

High Dimensional Health Care Privacy Approach using Blockchain Technology for Emergency Medicine Tracking System

¹Pratiksha Lahamage, ²Snehal Borhade, ³Rutuja Kasar, ⁴Pooja Rao, ⁵Mr. P. B. Vikhe

^{1,2,3,4} Students and ⁵Asst. Prof. in Department of Computer Engineering,
Pravara Rural Engineering College, Loni

Savitribai Phule Pune University.

pratikshalahamage@gmail.com

snehalborhade2000@gmail.com

rutujakasar41999@gmail.com

poojarao23061999@gmail.com

Abstract –

In the present conditions of a health-aware society, organization of pharmaceutical supply chains has become more complicated because it involves the life-saving of human beings and requires the participation of different collaborators such as pharmaceutical manufacturers, dealers, distributors, patients, information service providers and regulatory companies. Pharmaceutical companies are always the most important providers of the drug supply chain, causing too many risks. These risks break the quantity, quality of supply of medicine, their delivery to the accurate place and at the correct time to the customers. Drug Trafficking is a worldwide illegal business involving the cultivation, manufacturing, distribution and sale of items which are causes to drug prohibition laws. Counterfeit drugs are one of the effects of such limitations within existing supply chains which not only has a serious disadvantageous impact on human's health but also causes to severe economic loss on the healthcare industries. Accordingly, existing studies have emphasized the need for end- to-end track and detect, a robust system for pharmaceutical supply chains. In that matter, an end-to-end product tracking system across the pharmaceutical supply chain is mainly to ensure product safety and removing counterfeits and drug trafficking issues. In this system we present a Custom blockchain-based approach leveraging smart contracts and decentralized off-chain storage for efficient product traceability in the healthcare supply chain. The Intelligent contract guarantees data provenance, eliminates the need for intermediaries and provides a secure, immutable history of transactions to all stakeholders.

Keywords: *Blockchain Technology, Drug Counterfeiting, Drug Trafficking, Traceability, CDSCO.*

I. INTRODUCTION

A blockchain system considered as a truly incorruptible cryptographic database where important clinical facts may be recorded. A network of computers that is available to all of us jogging the software program maintains the system. Blockchain operates as a pseudo-nameless machine that nonetheless has privacy problems on account that all transactions are uncovered to the public, although it is tamper-proof in the experience of records integrity. They get admission to manage heterogeneous patients' healthcare statistics throughout multiple health institutions and devices needed to be carefully designed. Blockchain itself is not designed as a huge-scale storage system. Inside the context of healthcare, a decentralized garage answer would significantly complement the weakness of blockchain in the perspective.

Healthcare supply chain is a complicated network of various independent constituents that include raw material suppliers, manufacturer, distributor, pharmacies, hospitals and patients. Tracking supplies through this network is important due to various factors containing lack of information, centralized control and competing behaviour between stakeholders. Such complexity not only results

in in-efficiencies such as those highlighted through COVID-19 pandemic but can also aggravate the challenge of mitigating against the counterfeit drugs and drug trafficking as these can easily permeate the healthcare supply chain. The effect of illegal drug use is global, causing constant physical and emotional harm to users and adversely impacting their families, helpers, and many others with whom they have contact. Counterfeit drugs are products intentionally and illegally produced and/or mislabelled with respect to identity and/or source to make it appear to be an actual product. Such drugs can include painkillers that contain no active pharmaceutical ingredient (API), an incorrect amount of API, a minor-quality API, a wrong API, contaminant, or rewrapped expired products. Some counterfeit drugs may even be improperly formulated and produced in acceptable conditions.

The blockchain network as a decentralized machine is extra resilient in that there's no single-factor attack or failure to examine centralized systems. But, due to the fact that all the bitcoin transactions are public and all people have got entry to, there already exist analytics tools that become aware of the contributors in the community based totally on the transaction records. With popularity analytics, similarity or closeness amongst subjects within large extent of statistics may be detected.

