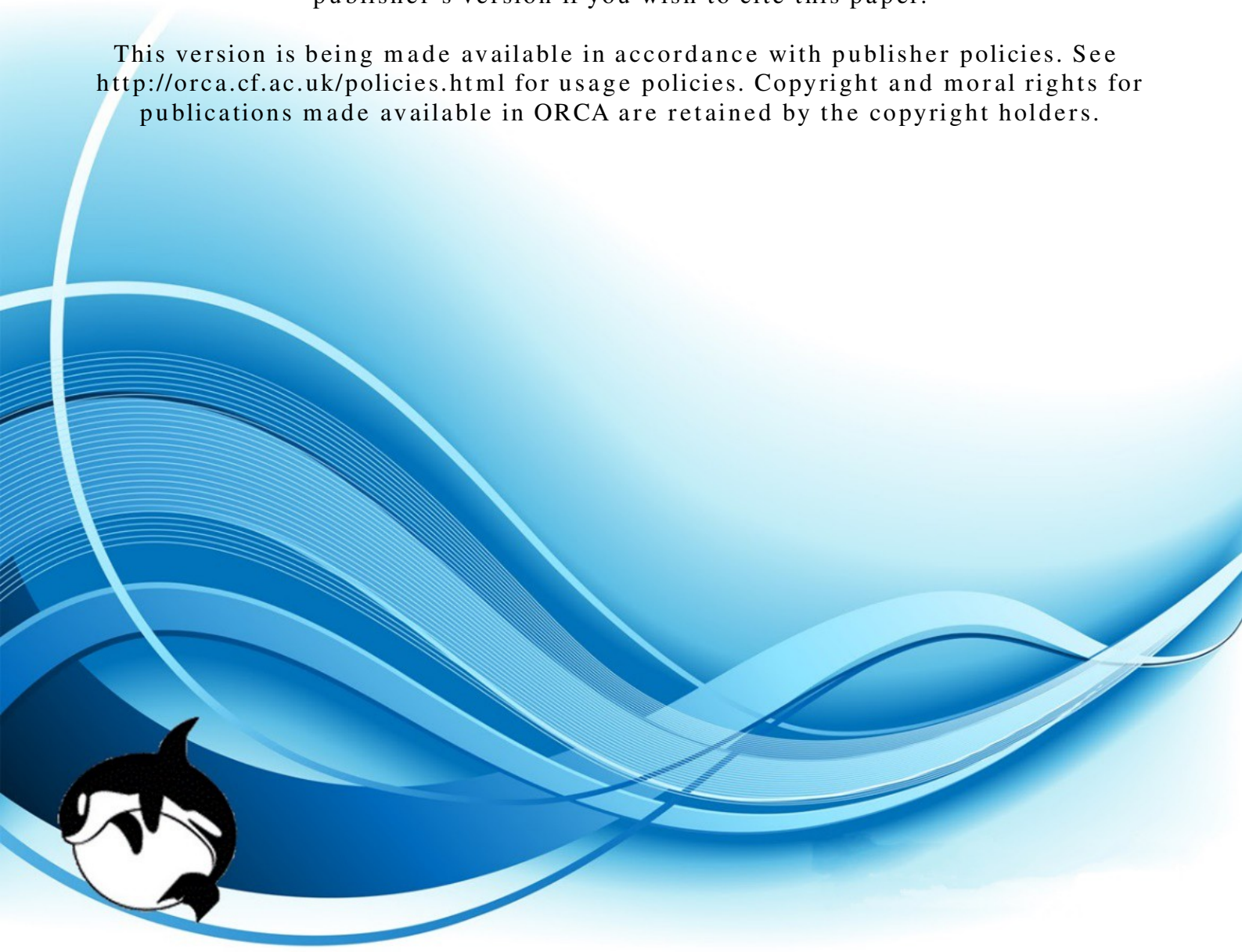


PharmaCrypt: Blockchain for Critical Pharmaceutical Industry to Counterfeit Drugs

N. Saxena
School of Computer Science and Informatics, Cardiff University, UK

I. Thomas
Department of Computing and Informatics, Bournemouth University, UK

P. Gope
Department of Computer Science, University of Sheffield, UK

P. Burnap
School of Computer Science and Informatics, Cardiff University, UK

N. Kumar
Department of Computer Science Engineering, Thapar Institute of Engineering and Technology, India

***Abstract*—This research analyses the impact of counterfeit drugs on the healthcare supply chain industry and evaluates the solutions currently in place to reduce the number of fake counterfeits coming to the market. The discussions are undertaken to determine what conceptions industry professionals have about applying Blockchain in the pharmaceutical industry, especially in the supply chain. The obtained feedback information is used to build requirements for a Blockchain driven tool called "PharmaCrypt". This tool will be used to track and trace drugs as they move through the supply chain, uploading the data collected to a distributed Blockchain ledger validating the authenticity of the drug. Through a setup, we have built a tool prototype that uses the Amazon Web Services Blockchain platform to show the feasibility of implementing such technology within the industry.**

Keywords- Blockchain, Counterfeit drugs, Pharmaceutical industry, Security, Amazon web service.

Introduction

The presence of counterfeit medicines within the healthcare industry is evident with 1 in 10 medical products in developing countries being substandard or falsified [1]. Falsified medicines can contain incorrect ingredients and doses or show no presence of the active ingredient. This means that there are millions of patients unaware that they are taking medicines that fail to work as prescribed. Not only will they fail to treat individuals, but some counterfeits can cause serious illness or even death. A modeling exercise developed by the University of Edinburgh estimates that 72,000 to 169,000 children may be dying each year from pneumonia due to substandard and falsified antibiotics [1]. Counterfeits are a huge commercial drain for individuals, health care systems, and in some cases, can lead to a further financial burden on the health care system if the patient requires treatment consequently.

Problem Statement

The healthcare industry is rife with counterfeit drugs that penetrate the industry's supply chain [2]. This is due to a complex supply chain, compounded by a lack of visibility of the products end-to-end journey. The effects of falsified and counterfeit drugs have the potential to cause devastating consequences.

The complexity of the drug distribution supply chain makes it difficult to prevent counterfeits infiltrating the industry. There are numerous companies involved in the supply chain where drugs change ownership between manufactures to distributors, repackages and wholesalers before reaching the patient. There is little or no visibility between the parties involved in the supply chain in order to track the authenticity of the drug. This causes a level of uncertainty for patients and dispensary's concerning the authenticity of the product sold at the end of the chain.

There are currently several solutions to the problem, but as the sophistication of counterfeit products and packaging rapidly improves, they have flaws and limitations. Some solutions endeavour to trace transactions of the products as they move through the supply chain and change ownership, although there is still a central organisation present that is at risk of being compromised whereby documents can easily be falsified. Also, a central system is prone to a single point of failure. Solutions like our proposal could potentially be adapted to include the anti-tampering and distributed database capacities of Blockchain.

Proposed Solution and Contributions

The proposed solution is to create a Blockchain driven tool that can be used to record and timestamp the transfer of goods at each point in the pharmaceutical supply chain. As the drug travels through the supply chain, every transaction of goods will be noted and timestamped by scanning the barcode. The ledger will be used in order to ensure the security and safety of the product. A three-fold contribution to this work is as follows:

- Analysis of the problem and a demonstration whether utilising Blockchain could be a better solution to the supply chain of drugs than the existing solutions.
- Designing and creation of an application tool that can be used to record the origin of the drugs manufactured, its contents and timestamp the transfer of goods.
- Provide recommendations based on the tool's functioning as to whether (and how) utilising Blockchain technology is the best way to solve this problem.

