A Blockchain Based Technique for Storing Vaccination Records

Sanjib K. Deka
Computer Science & Engineering
Tezpur University
Tezpur, India
sdeka@tezu.ernet.in

Subhasish Goswami
Computer Science & Engineering
Tezpur University
Tezpur, India
subhasishgoswami00@gmail.com

Abhinav Anand
Computer Scence & Engineering
Tezpur University
Tezpur, India
abhinavanand397@gmail.com

2020 IEEE Bombay Section Signature Conference (IBSSC) | 978-1-7281-8993-2/20/$31.00 ©2020 IEEE | DOI: 10.1109/IBSSC51096.2020.9332171

Abstract*— Maintenance of immutable vaccination records and provision of accessing the records in order to prove immunity has been the need of the hour. The recent spread of Covid19 and related uncertainty over vaccinations and immunity have made the search for a secure trustable system for reporting vaccination data more essential. Multiple digital, as well as paper-based solutions have been tested but none has been reported successful enough. In this paper, a technique has been proposed to solve the problem by introducing blockchain-based solution to maintain records of vaccination and proof of immunity for individuals. The purpose has been to present a safe and efficient solution to the problem and hence the model proposed is based on concepts of smart contracts and built over Ethereum blockchain. The paper goes on to give a detailed study of the technique based on discussions of its various aspects like design, development and feasibility.

***Keywords*— Blockchain, Ethereum, Immunization, Vaccination**

I. Introduction

Vaccination is an important tool to handle the pandemics and hence it is very important to ensure mass vaccination wherever possible. The concept of herd immunity [1] is used to tackle infectious diseases using mass immunization. Recently, coronavirus pandemic has made the need for proper system of vaccination more important.

Coronavirus has affected the entire globe in a very short span of time, inadequately impacting the lives, livelihoods, industries, and economies. There are no sectors out there that have not been affected by this virus. The virus has not only affected the lives but has also taken the lives of people on a large scale, creating panic across the globe in response to which many governments imposed tough actions like lockdown. It has been recently found that even the survivors of Covid19 have high chances of being attacked by the virus again in the future [2]. The human body, in many cases, is not able to develop a permanent immunity towards the coronavirus

Amid the pandemic, where a full-proof medical remedy to fight the virus is awaited, extensive research by many experts are being carried out at a global level to fight the virus. The day is not far when the world will have a full-proof medical remedy of the highly contagious coronavirus.

Once the vaccine gets ready, the government of every nation will try to vaccinate its entire population in the least possible time, but there lies a problem with many heavily populated undeveloped nations on this planet for which the vaccination process will take a huge amount of time Also, on the other hand, those nations will have to unlock their sectors including education, tourism, and transport.

Once the nations across the globe start getting unlocked and getting restored to what they were prior to the coronavirus era, there will be a need for a mechanism to verify the immunity status of every individual at certain places where public gathering occurs. Here, immunity status refers to the vaccination status of that individual i.e. whether the person has been vaccinated or not, as no public places shall be allowing the entry of a person who has not taken a vaccination.

Record of vaccination can be managed using a centralized ledger and physical proof of vaccination can be provided to individuals. But in that case, there is a question about the integrity of the records of vaccination, also, various enforcing authorities can manipulate the data or records as they have the authority over the records. The world will be in the utmost need of a mechanism that stores the immunity status of a person with guaranteed security and verifies the vaccination status of a person wherever needed.

This paper attempts to address the above-mentioned challenge of storing the vaccination status' data and verifying the immunity status of a person at different checkpoints, wherever necessary, to establish a security system for the people to create a trusted vaccination report. This paper uses blockchain technology to provide a security mechanism. The fundamental concept of blockchain data structure is similar to a linked list of blocks containing information, the data is shared across all the nodes of a network and all the participating nodes have a copy. Recently, many applications have been using the blockchain technology as their databases to avoid any security breach and minimize the disputes over events.

The advantages of blockchain-based systems are:

1. It is a distributed ledger of transaction record in a peer to peer network which is publicly available to all the participants in the blockchain network.

2.It uses hash functions which makes it a self-cryptographic validation structure.

Creating a chain of block connected by cryptographic hashes makes it almost impossible for the hacker to tamper with the data or change the data. If the attacker anyhow succeeds in attacking a node-based in a blockchain network, the hash value of the attacked block will change leading to changing the hash value of all the blocks added after the block which has been attacked. When the nodes connected to the attacked node will report the occurrence of invalid blockchain, the attacked node will update its content as per the majority hence in order to attack a network, the attacker must attack decent majority of the total nodes with an extra node at once which is quite impossible and impractical in a blockchain network of a decent size.