According to the Health Research Funding Organization, up to 30% of the drugs sold in developing countries are counterfeit. Further, a recent study by World Health Organization (WHO) defined counterfeit medicines as one of the important reasons of deaths in developing countries and in most cases the victims are children. In addition to the disadvantageous impact on human being, counterfeit medicines also cause major economic losses for the pharmaceutical companies. In this respect, the annual economic losses to the US pharmaceutical industries due to counterfeit medicine is estimated around \$200 billion.

A typical process of drug supply chain distribution is illustrated in Figure 1.

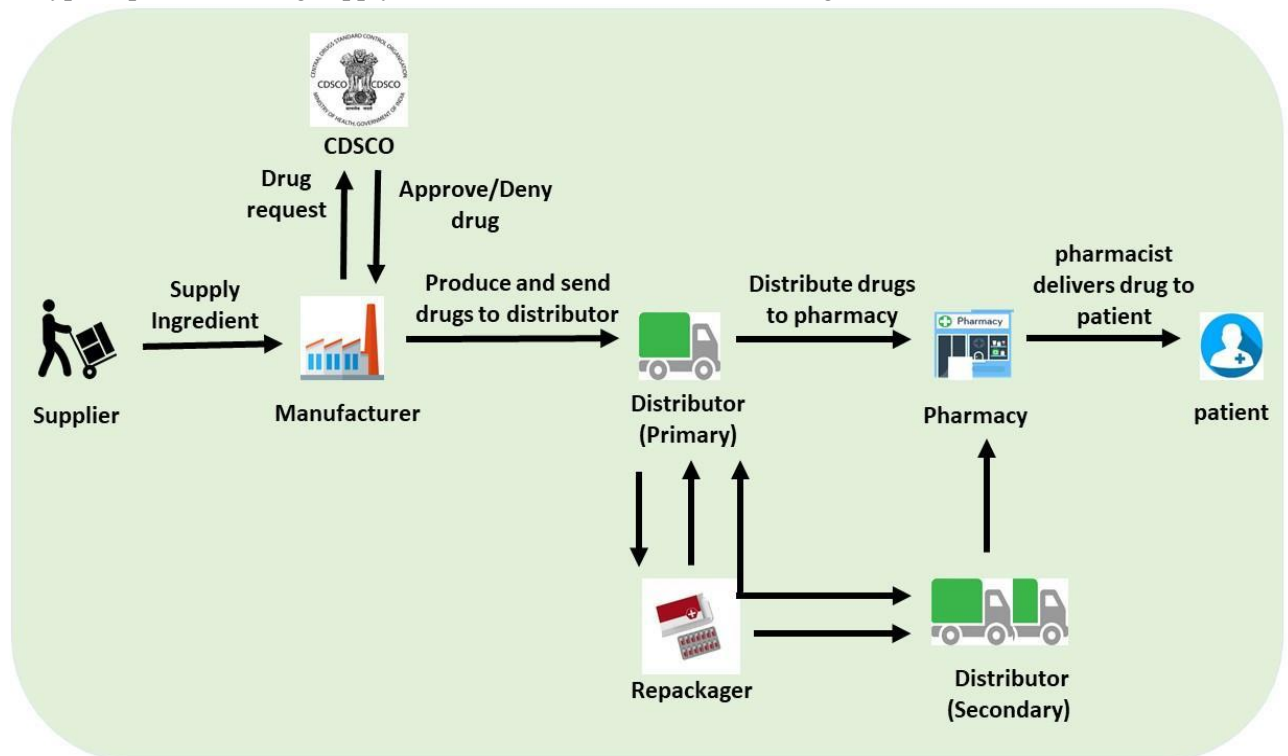


Fig. 1: Drug Supply Chain

The importance of drug traceability (track and trace) is moderately claimed and authorised by various countries all over the world. For example, the US Drug Supply Chain Security Act (DSCSA) has made it compulsory for the pharmaceutical companies to develop an electronic and compatible system

that indicates and tracks prescription drugs as they are distributed across the US. Hence, drug traceability has become necessary part of the pharmaceutical supply chain as it determines authenticity, and aims to track and trace chain of custody of the product across drug supply chain.

