



Blockchain Powered Smart Cities

Amol Dhondse
IBM Software Lab (ISL)
Bengaluru, India

Sachchidanand Singh
IBM Software Lab (ISL)
Pune, India

ABSTRACT

Typically, when a healthcare provider fails to give reasonable treatment to a patient which could cause injury, death or overcharges then it is termed as medical malpractice. The medical negligence and cut practice are prevalent in developing and developed societies in one form or other. In the past there has been unfortunate cases where doctors pretend to give treatment to an already expired patient to overcharge and even in some cases hospital authorities try to influence postmortem reports in their favor to avoid any medico-legal case. This paper attempts to provide a solution to restrict such medical malpractices in case of critically ill patients admitted to ICU having cancer, heart attack, coronary bypass surgery etc. The paper suggests building a permissioned private Blockchain solution with the help of Cloud, IoT, wearable devices and smart medical devices fitted with sensors. The Cloud based system will receive vital health parameters of patient with help of wearable and sensors devices on regular interval of time which is configurable and append new hash block to immutable Blockchain ledger using cryptographic hash function. It will provide role-based access to all the ecosystem partners for due diligence in the case of any unfortunate events.

General Terms

Blockchain, Smart City, Consensus Protocols.

Keywords

Hash function, Permissioned network, Cloud Control Center, Cryptographic Hash Block, Public Key Cryptography, Asymmetric Encryption algorithm, MD5, SHA-1.

1. INTRODUCTION

According to the United Nations report, 55 percent of the world's population lives in urban areas which will go up to 68 percent by 2050. India, China, and Nigeria combined will represent 35 percent of the projected urban population growth between 2018 and 2050. Smart cities should be ready for population explosion and must plan accordingly ^{[1],[2],[3]}.

As per report from Directorate of Medical Education and Research (DMER) in India, around 60% of the doctors indulge in 'cut practice'. And another report from Medical Malpractice Center states that around 15,000 to 19,000 medical malpractice suits are filed against doctors every year in United States. There have been attempts by Government authorities to curb growing menace of the referrals against a commission in healthcare but nothing concrete materialized.

2. WHAT IS BLOCKCHAIN

Blockchain is immutable, decentralized, append only digital ledger of transactions stored as node or blocks. Many computers are connected to the Blockchain network which compete to solve a given problem and the results are shared among all computers nodes on the network. The computers, or

nodes, connected to this network must agree on the solution, hence Blockchain is called consensus-driven network ^[4].

Blockchain is a distributed database and decentralized ledger that maintains a continuously growing list of records, called blocks, in chronological order. New blocks and the data within are defined, confirmed and verified through a consensus process called mining. Block is derived and there is verification process which is decentralized process with acceptance from multiple parties involved in this transaction. The transaction is transparent to all the stakeholders. Each block is a time stamped transparent transaction across multiple parties associate with time stamp. It's like transparent events across stakeholders which looks like chain of events across different blocks ^[4].

Important elements of the blockchain is Cryptographic hash function. Transactions are verifiable when the miners define and produce a unique cryptographic fingerprint using a hash function. The hashed block must have a definite, but random, number of zeroes at the beginning. The hash with the correct number of zeroes is entirely unpredictable, so the miners keep trying different hashes. Hash function defines and set of digital data and produces a numeric piece of data with a defined fixed range. Delivering the same exact data to a hash function, is something like same input provided to every piece of data every time. If the data input varies even by one variable, the hash function's output will change.

There are 3 different types of blockchain - Public, Private and Hybrid.

2.1 Public Blockchain

An open platform that anyone in the world can join, if he or she is able to show proof of work. A public blockchain is considered fully decentralized.

2.2 Private Blockchain

Only the owner can make changes. This is like the current infrastructure, wherein the owner (a centralized authority) has the power to change the rules, revert transactions, etc., based on need.

2.3 Hybrid Blockchain

A mix of both public and private blockchains. The ability to read and write can be extended to a certain number of people/nodes. A consortium blockchain can be used by groups of organizations that work together on developing different models by collaborating with each other, thereby developing solutions while maintaining intellectual property rights.

