Blockchain Based Counterfeit Medicine Authentication System

Nazmul Alam
Dept. of CSE
Bangladesh University of Business and Technology
Mirpur-2, Dhaka, Bangladesh
nazmulalam0088@gmail.com

Md Rabiul Hasan Tanvir
Dept. of CSE
Bangladesh University of Business and Technology
Mirpur-2, Dhaka, Bangladesh
tanvir3550@gmail.com

Sadah Anjum Shanto
Dept. of CSE, Lecturer,
Bangladesh University of Business and Technology
Mirpur-2, Dhaka, Bangladesh
sshanto@bubt.edu.bd

Fateha Israt
Dept. of CSE
Bangladesh University of Business and Technology
Mirpur-2, Dhaka, Bangladesh
fatehaisrat435@gmail.com

Aysha Rahman
Dept. of CSE
Bangladesh University of Business and Technology
Mirpur-2, Dhaka, Bangladesh
ayshashifa55027@gmail.com

Sabrina Momotaj
Dept. of CSE
Bangladesh University of Business and Technology
Mirpur-2, Dhaka, Bangladesh
sabrina.erina13@gmail.com

2021 IEEE 11th IEEE Symposium on Computer Applications & Industrial Electronics (ISCAIE) | 978-1-6654-0338-2/21/$31.00 ©2021 IEEE | DOI: 10.1109/ISCAIE51753.2021.9431789

***Abstract*— For a few decades, it is a very big challenge to monitor and keep track of genuine medicine in health care. Lacking a trust system and strong monitoring authority, syndicates can make counterfeit medicine easily. With the shifting of life-critical healthcare, it becomes an emergency to ensure substandard drugs. Because counterfeit medicine has a deadly effect on the human body and has disastrous results. To detect the falsified medicine, we proposed a drug tracing system using blockchain technology. Our system is able to detect substandard and anomaly drugs from manufacturer company to patient's hand. Also can verify the defective and expired drugs in the market using smartphones by scanning QR (Quick Response) code. Blockchain security could make the system more transparent and reliable. This paper aims to ensure drug quality, transaction security, and data safety using blockchain technology.**

***Keywords*— *blockchain, security, smartphone, traceability, counterfeit*.**

I. Introduction

Counterfeit medicine authentication is essential for patients' health and business operations. Counterfeiting of several products creates many issues for various manufacturing sectors and causes serious threats to medicine. This is very harmful to public health and also creates profit loss to the pharmaceuticals company. The yearly sales of counterfeit products in the world is 650 billion USD reported on the International Chamber of Commerce of Geneva [12].

To trace counterfeit drugs already several techniques have been used in the medicine supply chain. Authors in [15], proposed the usage of barcode or RFID code on medicine for verifying its legitimacy. Same as, a Data-Matrix tracking process has been proposed in [16], where every medicine has a Data-Matrix where contains Id of Product, Id of Manufacturer ID, unique ID of the package, the authentication code and optional metadata. The central verification register (CVR) is also mentioned. Most of the authors use RFID to their works on the medicine supply chain [1, 2, 16, 17]. But implementation of RFID is costly according to medicine price.

In this paper we present a prototype of blockchain system for medicine traceability and regulation that rebuilds the full service architecture, ensuring authenticity and privacy of traceability data, and meantime achieves a ultimately stable blockchain data storage. Pseudocode explains the practical workflow of the medicine supply chain has also been given. This paper is arranged as follows. Blockchain based medicine traceability related works are presented in Section II, Design framework of our prototype is explained from three aspects from four aspects, Medicine Supply Chain Data Storage in blockchain, Detecting counterfeit medicine, and Methodology for the prototype work in Sections III. Then, Section IV explains the implementation and evaluation of the prototype. Finally, the paper is concluded in Section V.

Motivation

The counterfeiting of medicines causes a severe threat to society. The counterfeit medicines make an untoward impression on the health of the people and also cause revenue loss to the legitimate medicine manufacturing establishments. The defective supply chain system is also the reason for counterfeit drugs in the pharmaceutical industry. Thus far various anti-counterfeiting techniques have been offered, but most of the existing systems are not good. Blockchain technology is one of the best alternatives in a series where we need data privacy and data access at the same time. Thus we are attempting to assure the caliber of the drug, the refuge of the transaction, and the surety of the data by using blockchain technology.

