Secure Blockchain Based Pharmaceutical Supply Chain Management

Ms. Madhuri. R. Shinde[1] Ms. Pooja. M. Wagh[2] Ms. Dhanashree. R. Chavan[3] Ms. Komal. A. Shelar[4]

[1,2,3,4]Department of Information Technology

[1,2,3,4]MET's Bhujbal Knowledge City, Institute of Engineering, Adgoan, Nashik, India

Abstract— The importance of improving the distribution structure of the products has increased worldwide over the past few years. Distribution prices are therefore now disclosed and information about the product is shared with consumers. Distribution channels, however, are complex and supply chain management (SCM) is conducted autonomously in each company. For this reason it has been frequently pointed out that the method of distribution is not straightforward and the margin of distribution high. In this paper we propose a system that ensures drug delivery process transparency by implementing blockchain and monitoring portion of supply chain management systems. This approach enables businesses to monitor their trades by improving SCM transparency, thus preventing businesses from excessive profits. Moreover, by automatically storing delivery data in a blockchain network and handling information more efficiently, organizations can cut management costs. Therefore, businesses can minimize management costs by automatically storing delivery data in a blockchain network and handling information more safely. And our solution to this problem is to monitor the system right from the manufacturer to the customer, minimizing counterfeiting of the drug that the manufacturer produced. This system is mainly useful for the manufacturer as compare to other modules of the system.

Keywords: Blockchain, Information Security, Counterfeiting, Pharmaceutical Supply Chain

I. INTRODUCTION

In a recent report by the world health Organization, drug counterfeiting has been identified as a global problem. It estimates that in low- and middle-income countries, every 10th drug in market circulation is counterfeit or has a poor quality [1]. The use of such substandard products may have a negative impact on the mortality rate. Medicines move through a supply chain in which several participants participate. These usually include the manufacturer, wholesaler, retailer, pharmacist and consumer. They are engaged in the production, transportation and sale of these products There is also a key participant in these processes- the regulatory authority responsible for moving batches of goods throughout the chain at each level. At the state level in particular, this individual may be some approved body of the state apparatus, for example, a special agency for the monitoring of medicinal drug turnover. The main task is to transfer the rights to produce pharmaceutical products in compliance with state standards and to control the movement of all units of goods ever produced. As for the user, there's another question drug regulation, which is provided by prescription only.

Dispensing without a prescription is illegal, but regulating retailers ' integrity as well as for falsified drugs is not easy and requires a special approach. Many pharmaceutical companies have already begun application of blockchain technology in the management of the drug supply chain[2]. Blockchain is an electronic cryptographic ledger based on a decentralized model of the network in which information is distributed and synchronized among all the network nodes.

This functionality is supported by a consensus algorithm implemented in the network to remove duplicate transactions problem, allowing nodes to check information truth before it is written directly to the registry. This system also has a high degree of fault tolerance.

The criterion for the number of nodes failed before a complete failure of the network depends on the total number of nodes connected to the network. Therefore, the more nodes in the blockchain network run, the less likely a complete system failure occurs.

A properly designed blockchain-based system will dramatically simplify the product turnover management process for approved government bodies[3-5].

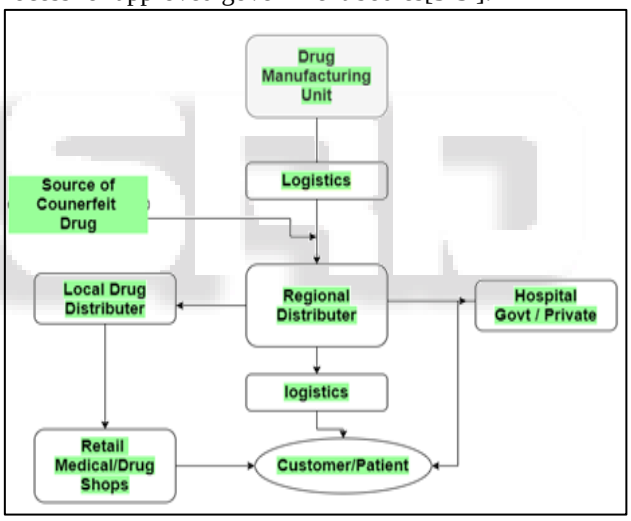

Fig. 1: Securing E-health network from counterfeiting

At the same time, a decentralized approach has a number of benefits which increase the information security of such systems compared with centralized counterparts[6]. The main characteristics and operating methods of blockchain systems will be discussed in section 1 of this study. Section 2 is dedicated to the study of the definition of the structured drug turnover control system with state-level regulation.