3. BLOCKCHAIN FOR SMART CITIES

The social security systems can be implemented on the Blockchain and take advantage of it ^{[5],[6],[7],[8]}. For example, Asure Foundation brings the mechanics of the German statutory pension system onto the Blockchain to research the

advantages for social security systems. Its implemented on the Ethereum blockchain and Asure protocol / platform.

Asure Foundation used the German pension system as a model which has 125-year history. It's based on the pay-as-you-go model. The companies and employees pay a percentage of salaries into this system which is not invested but used to pay current pension obligations.

The amount paid to retirees is based on average salaries. And value of each year's contribution is published by German pension insurance agency. This is then multiplied the number of years contributed and the percentage of the average salary earned during the person's lifetime. In our opinion, pay-as-you-go-based systems are particularly suitable for implementation on the blockchain, since no funds must be invested in the capital market. Instead, the available funds are only redistributed.

Blockchain-based solutions have potential to make operations more efficient and improve delivery of services. Use of Blockchain technology in the emerging markets could help to solve delivery issues of essential public services [5], [6], [7], [8].

The delivery of social welfare is quite compelling like blockchain-enabled birth (or death) certificate, blockchain based property title management. One classic example is MPESA, observers estimate that around 40% to 60% of Kenya's GDP flows through M-PESA which is centralized in nature and not recommended to allow just one company controlling position.

Blockchain technology offers unique opportunities to city and state governments to streamline basic services and engage with common people. For example, in case of an unfortunate event like death, Blockchain system can trigger a series of action automatically to following department to for advisory actions:

- Insurance company
- Banking and Financial Institutions
- Land registry offices
- Post-mortem House
- Pension Office
- Municipal Corporation or County

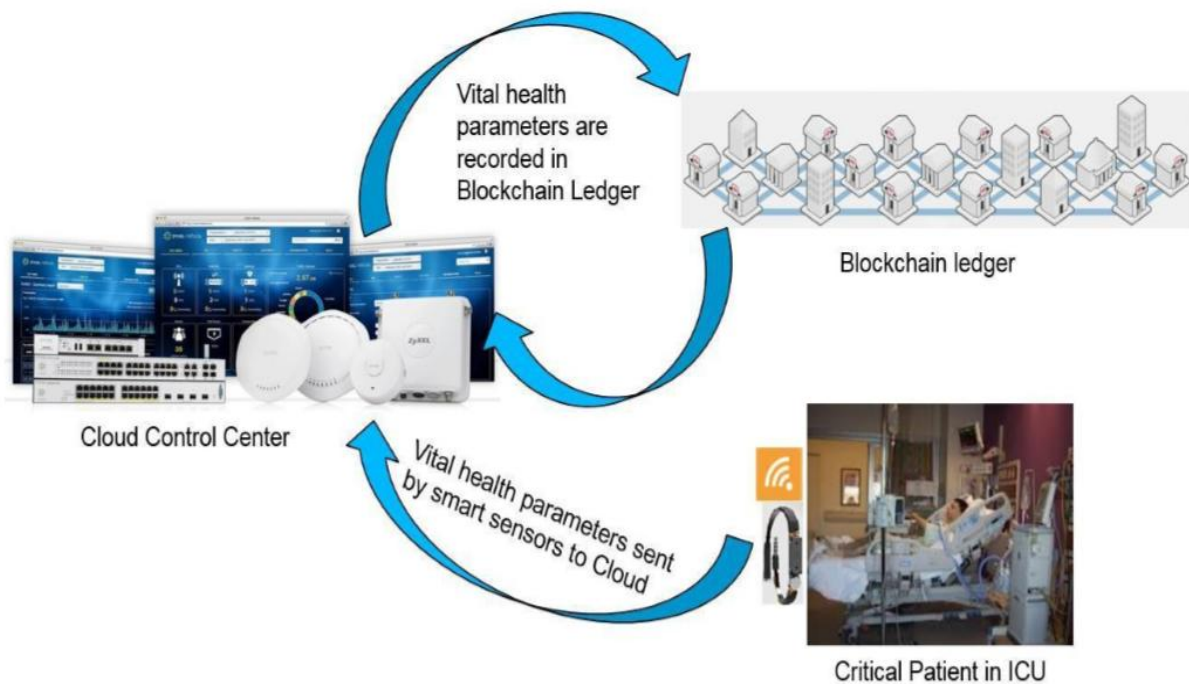


Fig 1. Blockchain based Healthcare Solution

3.1 Blockchain in Waste Management

Waste management is one of the critical challenges faced by most countries around the world. Blockchain and IoT together can make waste management effective and help to make the city clean and tidy.

