately. Subsequently, the wholesaler sold the drugs to the retailer along the supply chain by clicking on the ship drug button on their page of the application. These two respective activities of the wholesaler buying drugs in bulk from the distributor and selling such drugs in smaller quantities to the retailer yielded two drug transactions (*wholesalerReceiveDrug* and *wholesalerShipDrug*), which were written to the ledger to effectively represent the current state of the drugs.

The retailer (6) received the drugs from the wholesaler by alsoscanning the 2D barcode attached to the drug package to authorize the receipt of such a drug, which further updated the state of the drug on the blockchain network appropriately. Subsequently, the retailer sold the drugs to the consumers in retail outlets by clicking on the sell drug button on their page of the application. These two respective activities of the retailer buying drugs in smaller quantities from the wholesaler and eventually selling such drugs to the final consumers in retail outlets such as pharmacies and hospitals yielded two drug transactions (*retailerReceiveDrug* and *retailerSellDrug*), which were written to the ledger to effectively represent the current state of the drugs.

The final consumers (7) did not take part in any transaction as they could not update the ledger state. However, as can be seen in figure 1, they could only verify the genuineness of a drug by querying the transaction log for the drug in question. This was done by scratching the embedded covert unique ID associated with the drug and sending the ID to the system which queried the transaction log to establish the genuineness of such a drug after they bought the drug. This ensured that the consumers could determine the actual manufacturer of the drugs they bought and the different supply chain actors such drugs had gone through, thereby making sure the drugs they bought originated from a genuine source.

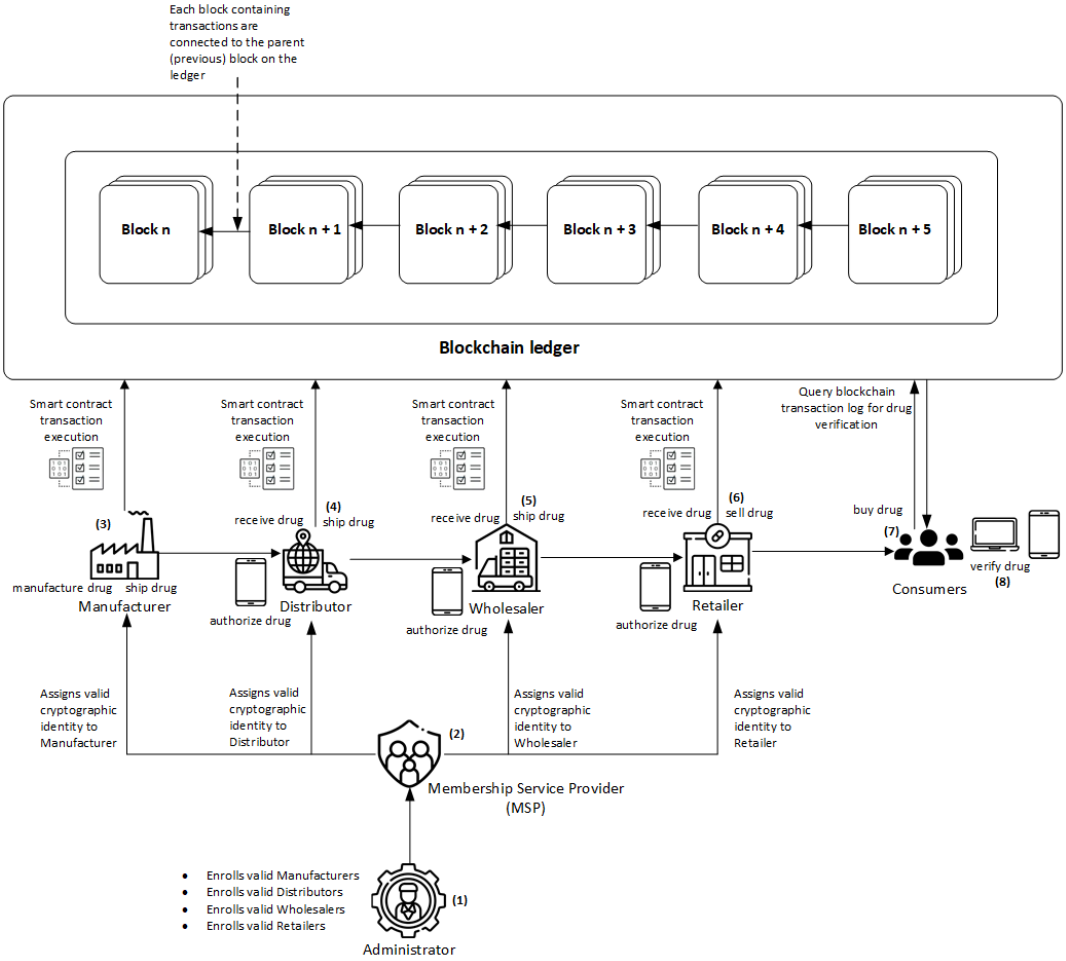

Fig 1: Architecture of the Proposed System

4. SYSTEM IMPLEMENTATION

The system implementation involved the conversion of the proposed system into a working software application. The implementation was divided into three major parts, namely:

1. Blockchain development
2. Backend API development
3. User Interface development

4.1 Blockchain Development

Hyperledger Fabric was the blockchain platform used for the implementation of the proposed system. It uses Docker, an open-source software tool for packaging, deploying, and running software using Operating System level virtualization construct (called containers), to host smart contracts to ensure they run in isolation.

