Blockchain Technology for Detecting Falsified and Substandard Drugs in the Pharmaceuticals Distribution System

Patrick Sylim¹, Fang Liu¹, Alvin Marcelo², Paul Fontelo¹
1 National Library of Medicine, National Institutes of Health, 8600 Rockville Pike, Bethesda Maryland 20894
2 Standards and Interoperability Lab for Asia, University of the Philippines, Manila, 2nd floor Philippine General Hospital, Taft Avenue, Ermita Manila 1000

INTRODUCTION

A recent report from the World Health Organization (WHO) classified drug counterfeiting as a global problem. In low to middle income countries, an estimated 1 in 10 drugs in market circulation are falsified or substandard [1]. The consequences of this phenomenon pose significant risks to individuals and the public. They are most prevalent in areas where surveillance and regulation need improvement or are deficient and where medicines are in high demand but remain mostly unaffordable [9,10]. They are also rampant during disease outbreaks and epidemics when shortages of essential drugs tend to occur, and when counterfeiting is most likely to rise.

Substandard drugs are dangerous. Falsified and substandard drugs, which could contain inactive ingredients, active ingredients but in the wrong dosage, or potential contaminants could be lethal [2]. The lay press [11,12,13,14], replete with many of personal anecdotes, and medical journals [15,16,17,18] have reported on the dangers of fake drugs. The use of antimicrobials of low quality may result in treatment failures and, in turn, may increase antibiotic resistance in individuals and within the community, resulting in higher mortality rates and the spread of highly-resistant pathogens worldwide. Contaminants and impurities may induce allergic reactions and adverse drug reactions. Counterfeit drugs waste individual incomes and lead to increases in government economic burden. Furthermore, these may decrease the overall public confidence in the efficacy of authentic medicines [3,4].

In the Philippines, just like in the United States, the Food and Drug Administration (FDA) has the mandate to ensure the safety, quality and efficacy of food, medicines, and medical devices. The agency has repeatedly warned the public of fake pharmaceutical products peddled by counterfeiters that are circulating in the market. This warning comes with an advice to the general public to ensure that retailers where they obtain their drugs are certified by the FDA and that pharmacies display the Certificate of Product Registration (CPR), which the agency issues. In addition, the agency has a joint task-force with the “Destroying Products Unfit for Human Consumption” (D-PUNCH) unit of the Philippine National Police (PNP) [5]. D-PUNCH’s approach relies on reports of suspicious products or transactions from the public to initiate action. In 2003, FDA reported that 30% of inspected drugstores were selling substandard/spurious/falsely-labelled/falsified/counterfeit drugs (SSFFC) [6].

Drugs move across a distribution chain that involves several participants. These usually include, but are not limited to, a manufacturer, a wholesaler and a retailer. A regulatory body may get involved in testing authenticity and efficacy before a drug product is distributed. These participants enter into direct contract-based relationships with each other: for instance, a retailer may enter a contract with a certain wholesaler to purchase stocks of a certain drug product regularly, and another contract with another wholesaler to purchase stocks of a different drug product regularly.

Blockchain technology follows a decentralized network model -- instead of storing all information into one database like in conventional cloud-based applications, the information is distributed and synchronized across all nodes in the network. To tamper with information in a blockchain network would entail breaking through all of the nodes, since data is entered into blocks – sets of data that reference previously entered data. Data is commonly represented by a hash code – a set of letters and numbers readable only by machines - and appended to the previous hash values to form a block. This method, in addition to the network forcing continuous synchony among all member nodes, makes
tampering difficult and discoverable. Furthermore, the network can persist amidst node failure. The threshold for the number of non-functional nodes before network failure is a function of the number of nodes connected to the network. The more nodes there are in the network, the less likely for it to fail [7].

Applications of Blockchain technology in clinical practice and healthcare research are currently of great interest and are being explored for the potential for increased security of health information amidst the increasing frequency of cyberattacks. This study will test the feasibility of applying the technology and its principles in a pharmaceuticals surveillance system and its resistance to tampering.

In our review of the literature, we found no previous studies or reports on the effectiveness or impact of consumer-driven CPR checking and initiation of D-PUNCH investigations on mitigating the counterfeiting issue. In this study, we propose a more active approach to surveillance - monitoring the movement of products from certified manufacturers and detecting unauthorized transactions along the distribution network using the principles of Blockchain Technology to insure the quality, safety, and efficacy of food, medicines and medical devices.