3.2 Blockchain in Logistic [9]

Blockchain technology can streamline logistics, supply chain operations and help to provide better service to their clients. Blockchain in Trucking Alliance (BiTA) is actively using Blockchain solutions for trucking-related transactions in the world. It helps in bringing proper traceability and transparency using IoT sensors whereas blockchain lets the

transaction validated and recorded in the digital ledger. After validation, it gets added to blockchain as a block which is immutable and can't be altered unless the connected nodes approve the change.

3.3 Blockchain in Real Estate

Real estate is another space which can be revolutionize using blockchain-based smart contracts. We can track real estate investments using blockchain and limit the risk of possible fraud since each transaction is time-stamped and immutable.



3.4 Blockchain in Power Management

Blockchain can help to better manage power and energy sector. It can help to manage consumers, how much power they are consuming, the payment side, and much more.

3.5 Blockchain in Data Security & Identity

Data is valuable and needs to be protected with high-level security to avoid misuse. Various records are kept by local businesses, Government and Mayor Offices and shared among different branches or organizations. Using permissioned blockchain, data can be safely shared among interested authorized parties and we can restrict unauthorized access of data. The nodes connected on Blockchain network needs to validate for any changes made and if not, it will be void. Therefore, confidential data and sensitive personal information can be kept safe using blockchain^{[10], [11], [12], [13]}.

3.6 Blockchain for Transaction

Every type of transactions, starting from financial sector to basic transactions can be easily tracked and recorded using blockchain technology. Banking and financial institutions are becoming smart with cryptocurrency and blockchain which can be used as the mode of transaction and validation. Alongside the normal fiat currencies which is government regulated physical money, digital currency can also be used for transactions as an alternate option.

4. BLOCKCHAIN BASED HEALTHCARE WORKFLOW

In Blockchain-based healthcare we are proposing a Cloud based system which can receive vital health parameters like heartbeat, blood pressure, sugar level, body temperature, pulse rate etc of critically ill patient from Intensive Care Unit (ICU), Coronary Care Unit (CCU), Cardiac Intensive Care Unit (CICU), Neonatal Intensive Care Unit (NICU) with help of IoT sensor and wearable sensors devices on regular time-interval which is configurable. Obviously, patients and his/her family's prior consent will be taken to records personal health records.

Cloud based system linked to a distributed Blockchain ledger will record all vital health parameters in a chronological order which is immutable. When patient's physiological parameters suddenly change, then IoT sensor and wearable devices will take corrective actions like raise alert messages and send proactive recommendations (using back-end machine learning) to doctors and hospital staff.

And in case of any unfortunate events like death, the vital health parameters recorded in distributed Blockchain ledger will provide leads for preparing correct postmortem reports, useful evidences for insurance claims etc.

In case patient expires during treatment, then doctors can't pretend treatment post-expiry to overcharge on medical bills since details will be captured on immutable distributed ledger. The Blockchain ledger records will help in identifying the exact cause of patient's death and postmortem reports can't be manipulated.

Fig 2 on next page talks about Blockchain based healthcare workflow. The participants nodes are:

- Insurance company
- Govt Organizations
- Patients Office
- Family Members
- Hospital Network
- Legal attorney/Lawyers
- Municipal Corporation
- Land Registrar Office
- Pension Department
- Privacy/Data Breach Insurance policy
- Re-insurance company
- Laboratories/Pathology
- Pharmacists
- Pharmaceutical company
- Forensic Pathology
- Coroner (in US)
- Patient-safety advocate

4.1 What are Cryptographic Hash Functions?

Cryptographic hash function is an algorithm which can be run on a given data to produce a value called a checksum. It's used to verify the authenticity of given piece of data. If the checksums generated by 02 files using the same cryptographic hash function are identical then they can be assumed to be identical. Most commonly used cryptographic hash functions are MD5 and SHA-1

4.2 Cryptography Ensures Consensus

Blockchain must create new blocks. Since blockchains are decentralized systems, new blocks must be created not by a single authenticating entity, but by all participating nodes in the network. To add a new block, the network must arrive at a consensus.