In contrast to open permissionless blockchain networks like Ethereum, where unknown identities participate in the network, the participants of a Hyperledger Fabric network are known and therefore must enroll through a trusted entity which is called a Membership Service Provider (MSP). Hence in this research, an MSP was used for the generation of cryptographic identities, to preclude unauthorized access and ensure only valid actors could access the ledger.

The ledger is the shared, immutable, sequence of records, stored in blocks, such that the current record is cryptographically linked to the previous record. These records are called transactions. Hyperledger Fabric ledger has two major components called: the world state and the transaction log. The world state contains information about the current state of the ledger while the transaction log contains a historical log of all the transactions that have led to the current state of the ledger – the world state. The world state is especially useful to query the current state of a transaction item, for example, the world state can be queried to determine the current state of a drug transaction (for example, has it just been manufactured? or has it been sold by the retailer?). The transaction log on the other hand could be queried to determine the provenance of a particular drug item, for example, before a consumer purchase a drug, the transaction log could be queried, based on the unique ID of the drug, to determine all the previous possessors of the drug, back to the manufacturer, to establish the genuineness of such drug. A ledger with a world state and a transaction log was set up in

the blockchain network of this research for this purpose of respectively determining the current state of a drug and the transaction log of a drug.

The smart contracts (called chaincode in Fabric ecosystem) were written in NodeJS, a supported language for writing smart contracts in Hyperledger Fabric, by leveraging on the Hyperledger Fabric NodeJS Software Development Kit (SDK). This SDK contains all the libraries used for writing smart contracts that will interact with a Hyperledger Fabric blockchain network, using NodeJS. Figure 2 shows a sample smart contract transaction for a manufacturer who wants to ship a drug that has just been created to the next supply chain actor – the distributor.

```
/**
 * manufacturerShipDrug
 *
 * @param {Context} ctx the transaction context
 * @param {String}  drugId
 * Usage:  submitTransaction ('manufacturerShipDrug', 'drug001')
 */
async manufacturerShipDrug(ctx, drugId) {
    console.info( message: '============ manufacturerShipDrug ==========');

    //  The manufacturer ships the drug after the production of the drug

    // Access Control: This transaction should only be invoked by a designated manufacturer
    const userType = await this.getCurrentUserType(ctx);

    if ((userType !== supplyChainActors.admin) && // admin only has access as a precaution.
        (userType !== supplyChainActors.manufacturer))
        throw new Error(`Error Message from manufacturerShipDrug: This user does not have access to ship drug of id ${drugId}`);

    if (!drugId || drugId.length < 1) {
        throw new Error('Error Message from manufacturerShipDrug: drugId is required as input')
    }

    // Retrieve the current drug using key provided
    const drugAsBytes = await ctx.stub.getState(drugId);
    if (!drugAsBytes || drugAsBytes.length === 0) {
        throw new Error(`Error Message from manufacturerShipDrug: Drug with drugId = ${drugId} does not exist.`);
    }

    // Convert drug so we can modify fields
    const drug = Drug.deserialize(drugAsBytes);
    const userId = await this.getCurrentUserId(ctx);

    // Change currentDrugState to MANUFACTURER_SHIPPED;
    drug.setStateToManufacturerShipped();
    // Track who exactly invoked this transaction
    drug.currentOwner = userId;
    drug.manufacturerId = userId;
    drug.timeStamp = this.getCurrentDateTime();

    // Update ledger
    await ctx.stub.putState(drugId, drug.toBuffer());

    const queryEvent = this.createEvent(drugId, userId,  eventType: 'manufacturerShipDrug');

    await this.setEvent(ctx, queryEvent);

    // Must return a serialized drug to caller of smart contract
    return drug.toBuffer();
}
```

Fig 2: Smart Contract Transaction for a Manufacturer shipping a drug

4.2 Backend API Development

The backend API (Application Programming Interface), which interacts directly with the smart contracts on the blockchain network on behalf of the user, was also written in NodeJS. The backend API was primarily responsible for hosting an HTTP server, which could be interacted with via HTTP request, to interact with the Hyperledger Fabric blockchain network.

Hence, this backend API provided appropriate endpoints to interact with each of the smart contracts defined on the blockchain network.