Background Study

This section discusses the problem domain in greater depth, highlights existing solutions and evaluating their limitations. The segment will also deliberate as to why a Blockchain solution could be an improved idea compared to the current solutions.

Drug Supply Chain in the Pharmaceutical Industry

The Pharmaceutical supply chain is the means in which prescription medicines are delivered to patients [3]. Ingredients for medicines are normally sourced from a variety of places before reaching its final formula. Once the final formula is achieved, the drug can be distributed. During the supply chain life cycle, the drug will transfer among many different entities, specifically between the manufacturer and the patient. Every transaction offers an opportunity for counterfeit or falsified products to penetrate the supply chain and the industry. Figure 1 shows a typical supply chain scenario in the Pharmaceutical industry.

Manufacturers, Wholesalers and Pharmacies The Manufactures' role within the supply chain is to ensure the readiness of their inventory of drugs so they can be distributed to wholesalers. Manufactures receive orders from distributors/wholesalers, they then ship the products to the distributor's warehouses where they will be put away in storage. Distributors will provide manufactures with inventory data reports to maintain transparency throughout the process.

The role of wholesalers is to make the process of purchasing pharmaceutical drugs a simpler and more efficient process. Wholesalers connect and deliver to thousands of pharmacies and dispensers. This saves manufactures efforts of dispatching drugs to pharmacies individually, instead they can send large batches of medications to

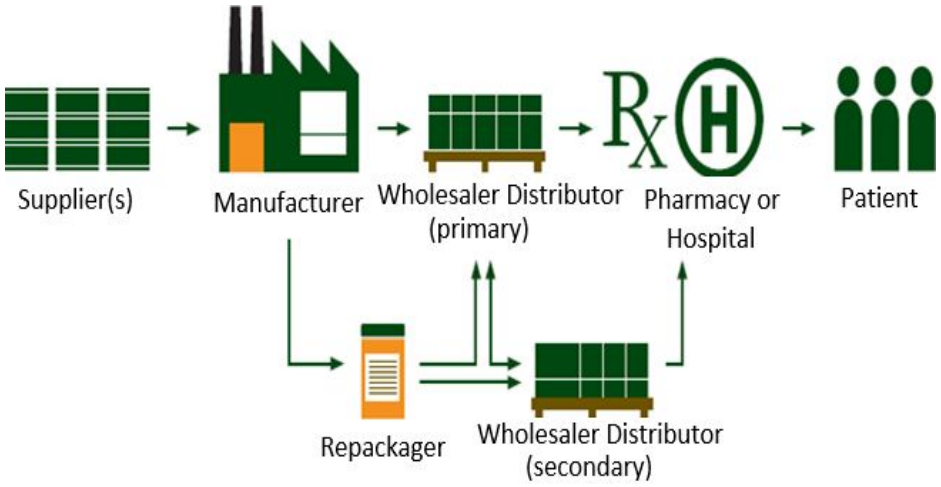


Figure 1: Pharmaceutical supply chain.

a relatively smaller number of wholesalers in comparison. Once the product is in the hands of the wholesaler, they provide a range of services, including drug distribution, electronic order services and repackaging.

The final entities in the supply chain is Pharmacies and Hospitals. Pharmacies account for approximately 75% of the prescription drug market, whereas Non-retail providers such as hospitals comprise the remaining 25% [4]. Pharmacies and Hospitals purchase products from wholesalers where they are then sold to the final patient.

The Wholesaler Problem Primary wholesalers have direct distribution contracts with the manufactures they purchase from. Whereas, secondary wholesalers purchase products from a range of other parties. Shown by the arrows between the two wholesalers in Figure 1, it may not always be obvious to distinguish whether a company is a secondary or a primary wholesaler. For example, a primary wholesaler may not only purchase products directly from the manufacturer, they may also purchase from secondary wholesalers depending on the demand for certain medicines. The buying and selling between wholesalers is common within the industry, products move between a variety of different companies and can be repeatedly repackaged by each wholesaler before reaching the patient.

In a process called Sating, counterfeit drugs can be merged and be confused with legitimate products at the wholesalers. This can be caused unknowingly if for example a wholesaler purchases from a secondary wholesaler company where they have accidentally purchased counterfeit goods. During the repackaging process at the wholesaler, the counterfeit drugs may be given genuine labels. Manufacturers initially deliver medicines in fraud protection packaging. These can be removed during the repackaging phase and batch numbers may be reprinted.

Drug Diversion Drug diversion is when drugs that have been authorised to be sold in one country are sold in another. Criminals take advantage of segments in the supply chain where products leave a documented chain of custody and they can implant falsified goods. Markets that trade in diverted drugs usually have little oversite from authorities and are known as Grey markets.

Existing Solutions

This section briefly discusses the current solutions that are in place.

Packaging In an attempt to reduce the impact of counterfeit drugs, several pharmaceutical companies have adopted a more sophisticated packaging approach. One of these approaches is the use of holographic technologies. The concept is that a patient will know if the product is legitimate when they see that the packaging contains a hologram. A major advantage of this type of packaging is that it can be applied to every individual item. Although, this type of packaging

Table 1: Comparing Existing Solutions

Solution	Pros	Cons
Packaging	Easy for patients to determine whether the drug is legitimate if they see a hologram on the packaging	Expensive, Can be cloned, Origin of fraudulent products cannot be located
Mass serialization	Ability to track and trace, Chips can be disguised in large batches to avoid tampering	Costly, Potential to be hacked, Compatibility issues, Chips have the potential to be tampered with
Mass encryption technology	Each batch is given a unique code to them	Complicated to implement
Falsified Medicines Directive	EU wide directive, Set the standards for all Manufacturers	Only exists in the UK, Packaging can be forged, A centralised authority that could be liable to attack

can be costly to implement depending on the complexity of the hologram. Holograms can also eventually be cloned by counterfeit companies making the original secure packaging ineffective. Another disadvantage to this solution is that it does not offer companies intelligence for when a counterfeit product penetrates the supply chain.

Mass Serialization Mass serialization is a technology used to identify and track objects and individuals using radio frequency waves. Manufacturers can use Radio Frequency Identification (RFID) coding to allocate packages with unique identifiers. As the product makes its way through the supply chain, the products information is captured by a chip reader. The chips can be disguised within large batches of products to avoid tampering. However, RFID is costly to implement as the RFID tags themselves are expensive. There are many types of systems that include varied readers and tags creating compatibility issues [5]. Another concern with the technology is that they have the potential to be hacked and information on the tags can potentially be altered [6].

Mass Encryption Technology Software based mass encryption technology can be used in the pharmaceutical industry to fight against counterfeit drugs. The same software is required to decrypt the digital code [7]. This technology requires a large database server to store the data.

Falsified Medicines Directive: Safety Features The Falsified Medicines Directive is an EU directive (as of 9th February 2019) that aims to ensure that medicines in the EU are safe by including a unique identifier and an anti-tampering device on the packaging and a trade of them is properly controlled [8]. As the product goes through the supply chain, at various point it is mandatory that the barcode is scanned again. This aims to certify the authenticity and trustworthiness of the medicine supplied. The unique identifier on the packaging must encompass a product code determining the medicine name, common name, Pharmaceutical form (strength, pack size and pack types), serial number, batch number and expiry date.