II. Related Works

Nowadays, some technical and practical works which are already proposed in the medicine supply chain to detect substandard drugs with blockchain, but there are some general discussions. Such as, Mettler et al. [5] mainly proposed the possibility to prevent counterfeit medicine in the drug industry using blockchain. Kurki [6] discussed the advantages and instructions for utilizing blockchain within the drug supply chain. Bocek et al. [4] had developed a prototype of Ethereum smart contract based drug supply chain traceability system [7], without explaining the specific design of the workflow. Author in [1] proposed a novel product ownership management system (POMS) of Radio frequency identification (RFID)-attached products for anti-counterfeits that can be used in the post supply chain. Similarly, a food company uses RFID to detect hazards in their food supply chain [2]. Author in [3] proposed a hybrid

Authorized licensed use limited to: University of Prince Edward Island. Downloaded on July 04,2021 at 02:35:13 UTC from IEEE Xplore. Restrictions apply.

P2P physical distribution (HP3D) framework that used a semi-public ledger and a private ledger blockchain to enhance the validity and security of the information being exchanged.

On the above methods, none of them proposed the authentic and automatic verification of drug genuinity from manufacturing to the patient's hand. When we need to prevent counterfeit medicine in the supply chain, blockchain technology makes sure a static chain of transaction ledger, in individual drug levels, every step of the supply chain is tracked.

III. Designed framework

A. Medicine Supply Chain Data Storage in Blockchain

In the model, the supply chain is created among drug administration, manufacturer, distributor, and pharmacy. Verification authority drug administration verifies several kinds of participants in the blockchain network. Designed systems transaction data storage is similar to bitcoin transaction data. Each participant has a public key which is shown in figure 1. Transactions between each participant share public key, hash value of previous transaction, encrypted QR code by manufacturer. Manufacturer levels medicine with encrypted QR code which consists of hash values that are generated by a hash function. QR code contains the details of medicine which is manufactured by drug organizations. The medicine labels, ingredients, manufacturing-expire date, quantity on the medicine package taken as input to the CRC-32. Each medicine has a unique QR code using a hash function to prohibit reused leveling by the manufacturer. The transaction of the supply chain is secure and unshakeable for complex algorithms. This design gives the successful validation of the sender cryptographic signature. Unauthorized parties cannot get access to the data storage due to the public key and sender's digital verified signature, and encrypted QR code prevents the duplication of medicine.

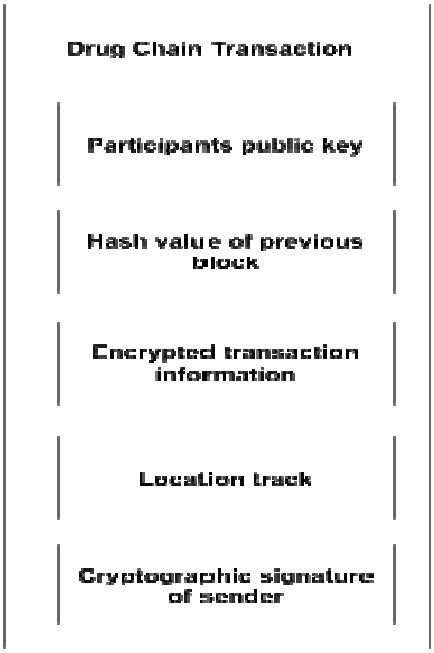

Fig. 1. Drug chain storage for medicine safety.

B. Detecting counterfeit medicine

In this system, we take some affordable and easily usable steps to detect the falsified medicine in the drug supply chain. To make it simple we implement some features into our blockchain prototype, which makes the work unique. Generally, a block of a chain consists of some basic elements such as the previous block's hash, information of this block, and the hash value of this block [8]. Information of a block can be a timestamp, transaction details, or transaction quantities. The hash value of the current block is made by a hashing algorithm that takes the information of this block and output the hash value for the current block. In this section, we add a location tracker that takes the current location where the transaction created. As a result, if the location of the transaction doesn't match the authorized participant's location the block will not be valid and it would not add to the chain. To get the location we use google ***Geolocation API*** [9]. The pseudocode in Pseudocode 1:

Pseudocode 1 Matching with the location.

```
1.  getLocation( ){
2.      navigator.geolocation.getCurrentPosition(x,y);
3.      x ← position.coords.latitude;
4.    y ← position.coords.longitude;
5.  }
6.
7. isBlockValid(location){
8.     if Other conditions && (location === this.fromAddress.location)
9.              then     return true;
10. }
```

Here, ***fromAddress*** is the address of a participant of the network from where medicine will be supplied. If unknown address is detected on any transaction then it will not match with the recorded location of a valid participant also the block will not be valid and will not be added in the chain. As a result, unauthorized sellers or fraud cannot mix falsified medicine in the authentic supply chain from unknown address.