4.3 User Interface Development

A user interface was developed to enable a convenient interaction with the entire system. The user interface was written with HTML, CSS, and JavaScript. More specifically, a JavaScript framework called Angular was used to write the logic that managed the state of the application and other pertinent actions such as HTTP requests.

4.4 Development Environment

The system was developed on a Windows 10 Pro 64-bit Operating System, with 8 GB of RAM and an Intel(R) Core(TM) i7-7660U CPU @ 2.5GHz processor. The Integrated Development Environment (IDE) used for development was Visual Studio Code v1.39.2.

For development and testing, docker, an open-source tool for containerizing, deploying, and running applications in a container environment was used for the running environment for Fabric. Fabric's docker image and other pertinent docker images were pulled from the docker hub and used to develop and test locally on the development machine. The docker engine used was v19.03.5.

5. RESULTS AND DISCUSSION

The results from the implementation of the entire system are presented here where snapshots are provided to illustrate this process.

5.1 Administrator

An administrator was in charge of creating users on the system and enrolling them, which will in effect issue these created users with the appropriate certificates for interacting with the blockchain network. This administrative and supervisory role was a key role as this was the person in charge of adding valid manufacturers, distributors, wholesalers, and retailers who would take part in the drug

supply chain. This administrator did not take part in the operations of moving drugs across the supply chain. This administrator in this research was considered as a regulatory agency in the country, overseeing health and other related activities in such a country, such as the FDA in the United States and NAFDAC in Nigeria.

5.2 Manufacturer

A manufacturer created the finished drug products, which could be sold to final consumers after the successful movement of the drug across the supply chain. Figure 3 shows the process of manufacturing a drug. Pertinent information about the drug is input, after which it is sent to the backend API which then invokes the associated smart contract to record the newly manufactured drug on the ledger as a drug transaction.

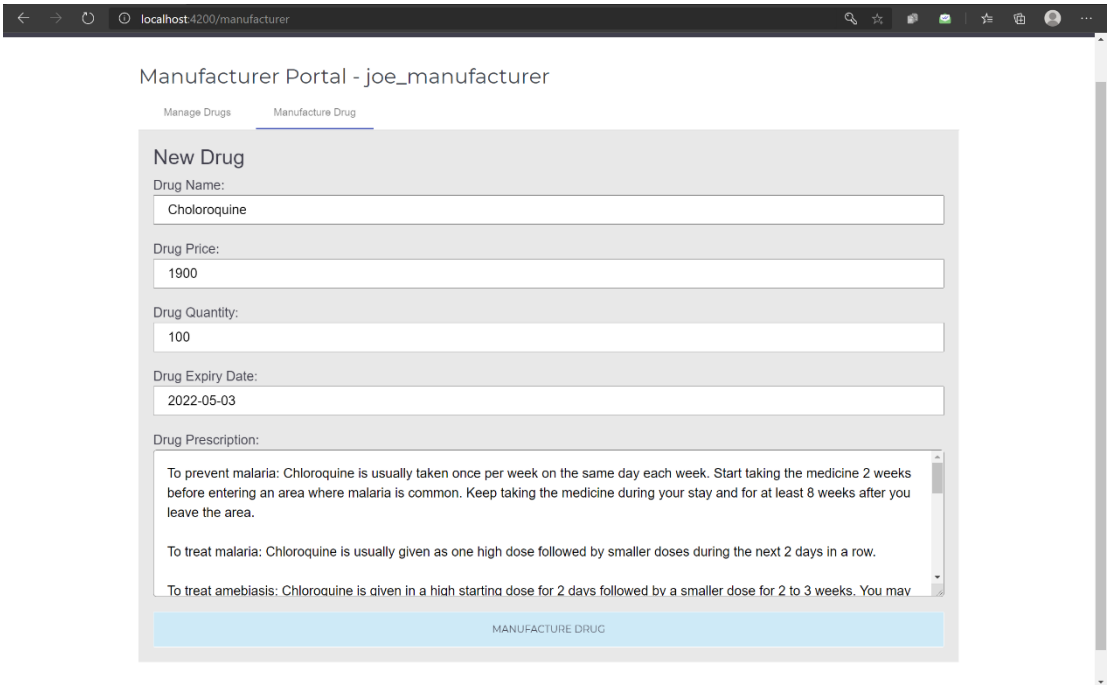

Fig 3: Manufacturer creating a drug on the system

Also, as part of the manufacturing process, a 2D barcode, containing the encrypted drug's SGTIN was printed on the package of the drug, to enable only valid supply chain actors to authorize the movement of the drug across the supply chain.

After the manufacturing process, the manufacturer could now ship the drug for the next supply chain actor, the distributor, to receive it. Figure 4 illustrates this process.