II. LITERATURE SURVEY

According to Cameron Faulkner et al.2020 [2], Near Field Communication (NFC) tags have been proposed to achieve visibility and authenticity across pharmaceutical supply chain. This NFC-based system afford the visibility throughout the all pharmaceutical supply chain stages. Here, Every drug is registered and authenticated by using key-value pair and NFC tag which attached to it. Before, patient can verify the authenticity and therefore the origin of drug by scanning the NFC tag using mobile application.

For the approach adopted by Hulse apple et al. 2019 [3], Similar concerns are valid, who developed a personal blockchain concurrently with the Bitcoin, which used as a ledger to hash of knowledge to secure the transactions in chain. Every product has its own permanent record which stored on their blockchain, making it impossible to control with the private keys. this technique creates a trust less system of transparency which designed to guard every stage of product transfer within the supply chain.

According to Faisal et al. 2019 [4], who proposed a Hyperledger-based in the pharmaceutical supply chain for drug traceability. Authors report increase within the performance in terms of throughput and minimizes latency of the proposed system with less utilization of resources, however their solution wasn't rigorously tested and was implemented in a small-sized network. This effort also highlighted the challenge of achieving scalable solutions with blockchain which has received significant attention in recent literature like [5].

According to Bilal Hawashin, Ayman M Mansour 2018, a healthcare system has been proposed which will provide NFC tag to patients. Each patient has NFC tag with a unique ID. This tag contains information of patient. This smart tag is use when patient go to hospital or emergency units. At that time patient should carry NFC tag instead of many files. This smart tag is read using reader or smart phone to retrieve information of patient and Every time it will update after health check-up. This eliminate the paper based documentation which decrease mistake in healthcare and Pharmacist can able to view medicine prescription given by doctor.

According to Huang et al. 2018 [6], proposed a drug traceability system, Drug ledger, which reflects the sensible drug transaction logic in the supply chain, and generates both authenticity and privacy of stakeholders' traceability information without losing the resilience of system. Drug ledger completes its workflow supported the expanded UTXO arrangement, especially that of package, repackage, and unpackage. However, recent studies like have highlighted concerns with the utilization of UTXO arrangement with reference to its weakness in programmability, high storage cost, and low state space utilization.

According to Corrado et al. 2013 [2], Djearmane and Supriya et al. 2013 [7], and Jamal et al. 2013 [8], For traceability, have proposed solutions but they use a centralized database which makes tampering goods information relatively easy and difficult to detect. In addition to, the utilization of various sorts of centralized databases may result within the proposed solutions to possess lack of interoperability and scalability

III. OBJECTIVES

In this proposed model we implemented following things:

- We preferred a blockchain based solution for the pharmaceutical supply chain that provides security, traceability, immutability, and accessibility of data provenance for pharmaceutical drugs.

- We designed a smart contract capable of handling various transactions among pharmaceutical supply chain stakeholders.
- We implement and test the smart contract that describes the working principles of our proposed solution.
- We perform security and cost analysis to estimate the performance of the proposed blockchain-based solution.
- We implemented an emergency medicine tracking system and gave it to the valid patients.

IV. PROPOSED WORK

The security demanding situations are nevertheless a few of the fundamental boundaries when thinking about cloud adoption services. The primary reason is that the database is hosted and processed inside the cloud server, which is beyond the control of the data owners. For the numerical question, those schemes no longer offer sufficient personal safety towards sensible demanding situations. In this system, we suggest different statistics example architectures for a ease database that protects several questions associated with the numeric variety. We put in force a three-layer/instance garage framework primarily based on facts computing.