Manufacturers are required to comply with this EU directive as of 9th February 2019. Table 1 displays the pros and cons of the current solutions discussed.

Why Blockchain?

This section explains why we believe that Blockchain is the suitable solution.

Blockchain - Technical Feasibility

Blockchain is a digital technology model that can be utilised to store data, it consists of a chain of blocks containing transaction information [9]. It is a decentralized system where data can be shared across a network in an encrypted fashion.

Before a transaction can be added to a Blockchain, it needs to be verified by the network nodes by utilizing a majority consensus protocol, where nodes on the network agree that the transaction is legitimate. Any transactions that have been recorded cannot be altered or erased and the full transactional history can be viewed at any time. Each block in the chain contains data: the hash of the block, the hash value of the previous block and the nonce of the existing block. Hashing is used to make integrity-protected blocks together to create the secure chain. Every data block in the Blockchain is given a unique digital signature that directly corresponds to the data in its block (the hash). If the data in the block is

changed, the digital signature of the block will also subsequently change.

A block registers transactions as they occur and the Blockchain increases in size periodically as new transactions execute. Once the block is filled, it is allocated a digital signature that directly corresponds to the string of data in that block (hash). The first block in the chain is known as the genesis bock and do not point to any previous blocks. In order to link another block of transaction data, the signature in the first block is added to the data of the following block. The digital signature of the second block is now partially dependent on the signature of the block before it, as it is included in the data of the block. This process is repeated every time new transactions occur to create the chain.

Blockchain Platforms

We discuss three main platforms that were considered in this work - Ethereum App Platform, Amazon Web Service (AWS), and Oracle Blockchain.

Ethereum App Platform Ethereum is a public distributed Blockchain network that provides users with the appropriate environment to deploy decentralized applications. The platform runs the smart contracts that have been set by the application developer. The Ethereum network is made up of a series of distributed nodes and Ethereum wallets. The distributed network of nodes is established when computers or miners join the network. The network does not hold any permissions to join, as any node with enough computing power is able to join the network.

Amazons Web Services (AWS) Amazons Web Services provides cloud computing platforms. Amazon offers Blockchain templates as part of their platform, which provides users a simple way to build Blockchain applications for businesses. AWS provides the ledger database behind the application that eradicates the need for the application owner to develop the complex Blockchain network. The service offers two types of use cases: to track and verify transactions with centralized ownership and execute transactions and contracts with decentralized ownership [10]. Using the AWS Blockchain template, an Ethereum Blockchain network on a cluster made up of multiple instances with an Application Load Balancer (ALB) can be created.

We have used AWS platform since its service makes easy to setup, deploy, and manage scalable blockchain networks, which eliminates the need to rely on other expensive implementations.

Oracle Blockchain Oracle is extremely similar to AWS as it is a Blockchain-as-a-Service (BAAS) provider. It offers businesses to deploy applications over an immutable electronic distributed ledger database.

Blockchain Security

Blockchain not only allows user to integrate with suppliers, customers, regulatory agencies and stakeholders, but also provides such a high degree of accuracy [6]. It also offers a higher level of security compared to the existing solutions.

Immutability and Consensus The immutable characteristics of Blockchain is one of the main reasons companies are starting to implement the technology. If a block is altered, it will unchain itself from the consecutive blocks. For an altered block to be accepted on the Blockchain, it needs to be chained to the rest of the blocks. All the nodes in the network work together to create a consensus about which blocks are valid and which are not. Users in the Blockchain will be notified that data has been altered and will deny the change. The Blockchain will then be returned to a previous state of the Blockchain where all blocks are still chained together.

Private Keys Participating nodes in the network are assigned their own private keys that are linked to transactions they make. The private key is used to create a digital signature and sign each transaction. Each node in the network is allocated a private key, which grants ownership to their data entry [11].

Decentralization Rather than relying on a single database to secure transactions with users, Blockchain is completely decentralized. This means there is no single point of failure. Being decentralized means that there are multiple copies

of the same transactions, a hacker would need to change all copies and break the consensus protocol before they could alter anything.

Existing Solution Case Study: Cisco Supply Chain Management

Cisco loses out on over $500 million dollars of revenue a year due to counterfeit products (similar to the UK loses £218 million every year from counterfeit wine and spirits [12]; clearly it is not just a problem faced by the developing countries). As a result of this, Cisco are currently working on a Blockchain solution designed to combat against counterfeit products on their own supply chain. Although Cisco works in a different industry to the one the projected in this work, their application of the technology is extremely similar. A few other Enterprise Blockchain use cases include [13]: Supply Chain Management (IDM Food Trust), Protecting Digital Identity (Civic's Secure Identity Platform), Smarter Predictive Analyses (Endor), and Healthcare Medical History and Records (Medicalchain).

There are some limitations too with the technology and we must know how these drawbacks might be overcome. As the participation of each organisation in the supply chain requires complex infrastructure to be able to run a single node, one of the main issues with Blockchain is the cost of this infrastructure. To be able to sell the solution to customers and suppliers, it is hard for them to justify the cost. A possible resolution for smaller companies could be to provide a cloud-based solution, but it is not quite clear that how well does this scale up. There is currently lots of research being carried out to work out ways of reducing the costs and monetising the process of Blockchain.

Another limitation of Blockchain arises when considering the consensus mechanism used. There are multiple consensus protocols available. In a public Blockchain, it is possible to specify a single consensus mechanism used. Although, in a private enterprise solution, it is not possible to make an application as rigid. There is ongoing research on how to make the consensus as quick as possible and pluggable so that suppliers can appoint the consensus they wish to use. For a Blockchain enterprise application to be successful, the consensus times need to ideally be minutes or seconds. When choosing a consensus mechanism, it is important that the protocol is Byzantine Fault Tolerant.

Proposed Solution: Requirement and Analysis

During the analysis stage of this work, professionals working or researching on the Blockchain as well as in the pharmaceutical field were contacted and collaborated with. The whole purpose was to determine the current use cases of Blockchain that are in practice in the industry, people's conceptions of the technology and how staff in the pharmaceutical industry might cope or react to a new supply chain management system.

Pharmaceutical Interviews/Discussions

The participants chosen were individuals who either work in the healthcare industry in a dispensary/pharmacy or as a pharmacist.

Pharmaceutical Feedback

We have interviewed 30 people who are directly or indirectly working in pharmaceutical industry. Roughly 60% of the people said they were aware of the counterfeit drugs problem. Medicines are scanned on arrival, but this is more for stock check purposes than authenticity. The Medicines and Healthcare products Regulatory Agency (MHRA) regularly alerts us if there are any concerns regarding medicines and these are relayed to all pharmacies and dispensary's with relevant batch numbers, they added. If you look at what the Falsified Medicines Safety Features Directive (FMD) requires, it might give you a good idea on what to include. Off the top of my head, I believe it is required that manufactures provide the name, serial number, expiry date, strength and batch number, but there maybe more. To the answer of whether they will put their trust in a Blockchain driven application that was designed to track and trace a medicine as it makes its way through the pharmaceutical supply chain, most of the people were interested. The information gathered indicated that the most important material perceived by pharmacists required by an application (tool) to ensure the trustworthiness of a product would be: batch number, name, expiry date and manufacturer. The majority of people interviewed suggested barcode scanning is

already in used for barcode scanning in their day-to-day job and implied that they would consider using an application (tool) that requires the use of barcode scanning. The original data collected from the focus group and interviews can be found in the Appendix.