Pseudocode 2 illustrates bellow:

Pseudocode 2 validation at the customer end.

```
1.   qrScanning(scannedValue, buyQuantity){
2.     for (value ← this.chain.block){
3.          if  value === scannedValue
4.              then  chain.block( );
5.      }
6.     x ← this.fromAddress.quantity('Medicine name')
7.    if  buyQuantity <= x
8.   then  valid;
9.   x -= buyQuantity;
10.  else  invalid;
11.  }
```

We mentioned before the use of QR code on the medicine pack to test the authenticity with the QR code reader. When someone scans the code, it immediately shows the information associated with the medicine from the blocks of this chain. Actually QR code return an identity number or identity key that will use as an input to the blockchain

Authorized licensed use limited to: University of Prince Edward Island. Downloaded on July 04,2021 at 02:35:13 UTC from IEEE Xplore. Restrictions apply.

network. There will run an iteration on the blocks of the blockchain for finding the medicine associate with the same identity number or key of the input value. If it does not find the desire medicine it will shows that the medicine is not authentic and if it is found on the blockchain, it will shows that the medicine is authentic. But still there remains a security question that QR code reader is available and it is very much easy to make the same QR code at a short time and put it on the falsified medicine and mixed it to the authentic supply chain. To improve that security we use the number quantity of medicine stored in the retailer shop. We associate a quantity for every particular type of medicine that will be assigned with the number quantity of medicine from the wholesaler. At the time of customer's scanning, it will show the available quantities of the address of the retailer shop. As a result, it will very easy to detect weather the retailer sell authentic medicine or falsified medicine. As the same way, a retailer also can check the authenticity of a wholesaler's medicine by the time of order.

C. Methodology for the prototype work

The methodology for prototype work is given in Fig-2 that is based on a private blockchain system, where all the participants have to get validation by the drug administrator.

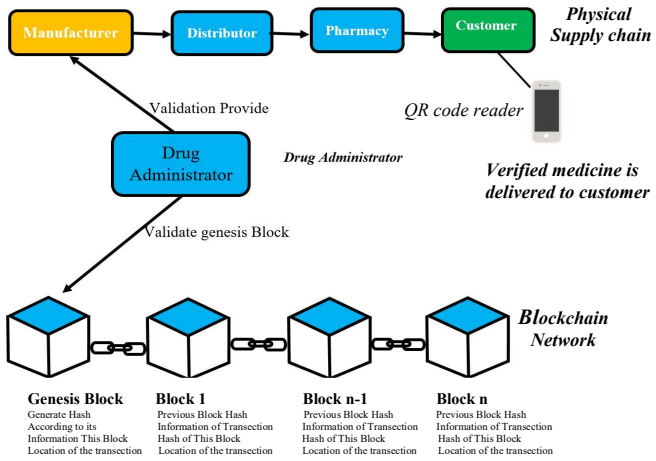

Fig. 2. Work flow of the prototype

The public address of digital signature of a participant will also be provided by the drug administrator authority after, hence the participants are trusted on it. There are some following steps that we take to ensure medicine safety in the transection of supply chain:

1) Transaction between two participants in the network will consist of the public key of a sender, public key of a receiver and the transacted information which is sent by the sender such as basic information and quantity of medicine.
2) The participants' shared information will be encrypted in the block of the chain that can be only shown to the receiver. The quantity and timestamp only be visible to the network that everyone can see on the network.
3) Along with the general information of the transaction, the current location of the transaction also added to the block which is described in section B in pseudocode 1.
4) When the transaction is successful, a new block will be added to the chain then it will be distributed to all the participants on the network and it will repeat in every transaction.
5) We introduce a data reducing process in the blockchain where information of expired medicine will be removed from the network.
6) Finally a customer can easily scan the QR code to check the validity of the medicine which is described in section B in pseudocode 2.

IV. IMPLEMENTATION AND EVALUATION

A. Implementation

At present, we developed a prototype mainly with Javascript and Angular web application framework. The key modules of this prototype include the validation module, blockchain module, key generator module, and transaction logic module. There are some most popular open-source libraries used in the present worked prototype, as SHA256 [13], elliptic [10], qrious[11], etc. The key generator module uses elliptic to generate a public and private key for the participants. The validation module gets the pending request of the participant validation and gives them the public and private keys using the key generation module. The validation process is maintained by the drug administrator. The transaction module makes the transaction between participants, when the transaction gets valid the blockchain module adds the transaction on a block to the chain.