The generation of block-chain attracts high attention first because of the opportunity of decentralizing incredibly unstable operations, which are traditionally carried out in predetermined records centers. The most famous example of use is the substitute of the feature of engaging in transactions within the system of financial institution transfers to a decentralized community of cryptographic handlers. The essence of this approach of processing financial transactions is the encryption of transaction sets combined into blocks with the inclusion within the code of the specific identifier code of the preceding block.

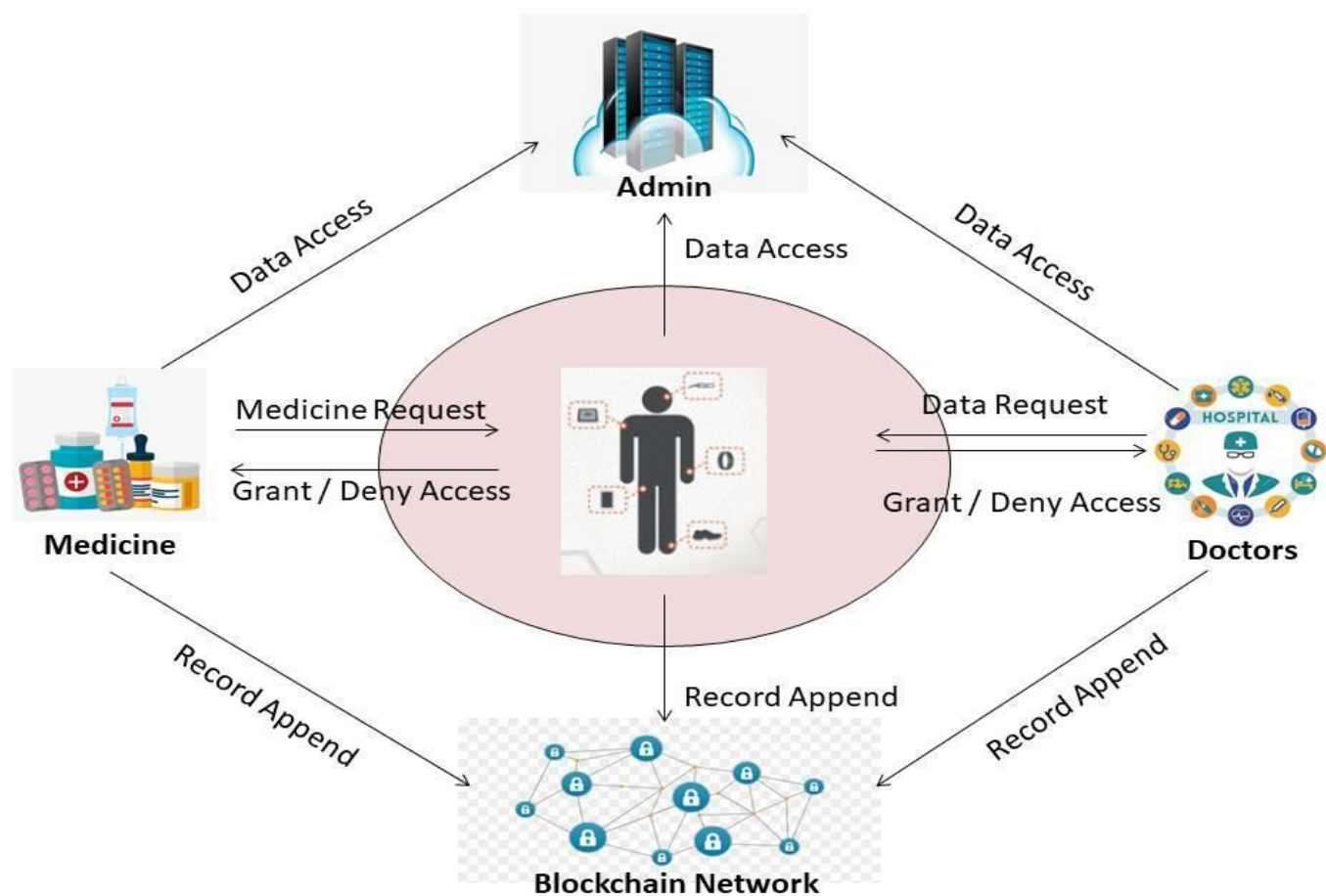


Fig. 2: System Architecture

We take a holistic view of the pharmaceutical supply chain, presenting an end-to-end solution for drug traceability whereas only focused on a subset of these challenges. Firstly, our approach recognizes and engages major stakeholders in the drug supply chain i.e. the CDSCO (Central Drugs Standard Control Organisation), supplier, manufacturer, distributor, pharmacy, and patient, whereas is limited to the supplier, manufacturer, and wholesaler as the stakeholders. hence, the pharmacists are constituted as an external entity, which is not the case in a actual drug supply chain. Secondly, we make clear-cut efforts to spot and clarify relationships among stakeholders, on-chain resources, smart contracts, and decentralized storage systems, which are lacking in solution. Furthermore, because of the significance of interactions among stakeholders, we have included precise definitions to remove any ambiguity, whereas such interactions have not been defined as part of the system. Thirdly, we use smart contracts technology to attain real-time, seamless traceability with push notifications to minimize