Setup and the "PharmaCrypt" Tool

This section explains the experimental set up for the development of the proposed application tool called "PharmaCrypt" using Ethereum Blockchain, which is created using the Amazon Web Services (AWS). The tool interface can be seen in Figure 2. The network is utilised to create a smart contract where products can be created and transferred between accounts.

PharmaCrypt Features

The developed prototype of the tool has the following features:

- *Barcode Scan:* Hand-held smart phone devices are able to scan barcodes and upload the information to the Blockchain.
- *Asset Creation:* The application is able to create new assets for when products first enter the supply chain. A products information is uploaded to the Blockchain number and assigns a unique identifier number.
- *Transfer of Asset:* When a product is moved on to the next supplier or entity in the supply chain, the application tool records the transaction.
- *View Scanned Products:* User is able to view all products scanned by them.
- *Performance Requirements:* The application tool scans barcodes instantly with no lags or glitches. Consensus should be reached under a few seconds.
- *Security Requirements:* (i) Separate accounts for each user, (ii) Users are enrolled with their business network accounts, (iii) Each password is at least 8 characters long composed of at least 1 upper case letter a number and 1 special character, and (iv) Each user is operated using the least set of privileges required to do their job.

Blockchain Implementation

Amazons Web Services is chosen to create the prototype of the proposed tool. The overall software is hosted on a computer-based system, which is configured with i7 processor, 500GB HDD, 4GB RAM, and Windows 10 OS, and the required data can be fetch to a mobile application. The AWS Blockchain for Ethereum creates a private Blockchain network on the AWS CloudFormation. The final network is made up of the following entities: two Ethereum clients, one miner running on Amazon EC2 instances in an Amazon EC3 cluster, on-Demand EC2 instances, and an internal Application Load Balancer (ABL). The entire process of the proposed solution and building the PharmaCrypto tool is as follows:

(i) PharmaCrypt Tool Interface: As the functions of the application tool run on smartphone devices are relatively limited, the user interface, as shown in Figure 2, will largely be the same for each company. Here, the user will be able to scan the barcode of the product. Once the barcode has been scanned, if the transactional data is deemed legitimate by the network, it will be automatically uploaded to the Blockchain. Users of this interface will only be able to view the transactions they have scanned themselves. If the transaction is deemed illegitimate by the Blockchain network, an error message will take over the screen. The error message will trigger a notification sent to the main computer-based interface controlled by a senior personal. The supply chain management team can then investigate this product further. Figure 3 explains the information flow of the proposed solution.

(ii) Key Pair Generation: AWS uses public-key cryptography to secure the login information of the instances in the network. As shown in Figure 4(a), we created a key pair for the Blockchain Ethereum network, which is used to sign every transaction over the network. The key pair must be created in the same region you wish to launch the instance in. The key pair will download and the file name is the name you specified with a .pem extension.

(iii) Subnets, Security Groups, and Rules: The Amazon Virtual Private Cloud (VPC) is used to define the virtual network where resources will be launched. An Application Load Balancer (ALB)

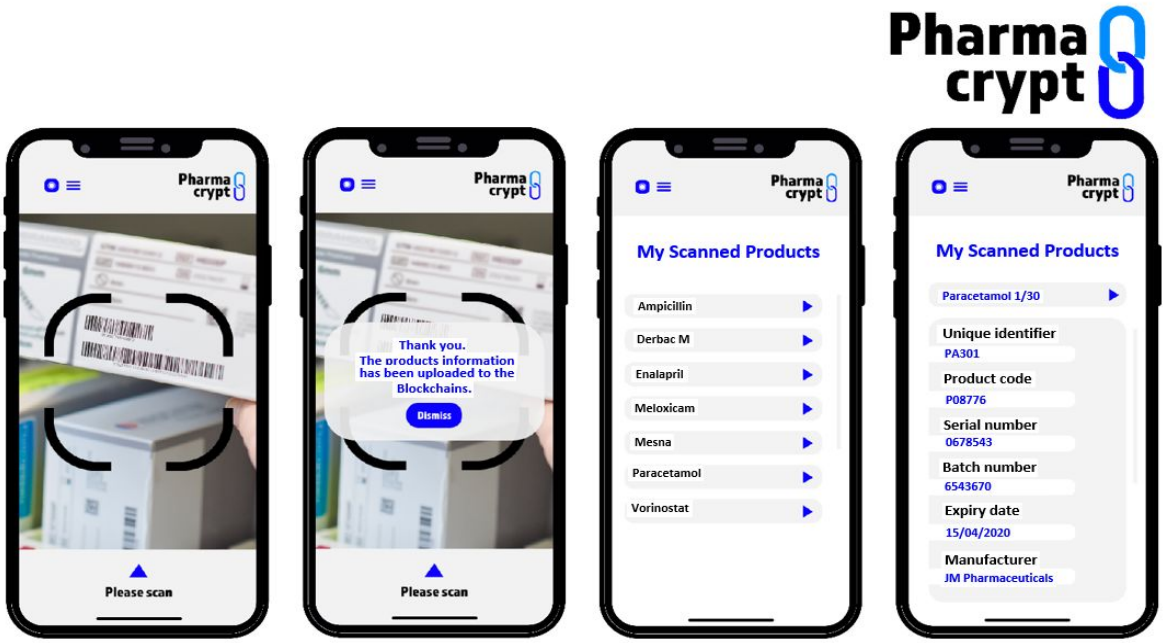


Figure 2: Proposed "PharmaCrypt" Application Tool User Interface.

is created requiring two public subnets to be configured locating in two separate availability zones. A private subnet is also necessary for the container instances. The availability zone should be located in the same zone as the ABL.

AWS Security groups control the inbound and outbound traffic to your resources. We specify two security groups: one is for controlling the traffic between the EC2 instances in the cluster and the other is for controlling the traffic between the Application Load Balancer, EC2 instances and the bastion host. Thereafter, we have applied the following incoming rules to these groups, as shown in Figure 4(b):

- Allow all traffic from the ALB security group allowing the ALB to broadcast with itself and the bastion host.
- Allow all traffic from the EC2 security group allowing instances in the security group to broadcast to the ALB and the bastion host.
- Allow SSH traffic from the IP address which allows traffics from the computer to the bastion host.

The below outbound rules also need to be applied on the same security group:

- Allow all traffic from the EC2 security group which allows outbound traffic from the ALB and the bastion host to the instance.
- Allow all traffic from the ALB security group which allows the ALB to communicate with the bastion host and itself.

(iv) Identity and Access Management (IAM) and Bastian Host: We have created a role for AWS service selecting Elastic Container Service for the service and Elastic Container Service for the use case. Make a note of the Role - Amazon Resource Name (ARN), as it will be needed later. The Bastion Host is an Instance that is used to connect to the web interfaces and other instances in the network. To do so, the Bastion Host forwards SSH traffic from trusted clients that are outside of the VPC.