Currently, we run the prototype on localhost. We use windows 10 operating system to build and run the prototype. Mainly the project is built on nodeJS. Node.js is a cross-platform, an open-source, back-end JavaScript runtime environment that runs on the V8 engine and executes JavaScript program outside a web browser. Anguler web application framework is used for the frontend development. AngularJS is also a JavaScript-based open-source front-end web framework mainly maintained by Google and by a community of individuals and corporations to address many of the challenges encountered in developing single-page applications.

B. Evaluation

1) Practicality: The most initial demand for a medicine supply chain traceability system must be its practicality, which might have been neglected mentioned in related works in Section II. We designed the prototype for practical medicine supply chain traceability and regulation to trace and track the authentic medicine as if fraud manufacturers or suppliers cannot mix any kind of counterfeit medicine in the authentic supply chain. First, our prototype maintains data privacy and authentication of the participants. Additionally, the prototype as a blockchain solution first uses the current location of the transactions to its block, which really makes it easy to detect the fraud distributor and falsify medicine on the supply chain network. As well as the prototype is very simple to use. There also a user friendly interface that makes simple and encouraging to use. Finally, we added the single unit of medicine validation checking on

Authorized licensed use limited to: University of Prince Edward Island. Downloaded on July 04,2021 at 02:35:13 UTC from IEEE Xplore. Restrictions apply.

the prototype and also proposed an optimized data decreasing process on the blockchain storage removing the information of expired medicine according to the expired date. This was an important priority concern because researchers are not proposed about data reduction in previous works described in section II. The prototype achieves ultimately stable and admissible data storage with medicine expiration date.

2) Security: Our prototype is implemented to be an authorized blockchain system for contrary Cyber-attacks. Drug administrators control the access of participants to the blockchain network. As a result, fraud distributors or retailers are cannot make any transaction in the network. Also participants who are not in the medicine supply chain or retailers with a bad commercial review in medicine supply chain are therefore prohibited to use the blockchain network. Hence the prototype is secured from those frauds. The prototype is a low possibility of DoS attacks [20] in respect to existing server-client solutions because of the peer to peer architecture. Formal analysis of secure blockchain technology [18, 19] in the prototype may require an extra-large section to describe the basic principal of blockchain, where many of researchers explain in their work and thus be ignored here.

3) Efficiency: Mainly the consensus protocol is the way to determine efficiency of blockchain. The prototype focuses on the practical requirement of medicine supply chain to detect authentic medicine. In this prototype, the communication over with drug administrator, efficiency of consensus algorithm, and the practical throughput requirement of medicine supply chain together decide whether it could be applied in real medicine supply production system. After the implementation of current prototype, Quantitative assessment is presented which will be explained in future work.

V. Conclusion

In this paper, we develop a practical blockchain based secure infrastructure for the medical supply chain among authorized participants on the traditional medicine supply chain. Our application stands on blockchain security to identify the drugs uniquely and individually therefore, a falsified medicine or fraud distributor can be identified easily without any complexity. The prototype reconstructs the whole traditional medicine supply chain service architecture that can provide medicine security as well as authenticity of the manufacturer. It also introduce the current location of every transaction that makes the system more reliable. Optimization of blockchain data storage by removing expired medicine data makes the chain stable and acceptable.

References

[1] K. Toyoda, P. T. Mathiopoulos, I. Sasase and T. Ohtsuki, "A Novel Blockchain-Based Product Ownership Management System (POMS) for Anti-Counterfeits in the Post Supply Chain," in IEEE Access, vol. 5, pp. 17465-17477, 2017, doi: 10.1109/ACCESS.2017.2720760.

[2] Feng Tian, "A supply chain traceability system for food safety based on HACCP, blockchain & Internet of things," 2017 International Conference on Service Systems and Service Management, Dalian, 2017, pp. 1-6, doi: 10.1109/ICSSSM.2017.7996119.

[3] Z. Li, H. Wu, B. King, Z. Ben Miled, J. Wassick and J. Tazelaar, "On the Integration of Event-Based and Transaction-Based Architectures for Supply Chains," 2017 IEEE 37th International Conference on Distributed Computing Systems Workshops (ICDCSW), Atlanta, GA, 2017, pp. 376-382, doi: 10.1109/ICDCSW.2017.51.

[4] T. Bocek, B. B. Rodrigues, T. Strasser, B. Stiller, "Blockchains every- where - a use-case of blockchains in the pharma supply-chain", in IEEE IFIP/IEEE Symposium on Integrated Network and Service Management (IM), May. 2017, pp. 772-777.