METHODS
Pharmacosurveillance Blockchain System
System Design and Development
The system prototype will be a hybrid Blockchain built on the Ethereum Blockchain platform [8]. It will be developed in a simulated network environment. It will initially be designed with four basic nodes, one for each participant in the traditional drug distribution model - the manufacturer, the wholesaler, the retailer, as well as the FDA. The design will include a profiling mechanism that identifies and distinguishes contract-based relationships between participants, information on which will be stored in a contract registry, filtering transactions that are beyond the scope of specific relationships from certain interfaces. The system design will acknowledge the existence of brand-based contracts among participants in the drug distribution chains by including a contract mechanism for filtering information for client-level interfaces. Transactions will be distributed among all nodes in the network, validating information through a contract registry distributed in the network. This will ensure that data shared in a network is filtered out from another network through the interfaces, but is still distributed, as shown in Figure 1.
Despite the orientation of the internode connections within the network, the movement of a drug product along the distribution network will be traceable by all nodes. Client applications would have the capacity to detect anomalies, unauthorized entries, and missing drug products. Each step will be tagged with a timestamp for auditing.

Client application will be installed in all nodes that will display transactions performed along the distribution chains as well as detect anomalies and information discrepancies in a dashboard interface. This client application will trace the drug product as it moves along the chain, using transaction information to generate graphs and timelines as well as to generate notifications for issues. Furthermore, it will have the capacity to conduct validation checks for transactions in real-time by referencing the contract registry. The registry’s database will contain all authorized manufacturers, wholesalers and retailers and anyone else in the chain.

**FDA account**
The FDA account will have access to functions that allow the user to add information to the drug product registry, the participant registry and the contract registry. Information uploaded by this account to the network will be considered authentic and authoritative, and will be used as the reference against which transactions in the network will be checked. All sections and functions of the client application will be accessible to this account.

**Manufacturer account**
Information uploaded by this account to the network will have credentials and certificates linked and will initiate distribution workflows which the system will subsequently track using information stored in the registries. Upon verification of identity and registered distribution contracts linked to the specific brand of drug product, the system will determine whether the merchandise moves along a registered chain and will verify consistency of information through each node.

**Wholesaler account and Retailer account**
Information uploaded by these accounts to the network will have credentials and certificates linked and will be validated by the system against the registries.

Distribution chains may branch out or merge at certain nodes and the system should detect such patterns when it visualizes them into timelines. For improved auditing, the system will also track the amount or stock number of each brand of drug product that moves across each node.
Figure 2. Possible branching and merging patterns in the drug distribution chain.

Branching and merging patterns in figure 2 will be visualized into 6 separate timelines, namely the following:

1) Brand 1: Manufacturer 1 (100), Wholesaler 1 (50), Retailer 1 (25)
2) Brand 1: Manufacturer 1 (100), Wholesaler 1 (50), Retailer 2 (25)
3) Brand 1: Manufacturer 1 (100), Wholesaler 2 (50), Retailer 2 (50)
4) Brand 2: Manufacturer 1 (100), Wholesaler 1 (25), Retailer 1 (25)
5) Brand 2: Manufacturer 1 (100), Wholesaler 2 (75), Retailer 1 (25)
6) Brand 2: Manufacturer 1 (100), Wholesaler 2 (75), Retailer 2 (50)

All stocks should be accountable if the distribution chains are working as intended; discrepancies in amounts signify an underlying problem and possibly a counterfeit attempt.
Figure 3 shows a contract registry in the network containing information on the drug product as well as the participants and their certificates. When a manufacturer ships a batch of a drug product, it records information into the network, and the record is distributed on all nodes. It is then counterchecked against the contract registry by client application in the distribution chain. It will display notifications if information is anomalous. Examples of anomalous information notifiable events are when certificates linked to the node ID do not match those in the registry (hinting at fraud), information supposedly recorded by a node is missing from the block (hinting at node failure or a skipped participant), and when specific drug product information does not match its counterpart in the registry (hinting at typographical error or tampering of the drug product). All scenarios would need action from the FDA (or the regulating agency).

**Database**

The system database will be distributed over a decentralized network. There will be four main tables in the database:

1) Transactions table, containing the hash blocks,
2) Contract registry, containing contracts approved by the FDA,
3) Participant registry, containing certificates issued by the FDA,
4) Drug product registry, containing information on drug products approved for circulation by the FDA.

**RFID Tags**
RFID Tags will be used as an additional data point linked to a particular drug product. Each node will have an RFID scanner that contributes the ID scanned to the transaction log. Tag IDs will be registered in the FDA registry and distributed to manufacturers. Anomalies will trigger a warning in client applications.

**Anomaly Detection**
The system will be designed to detect five types of anomalies anywhere along the chain:
1) Missing nodes in the distribution chain
2) Distribution chains that have not completed after a certain threshold
3) Invalid node certificates
4) Unregistered products entering the distribution chain
5) Primary data point (i.e. drug-related data, e.g. dose) discrepancies
6) Timestamp anomalies

**System Testing**
After development of the prototype, testing will be done in a simulated network environment, evaluating two main parameters:
1) Benchmarks on various data corpus sizes (as a function of the number of transactions)
2) Capacity of the system to reliably detect the anomalies described above
Analyses will be done on the feasibility of the system for large-scale implementation based on these two main parameters. Assumptions and recommendations will be discussed in their respective sections.

