Webology (ISSN: 1735-188X)
Volume 18, Number 4, 2021

Importance Of Blockchain Technology To Implement Healthy Healthcare Ecosystem

[1]Manish Pundlik, [2]Pramod Pandurang Jadhav, [3]Santosh Pawar, [4]Taranjeet Sood and [5]Deepak Sukheja

[1,2, 3] Dr. APJ Abdul Kalam University Indore (M. P.) India
[4] SICA College, Indore.

[5]VNR Vignana Jyothi Institute of Engineering &Technology, Hyderabad, India

Abstract

Background: Healthcare data is more common in the world today than it was even a decade ago, as cloud computing becomes ubiquitous. In the recent past, it has been seen that digitization is increasing in healthcare. Understanding the importance of healthcare and the need for digitization among our Kovid-19 has further accelerated the process of digitization in this area.

Objective: It is critical that data for patient use be secure and protected. This article is focus on, understanding the process of digitization in the field of Healthcare, we have tried to know how far blockchain technology can be used as a revolutionary technology in healthcare system.

Methodology: To achieve mentioned objective, we have first gathered information about today's healthcare system and studied the quality and acceptability of blockchain technology. Prepared and suggested a model in which how blockchain technology can be implemented in the healthcare world.

Keywords: Block, Block-chain technology, ledger, cryptography, hashing, Health care.

1. Introduction

Blockchain has various advantages, for example, decentralization, pertinacity, namelessness and auditability. People use the term ‘blockchain technology’ to mean different things, and it can be confusing. Sometimes they are talking about The Bitcoin Blockchain, sometimes it’s other virtual currencies, sometimes it’s smart contracts. Most of the time they are talking about distributed ledgers, i.e. a list of transactions that is shared among a number of computers, rather than being stored on a central server. The use of blockchains means that parties who don't trust each other must maintain a shared ledger of data. According to their submissions, the parties agree on the states, their values, and the facts of the matter are the same. In contrast to the blockchain, a peer-to-to-peer (P2P) network was initially used to make the blockchain distributed. Newly, blockchain has seen a surge in popularity because it is helpful for many different applications other than currency, such as transferring non-monetary assets and smart contract operations. The world is strongly leaning towards blockchain technologies due to their transparent, non-tampered and good governance services. This is conceptually hard work because every new block has its own hash and its also reference. So if anyone will change in any block of blockchain the hash that block would change. The foundation of blockchain is based on list of records, called blocks, which are linked using cryptography to provide the security. Nowadays block-chain technology is considered as the most significant invention of the internet. Directly, block-chain technology has been applied in different fields. The blockchain is controlled through group selection of nameless nodes, therefore both honest and adversary nodes take part in making of blocks. Simplified representation of Block chain shown in figure 1.

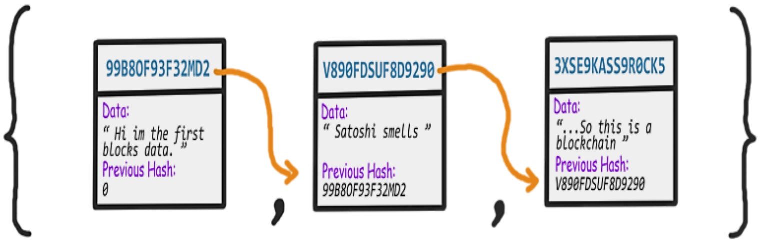

Figure 1: Simplified representation of Block chain

Blockchain is a database, but it does not hold data on one central server as a traditional database does. There is a constant stream of public data, but it is accessible only to those who have permission to look at it because the data part of a block comprises one or more transactions, with one block generally consisting of several consecutive transactions. It uses a cryptographic approach and produces a set of data that verifies the identity and ensures the integrity of the message. Blockchain has come to represent a disruptive technology in industries including healthcare, retail, finance, and more recently, the food. Industry.

2. Data Structure of Blockchain

In Mastering Bitcoin [1], data structure of blockchain explain very well. According to this book the blockchain data structure is an ordered, back-linked list of blocks of transactions. The blockchain can be stored as a flat file, or in a simple database. The data structure of Blockchain is summarised in Figure 2.a and 2.b. The structure of blockchain technology is represented by a list of blocks with transactions in a particular order (2.a) and each blocks which contains information such as the block ID, the preceding block ID, and the contents of multiple transactions (2.b). The prior block ID links a block to its predecessor, and this connection extends to the first block. A block ID is generated as a hashed value of the data in the block, impacting all subsequent blocks. As a result, if the content of a block is modified, all subsequent block IDs should be updated as well. This implies that even if an attacker tampers with just one transaction in a block, the Blockchain's tamper resistance is extremely strong since an attacker must change all subsequent block IDs.