[5] M. Mettler, "Blockchain technology in healthcare: The revolution starts here", in IEEE 18th International Conference one-Health Networking, Applications and Services (Healthcom), Sep. 2016, pp. 1-3.

[6] J. Kurki, "Benefits and guidelines for utilizing blockchain technology in pharmaceutical supply chains: case Bayer Pharmaceuticals", Bachelor thesis, Aalto University, 2016.

[7] Ethereum. Available: https://www.ethereum.org

[8] T. T. A. Dinh, R. Liu, M. Zhang, G. Chen, B. C. Ooi and J. Wang, "Untangling Blockchain: A Data Processing View of Blockchain Systems," in IEEE Transactions on Knowledge and Data Engineering, vol. 30, no. 7, pp. 1366-1385, 1 July 2018, doi: 10.1109/TKDE.2017.2781227.

[9] Pahlavan K., Li X., Ylianttila M., Chana R., Latva-aho M. (2000) An Overview of Wireless Indoor Geolocation Techniques and Systems. In: Omidyar C.G. (eds) Mobile and Wireless Communications Networks. MWCN 2000. Lecture Notes in Computer Science, vol 1818. Springer, Berlin, Heidelberg. https://doi.org/10.1007/3-540-45494-2_1

[10] S. Maria Celestin Vigila and K. Muneeswaran, "Elliptic curve based key generation for symmetric encryption," 2011 International Conference on Signal Processing, Communication, Computing and Networking Technologies, Thuckafay, 2011, pp. 824-829, doi: 10.1109/ICSCCN.2011.6024664.

[11] qrious. Available: https://github.com/neocotic/qrious

[12] H. H. Cheung and S. H. Choi, "Implementation issues in RFID-based anti-counterfeiting ystems," Comput. Ind., vol. 62, no. 7, pp. 708–718, 2011.

[13] SHA 256. Available: https://github.com/feross/simple-sha256

[14] Paik, Michael, Ashlesh Sharma, Arthur Meacham, Giulio Quarta, Philip Smith, John Trahanas, Brian Levine, Mary Ann Hopkins, Barbara Rapchak, and Lakshminarayanan Subramanian. "The case for Smart-Track." In Information and Communication Technologies and Development (ICTD), 2009 International Conference on, pp. 458-467. IEEE,2009.

[15] E. Engineering and C. Science, "Reliable Identification of Counterfeit Medicine Using Camera Equipped Mobile Phones Saif ur Rehman, Raihan Ur Rasool, M. Sohaib Ayub, Saeed Ullah, Aatif Kamal, Qasim M. Rajpoot, and Zahid Anwar," pp. 273–279.

[16] Sylim P, Liu F, Marcelo A, Fontelo P. Blockchain Technology for Detecting Falsified and Substandard Drugs in Distribution: Pharmaceutical Supply Chain Intervention. JMIR Res Protoc. 2018;7(9):e10163. Published 2018 Sep 13. doi:10.2196/10163.

[17] Feng Tian, "An agri-food supply chain traceability system for China based on RFID & blockchain technology," 2016 13th International Conference on Service Systems and Service Management (ICSSSM), Kunming, 2016, pp. 1-6, doi:10.1109/ICSSSM.2016.7538424.

[18] Pilkington, M. (n.d.). Blockchain technology: principles and applications. Research Handbook on Digital Transformations, 225–253. doi:10.4337/9781784717766.00019.

[19] Nofer, M., Gomber, P., Hinz, O., & Schiereck, D. (2017). Blockchain. Business & Information Systems Engineering, 59(3), 183–187. doi:10.1007/s12599-017-0467-3.

[20] Mirkin, M., Ji, Y., Pang, J., Klages-Mundt, A., Eyal, I. and Juels, A., 2020, October. BDoS: Blockchain Denial-of-Service. In Proceedings of the 2020 ACM SIGSAC conference on Computer and Communications Security (pp. 601-619).

[21] Shen, M., Tang, X., Zhu, L., Du, X., &Guizani, M. (2019). Privacy-Preserving Support Vector Machine Training over Blockchain-Based Encrypted IoT Data in Smart Cities. IEEE Internet of Things Journal, 1–1. doi:10.1109/jiot.2019.2901840.

Authorized licensed use limited to: University of Prince Edward Island. Downloaded on July 04,2021 at 02:35:13 UTC from IEEE Xplore. Restrictions apply.