human intercession and therefore undesired delays. Particularly, each drug Lot is allocated a unique smart contract that create an event whensoever a change in ownership take place and a list of events is delivered to the DApp user. However, the smart contracts are programmed for specific roles such as supplier, manufacturer and wholesaler, which require each participant to manually confirm which drugs are received. Such an approach can introduce delays and inaccuracies in the immutable hence data stored on the ledger. eventually, we have conducted a cost and security analysis to assess the performance of the proposed solution including discussion on how the proposed solution can be generic to other supply chains.

V. TRACEABILTY ANALYSYS

In this context, the different steps involved to verify the authenticity of the drug Lot are illustrated. Every medicine Lot is manufactured with a smart contract that is specifically designed for it and is responsible for provoking events and logging them on the ledger. A unique Custom block-chain address is generated for every drug Lot. However, copying Custom block-chain address of each drug is cumbersome, time consuming, and error prone process. Therefore, a QR code is used which can be easily scanned using android app. A QR code is a two-dimensional barcode that is readable by using smartphones, and it can allows encoding over 4000 characters in a two-dimensional barcode. Mapping a Custom block-chain address to a QR code can be done by using a Custom block-chain QR code generator in which the Custom block-chain address is passed and a unique QR code is generated which will exclusively map to that Custom block-chain address every time it gets scanned. Once the QR code gets attached to the drug Lot, it can be dispensed to patients.