(v) CloudFormation Stack: Now the tool has been configured and the Ethereum Network can be created. To do so, an AWS CloudFormation Stack needs to be set up. The AWS CloudFormation Stack establishes an Amazon EC3 cluster of EC3 instances. Launching this stack create some nested stacks where we are able to connect to the networks resources using the Bastion Host. In the dashboard, their progress can be observed by selecting "Stacks". When the Stacks have finished creating, the Output tab displays

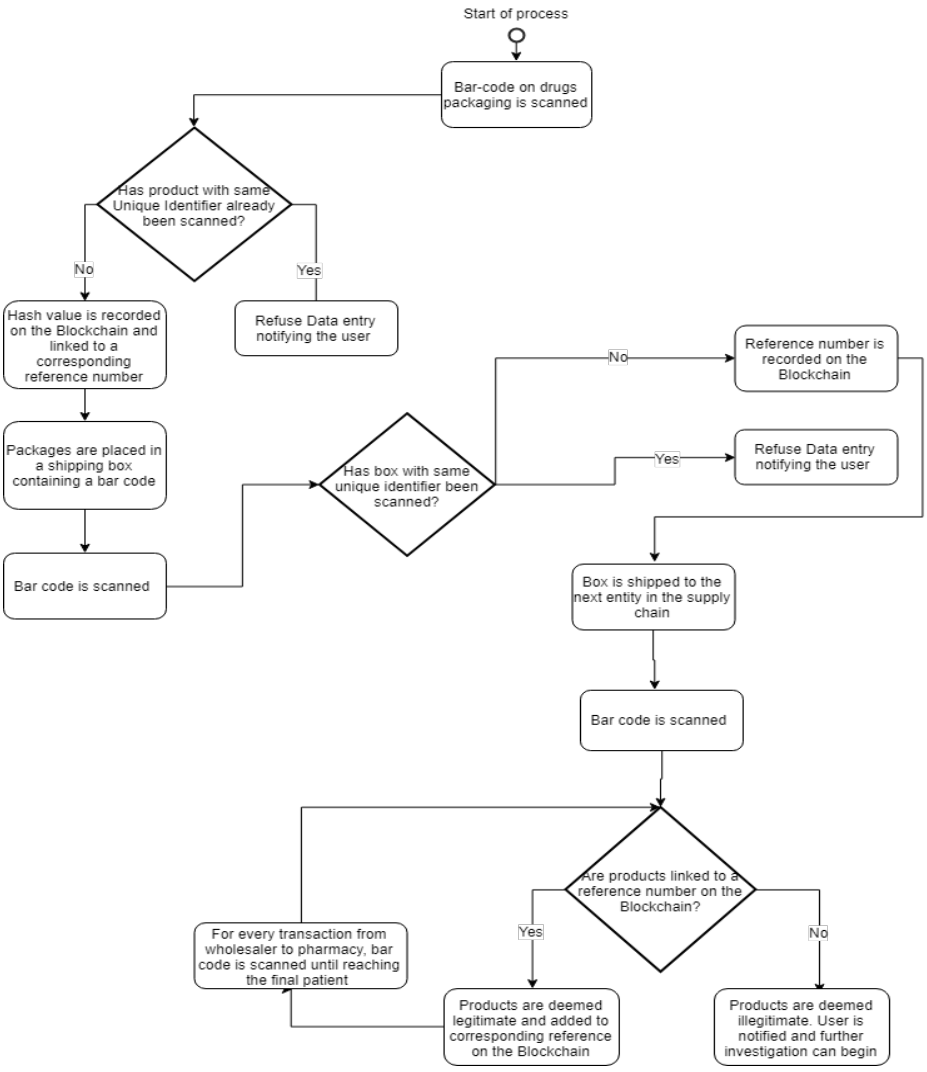
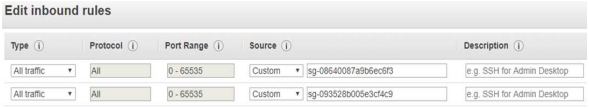


Figure 3: Proposed solution information flow.

(a) Key pair creation for signing the transaction data.

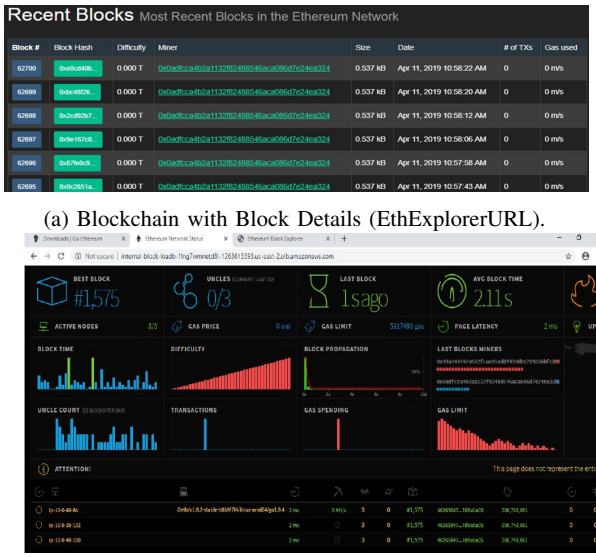


(b) Security group control: inbound rules for the traffic.

Figure 4: Key-pair generation and security group control.

Ethereum URLs we can connect to where the EthStats (shows the time since something was mined), EthExplorer (Blockchain explorer) and EthJsonRPC (a stateless, light-weight JavaScript Object Notation (JSON) Remote Procedure Call (RPC)) are displayed.

(vi) Connect SSH port, Authenticate, and Setup a Proxy: Now, to connect to the bastion host, an SSH port forwarding connection is established using PuTTy. The key pair needs to be converted to a .ppk format as PuTTy does not support the default .pem format. WE have used RSA for the key generation. We have set the following configurations: select Connection, SSH, Tunnels; add 9001 as the source port and leave destination as default (blank). Thereafter, use



(a) Blockchain with Block Details (EthExplorerURL).

(b) Ethereum Blockchain Real-Time Network Status.

Figure 5: Ethereum Blockchain Network with Block Details.

"Open" to authenticate the bastion host. We have then configured a proxy (FoxyProxy for Chrome browser) on port 9001 so that the forwarded port can be used to connect to the Ethereum URLs.

The EthStatsURL displays the status of the Ethereum Network. The EthExplorerURL where transactions that have been made on the network, is shown in Figure 5.

(vii) Smart Contract, Genesis Block Creation, and Mining: Now, we need to create smart contracts and run them (with Admin permission) on the Blockchain network as shown in Figure 6. To do this, we connect over to the Windows Bastion Host using Remote Desktop Protocol (RDP) with a decrypted password (using .pem private key). Ethereum Wallet (allows to manage Bitcoin, Ethereum, XRP and over 300 coins and tokens) and geth (a command line interface for running a full Ethereum node implementation) are not designed to securely connect to the remote nodes in the network using RPC. To set up a secure connection, we run a local geth node that joins the network.

The Genesis block is the first block in the Blockchain network. The genesis block must be compatible with the private Blockchain network that has been created. Creating a genesis block allows you to sync the node with the network. To do so, define static node mapping in a JavaScript Object Notation (JSON) file using the information available in the Amazon DynamoDB table.