The contribution of this paper is to provide a blockchain-based application to overcome the vulnerabilities and the challenge mentioned above. The best way to avoid changes in data record is to maintain using a distributed ledger. There are multiple new technologies to maintain distributed ledger apart from blockchain like acyclic graph [3]. The benefit of blockchain is that it is already widely used in multiple fields and hence can be easily used to establish a system of vaccination records.

Solution presented in this paper has been developed on the Ethereum blockchain network using smart contracts and to store documents related to vaccination InterPlanetary File System (IPFS) has been used which stores the documents in a distributed system.

This paper presents related work done in this field followed by a study of proposed solution and implementation of the technique. Discussions are studied related to the results and finally a conclusion has been presented for the proposed solution.

II. RELATED WORK

Maintenance of proper vaccination has been a challenge since long and continuous developments have been made to come up with new solutions. Initially, records were stored physically with physical records of vaccination provided to individuals but the problem with such a solution is the integrity of the data and because of this, various enforcement agencies, like governments, ask for certificates from individuals [4]. Maurer et al. [5] studied the need for standardization and simplification of vaccination records. The authors also emphasized on the need to have digital universal record for vaccination so that it is easier to provide a universally accepted record wherever necessary. Even though the need for a standardized system is important, there are always concerns of data security while storing centrally and hence a decentralized system is a more suitable one. Groom et al. [6] studies how having knowledge of vaccination records effects on increasing the vaccination rates. Authors study, having a well-maintained record of vaccination helps in preventing vaccine-preventable disease. Blockchain has been already used in the medical field and work has been done to use blockchain where there is need to maintain immutable ledger. Chen et al. [7] has studied the use of blockchain to store medical records. Xia et al. [8] has studied and presented how data stored can be shared using blockchain in a limited manner. Authors have used the blockchain technology to control the approach to the data stored in cloud. Recently many new works have been done to tackle Covid19 using blockchain. Resiere [9] proposed a system to update medical system in the Caribbean by using blockchain to increase the research in medical field to fight against Covid19. Khatoon [10] also researches on the use of blockchain for healthcare management. Bansal et al. [11] demonstrated the use of blockchain in creating immunity certificates. The authors also proposed the use of immutable blockchain technology to avoid the spread of false reports and information. The proposed solution also attempts to address the challenge of privacy and anonymity of the test-takers. However, the authors have not included a design scheme or an implementation method to achieve the results of the proposal. In summary, new technologies have been used in maintaining the vaccination record and much research have been done to use blockchain in medical field. Authors have tried to showcase the use of blockchain to give immunity certificates or health passports but the use of blockchain to keep a standardized vaccination record has not been studied for the practical use in real world.

III. PROPOSED SOLUTION

Here, we discuss our solution developed using Ethereum Smart Contracts. Our solution is helpful in maintaining the records of vaccination and the individual can access the vaccination records whenever needed. The records are secure on a blockchain and hence the records can be universally accepted.

Figure 1 shows how vaccination centers, like hospitals, interact with the blockchain and store data records of individuals. Similarly, individuals can interact with the blockchain and access vaccination records using a specific smart contract.

A. InterPlanetary File System

The contemporary web is a centralized web where data are stored on huge, centralized servers owned by different institutions. These institutions have all the administrative rights on and off the records and control the data flow unanimously. Non-transparency and monopoly in the data management lead to a lot of undesired consequences and events and in any case, if the centralized servers fail or crash, then the web cannot access the data stored in those servers. To summarize, it is believed that the contemporary web is inefficient and expensive in front of the possibilities lying in the future. Keeping these limitations in mind, Protocol labs started a project which they named as IPFS (InterPlanetary File system) which got immediate attention and appreciation from the developers and believers of the decentralized web. Work has been proposed to use IPFS with blockchain as a secure file sharing system [12].

The IPFS is a protocol and peer-to-peer network for storing and sharing data in a distributed system. Unlike the centralized databases that use location-based addressing, the IPFS uses content-based addressing to access the data in the network. The very basic principle of IPFS is that instead of storing the data on a single centralized server, the data are stored on a node in a peer to peer network. The copy of the same data is present on several nodes so that the same data can still be obtained in case of failure of some nodes, unlike the centralized servers. The data are distributed over the network in such a way that the contents are always available on the web irrespective of the failures of several nodes in the network. The IPFS also guarantees the authenticity and correctness of the data provided by a node in the network due to its cryptogenic nature as every file in the network has a unique hash and the hash can be verified anytime.