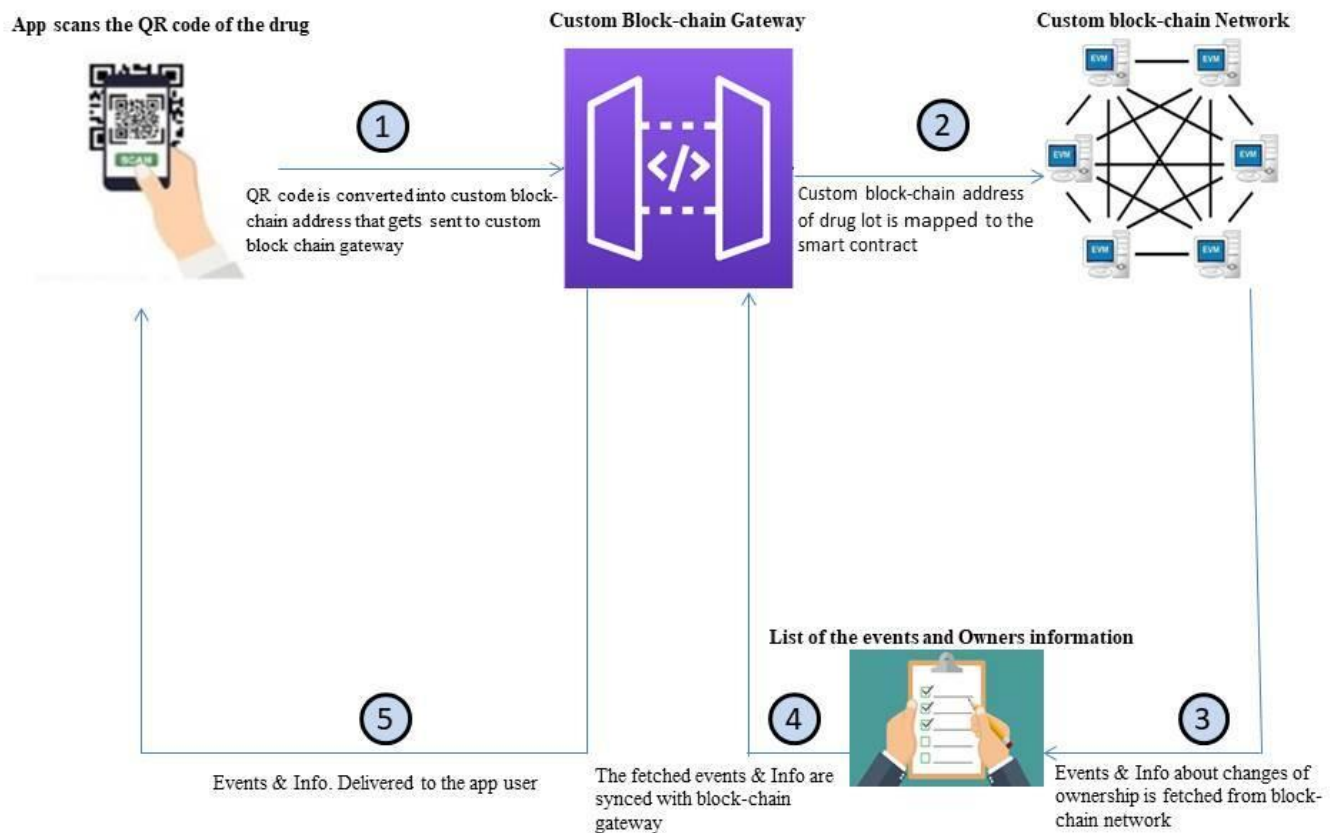


Fig. 3 Traceability Analysis

VI. ALGORITHM

A. Blockchain:

Block-chain is an virtual ledger that provides decentralized and transparent data sharing. With distributed recordings, all transaction data (stored in nodes) are concentrated and added to different blocks. Data of several types are distributed in distinct blocks, activating verifications to be made without the use of representatives. Then all the nodes form a block-chain along with timestamps. The data stored in each block can be verified concurrently and become fixed once entered. The whole process is open to the public, secure and transparent.

B. Custom Blockchain:

Custom Blockchain is a decentralized distributed database. The working processes of the system developed in this study are as follows:

Custom Blockchain provides low-cost off-chain storage to store supply chain transactions data to ensure reliability, accessibility, and integrity of the stored data. The integrity of data is maintained by generating a unique hash for every uploaded file on its server, the different hashes for the different uploaded files are then stored on the blockchain and accessed through the smart contract, and any change that arises to any of the uploaded file is reflected in the related hash.

C. Smart Contract:

Smart contracts are lines of code that are saved on a block-chain and always execute when pre-decided terms and conditions are match. At the most basic level, they are programs that run as they have been set up to run by the people who developed them for authentications. A smart contract is an agreement between two modules in the form of computer code. They run on the blockchain, so they are saved on a public database and remains fixed. The transactions that happen in a smart contract handled by the blockchain, so they can be sent automatically without a third party.