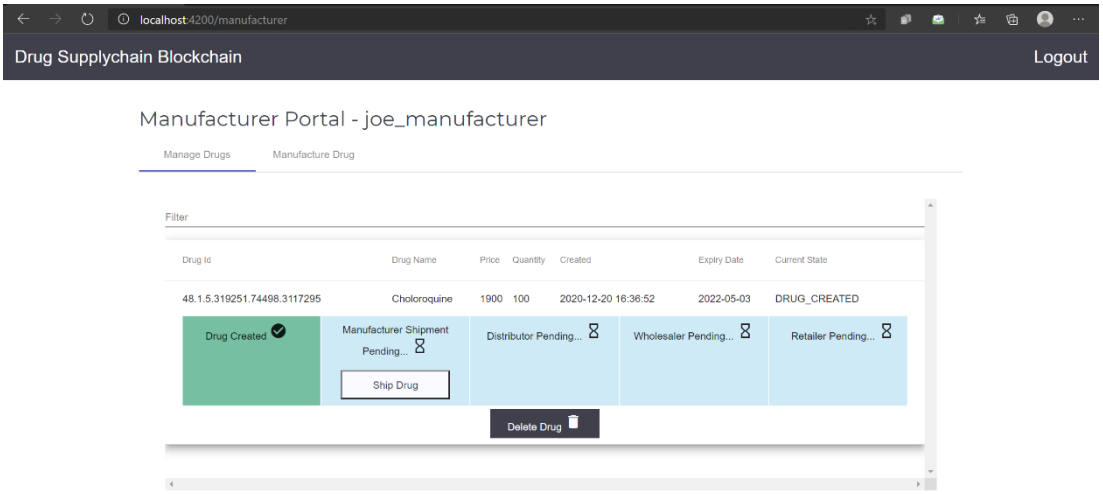

Fig 4: Manufacturer shipping a drug on the system

5.3 Distributor

In this research work, the distributor was solely responsible for selling manufactured drugs to a wholesaler. Figure 5 shows the authorization of the receipt of a drug by the distributor, which must have been previously shipped by the manufacturer. This process, as can be seen, involved the scanning of the 2D barcode on the drug package by the valid distributor supply chain actor with their smartphone, after they must have signed in, which then calls the appropriate backend API, which in turn invokes the appropriate smart contract on the blockchain network to authorize the drug by updating the state of the drug. After the authorization by the distributor, the drug is shipped for the next supply chain actor, the wholesaler, to likewise authorize and receive.

Fig 5: Drug authorization on the system

5.4 Wholesaler

A wholesaler did not sell drugs directly to the consumers, but instead to retailers. They bought drugs in bulk from the distributor, which were sold to the retailers later in the supply chain. The wholesaler likewise had an identical screen like the one in figure 5 for the authorization of the drug from the distributor and another one similar to the one in figure 4 for shipping the drug to the retailer.

5.5 Retailer

A retailer was the end actor, who purchased drugs from the wholesalers and eventually sold the drugs to the final consumers. The retailer likewise had an identical screen like the one in figure 5 for the authorization of the drug from the wholesaler. The retailer had a slightly different one for selling the drug to a consumer who comes to the retail outlet to purchase a drug, as shown in figure 6.

5.6 Final consumers

The final consumers did not take part in any transaction as they could not update the ledger state. However, they could verify the genuineness of a drug by tracing it back to the origin, which was the manufacturer. This was done by leveraging the current technique of embedding a covert code on the drug package associated with the drug, which could be scratched at purchase to reveal the code, and then using that code to perform the verification. This ensured that the consumers could determine the actual manufacturer of the drug, thereby making sure the drugs they bought originated from a genuine source. Figure 7 shows this process of verifying a drug purchased by a consumer. It further shows the provenance of the drug, identifying from the manufacturer down to the different actors who had previously been in possession of the drug. This information is gotten by querying the transaction log of the particular drug from the blockchain network via the unique ID associated with the drug and then retrieving the transaction history of that drug.