Storing data like media files directly on chain is not efficient as directly storing large data on the blockchain will cost too much for the whole process to be successful. In our solution files to be stored on IPFS are encrypted and hence only authorized people can read the data. The IPFS secures the file and maintains the correctness of data by avoiding any kind of hacking or unauthorized access approach which can be done in centralized databases.

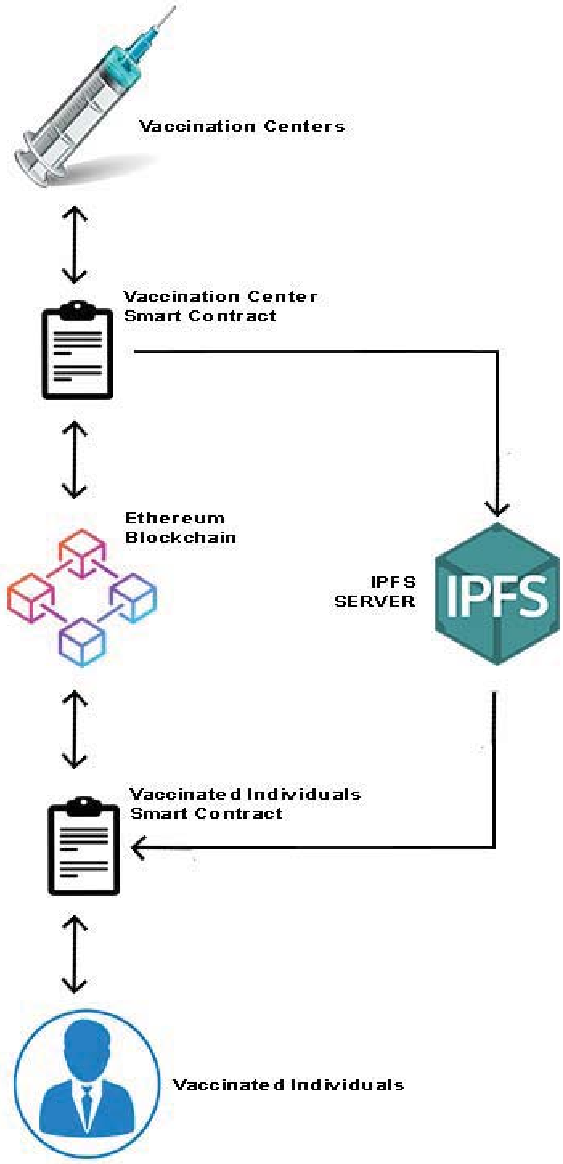


Fig. 1. Communication by the smart contracts

B. *Smart Contracts Involved*

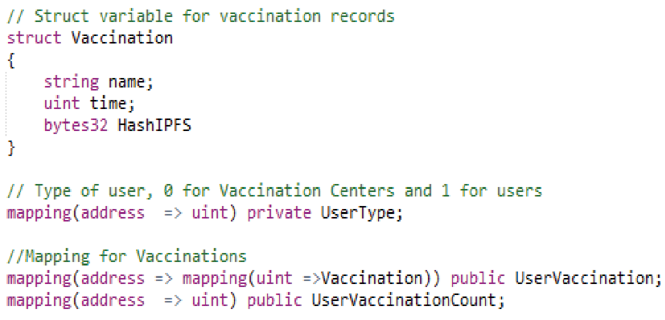
In general, there are two sides interacting with the blockchain. Vaccination centers interact with the blockchain using a smart contract. Vaccination centers can store records of vaccination and at the same time they can store files related to vaccination in InterPlanetery File System. Vaccination centers can encrypt the data such that only individuals with correct access such as government agencies or the individual whose vaccination record has been stored can read the files. On the other side, individuals who are taking vaccination can interact with the blockchain and get access to their previous records whenever needed. Privacy of data is maintained as each individual has a unique Ethereum address. The concerned smart contract has functions to show specific vaccination records like date of vaccination and its types. Individuals can access their records stored in IPFS by showing the proof of vaccination wherever needed.

C. *Hashing Functions Used*

Hash functions are used throughout Ethereum. Transactions are stored as hash and address are the last 20 digits of public key hash. In most places Ethereum uses the Keccak-256 cryptographic hash function. Keccak-256 uses series of functions and rotations to produce the hash from input. All files stored in IPFS have corresponding hash and the protocol used is multihash. Multihash is a protocol for cryptography by using addressing size + encoding considerations. Multihash uses a TLV (Time Length Value) format where each hash is shown in the format <hash-function-type><hash-length><hash-value>. Multi hash is efficient in the sense that it mentions the algorithm used in the hash itself.