The goal of choosing this subject is to reduce the drug piracy created by the manufacturer and to provide transparency in the pharmaceutical industry's supply chain management.

II. LITERATUTE SURVEY

Blockchain technology was developed specifically for making cryptocurrency (i.e. bitcoins) and other financial services. After some years of that invention, many more blockchain implementations were proposed in various fields,

and blockchain became more effective after the introduction of smart contracts. Despite Blockchain's immense ease, proposals have been proposed to cope with its medication and healthcare apps. Benchoufi and Ravaud have clarified how blockchain is used to improve the additive effect of the standard of clinical research.We told about the overall use of blockchain in healthcare and medicine but there is no reason for the use of blockchain in the drug supply chain. Med Share is another research paper that has a reason to use blockchain technology in health care to share medical data from one individual to another in a secure environment [9].

Med Rec, a white paper released that proposes a framework for the collection and potential distribution of confidential medical data to researchers for study purposes. This provides a mechanism for storing patient data and making this easy to access the data by integrating protection in blockchain [10]. M. Mettler also discussed the use of blockchain in the pharmaceutical supply chain but lacks information about implementation[11]. Besides that, several articles and academic journals on this topic have been published, Those interested in reading the papers can read it from the following references.[12][13][14].

Apart from health services, supply chains of healthcare pro-ducts are important contributors to the healthcare system. Different healthcare products are distributed and traded differently andvary in their cost, criticality to delivery of patient care andpotential impact on service improvement (Zheng et al., 2006).Among healthcare products, medicines account for 20–30% of global health spending (World Health Organization, 2010). The United Nations Millennium Development Goals also identify the pharmaceutical industry as one of the major drivers of the healthcare sector. Hence, the effective management of the pharmaceutical supply chain (PSC) is crucial for the healthcare system. While consumer/physician level behaviors and health expenditures are areas of immense research interest in the pharmaceutical industry, supply chain management (SCM) and research and development (R&D) have also emerged as significant avenues for research (Narayana et al., 2012). However,Shah (2004)observes a low focus of healthcare research on the PSC, that historically addresses sales/marketing or drug discovery, which form the two extreme ends of the chain. Recent reviews are also restricted to specific issues in the PSC such as optimization (Shah,2004), implementation of just-in-time (Jarrett, 2006)or issues in specific countries such as healthcare reforms (Yu et al., 2010),sourcing decisions (Pazirandeh, 2011), etc. Among other areas of research, there is a need to review research efforts on SCM in the pharmaceutical industry (Narayana et al., 2012). Thus, the overall aim of this study is to provide a holistic review of currenttrends in management research on the PSC.

Specifically, the paper aims to:

1) Analyze the progress of research interest in recent literature on the PSC across themes of study and across the structure of the PSC.
2) Analyze the research interest in pharmaceutical supply chains across geography and through methodological approaches applied in literature.
3) Explore the contribution of research to final value delivered to the end-consumer in the pharmaceutical supply chain.

III. PROPOSED METHODOLOGY

Hash functions transform arbitrary large bit strings called messages, into small, fixed-length bit strings called message digests, such that digests identify the messages that produced them with a very high probability. Digests are in that sense fingerprints: a function of the message, simple, yet complex enough that they allow identification of their message, with a very low probability that different messages will share the same digests.

In SHA-256, messages up to 2^{64} bit (2.3 exabytes, or 2.3 billion gigabytes) are transformed into digests of size 256 bits (32 bytes). For perspective, this means that an object 7 times the size of Facebook's data warehouse in 2014 passed to SHA-256 would produce a chunk of data the size of a 32-letter string of ASCII characters, and that string would the object's very special fingerprint.

A prominent use case of hashing is data integrity verification of large files, which relies on the comparison of actual and expected message digests, or checksums. Another is hashing as part of the encryption/decryption journey. Before a message can be encrypted with an algorithm like RSA, it needs to be hashed. In the rest of this article, we explore what hashing does to a message, with a view to later develop a better understanding of RSA.