D. SHA Hash Generation:

The SHA-256 algorithm is a hashing algorithm that performs on data in one-way and Ron Rivest develops it. It is an evolution of previous algorithms such as SHA 0, SHA 1, SHA 256, SHA 384. Hashing is also known as compression or message summary function, which takes the entire variable length and changes it into a binary sequence of fixed length.

VII. CONCLUSION

In this paper, we have examined the challenge of medicine traceability inside pharmaceutical supply chains highlighting its significance specially to protect against counterfeit medicine and medicine trafficking. We have developed and determined a blockchain-based solution for the pharmaceutical supply chain to track and trace medicine in a decentralized manner. Specifically, our proposed solution holds cryptographic fundamentals of block-chain technology to achieve protected logs of events within the supply chain and uses smart contracts within Custom blockchain to achieve automated recording of events that are accessible to all participating collaborators.

REFERENCES

- [1] Sujit Biswas, Kashif Sharif, Fan Li, Zohaib Latif, Salil S. Kanhere, and Saraju P. Mohanty, "Interoperability and Synchronization Management of Blockchain-Based Decentralized e-Health Systems". *IEEE Transactions on Engineering Management* 2020
- [2] Corrado, C., Antonucci, F., Pallottino, F., Jacopo, A., David, S. and Paolo, M. (2013), "A review agri- food supply chain traceability by means of RFID technology", *Food and Bioprocess Technology*, Vol. 06 No. 3, pp. 353-366
- [3] Hulseapple, "C. Block Verify Uses Blockchains to End Counterfeiting and Make World More Honest". 2015. Available: <https://cointelegraph.com/news/block-verify-uses-blockchains-to-end-counterfeiting-and-make-world-more-honest>. Accessed [5-June-2020]
- [4] Jamil, Faisal & Hang, Lei & Kim, Kyuhyung & Kim, Dohyeun. (2019). "A Novel Medical Blockchain Model for Drug Supply Chain Integrity Management in a Smart Hospital". *Electronics*. vol 8. DOI: 10.3390/electronics8050505.
- [5] Delgado-Segura S., Pérez-Solà C., Navarro-Arribas G., HerreraJoanco- martí J. (2019) "Analysis of the Bitcoin UTXO Set". In: Zohar A. et al. (eds) *Financial Cryptography and Data Security*. FC 2018. *Lecture Notes in Computer Science* vol 10958. Springer, Berlin.
- [6] Yan Huang, Jing Wu, Chengnian Long, "Drugledger: A Practical Blockchain System for Drug Traceability and Regulation", *IEEE Conference on Internet of Things*, 2018.
- [7] Supriya, B.A. and Djearamane, I. (2013), "RFID based cloud supply chain management", *International Journal of Scientific and Engineering Research*, Vol. 04 No. 5, pp. 2157-2159.
- [8] Khalid Jamal, S.M., Omer, A. and Abdus Salam Qureshi, A. (2013), "Cloud computing solution and services for RFID based supply chain management", *Advances in Internet of Things*, Vol. 03 No. 4, pp. 79-85.
- [9] Hardwick, Freya Sheer, Raja Naeem Akram, and Konstantinos Markantonakis. "E-Voting with Blockchain: An E-Voting Protocol with Decentralization and Voter Privacy." *arXiv preprint arXiv:1805.10258* (2018).