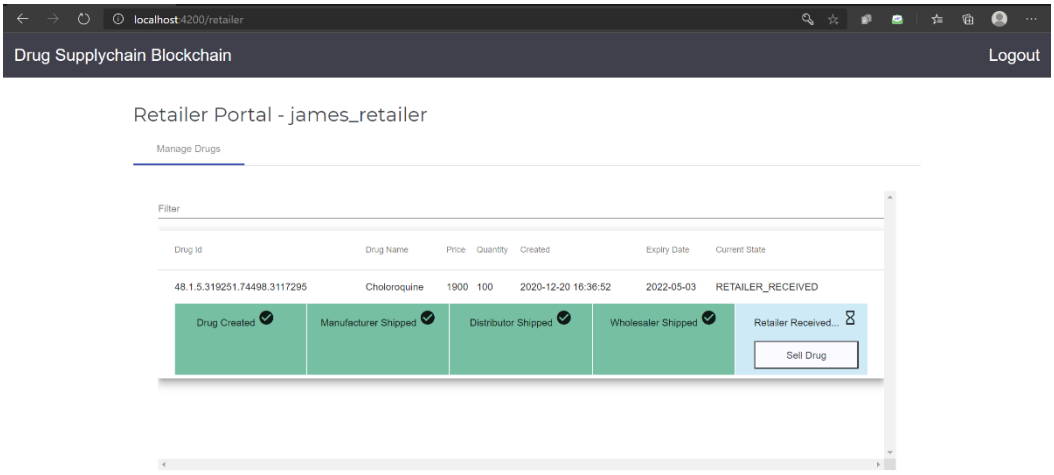

Fig 6: Retailer Selling a Drug on the System

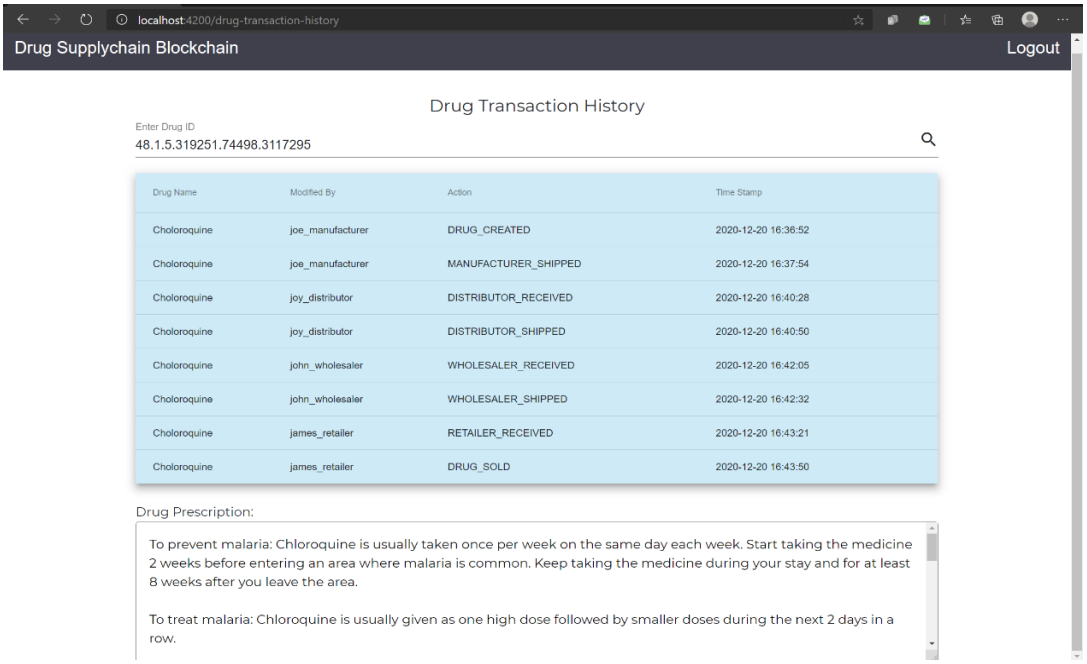

Fig 7: Drug verification on the System

6. SYSTEM EVALUATION

The system evaluation involved benchmarking the system against certain key metrics to evaluate its performance. Hyperledger Caliper, a blockchain performance benchmark framework, was used to evaluate the system based on key metrics such as transaction latency, transaction throughput, and resource utilization (CPU and Memory).

Two groups of transactions were run against the system using the Hyperledger Caliper, to evaluate the performance of the system. The first was a 500 set of drug transactions, while the second was a 1000 set of drug transactions, all issued against the system. In each of these sets of drug transactions benchmark, the key metrics of transaction throughput, transaction latency, and resource consumption were measured to determine the system's performance. Furthermore, a base transaction issue rate of 50 transactions per second was used for both the 500 and 1000 drug transactions benchmark.

6.1 Transaction Throughput

Figure 8 investigates the throughput (measured in transactions per second) of the benchmarks run against the system. From figure 8, for the 500 drug transactions benchmark, the smart contract execution of the *manufacturerCreateDrug* yielded a throughput of 43.6 TPS, while for the 1000 drug transactions benchmark, a throughput of 38.3 TPS was obtained for the same smart contract execution, thereby yielding an average throughput of 41.0 TPS. Furthermore, the smart contract execution for the *consumerVerifyDrug*, which was responsible for querying the transaction log of the blockchain to verify the genuineness of a drug, yielded a throughput of 47.5 TPS and 45.2 TPS for the 500 and 1000 drug transaction benchmark respectively, further yielding an average throughput of 46.4 TPS. The wider implication of this average throughput of 46.4 TPS for the consumerVerifyDrug smart contract execution indicates that about 46 drugs could be verified in a second, based on the blockchain network that was set up. This is a good performance for this network setup, given the context that only a single orderer node, was responsible for achieving consensus on the order of all issued transactions within the system.