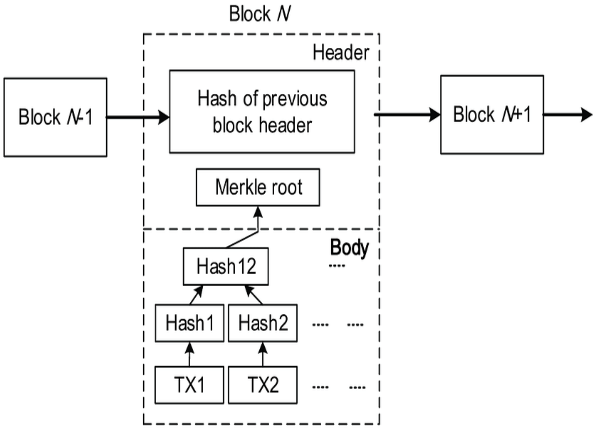

Figure 2: Data structure Block chain

The base part of the diagram depicts a transaction's data structure in general. A transaction ID and transaction contents are assigned to each transaction. The sender's and receiver's details and the remittance amount are all included in the transaction's contents. The transaction ID is a hashed value that represents the contents of the transaction. In the Blockchain, a typed query appends a new block to the previous block. Any blocks, including transaction contents, transaction ID, and block ID, are not updated or deleted.

3. Technical View of Blockchain

Technically, Blockchain is a system of recording information in a way that makes it difficult or impossible to change, hack, or cheat the system. Cryptography is used in blockchain to secure it. New generation blockchains enable a more comprehensive range of digital assets to be recorded and include assets as well.

3.1. Electronic digital signatures

A collaborative communication network of peers This network has been built to authenticate transactions and participate in the process of consensus. To grasp the nature of the name block, we must think of transactions in the context of being recognized and signed. Transactions are bundled and submitted to network nodes that must vouch for them every time a block is verified; it is published to the blockchain and broadcast to all network participants. The chain of all blocks is a timestamp and a pointer to the first block; therefore, it is a timestamp chain. The decentralized consensus network says that it delivers transactional security across the board. Every time a piece of new information is confirmed, each node registers it in the chain and adds a new block to its own database, which authorizes the solution. Blocks obey the embedded database protocol rules; if there is no single source of truth, the blockchain will maintain that. In a distributed architecture, one central database is established by a single entity, whereas every node has a replicated local database in blockchain architecture. Even if two separate blocks may temporarily form in the network circulation for a short time, the consensus protocol allows for quick and fluid recovery when they eventually converge. He identifies various types of consensus mechanisms

3.2. **Different types of consensus mechanism are as follows**

One key property of a blockchain system is that the nodes do not trust each other, meaning that some may behave in Byzantine manners. Blockchain consensus models are methods to create equality and fairness in the online world. The consensus systems used for this agreement is called a consensus theorem. Various types of consensus mechanism studied in [2], Proof of Work (PoW), Proof of work is the first Blockchain algorithms introduced in the blockchain network. Many blockchain Technologies uses this Blockchain consensus models to confirm all of their transactions and produce relevant blocks to the network chain. Proof of Stake (PoS), Proof of Stake consensus algorithm replaces the PoW mining with a mechanism where blocks are validated according to the stake of the participants. Delegated Proof of Stake is a variation of the typical proof of stake. The system is quite robust and adds a different form of flexibility to the whole equation. Similarly, the list consensus mechanism are available like Leased Proof-Of-Stake, Proof of Elapsed Time, Practical Byzantine Fault Tolerance, Simplified Byzantine Fault Tolerance, Delegated Byzantine Fault Tolerance, Directed Acyclic Graphs, Proof-of-Activity Proof-of-Importance, Proof-of-Capacity, Proof-of-Burn, and Proof-of-Weight etc.