IV. IMPLEMENTATION

The project has been implemented as smart contracts which are then deployed on Ethereum Network. There are two smart contracts of which one is for the Vaccination Centers and the other is for users who want to access the vaccination records. Any file related to the vaccination is stored on IPFS and hash of the IPFS id are stored on the smart contract. Deployer of smart contracts are registered as owner and they can decide whether any address interacting with the smart contract can use functions meant for Vaccination Centers only. Hence the deployer of the smart contract can register new addresses as vaccination centers as seen in figure 2. Each vaccination record is in form of a structure variable where details like name of the vaccination and date of vaccination are taken and any file related to vaccination is stored on IPFS and hash ID is stored in the vaccination. Now going in detail about all the smart contracts.



```
// Struct variable for vaccination records
struct Vaccination
{
    string name;
    uint time;
    bytes32 HashIPFS
}

// Type of user, 0 for Vaccination Centers and 1 for users
mapping(address  => uint) private UserType;

//Mapping for Vaccinations
mapping(address => mapping(uint =>Vaccination)) public UserVaccination;
mapping(address  => uint) public UserVaccinationCount;
```

Fig. 2. Vaccination record and mappings used

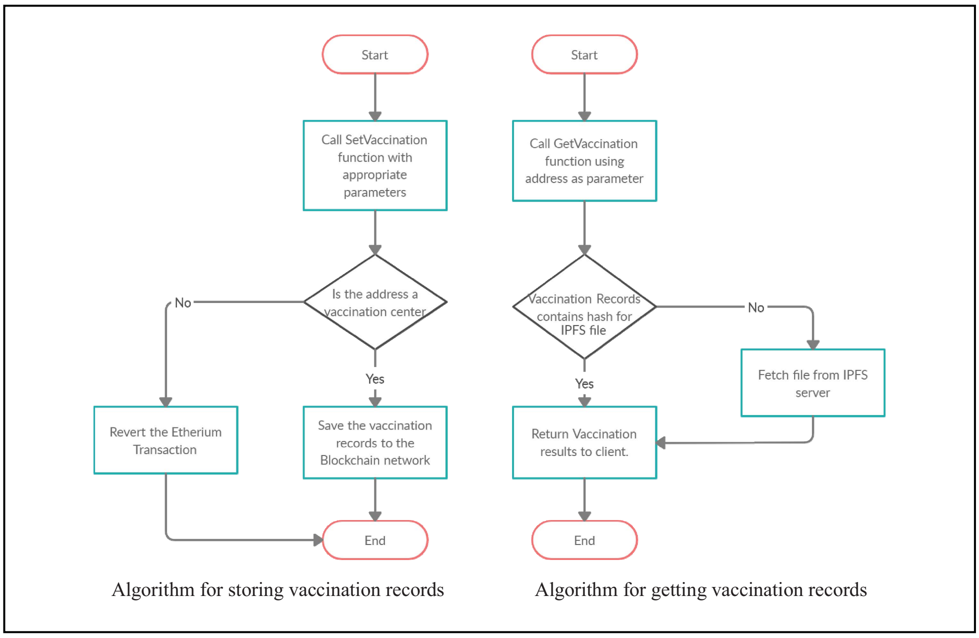
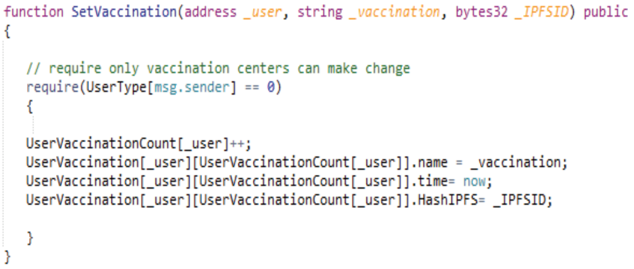

Start
Call SetVaccination function with appropriate parameters
Is the address a vaccination center
No
Yes
Revert the Etherium Transaction
Save the vaccination records to the Blockchain network
End
Algorithm for storing vaccination records
Start
Call GetVaccination function using address as parameter
Vaccination Records contains hash for IPFS file
No
Yes
Fetch file from IPFS server
Return Vaccination results to client.
End
Algorithm for getting vaccination records

Fig. 3. Flow chart for algorithms of proposed solution

A. *Vaccination Center Smart Contract*

Vaccination centers can interact with the smart contract and file a vaccination for a particular address. Vaccination centers can upload any file related to vaccination which support the proof of vaccination which are uploaded to the IPFS server and the hash of id can be stored in the vaccination details. Vaccinations can be uploaded by only those addresses which have been registered as vaccination centers. To set the time of vaccination, ‘now’ keyword has been used which sets the time of vaccination as the timestamp of the Ethereum block which can be also used to validate expiry of a vaccination.