A. Step by step hashing with SHA-256 Pre-processing

1) Padding. If we note M the message to be hashed, and l its length in bits where $l < 2^{64}$, then as a first step we create the padded message M', which is message M plus a right padding, such that M' is of length l', a multiple of 512.
2) Blocks. M' is parsed into N blocks of size 512 bits, M^1 to M^N, and each block is expressed as 16 input blocks of size 32 bits, M_0 to M_{15}.
3) Hash initialization. The initial hash value H^0 of length 256 bits (8 input blocks of 32 bits) is set by taking the first 32 bits of the fractional parts of the square roots of the first eight prime numbers

B. Algorithm

The hash is produced by processing each message block M^i of M' in order. For each of message block M^i :

1) Message schedule. We create a message schedule W^i, consisting of four 512-bit message blocks (each made of 16 input blocks). The first block of W^i is message block M^i, and the next three blocks are variations of M^i
2) The big shuffle. The input blocks of message schedule Ware fed, one after the other, to a function represented below as a graph. The graph takes as inputs a hash ω^i (t) and a message schedule input block W^i (t), and outputs a hash ω^i (t+1). The initial hash ω^i (0) fed to the graph is the intermediate hash H^{i-1}: in the case of W^1, it's H^0 defined in the pre-processing step. ω^i (0) and W^i (0) produce ω^i (1); in turn ω^i (1) and W^i (1) produce ω^i (2), etc., until ω^i (63) is produced.

3) New hash. After all input blocks from W^i have been used and we ω(63) has been created, we can create the new hash H^i such that each input block of H^i is the sum of the corresponding input block of H^{i-1} plus the corresponding input block of ω^i (63):

$H^i(j) = H^{i-1}(j) + \omega^i(63)(j)$ where + is the addition modulo 2^n

If other message blocks M^i remain, repeat the process (message schedule, big shuffle, creation of the new hash H^i)

If W^i was the last message schedule, then H^i = H is message M's final hash or digest — its so very special fingerprint.

IV. IMPLEMENTATION

The blockchain technology in pharmaceutical supply chain system, we should first understand how blockchain ledger works under the hood. Blockchain has a built-in identity mechanism, a cryptographically secure key pair (as mentioned in the above section). These keys are used to assign each participant a specific activity on the network. A participant can be a device, person or an entity. The original identities of participants are hidden and they are known by these keys. A key pair contains no clue about the participant, but additional information (e.g. name, contact or professional credentials) can be associated with it But the best approach is to keep these additional information off-chain and merge them with on-chain data (key pair) using there IDs. In the context of pharmaceutical supply chain management, the participants will be the manufacturer, packager, distributer and doctor etc. Each of these participants will be identified by their unique key pair on the network. Drugs will be considered as the assets, with each of them having a unique key (or hash). The ID will be attached with drug in the form of QR Code.

While keeping in mind the basic architecture, the proposed system can be implemented on different ways depending on one's preferences. A lot of third party APIs are also available that can be used to push the data and transactions to blockchain network, a few of them are here. Each of these APIs provide different types of services. Regardless of which programming language or API we use, the basic architecture of our system will be the same.

The selection of a specific blockchain network for storing transactions is also a crucial part, but before that, we should know the types of blockchain. Blockchain has two main types – Public blockchain and Permissioned (or private) blockchain, a detail is given here. In a permissioned blockchain not everyone can write to blockchain, only those participants who have given access, can write or access information on the blockchain. In the context of pharmaceutical supply chain – the better option is to use a permissioned blockchain. The next step is to use a specific blockchain network to save the transactions record, but it totally depends on the developer's choice. Few types of blockchain networks are available in the market now, e.g. Bitcoin Blockchain that is the pioneer one, Ethereum , Hyperledger or even BigchainDB can also be used. But the one we suggest is permissioned Ethereum blockchain.

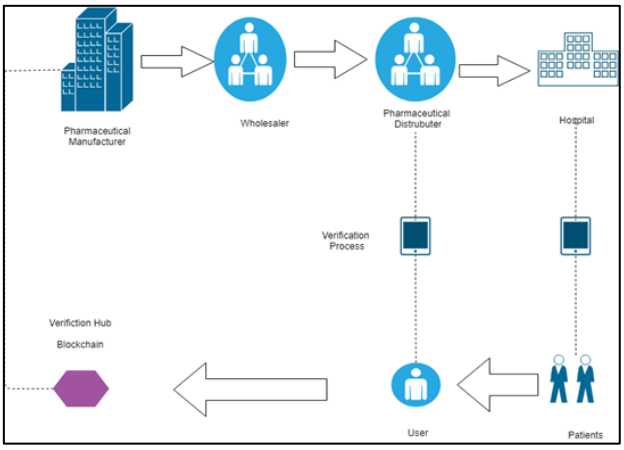

Fig. 2: SCM of Pharmaceutical Industry

How a blockchain based pharmaceutical supply chain management system will work. Let say we have setup a secured and trusted network, where only the trusted parties are given permission to join the network. On the backend there is a permissioned blockchain to store all the required transactions, and once the information entered to it – can never be changed. Besides that we have a user-friendly mobile APP that the participants will use to make transactions to the blockchain.