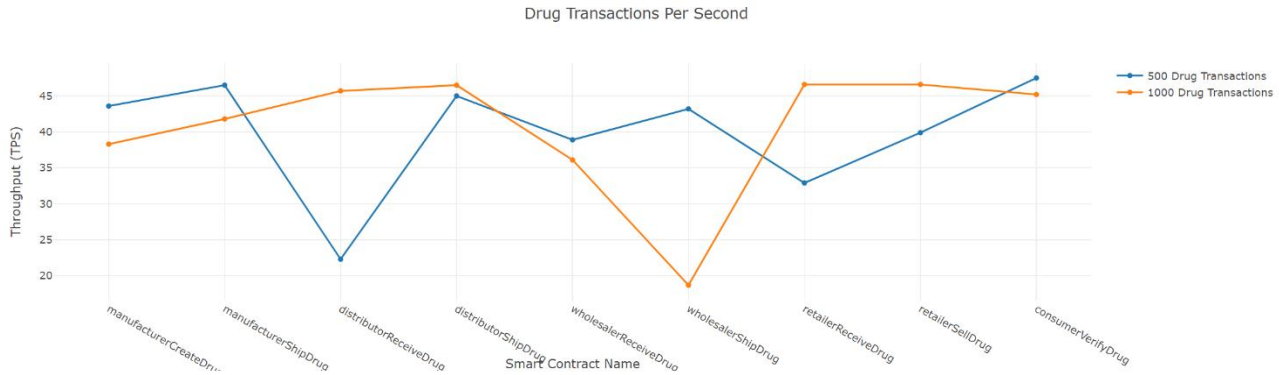

Fig 8: Transaction throughput (in transactions per second) of the system

6.2 Transaction Latency

Figure 9 investigates the average transaction latency (average time measured in seconds for an issued transaction to be completed) of the benchmarks run against the system. From figure 9, for the 500 drug transactions benchmark, the smart contract execution of the *manufacturerCreateDrug* yielded an average latency of 2.09s, while for the 1000 drug transactions benchmark, an average latency of 7.29s was obtained for the same smart contract execution, thereby yielding an average latency of 4.69s. Furthermore, the smart contract execution for the *consumerVerifyDrug*, yielded an average latency of 1.79s and 4.29s for the 500 and 1000 drug transaction benchmark respectively, further yielding an average latency of 3.04s. This, as was the case for the benchmark on throughput, is also indicative of good system performance, given the same context that only a single orderer node was solely responsible for achieving consensus on the order of all issued transactions within the system.

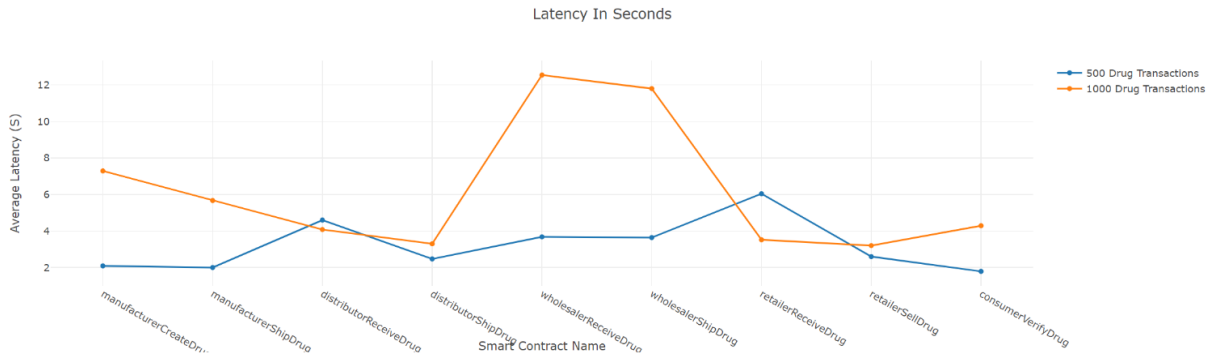

Fig 9: Transaction latency (in seconds) of the system

6.3 Resource Consumption

Tables 1 and 2 investigate the average resource consumption of the system for all the smart contract execution for the 500 and 1000 drug transactions benchmark respectively, with a focus on the CPU and memory consumption. Examining table 1 reveals an average maximum CPU consumption of 25.43% and an average maximum memory consumption of 83.51 MB for all the nodes running in the respective docker container for the 500 drug transactions benchmark. Furthermore, table 2 reveals an average maximum CPU consumption of 37.27%

and an average maximum memory consumption of 112.33 MB for all the nodes running in the respective docker container for the 1000 drug transactions benchmark. This is indicative of the minimal CPU and memory consumption of the proposed system, which is further indicative of the high performance and the robustness of the system.