4. Literature Survey

Author El-Gazzar R, et al in [3], Discuss innovation and security implications concerning blockchain technology in health care and state that there is a need for more use cases to ensure the secure sharing of data within the health care sector. Meinert E, et al in [4], summarize the reviews on strategies and frameworks used to implement blockchains in health care to increase data privacy, interoperability, and scalability. Also mentioned the requirement of operationalization of blockchains in healthcare to ensure the privacy of patient data. Gaynor M et al in [5] article studied about capability of blockchain and find the answer, can blockchain solve current health care issues in three main arenas: data exchange, contracts, and supply chain management? In [6] author Zhetao Li, Jiawen Kang, Rong Yu in 2018 have discuss in various contexts, the term "Peer-to-to-Peer" has been used, e.g., microgrids, renewable energy harvesting, and P2P networks. Unfortunately, the untrustworthy and nontrans parent energy markets do pose a common threat to security and privacy. Blockchain addresses the security issues by providing a secure energy trading system. An energetic trust chain can be used in most aspects of P2P energy trading. Instead of fixing transaction rate limiting due to transaction delays on the energy chain, the author resorted to a credit-based payment system. The Strasberg game is applied for credit-based loans. A three-dimensional analysis system and robust results are put to the energy chain and the concept of pay-for-performance. androgenous material. In[7], authors, examines a shifting model in healthcare that observes rising data and services in the cloud, especially convenience (such as having all of one's medical records at the fingertips in real-time) (e.g., the economics of healthcare data management). There are, however, shortcomings in the application of conventional primitives and access models to cloud-based environments. This paper considers how healthcare records could be secured using the Blockchain technology. There is a large amount of information being created, stored, and accessed within the healthcare industry, and that much of it is also disseminated. Most data is created during the time the CT or CT imaging is performed, and then it needs to be shared with the radiologist and the doctor. Thus, the results will be collected and stored in the hospital and made available to other members of the network at a later time. It is apparent that technology can contribute significantly to the quality of care by optimizing personnel, equipment, etc. For example, data contained in the paper is expensive to keep, difficult to archive and may be necessary to access. This, as you know, is the case because individuals working in the learning process find it difficult to view others as workers unless they are contributing to something of value. In [8] Peer-to-to-peer (P2P2P) electricity model for providing locally generated electricity for plug-in hybrid vehicles (PHEVs) has been described in this paper. Modelling does just what traditional systems do in another way: It provides incentives for people to unplug their plug-in hybrids to help balance the region's overall electricity use. Since transaction security and anonymity are significant problems, consortium blockchain technologies are inapplicable for most general use, though. the Block-consortium electricity trading method is used to demonstrate detailed transactions in a localized P2P market as well as the double-auction algorithm iterative solution is utilized to maximize social benefit in the electricity trading Used PETCOWS analysis shows that transaction and privacy protection are each improved. Real maps for Texas have demonstrated that double auction will also maximize social welfare without jeopardizing privacy for PHEV owners. Dads never read the latest sci-fi or comic books; they only remember the books from the days when they were being seen as entertaining, successful, and really nerdy, with dust jackets removed and insides read. Article In [9], presents a novel power-sharing system that reduces the strain on electric vehicle systems while at work. Also, this trading method is mutually beneficial for all those who are in the process of trading. An artificial population is assigned daily activities and a trip pattern to be calculated using all that data (Belgium). These drivers may be initially limited to three groups; for those who have a full day's charge at their disposal, this question deals with the two groups who aren't. These last customers have the option to take into account grid electricity pricing and their mobility constraints to customize their energy costs of operation. Finally, when all available offer/need information about vehicles in the parking areas are taken into consideration, an aggregator can produce an optimal per-vehicle and per-time price offer for the supply of renewable energy. This allows customers to benefit from excess renewable energy while driving. This driver's bill will be reduced by 71 in one minute and one zone by applying the trading. In [10], It's quite a delicate task to allow both security and operational staff the flexibility needed to assess the potential consequences of each proposed new change to procedures, design, and security design policy on the application of current policies and procedures for making future changes more secure. There is a proposal for a purely peer-to-peer version of electronic cash that does not require the use of a financial institution. Most of the benefits are lost if the transaction must be locked down with a trusted third party like digital signatures. There is no doubt that the most significant chain in the chain of events. In the absence of enough cooperating nodes, an attacker's chain will be split into multiple parts, each of which will outpace the others, as non-colluding nodes always control a majority of the CPU power. It does not need much of a framework to get running. Messages are not authenticated. Every node does the best to find a proof-of-work, and messages are no more verifiable after other nodes see them. In [12], Transactional security is studied in this paper by N. Z. Z. Aitzhan and D. Svetinovic presents as well as long-standing. They've created a testbed for decentralized energy trading with block technology, multi-signature signatures, and encrypted messages to establish transactions without exposing private data. On June 3, 1920, he was first knighted; on that date, he finally broke his silence and became a member of the Army Officers Club, although many believe that it was because he found the Miss America Pageant insulting. In [13], Author M. Mihaylov et al, presented a computerized currency, known as "Nergium" sustainable electricity system producers in the Smart Grid trades are referenced on the open market, with an estimation of its replacement cost already embedded in the system. Because of this, it uses various favorable circumstances compared to cash; it is similar to Bitcoin; however, it is unlike Bit-coin in that it's the process of being made by infusing computational energy. Additionally, they exchange one view of the universe for a better one based on efficient and renewable power production in the renewable energy grid network. In [14], Bitcoin has lured a large number of investors, say investors in the creative industry, as a result of being unconnected to the stock market. In contrast to e-money, they look at Bitcoin through a top-to-bottom study to comprehend why it has acquired massive acceptance. In [15] Blockchain is an emerging technology for distributed and transactional data sharing across an extensive network of untrusted participants, and in today's life, health care system storage data is increasing more. Patient data is more important; it should be more secure and accessible from anywhere.