When a factory produce a new product, they will create a unique hash and assign it to the product. The product will be registered on the blockchain using its hash (unique ID). The product will be considered as a digital asset on the blockchain network, and its hash will be used to track it any time on the network. Any additional information of the product can be stored off-chain or on-chain depends on manufacturer's choice. Off-chain data will be merged with on-chain data by using some kind of identifier. Conventionally, in most blockchain based applications a hash-digest (e.g. SHA-256) of all the off-chain data is generated and linked it to the on-chain data. But the best approach is to store large files (e.g. images) off-chain and text data on-chain. Once the product is registered to the blockchain by the manufacturer, its ownership will be easily transfer to another participant using a user-friendly mobile app. Let say the wholesaler want to purchase the drugs from the manufacturer, manufacturer will physically transfer the drugs to the wholesaler and a transfer transaction will be registered to the blockchain simultaneously.

V. CONCLUSION

In this paper we suggested the next further use of Blockchain technology in the healthcare sector. We described the drawbacks of the existing pharmaceutical supply chain management, and addressed how to use blockchain in various ways to add traceability and accountability to the supply of drugs, and how to get rid of the problem of supplying duplicate drugs in blockchain supply chain management. How they'll blockchain identity program when it's running. By which means, exchanging medical data is beneficial while keeping the patient's private data confidential is clarified. We pointed out the potential methods, blockchain forms and third party implementations that can be used to incorporate a pharmaceutical based blockchain supply chain.

REFERENCES

[1] S. F. Roy and M. Jerremy, "African Counterfeit Pharmaceutical Epidemic: The Road Ahead," ACAPPP, 2009.
[2] "WHO | Growing Threat from Counterfeit Medicines," Bulletin of the World Health Organization, vol. 88, no.4, pp, 2010.
[3] H. Julian, S. Philip and M. Julian, "Combating the spread of fake drugs in poor countries," International Policy Network, 2009.
[4] G. R, "Te state control of medicines: Te frst 3000 years.," Br. J. Clin. Pharmac.,, vol. 8, no. 2, pp. 93-305, 1979.
[5] "United Nations Interregional Crime and Justice Research Institute (UNICRI)," Global counterfeiting:, 2003.
[6] E. Roxanne, D. K. Lisa and P. W. George, "Anti-counterfeiting in the fashion and luxury sectors: trends and strategies," Anti-counterfeiting – A Global Guide, 2013.
[7] N. Satoshi, "Bitcoin: A Peer-to-Peer Electronic Cash System," 2008.
[8] X. QI, B. S. EMMANUEL, O. KWAME, G. JIANBIN, D. XIAOJIANG and G. MOHSEN, "MeDShare: Trust-Less Medical Data Sharing Among Cloud Service Providers via Blockchain," IEEE Access, 2017.
[9] A. Asaph, E. Ariel, V. Thiago and L. Andrew, "MedRec: Using Blockchain for Medical Data Access and Permission Management," in 2nd International Conference on Open and Big Data, Cambridge, MA, 02139, USA, 2016.
[10] M. Mettler, "Blockchain Technology in Healthcare: The Revolution Starts Here," in IEEE 18th International Conference on e-Health Networking, Applications and Services, Healthcom, 2016.
[11] C. Edward, L. Ying, Z. Jia and L. Yang, "Healthcare services across China – on implementing an extensible universally unique patient identifier system," International Journal of Healthcare Management , pp. 1-7, 2017.
[12] "Tierion - Blockchain," [Online]. Available: https://tierion.com/. [Accessed 24 1 2018].
[13] "Every Product Has a Story," Provenance, [Online]. Available: https://www.provenance.org/. [Accessed 2 1 2018].
[14] "Blockchain in Healthcare," [Online]. Available: https://www.hyperledger.org/wp-content/uploads/2016/10/ey-blockchain-in-health.pdf. [Accessed 23 1 2018].
[15] "Blockcypher," [Online]. Available: https://www.blockcypher.com/. [Accessed 11 1 2018]. "BlockRx," iSolve, [Online]. Available: https://www.blockrx.com/. [Accessed 1 1 2018].
[16] G. Jeff, "Public versus Private Blockchains - Part 1: Permissioned Blockchains," 2015.
[17] G. Jeff, "Public versus Private BlockChain ain - Part 2: Permissionless Blockchains," 2015.
[18] "Bitcoin," Bitcoin Blockchain, [Online]. Available: https://bitcoin.org/. [Accessed 1 12 2017].