Table 1: Resource utilization for all smart contract execution for the 500 drug transactions benchmark

Docker container	CPU % (max)	CPU% (avg)	Memory [MB] (max)	Memory [MB] (avg)
Org1Peer1-drugsupplychainnet-0.0.1	40.74	15.94	69.82	64.31
orderer.example.com	16.02	6.87	56.80	55.58
ca.orderer.example.com	0.02	0.00	6.03	6.00
peer0.org1.example.com	51.91	22.64	292.22	284.78
couchdb0.org1.example.com	43.88	18.48	69.81	68.48
ca.org1.example.com	0.02	0.00	6.40	6.36

Table 2: Resource utilization for all smart contract execution for the 1000 drug transactions benchmark

Docker container	CPU % (max)	CPU% (avg)	Memory [MB] (max)	Memory [MB] (avg)
Org1Peer1-drugsupplychainnet-0.0.1	63.98	22.46	86.78	81.18
orderer.example.com	22.56	8.88	82.1	79.56
ca.orderer.example.com	0.00	0.00	5.28	5.25
peer0.org1.example.com	67.68	29.51	400.11	391
couchdb0.org1.example.com	69.39	29.51	94.22	91.37
ca.org1.example.com	0.03	0.00	5.49	5.46

7. CONCLUSION

This research was premised on the fact that the global scourge of drug counterfeiting prevailed, despite concerted efforts at curbing the problem. It was discovered that most of the systems proposed to solve the problem had one gap or the other, ranging from the cost of implementation to the lack of adequate security features, and to the lack of a practical system geared at solving the problem. However, in this research, an enhanced drug anti-counterfeiting and verification system was designed and implemented to curb the pervading problem of drug counterfeiting along the supply chain. This system ensured only valid supply chain actors were responsible for writing drug transactions to the ledger controlling the supply chain, to prevent illegal and malicious actors from introducing counterfeits to the supply chain. It was established that it was of great importance for consumers to be able to determine the genuineness of the drugs they purchased, hence, this system also gave consumers the ability to verify the drugs they purchased. The system was implemented using Hyperledger Fabric blockchain, where pertinent security features were implemented to ensure only valid supply actors could write drug transactions to the ledger, after which the log of the transactions could be used to verify the drugs. The system was finally evaluated based on transaction throughput, transaction latency, and resource consumption, where it was concluded that the system was performant and robust due to the optimal throughput, low latency, and minimal resource consumption achieved from the benchmark performed against the system.

8. RECOMMENDATIONS

This research work designed and implemented an enhanced drug anti-counterfeiting and verification system using blockchain technology, to secure the drug supply chain from the nefarious activities of drug counterfeiting, while giving consumers the ability to verify the drugs they wanted to buy. The following recommendations should however be taken into consideration:

1. The health authority in any country, such as the FDA in the United States or NAFDAC in Nigeria can first implement the proposed system on a national level, where it can be observed to see how it performs with respect to ensuring drug anti-counterfeiting and verification within the jurisdiction of such countries. Afterwhich, the global health authority can implement the proposed system on a global level, where the authorized supply chain actors within different countries can partake in ensuring the global supply chain is secured from counterfeiting by adhering to the flow proposed in this research.
2. The health authority in any country, such as the FDA in the United States or NAFDAC in Nigeria, can use the proposed system to effectively monitor the activities within the supply chain, and use the insight to better serve the overall health interest of the citizens of the country.

9. REFERENCES

[1] P. N. Newton, M. D. Green and F. M. Fernández, "Impact of poor-quality medicines in the ‘developing’ world," Trends in Pharmacological Sciences, vol. 31, no. 3, pp. 99-101, 2010.

[2] World Health Organization, "Frequently asked questions," 2005. [Online]. Available: https://www.who.int/medicines/services/counterfeit/faqs/QandAsUpdateJuly11.pdf. [Accessed 22 November 2020].

[3] World Health Organization, "Substandard and falsified medical products," 2018. [Online]. Available: https://www.who.int/en/news-room/fact-

sheets/detail/substandard-and-falsified-medical-products. [Accessed 2 October 2020].

[4] A. Attaran, D. Barry, S. Basheer, R. Bate, D. Benton, J. Chauvin, L. Garrett, I. Kickbusch, J. C. Kohler, K. Midha, P. N. Newton, S. Nishtar, P. Orhii and M. McKee, "How to achieve international action on falsified and substandard medicines," BMJ, vol. 345, 2012.

[5] P. N. Newton, M. D. Green, F. M. Fernández, N. P. J. Day and N. J. White, "Counterfeit anti-infective drugs," The Lancet. Infectious Diseases, vol. 6, no. 9, pp. 602-613, 2006.