In [16] author presents a Case Study for Blockchain in Healthcare. This system gives patients a comprehensive, immutable log and easy access to their medical information across providers and treatment sites. Also, incentivize medical stakeholders (researchers, public health authorities, etc.) to participate in the network as blockchain “miners”. The purpose of this case study was to expose, in preparation for field tests, a working prototype through which author analyze and discuss the approach and the potential for blockchain in health IT.

5. Mathematical Model

We are using healthcare data along with blockchain to provide security and privacy. The purpose will secure the patient's drug data, patient's personal data, and data related to disease, along with doctor's data and admin's information. Thus, this data related to health care would be taken as transactions in blockchain nodes; thus, after processing with the private and public key, all Authenticated users access the healthcare data securely [10].

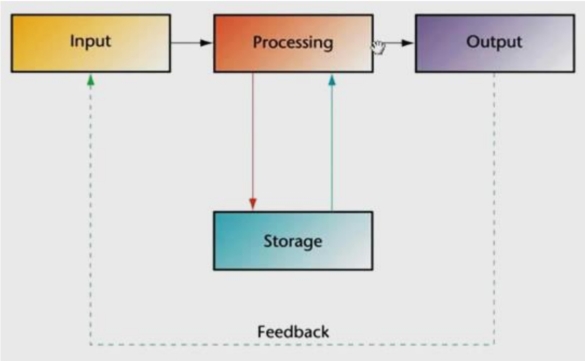

Figure 3: Mathematical model basic framework

U= User of the system
S - System - {I, P, O, Fc, Sc} Where I- Input
P- Process O- Output
Fc- Failure case Sc- Success Case I- {T1, T2, T3, T4}
Where,
{T1,T2,T3,T4}- Transaction of healthcare data in .text extension file. P- {Fc, Hc}
Where,
Fc- File is encrypted using advanced encryption standard Algorithm
Hc- Hash value is created for each transaction in block using Standard Hashing Algorithm Where
Fc - {Pt, Pk, De}
Where,
Pt- Transaction data in terms of Plain Text Pk- Private key is generated
De- HealthCare data Encrypted
O - File has been Encrypted and successfully stored.
Sc - It is success case when file of healthcare data stored successfully on network
FC - It is failure case when nodes containing all the transactions are not connected to Network.
The component level block diagram and internal level complete technical workflow of healthcare system shown in figure 4.a and 4.b.

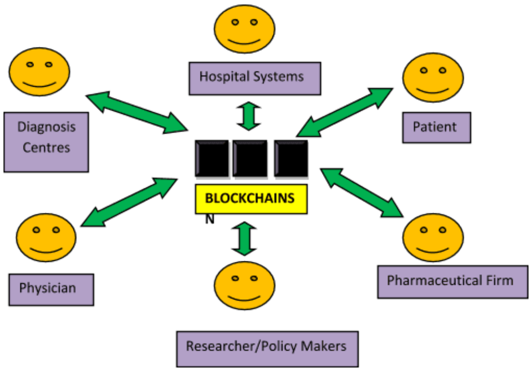

Figure 4.a : Healthcare using Blockchain Technology

6. System Architecture

This section covers system architecture and the flow of the system. System architecture shown in figure 5.