Now, the geth client needs to be initialized to use the genesis block you constructed. Thereafter, use Ethereum Wallet app to store the keys, contracts, tokens and ether. We have used mining with two threats for this demonstration work. Now we have Ether, so we deploy the first smart contract "Product Tracker" (Ethereum Wallet application → Contracts → Deploy New Contract). The smart contract uses the solidity coding language to create (using Remix tool) and transfer assets on the Ethereum Blockchain network.

Discussion

To demonstrate the working of this tool, we have used permissioned Blockchain, which is in fact more scalable and faster, but works towards centralized controls among a group of users (who were involved in this work). However, this work can be easily extended to permissionless Blockchain, when required, so that any registered user can validate transaction information and this will be tested with trials. We have tested this tool with 50 users making transactions on different items to demonstrate that this tool is useful for small and medium size pharmaceutical applications and we will further extend its capabilities (by testing) for the applications with a wide variety of drugs and a large number of users involved in the system. We have performed mining on the cloud without an Application-Specific Integrated Circuit (ASIC) miner. It does not yield any profit, but the primary purpose of having it to able to demonstrate the working of this prototype tool, which at present will be used privately with limited number of drugs and users involved in the system.

Comparison

Compared to Drugledger in [11], the proposed consumer-oriented application tool provides more controllability, user-friendly interface, added security through groups, and private network virtualisation. The proposed "PharmaCrypt" does not require Certificate Service Provider, Anti-attack Service Provider, and Query Service Provider, which is a requirement for the Drugledger . In other words, the proposed tool generates less

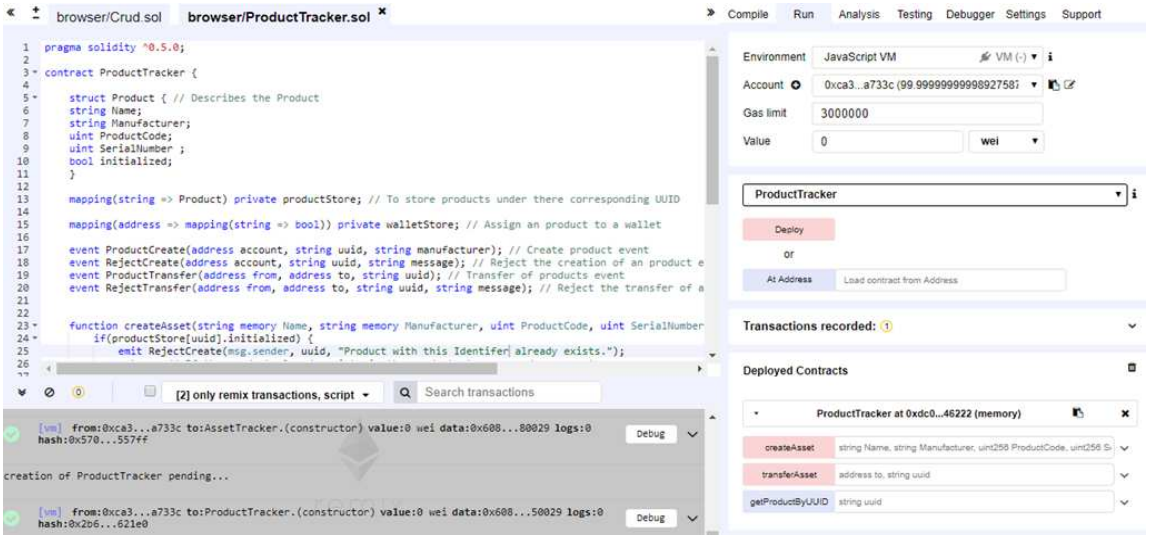


Figure 6: Smart contract in Remix.

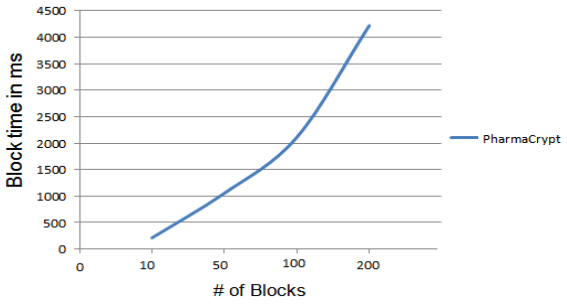
Table 2: Comparing Blockchain Solutions

Solution	Drugledger [11]	PharmaCrypt
Basic requirements included	More focus on packaging and repackaging (overall less efficient)	More focus on rapid scanning the product (barcode scanning), asset creation and transfer (overall much efficient)
Overhead	High, due to the maintenance of certificates, per transaction user weight computation, repackage	Low, none of them are required
Technology	Platform dependent, C++ in Ubuntu 16.04 LTS	Platform independent with AWS
Extra requirements for security support	Requires certificate of service provider	Free from such requirement
Performance (efficiency)	not specifically discussed, but much slower	Improved using barcode scanning, average block time 2.11s, page latency 2 ms, and consensus available in a few seconds
Security key and hash storage	There are issues with storing the public key and hash codes	There are no such issues as the AWS storage takes care of it

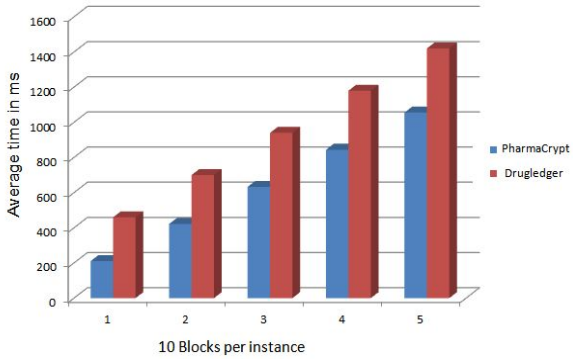
overhead compared to the Drugledger. A detailed comparison between the PharmaCrypt and Drugledger is presented in Figure 7.

Apart from this, a smart contract using smart storage containers is proposed in [14], which is based on a multi signature wallet of three parties to process the payment and arbitrate disagreements. The application requires extra hardware and protocol implementation, which is time consuming as well as not efficient. Similar to the approach in [6], the proposed tool is able to defeat tampering, spamming, physical layer attack, and preferential treatment. However, the approach in [6] requires new sensors, their set up, and a significant large storage for the algorithms to run. Whereas the "PharmaCrypt" does not rely on extra sensors, rather it used existing technology of scanning the barcodes. The only drawback of the proposed tool is that it may be affected by the service provided by AWS, as it is based on the AWS Blockchain.

A performance comparison between the PharmaCrypt and Drugledger is shown in Figure 7. The system used is 64 bits Windows 10 with core Intel i5 2.60GHz and 4GB RAM with Java. For generating random strings we have considered UUID.randomUUID().toString() and used System.currentTimeMillis() for calculating timestamps and execution times. SHA256() takes 20 ms for generating hash code for each block. Further, it took 1 ms each to create block lifetime, Merkle root, timestamp, and version. Due to the insufficient implementation details available in Drugledger [11] (the details are not provided, so we created simple functions for SynchronizeUTXO() - 20 ms, ReadDrugPackage() - 10 ms, GetUTXO() - 20 ms, ValidQuery() - 20 ms, CreateTX() - 20 ms, Gossip() - 10 ms, and IsCor-



(a) PharmaCrypt average block time where # of blocks range from 10 to 200.



(b) PharmaCrypt vs. Drugledger block time where # of blocks range from 10 to 50.