- [10] Dongsheng Zhang. "Resilience enhancement of container-based cloud load balancing service". Technical report, PeerJ Preprints, 2018
- [11] Gupta A, Patel J, Gupta M, Gupta H., "Issues and Effectiveness of Blockchain Technology on Digital Voting". *International Journal of Engineering and Manufacturing Science*, Vol. 7, No. 1, 2017
- [12] Navya A., Roopini R., SaiNiranjana A. S. et. Al, "Electronic voting machine based on Blockchain technology and Aadhar verification", *International Journal of Advance Research, Ideas and Innovations in Technology*, (Volume 4, Issue 2)
- [13] Panja, Somnath, and Bimal Kumar Roy. "A secure end-to-end verifiable e-voting system using zero knowledge based blockchain."
- [14] Martin A Makary and Michael Daniel. "Medical error-the third leading cause of death in the us". *BMJ: British Medical Journal (Online)*, 353, 2016
- [15] Till Neudecker, Philipp Andelfinger, and Hannes Hartenstein. "Timing analysis for inferring the topology of the bitcoin peer-to-peer network". In *Ubiquitous Intelligence & Computing, Advanced and Trusted Computing, Scalable Computing and Communications, Cloud and Big Data Computing, Internet of People, and Smart World Congress, 2016 Intl IEEE Conferences*, pages 358–367. IEEE, 2016
- [16] Dongsheng Zhang and James PG Sterbenz. "Robustness Analysis and Enhancement of MANETs using Human Mobility Traces". *Journal of network and systems management*, 24(3):653–680, 2016.
- [17] Paul Tak Shing Liu. "Medical record system using blockchain, big data and tokenization". In *International Conference on Information and Communications Security*, pages 254–261. Springer, 2016
- [18] Dongsheng Zhang and James P. G. Sterbenz, "Measuring the Resilience of Mobile Ad Hoc Networks with Human Walk Patterns", In *Proceedings of the 7th IEEE/IFIP International Workshop on Reliable Networks Design and Modeling (RNDM)*, Munich, Germany, October 2015.
- [19] Dongsheng Zhang and James P. G. Sterbenz. "Robustness analysis of mobile ad hoc networks using human mobility traces". In *Proceedings of the 11th International Conference on Design of Reliable Communication Networks (DRCN)*, Kansas City, USA, March 2015.
- [20] Dongsheng Zhang. "Resilience Evaluation and Enhancement in Mobile Ad Hoc Networks". PhD thesis, University of Kansas, 2015
- [21] Dongsheng Zhang and James P.G. Sterbenz. "Modeling critical node attacks in MANETs". In *Self-Organizing Systems*, volume 8221 of *Lecture Notes in Computer Science*, pages 127–138. Springer Berlin Heidelberg, 2014
- [22] Dongsheng Zhang and James P. G. Sterbenz. "Analysis of Critical Node Attacks in Mobile Ad Hoc Networks". In *Proceedings of the 6th IEEE/IFIP International Workshop on Reliable Networks Design and Modeling (RNDM)*, pages 171–178, Barcelona, Spain, November 2014.
- [23] Christian Decker and Roger Wattenhofer. "Information propagation in the bitcoin network". In *Peer-to-Peer Computing (P2P)*, 2013 IEEE Thirteenth International Conference on, pages 1–10. IEEE, 2013
- [24] Dongsheng Zhang, Santosh Ajith Gogi, Dan S. Broyles, Egemen K. C, etinkaya, and James P.G. Sterbenz. "Modelling Wireless Challenges". In *Proceedings of the 18th ACM Annual International Conference on Mobile Computing and Networking (MobiCom)*, pages 423–425, Istanbul, August 2012.
- [25] Dongsheng Zhang, Santosh Ajith Gogi, Dan S. Broyles, Egemen K. C, etinkaya, and James P.G. Sterbenz. "Modeling Attacks and Challenges to Wireless Networks". In *Proceedings of the 4th*

IEEE/IFIP International Workshop on Reliable Networks Design and Modeling (RNDM), pages 806–812, St. Petersburg, October 2012.

- [26]Bougdira, A., Ahaitouf, A. and Akharraz, I. (2019), "Conceptual frame- work for general traceability solution: description and bases", *Journal of Modelling in Management*, Vol. 15 No. 2, pp. 509-530.