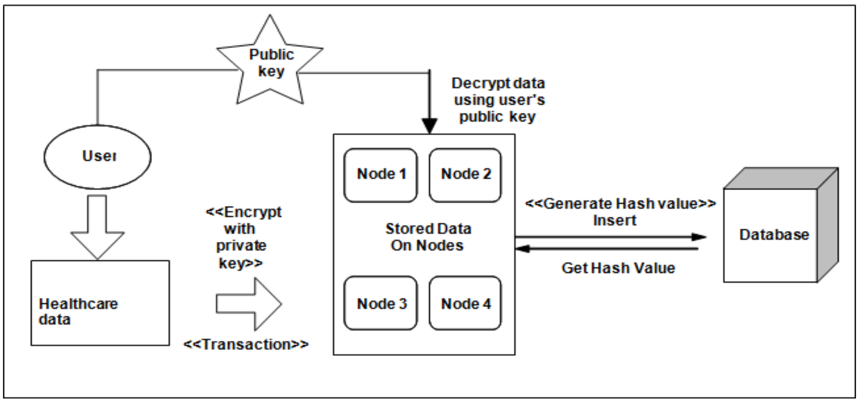

Figure 5: System Architecture

The foundation of an application is based on data, so the integrity of the data is critical. A set of data is generated by the digital signature of the identity and the signer's integrity that identifies it. To ensure that the information comes from the owner and that a certificate's digital signature is valid, the user verifies the signature with the owner's public key Hash is generated for every time a transaction is made in the network and each node, along with its subsequent block, making it possible for health care information to be distributed to the users. In the majority of cases, key-based cryptography is to verify the source of information is genuine.

There is a large amount of information being created, stored, and accessed within the healthcare industry, and that much of it is also disseminated. In the example, the data will need to be sent to the radiologist, the equipment (computerized tomography and computerized axial tomography) creates it. Thus, the results will be collected and stored in the hospital and made available to other members of the network at a later time. It is apparent that technology can contribute significantly to the quality of care by optimizing personnel, equipment, etc. Intellectual property captured in paper form is hard to archive and on hand when needed. Health challenges may result in decisions that are not always correct due to complete information, expensive due to missing information, and international trips to get better information (at increased cost and inconvenience for patients). In an industry like this, maintaining security, privacy, and keeping private healthcare data safe is critical. We understand how important it is to implement a sound and secure data management system

for security; this uses a chain concept of blocks and a digital signature. Storing the hash tables with data in the blockchain also ensures that other similar copies are immediately identified as outdated. To secure the entire node, Encryption is applied, and the Doctor app can return it.

6.1. Algorithm and Datasets

AES: 128bits (Advanced Encryption Standard). It's an equally simple algorithm. For many years, it had the capability of translating plain text into encrypted text. DES's failings necessitate the application of this algorithm. As opposed to 64-bit key search attacks, the 56-bit secret key should be considered insecure, as well. Blocks of 128 bits were required Rij created it. With this encryption key, the data owner key is being used to encipher the data.

Input: 128 bit ,192 bit,256-bit input in terms of 0 and 1
Process: 10/12/14, rounds for-128 bit ,192 bit,256 bit input Hard Disk: 20 GB
State block: Xor (i/p) Final round: 10,12,14

Each round consists: sub byte, shift byte, mix columns, add round key
Output: ciphertext (128 bit)

6.2 Secure hash algorithm (SHA)

The foundation of an application is based on data, so the integrity of the data is critical. A set of data is generated by the digital signature of the identity and the signer's integrity that identifies it. To ensure that the information comes from the owner and that a certificate's digital signature is valid, the user verifies the signature with the owner's public key Hash is generated for every time a transaction is made in the network and each node, along with its subsequent block, making it possible for health care information to be distributed to the users. In the majority of cases, key-based cryptography is to verify the source of information is genuine.

7. Conclusion

This article presents a new blockchain based method for health care environment monitoring. Health challenges may result in decisions that are not always correct due to complete information, expensive due to missing information, and international trips to get better information (at increased cost and inconvenience for patients). In an industry like this, maintaining security, privacy, and keeping private healthcare data safe is critical. We understand how important it is to implement a sound and secure data management system for security; this uses a chain concept of blocks and a digital signature. Storing the hash tables with data in the blockchain also ensures that other similar copies are immediately identified as outdated. To secure the entire node, Encryption is applied, and the Doctor app can return it. In this article, we have surveyed the overall concepts of the blockchain technology, which consists of basic definitions, characteristics, key concepts, advantages, limitations, consensus algorithms and along with security challenges. We intend to take an exhaustive exploration of smart contract in the future which incorporates both the centralized and decentralized models.