Figure 7: Details on average block time.

related() - 10 ms), we have assumed similar type of parameters and their sizes as the PharmaCrypt. Figure 7(a) demonstrates the average block time when number of blocks are 10, 50, 100, and 200. Figure 7(b) reflects on a comparative instances of average block time when number of blocks are 10, 20, 30, 40, and 50 for PharmaCrypt and Drugledger. Overall, it is clear that the PharmaCrypt outperforms Drugledger and is better suited for such an application.

Alzahrani et al. [15] proposed (i) BlockSupply, a decentralized anti-counterfeiting supply chain that is based on NFC and blockchain technologies and (ii) a decentralized consensus protocol. However, it is not clear whether this protocol can be used for Blockchain-related applications such as PharmaCrypt. Wang et al. [16] combined the emerging Blockchain technology with parallel healthcare systems for comprehensive healthcare data sharing, medical records review, and care audit-ability. However, implementation aspect of work is not discussed in detail. Jamil et al. [17] proposed a novel drug supply chain management using Hyperledger Fabric based on Blockchain technology to handle secure drug supply chain records. An open source framework Hyperledger fabric is used, but it is not much clear whether it supports existing healthcare systems and their services. We will further extend this research and see if any of these work can be extended and integrated with PharmaCrypt.

Conclusion and Future Directions

This work has analysed the counterfeit drugs' problem and existing solutions evaluating their effectiveness. The inputs from the relevant industry professionals working in both pharmaceuticals industry and in Blockchain technology are considered, which has actually helped to scope the requirements for the proposed application tool. In our primary research, 100% of the pharmacists interviewed were aware of the counterfeit drugs problem, underlining just how widespread and severe the issue is within the healthcare industry. The work is being done in an attempt to fight the issue, however, the current solutions have with a number of issues and limitations.

Further research is required to look at how we can achieve the smallest amount of time it takes for a transaction to gain consensus. When using an application, such as the one described, it is important that this time is as low as possible, otherwise it will not be efficient for suppliers to use. Another need for further research would be to look at how might it be possible to lower the cost of implementation or understand how the solutions may drive down other supply chain operational costs in the pharmaceutical industry so that the technology is commercially viable for larger enterprise solutions. Furthermore, the supply chain management system could be linked to a wider solution. There is currently work being undertaken to develop an Electronic Patient Record system that can be used to store patient's records on a Blockchain. This system could potentially be combined with a supply chain solution where by records in the Blockchain could contain both patient treatment records, alongside prescription history.

The Falsified EU Directive and RFID technology are currently the most effective in addressing the problem, up until now. The Blockchain solution would be able to incorporate the compliance

regulations so that the tool logs and tracks the information needed to comply with the directive. The way in which the Blockchain tool is used can mimic the RFID Mass serialization process, scanning of products can be carried out at the same points in the supply chain. This should enable a smooth transition to the new technology. Utilising the proposed solution, i.e., PharmaCrypt, means that both patients and dispensaries will be made certain of the provenance of the drug. The developed tool is relatively simple, meaning staff should not need extensive training due to existing product scanning experience in dispensaries.

Blockchain also has its limitations. Blockchain has a scalability issue attached to it. At this stage, it would be difficult to deploy a Blockchain solution to all parties involved in the supply chain. Large scale deployments across multiple customers would require much more rigorous testing to ensure success. Further research is required to look at how we can achieve the smallest amount of time it takes for a transaction to gain consensus. When using an application, such as the one described, it is important that this time is low as possible otherwise it will not be efficient for suppliers to use. Another need for further research would be to look at how might it be possible to lower the cost of implementation or understand how the solutions may drive down other supply chain operational costs in the pharmaceutical industry so that the technology is commercially viable for larger enterprise solutions.

On reflection, we believe that the proposed solution (PharmaCrypt application tool) has the capacity to be developed towards a successful working service and can be used as the basis for further research and development.

Appendices

Interview Answers and Questions

We have interviewed 30 people who are directly or indirectly working in pharmaceutical industry.

Q1. Are you aware of the counterfeit drugs problem in the pharmaceutical industry?

A1. (i) Yes X 19

(ii) Yes, but I believe it to be more of a problem in developing countries than in the UK. X 4

(iii) Yes I am aware, but I have never experienced it myself X 5

(iv) Yes. As a chief pharmacist of an NHS trust and a responsible person on a WDA from the MHRA I am acutely aware of the potential for falsified medicines entering the supply chain.

Q2. Do you know if there are any products or systems in place that are used to track and trace a drug through its supply chain before it gets to the dispensary? If yes, could you explain what?

A2. (i) I don't know X 4

(ii) The Falsified Medicines Directive is currently being implemented X 9

(iii) EU Directive X 2

(iv) We use registered wholesalers; however, the only system current being implemented is FMD scanning X 10

(v) Scanning the products - Barcodes, QR codes X 4

(vi) Up until recently some products have had 2D barcodes, holograms and tamper-evident packaging to reduce falsification, although the sophistication of counterfeiters now is such that even these can be replicated. The main intervention now is the introduction of the Falsified Medicines Directive which requires licenced medicines to have a 3D barcode, a Unique Identification Number traceable to individual packs, and tamper evident packaging. Each individual pack is tracked via a Europe-wide repository.

Q3. Are there any systems/methods in place you use personally that help to ensure the authenticity of the medicines supplied to customers? If yes, could you explain what?

A3. (i) Medicines are scanned in on arrival, but this is more for stock check purposes than authenticity. MHRA supply regularly alerts us if there are any concerns regarding medicines and these are relayed to all pharmacies and dispensary's with relevant batch numbers. X 2

(ii) No X 6

(iii) Ensuring everything we order is done through our trusted suppliers we use. X 2

(iv) FMD Scanners X 15

(v) Scanner but limited due to possible human error X 4

(vi) Only those already mandated.

Q4. What information about a medicine would you suggest needed to be logged to ensure its authenticity?

A4. (i) Batch number, expiry date, manufacturer X 7
(ii) If you look at what the Falsified Medicines Safety Features Directive requires, it might give you a good idea on what to include. Off the top of my head, I believe it is required that manufactures provide the name, serial number, expiry date, strength and batch number but there maybe more. X 2
(iii) Special packaging X 3
(iv) Name, batch number, wholesaler X 9
(v) Ingredient constituent and manufacturer who has approved it
(vi) Product, batch number, expiry, PL number, manufacturer. X 8
Q5. Would you consider using an application to ensure the authenticity of medicines if it meant scanning the bar code of each drug sold over the counter?
A5. (i) Yes X 17
(ii) Yes, but it's a hassle X 7
(iii) Possibly, depending on the efficiency of the system X 3
(iv) We already scan products so yes X 2
(v) This is effectively what FMD requires for prescription medicines. The same principle for OTC medicines would probably work ok where the process can be combined with another (e.g. scanning at POS).
Q6. Are you aware of Blockchain or cryptocurrency technology i.e Bitcoin?
A6. (i) Yes X 7
(ii) No X 4
(iii) Have heard of it but never used it. X 19
Q7. Would you put your trust in a Blockchain driven application that was designed to track and trace a medicine as it makes its way through the Pharmaceutical Supply Chain? (Blockchain is the technology behind cryptocurrencies like bitcoin)
A7. (i) Yes X 12
(ii) No X 8
(iii) Unsure X 9
(iv) Would consider using it but would need robust evidence and assurance before trusting it completely.