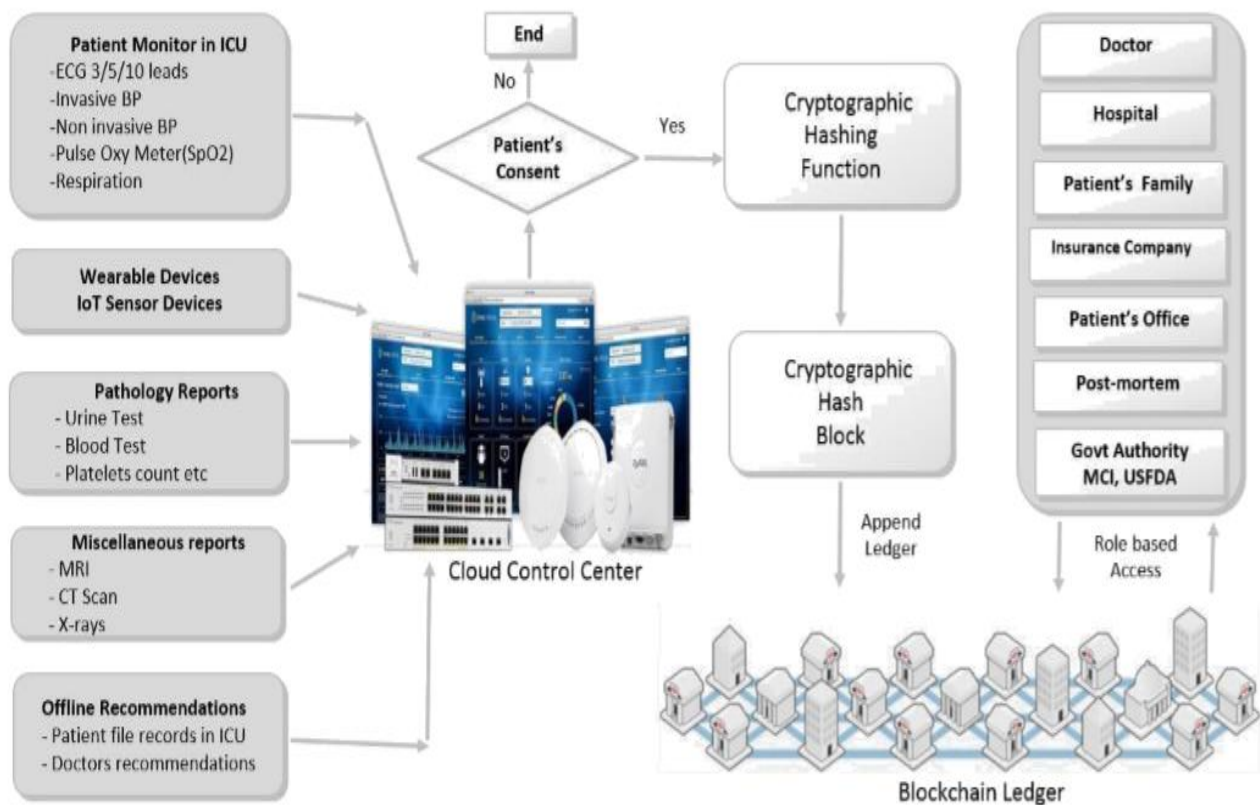


Fig 2. Blockchain based Healthcare Workflow

5. SUMMARY AND CONCLUSION

Blockchain technology into smart cities can play a paramount role in connecting all the smart city services and boost security and service transparency. It can be used in self executing smart contracts; these are agreements between the parties directly written into lines of code. Smart contracts allow for trusted and transparent transactions without the need for a mediating third party. This makes the process easier, cheaper, safer, and much faster. Blockchain technology can help in billing and transactions processing, handling facilities management, or facilitating smart grid energy sharing^[14].

Social security systems be implemented on the Blockchain and take advantage of it. For example, graduation rates of Nigerian girls were improved by automatically generating cash payments to families when their daughter achieves a 90% attendance rate using Blockchain technology. Help homeowners conserve electricity with a 'smart' refrigerator and then automatically donate the money saved to charity.