Reference

1. Mastering Bitcoin, by Released December 2014 Publisher(s): O'Reilly Media, Inc. ISBN: 9781449374044
2. D. Sukheja, L. Indira, P. Sharma and S. Chirgaiya, "Blockchain Technology: A Comprehensive Survey", Journal of Advanced Research in Dynamic and Control Systems, vol. 11, no. 9, pp. 1187-1203, 2019.
3. El-Gazzar R, Stendal K Blockchain in Health Care: Hope or Hype? J Med Internet Res 2020;22(7):e17199 DOI: 10.2196/17199.
4. Meinert E, Alturkistani A, Foley KA, Osama T, Car J, Majeed A, Van Velthoven M, Wells G, Brindley D Blockchain Implementation in Health Care: Protocol for a Systematic Review JMIR Res Protoc 2019;8(2):e10994 doi: 10.2196/10994
5. Gaynor M, Tuttle-Newhall J, Parker J, Patel A, Tang C Adoption of Blockchain in Health Care J Med Internet Res 2020;22(9):e17423doi: 10.2196/17423

6. Zhetao Li, Jiawen Kang, Rong Yu. Consortium Block chain for Secure Energy Trading in Industrial Internet of Things,14, Aug. 2018. 2015 IEEE. ISBN 978-1- 4503-3747-2/15/10.Available: http://dx.doi.org/10.1109/TII.2017. 2786307
7. Christian Esposito, Alfredo De Santis. Block chain: A Panacea for Health- care Cloud-Based Data Security and Privacy? Feb. 2018, INSPEC Accession Number: 17683528. [Online]. Available: http://dx.doi.org/10.1109/MCC.2018. 011791712
8. Kang, R. Yu, X. Huang. Enabling Localized Peer-to-Peer Electricity Trading Among Plug-in Hybrid Electric Vehicles Using Consortium Block chains,Dec. 2017.Copyright 2017 IEEE. INSPEC Accession Number: 17466402, Available: http://dx.doi.org/10.1109/TII.2017.2709784
9. R. Alvaro-Hermana, J. Fraile-Ardanuy. Peer to Peer Energy Trading with Electric Vehicles, Fall 2016. INSPEC Accession Number: 16157249. Avail- able: http://dx.doi.org/10.1109/MITS.2016.2573178
10. Gareth W. PetersEmail, Efstathios Panayi. Understanding modern banking ledgers through block chain technologies: Future of transaction processing and smart contracts on the internet of mone,18 Nov. 2015, Available: http: //dx.doi.org/10.2139/ssrn.2692487
11. Satoshi Nakamotoi. Bitcoin: A Peer-to-Peer Electronic Cash System,2009. Available: http://www.bitcoin.org/bitcoin.pdf
12. N. Z. Aitzhan. Bitcoin:Security and privacy in decentralized energy trading through multi-signatures, block chain and anonymous messaging streamse,Oct. 2018 . [Online]. Available: http://dx.doi.org/10.1109/TDSC.2016.2616861
13. M. Mihaylov, S. Jurado. Bitcoin:Nrgcoin: Virtual currency for trading of renewable energy in smart grids,21 July 2014. ISBN: 978-1-4799-6095-8. Avail- able: http://dx.doi.org/10.1109/EEM.2014.6861213
14. Barber et a. Bitter to better-how to make bitcoin a better currency,A.D. Keromytis (Ed.): FC 2012, LNCS 7397, pp. 399414, 2012.c International Financial Cryp- tography Association 2012. [Online]. Available: https://link.springer.com/ chapter/10.1007/978-3-642-32946-3_29
15. Das T.K., Banik A., Chattopadhyay S., Das A. (2019) Sub-harmonics Based String Fault Assessment in Solar PV Arrays. In: Chattopadhyay S., Roy T., Sengupta S., Berger-Vachon C. (eds) Modelling and Simulation in Science, Technology and Engineering Mathematics. MS-17 2017. Advances in Intelligent Systems and Computing, vol 749. Springer, Cham.
16. Ekblaw, Ariel et al. “A Case Study for Blockchain in Healthcare : “ MedRec ” prototype for electronic health records and medical research data.” (2016).