REFERENCES

1. World Health Organisation (WHO), 1 in 10 medical products in developing countries is substandard or falsified, 2017. [online]. https://www.who.int/news-room/detail/28-11-2017-1-in-10-medical-products-in-developing-countries-is-substandard-or-falsified.
2. T. Bocek, B. B. Rodrigues, T. Strasser and B. Stiller, "Blockchains everywhere - a use-case of Blockchains in the pharma supply-chain," IFIP/IEEE Symposium on Integrated Network and Service Management (IM), Lisbon, Portugal, 8-12 May, 2017.
3. D. Yue, X. Wu and J. Bai, "RFID Application Framework for pharmaceutical supply chain," IEEE International Conference on Service Operations and Logistics, and Informatics, Beijing, 2008, pp. 1125-1130.
4. M. Schapranow, C. Faehnrich, A. Zeier and H. Plattner, "Simulation of RFID-aided Supply Chains: Case Study of the Pharmaceutical Supply Chain," International Conference on Computational Intelligence, Modelling & Simulation, Langkawi, 2011, pp. 340-345.
5. P. Behner, M.-L. Hecht and F. Wahl, Fighting counterfeit pharmacueticals. PWC, 2017. [online]. https://www.strategyand.pwc.com/media/file/Fighting-counterfeit-pharmaceuticals.pdf.
6. S. Mondal, K. P. Wijewardena, S. Karuppuswami, N. Kriti, D. Kumar and P. Chahal, "Blockchain inspired RFID-based information architecture for food supply chain," IEEE Internet of Things Journal, vol. 6, no. 3, pp. 5803-5813, Jun. 2019.
7. S. Dechand, A. Naiakshina, A. Danilova and M. Smith, "In encryption we don't trust: the effect of end-to-end encryption to the masses on user perception," IEEE European Symposium on Security and Privacy (EuroS&P), Stockholm, Sweden, 2019, pp. 401-415.
8. Gov.UK, Implementing the falsified medicines directive: safety features, 2019. [online]. https://www.gov.uk/guidance/implementing-the-falsified-medicines-directive-safety-features.
9. R. Kumar and R. Tripathi, "Traceability of counterfeit medicine supply chain through Blockchain," International Conference on Communication Systems & Networks (COMSNETS), Bengaluru, India, 2019, pp. 568-570.
10. AWS, Using the AWS Blockchain Template for Ethereum. [online]. https://docs.aws.amazon.com/blockchain-templates/latest/developerguide/blockchain-templates-ethereum.html.
11. Y. Huang, J. Wu and C. Long, "Drugledger: a practical Blockchain system for drug traceability and regulation,"

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, Canada, 2018, pp. 1137-1144.

12. E. Hancock, The UK loses £218 million every year from counterfeit wine and spirits, Jun. 2018. [online]. https://www.thedrinksbusiness.com/2018/06/the-uk-loses-218-million-every-year-from-counterfeit-wine-and-spirits.
13. S. Aich, S. Chakraborty, M. Sain, H. Lee and H. Kim, "A review on benefits of IoT integrated Blockchain based supply chain management implementations across different sectors with case study," International Conference on Advanced Communication Technology (ICACT), Pyeong Chang, South Korea, 2019, pp. 138-141.
14. J. Hinckeldeyn and K. Jochen, "Developing a smart storage container for a Blockchain-based supply chain application," Crypto Valley Conference on Blockchain Technology (CVCBT), Zug, 2018, pp. 97-100.
15. N. Alzahrani and N. Bulusu, "A new product anti-counterfeiting blockchain using a truly decentralized dynamic consensus protocol," Concurrency and Computation: Practice and Experience, 2019, e5232.
16. S. Wang , J. Wang, X. Wang , T. Qiu, Y. Yuan, L. Ouyang, Y. Guo and F.-Y. Wang, "Blockchain-Powered Parallel Healthcare Systems Based on the ACP Approach," IEEE Transactions on Computational Social Systems, vol. 5, no. 4, pp. 942-950, Dec. 2018.
17. F. Jamil, L. Hang, K. Kim and D. Kim, "A novel medical blockchain model for drug supply chain integrity management in a smart hospital," Electronics, vol. 8, no. 5, pp. 505, 2019.

Neetesh Saxena is an Assistant Professor at Cardiff University (CU), UK and leads the Cyber and Critical Infrastructure Security (CyCIS) Lab. Before joining to CU, he was an Assistant Professor at Bournemouth University, UK, a Researcher at the Georgia Institute of Technology, USA and the Stony Brook University, USA & SUNY Korea. He earned his Ph.D. from IIT Indore, India. He has published several papers in international peer-reviewed journals and conferences. He was a draft committee member for IEEE Standards (IEEE SA 1912 and P2795). He was a DAAD and TCS Research Fellow, and currently is a senior member of the IEEE and an ACM member. Contact him at nsaxena@ieee.org.

Ieuan Thomas has completed his BSc (Hons) in Forensic Computing & Security from the Department of Computing and Informatics, Bournemouth University, UK. He worked on Cyber Security with the Spirax Sarco, UK (2017-18), and is currently working with Aptitude Software. His research interests include Blockchain security, IoT security, and digital forensics. Contact him at i7433979@bournemouth.ac.uk.

Prosanta Gope is a Lecturer in Cybersecurity at the University of Sheffield and is a member of the Security of Advanced Systems Research Group. Previously he was a Lecturer in the Department of Computer Science at the University of Hull. Before joining the University of Hull, he was a Research Fellow in the Department of Computer Science at National University of Singapore (NUS). He was associated with two research projects NETS, and NUS-Singtel Cyber Security Project funded by Ministry of Defence (MINDEF) Singapore, Singtel-Telecom Singapore and Prime Minister Office Singapore, respectively. He has authored over 60 peer-reviewed articles in several reputable international journals and conferences, and has four filed patents. Contact him at p.gope@sheffield.ac.uk.

Pete Burnap is a professor of Data Science & Cybersecurity at Cardiff University. He is Director of Cardiff's NCSC/EPSRC Academic Centre of Excellence in Cyber Security Research (ACE-CSR). He is also leading AI for cybersecurity research at Airbus DTO. He has been involved in grants in worth in excess of £14m, leading large awards from EPSRC, ESRC and industry on the topic of cyber security analytics – the fusion of AI, Cybersecurity and Risk. His research outcomes, which include 80 academic peer-reviewed articles – stemming from funded research projects worth over £14 million, are organised and disseminated via the Airbus Centre of Excellence in Cyber Security Analytics and the Social Data Science Lab. Contact him at burnapp@cardiff.ac.uk.

Neeraj Kumar received his Ph.D. in CSE from SMVD University, Katra, India, and was a postdoctoral research fellow in Coventry University, UK. He is working as a Professor in the Department of Computer Science and Engineering, Thapar Institute of Engineering & Technology, India. He has published more than 150 research papers in leading journals and conferences. He has h-index of 51 (Google scholar, Apr 2020) with 8880 citations to his credit. He is editorial board members of International Journal of Communication Systems, Wiley, Security and Communication, John Wiley, and Journal of Networks and Computer Applications, Elsevier. He is a member of the IEEE. Contact him at neeraj.kumar@thapar.edu.