**RESULTS**

**Interfaces**
The network will have a common interface for client applications across the nodes. This will be the ‘base app’. The client application for FDA will have an additional module and interface that allows addition of entries to the registry table, restricted by permissions.

**Login**

The application will be locked behind a login interface with two-factor authentication. It will ask for user credentials (username and password), as well as a verification code sent through an authenticator application. All credentials, including those for the authenticator application, will be issued by the FDA through the user management module integrated into the system.
The transaction history is a simple data visualization interface that will exist in all instances and can be accessed by all accounts in the system. However, transactions are role-based, filtered to display only those involved in distribution chains to which the participant viewing them is a part; distributed information in the network will be used for visualization. The “+” button at the lower right portion of the screen allows the participant to record transaction information.
Figure 5. The timeline dashboard to visualize transactions along a distribution chain to highlight manufacturer shipment time to consumer purchase at a retailer. Diamond markers signifying transactions. A red diamond denotes a possible problem based on the information distributed on the network.

The timeline dashboard presents graphic representations of the transactions as they are tracked along the distribution chain. Anomalies in the information recorded by nodes will be displayed in red as shown in Figure 5. These diamond markers can be expanded to show information from that particular node. Restricted information requiring authorization will not be shown. All nodes will be able to detect anomalies and report to the FDA, although the FDA node should also be able to detect such events. This also shows how entry of counterfeit products into the chain can be detected: such an event will cause the timeline to detect and show a wrong sequence because the correct flow will be checked against the directional distribution contracts in the registry.
**Contract Registry**

Figure 6 shows the screen after the [+ ] button in Figure 5 is selected, i.e. and a new contract form is opened. Hovering over the contract icons to the right will display a small window with the contract details.

The contract registry will contain the reference records by which the system can detect information anomalies and broken transaction sequences. Only the FDA can access and add new contracts, a specific role granted by permissions in the system. Moreover, once a contract is registered, it cannot be modified, tampered with or deleted. A contract will minimally contain the name of the drug product, a source and recipient (both should be FDA-certified and registered to the system prior to the creation of the contract), and other metadata such as unique identifiers, certificates and start and end dates.

By design, there will be one contract assigned to each drug product transaction and one contract for each drug product. A participant will have several contracts with other participants. This registry validates actual transactions in the distribution chain using two factors authentication: first, the existence of the previous step in a distribution chain or the certificate of the manufacturer as applicable, and second, the congruence of transaction information in the block record and an existing registered contract.
[Image of Drug Surveillance System showing interfaces for adding new participants and drug products into the network.]

Figure 7. Participant and drug product registries. The corresponding forms for adding participants and drug products into the network are shown. These interfaces will only be accessible by the FDA.
The participant and drug registries serve to feed the input fields of the contract registry, containing the necessary data to distinguish between participants as well as between drug products (Figure 7). As with the contract registry interface, these will only be accessible by the FDA, despite the information being distributed to the network. An option would be to allow other accounts to view the registries for reference, however, adding to the registry will be restricted to the regulating agency.

**DISCUSSION**

**Assumptions and Limitations**

Aside from assumptions on resources and infrastructure, the design of the prototype makes several additional assumptions that may affect applicability:

1) That a regulatory agency such as the Philippine FDA exists and is actively regulating the drug product marketspace
2) That such a regulatory agency has, or can keep, reliable and verifiable records of certificates it issues to participants in the drug distribution chains
3) That such a regulatory agency has, or can keep, reliable and verifiable records of drug products that it allows to be distributed in the marketspace
4) That participants in drug product distribution chains have, or can keep, reliable and verifiable records of drug products that they receive, process, and redistribute.

The study design has the following limitations:

1) The proposed system will only be able to detect drug movements that follow official distribution chains known to the regulatory agency. It cannot track falsified drugs that are distributed through routes outside of official distribution chains.
2) The proposed system will be developed and tested in a controlled, simulated network, therefore, results obtained from this study may not be reflective of actual performance when deployed in a real-world setting.
REFERENCES


7 Ichikawa D et. al. (2017). Tamper-resistant mobile health using blockchain technology. JMIR Mhealth Uhealth. 5(7): e111. PMCID:PMC5550736


ACKNOWLEDGEMENTS
This research was supported by the Intramural Research Program of the National Institutes of Health, National Library of Medicine and Lister Hill National Center for Biomedical Communications.

DISCLAIMER
The views and opinions of the authors expressed herein do not necessarily state or reflect those of the National Library of Medicine, National Institutes of Health or the US Department of Health and Human Services.