Northern European country Estonia has implemented blockchain technology into its government infrastructure like Estonian eHealth authority which uses blockchain technology to keep the medical data of citizens secure and easily accessible. Blockchain is gaining trust in enterprise and analysts suggest that more governments will implement blockchain technology into sensitive infrastructures to protect important data from individual or government-sponsored hackers.

6. ACKNOWLEDGMENTS

Our thanks to the experts who have contributed towards development of the template.

7. REFERENCES

- [1] C. Lazaroiu and M. Roscia, "Smart district through IoT and Blockchain," 2017 IEEE 6th International Conference on Renewable Energy Research and Applications (ICRERA), San Diego, CA, 2017, pp. 454-461.
- [2] R. Rivera, J. G. Robledo, V. M. Larios and J. M. Avalos, "How digital identity on blockchain can contribute in a smart city environment," 2017 International Smart Cities Conference (ISC2), Wuxi, 2017, pp. 1-4.
- [3] J. Xie et al., "A Survey of Blockchain Technology Applied to Smart Cities: Research Issues and Challenges," in IEEE Communications Surveys & Tutorials.
- [4] S. Singh and N. Singh, "Blockchain: Future of financial and cyber security," 2016 2nd International Conference on Contemporary Computing and Informatics (IC3I), Noida, 2016, pp. 463-467.
- [5] Z. Alhadhrami, S. Alghfeli, M. Alghfeli, J. A. Abedlla and K. Shuaib, "Introducing blockchains for healthcare," 2017 International Conference on Electrical and Computing Technologies and Applications (ICECTA), Ras Al Khaimah, 2017, pp. 1-4.



- [6] Sabyasachi Chakraborty, Satyabrata Aich, Hee-Cheol Kim, "A Secure Healthcare System Design Framework Communication Technology (ICTACT) 2019 21st International Conference on, pp. 260-264, 2019.
- [7] Thomas K. Dasaklis, Fran Casino, Constantinos Patsakis, "Blockchain Meets Smart Health: Towards Next Generation Healthcare Services", Information Intelligence Systems and Applications (IISA) 2018 9th International Conference on, pp. 1-8, 2018.
- [8] Kai Zheng, Ying Liu, Chuanyu Dai, Yanli Duan, Xin Huang, "Model Checking PBFT Consensus Mechanism in Healthcare Blockchain Network", Information Technology in Medicine and Education (ITME) 2018 9th International Conference on, pp. 877-881, 2018.
- [9] Zhijie Li, Haoyan Wu, Brian King, Zina Ben Miled, John Wassick, Jeffrey Tazelaar, "A Hybrid Blockchain Ledger for Supply Chain Visibility", Parallel and Distributed Computing (ISPDC) 2018 17th International Symposium on, pp. 118-125, 2018.
- [10] Giacomo Morganti, Enrico Schiavone, Andrea Bondavalli, "Risk Assessment of Blockchain using Blockchain Technology", Advanced Technology", Dependable Computing (LADC) 2018 8th Latin-American Symposium on, pp. 87-96, 2018.
- [11] Weizhi Meng, Elmar Wolfgang Tischhauser, Qingju Wang, Yu Wang, Jinguang Han, "When Intrusion Detection Meets Blockchain Technology: A Review", Access IEEE, vol. 6, pp. 10179-10188, 2018.
- [12] Xueping Liang, Sachin Shetty, Deepak Tosh, "Exploring the Attack Surfaces in Blockchain Enabled Smart Cities", Smart Cities Conference (ISC2) 2018 IEEE International, pp. 1-8, 2018.
- [13] Ryosuke Abe, Hiroki Watanabe, Shigenori Ohashi, Shigeru Fujimura, Atsushi Nakadaira, "Storage Protocol for Securing Blockchain Transparency", Computer Software and Applications Conference (COMPSAC) 2018 IEEE 42nd Annual, vol. 02, pp. 577-581, 2018.
- [14] Asraful Alam, Mohammad Tausiful Islam, Arafa Ferdous, "Towards Blockchain-based Electricity Trading System and Cyber Resilient Microgrids", Electrical Computer and Communication Engineering (ECCE) 2019 International Conference on, pp. 1-5, 2019.