[6] R. Cockburn, P. N. Newton, E. K. Agyarko, D. Akunyili and N. J. White, "The Global Threat of Counterfeit Drugs: Why Industry and Governments Must Communicate the Dangers," PLOS Medicine, vol. 2, no. 4, pp. 0302-0308, 2005.

[7] World Health Organization, "1 in 10 medical products in developing countries is substandard or falsified," 28 November 2017. [Online]. Available: https://www.who.int/en/news-room/detail/28-11-2017-1-in-10-medical-products-in-developing-countries-is-substandard-or-falsified. [Accessed 30 August 2020].

[8] R. Liu and S. Lundin, "Falsified Medicines: Literature review," Working Papers in Medical Humanities, vol. 2, no. 1, pp. 1-25, 2016.

[9] N. Shah, "Pharmaceutical supply chains: key issues and strategies for optimization," Computers & Chemical Engineering, vol. 28, no. 6-7, pp. 929-941, 2004.

[10] M. Tremblay, "Medicines Counterfeiting is a Complex Problem: A Review of Key Challenges Across the Supply Chain," Current Drug Safety, vol. 8, no. 1, pp. 43-55, 2013.

[11] M. Paik, J. Chen and L. Subramanian, "Epothecary: Cost-effective Drug Pedigree Tracking and Authentication Using Mobile Phones," in 1st ACM SIGCOMM Workshop on Networking, Systems, and Applications for Mobile Handhelds, Barcelona, 2009.

[12] S. Choi and C. Poon, "An RFID-based Anti-counterfeiting System," IAENG International Journal of Computer Science, vol. 35, no. 1, 2008.

[13] S. u. Rehman, R. U. Rasool, M. S. Ayub, S. Ullah, A. Kamal, Q. M. Rajpoot and Z. Anwar, "Reliable Identification of Counterfeit Medicine Using Camera Equipped Mobile Phones," in 8th International Conference on High-capacity Optical Networks and Emerging Technologies, Riyadh, 2011.

[14] M. Wazid, A. K. Das, M. K. Khan, A. A.-D. Al-Ghaiheb, N. Kumar and A. V. Vasilakos, "Secure Authentication Scheme for Medicine Anti-counterfeiting System in IoT Environment," IEEE Internet of Things Journal, vol. 4, no. 5, pp. 1634-1646, 2017.

[15] S. Nakamoto, "Bitcoin: A Peer-to-Peer Electronic Cash System," 2008. [Online]. Available: https://bitcoin.org/bitcoin.pdf. [Accessed 29 September 2020].

[16] M. Mettler, "Blockchain Technology in Healthcare The Revolution Starts Here," in 2016 IEEE 18th International Conference on e-Health Networking, Applications and Services (Healthcom), Munich, 2016.

[17] M. Kassab, J. DeFranco, T. Malas, P. Laplante, G. Destefanis and V. V. G. Neto, "Exploring Research in Blockchain for Healthcare and a Roadmap for the Future," IEEE Transactions on Emerging Topics in Computing, 2019.

[18] M. Paik, A. Sharma, A. Meacham, G. Quarta, P. Smith, J. Trahanas, B. Levine, M. A. Hopkins, B. Rapchak and L. Subramanian, "The Case for SmartTrack," in 2009 International Conference on Information and Communication Technologies and Development (ICTD), Doha, 2009.

[19] Y. Huang, J. Wu and C. Long, "Drugledger: A Practical Blockchain System for Drug Traceability and Regulation," in 2018 IEEE International Conference on Internet of Things (iThings) and IEEE Green Computing and Communications (GreenCom) and IEEE Cyber, Physical and Social Computing (CPSCom) and IEEE Smart Data (SmartData), Halifax, 2018.

[20] K. Toyoda, T. P. Mathiopoulos, I. Sasase and T. Ohtsuki, "A Novel Blockchain-Based Product Ownership Management System (POMS) for Anti-Counterfeits in The Post Supply Chain," IEEE Access, vol. 5, pp. 17465-17477, 2017.

[21] P. Sylim, F. Liu, A. Marcelo and P. Fontelo, "Blockchain Technology for Detecting Falsified and Substandard Drugs in Distribution: Pharmaceutical Supply Chain Intervention," JMIR Research Protocols, vol. 7, no. 9, 2018.

[22] A. Litke, D. Anagnostopoulos and T. Varvarigou, "Blockchains for Supply Chain Management: Architectural Elements and Challenges Towards a Global Scale Deployment," Logistics, vol. 3, no. 1, 2019.

[23] GS1 US, "How to Translate a U.P.C. to a GTIN to an SGTIN to an EPC," 2019. [Online]. Available: https://www.gs1us.org/DesktopModules/Bring2mind/DMX/Download.aspx?Command=Core_Download&EntryId=389&language=en-US&PortalId=0&TabId=134. [Accessed 12 December 2020].