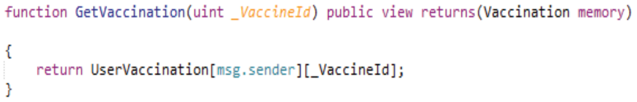


```
function SetVaccination(address _user, string _vaccination, bytes32 _IPFSID) public
{

   // require only vaccination centers can make change
   require(UserType[msg.sender] == 0)
   {

   UserVaccinationCount[_user]++;
   UserVaccination[_user][UserVaccinationCount[_user]].name = _vaccination;
   UserVaccination[_user][UserVaccinationCount[_user]].time= now;
   UserVaccination[_user][UserVaccinationCount[_user]].HashIPFS= _IPFSID;

   }
}
```

Fig. 4. Function to file a vaccination

B. *Vaccinated User Smart Contract*

User smart contract has rather much simpler functionality. Users can check vaccination they have taken and various details about it. User interface can be connected to the smart contract to fetch vaccination records stored on the blockchain and prepare vaccination certificate. Since, the vaccinations are stored for individual user addresses which are unique, vaccination record can be easily and quickly fetched from the blockchain taking address as parameters. Records are stored as mapping from user address to vaccination and these can be returned when a certain function is called.



```
function GetVaccination(uint _VaccineId) public view returns(Vaccination memory)

{
    return UserVaccination[msg.sender][_VaccineId];
}
```

Fig. 5. Function to get vaccination records

From figure 4 and 5 it can be seen that both the smart contracts interact with the blockchain network and there are specified functions for both sides in order to file vaccinations as well as get vaccination records.

V. DISCUSSION

Here, we discuss the feasibility of the model for use in real world with respect to aspects like cost, usability and security. When working with a blockchain network like Ethereum, one of the major concerns associated is the cost of gas fee. Transactions on the Ethereum blockchain cost a certain transaction fee. The transaction cost as well as the execution cost are always part of the logs of transaction. A unit of gas holds the unit Gwei and is paid for in Ether. The miners prioritize transactions that hold a higher amount of Gwei. It is always necessary to estimate the gas costs while developing a smart contract and so as to eliminate extra charges. Loops, arrays, mappings, variable storage, and manipulation as well as data types play a major role in transaction costs. The feasibility of the solution and efficiency are extremely important. In our model we have tried to minimize the storage on chain which may result in minimum possible cost. Costs associated with filing vaccination are on a higher side as it involves storage of crucial parts of vaccination like vaccine name or date of vaccination on chain. But since it is a part of whole vaccination process and the cost are feasible enough for the model to be used by established vaccination centers, the whole process can be justified to be financially feasible. Another cost is by the contract to set type of address to be registered vaccination centers, but this transaction fee is minimum for the authorities. Lastly, users get their vaccination records from a view function which means there is no cost associated with getting the vaccination records, which makes it feasible for common people to use it in real world. One thing to note is gas fees are dependent on time as they depend on amount of traffic on the network [13]. Table 1 shows various costs of the processes during writing of this paper.

TABLE 1. Transaction Costs

Process	Transaction Gas	Execution Gas	Cost in USD
Filing New Vaccination	89631	66119	$1.83546
Setting Type of Address	25276	2468	$0.06937
Getting Vaccination Records	0	0	$0

The integrity of the centralized web has always been questionable and debatable over the years due to the monopoly of big brains and companies in the data market. On many occasions, we don't even require an application that is highly secured and safe but as this paper proposes a solution to keep the vaccination record of mass population, it becomes a necessity to have a mechanism that stores the data securely. According to the solution proposed in this paper, the files are stored in IPFS which is then linked with blockchain to create a decentralized server available worldwide. The IPFS and Blockchain must promise a safe and secure environment to maintain the integrity of the application. IPFS guarantees the
security and authenticity of the data stored in it as it uses content-based addressing and hashes to store the data. Any content stored on IPFS has a unique hash value due to which the content remains secure and free from duplications over the network. An attempt to tamper the content results in changing its hash value, thus making it unauthentic and invalid. IPFS stores the data and to make the data available across the web, it must be linked with blockchain to create a decentralized server across the web. Blockchain networks are highly secure, resilient, and robust due to their cryptogenic nature and fundamentals. Blockchain is a list of blocks or records that are connected cryptographically in a series, also the local copy of the blockchain(records) is available on each participating machine across the network. All these make blockchain based solutions highly secure.

Ethereum is a public network that makes all transactions available to the public. However, based on the application requirements and the scenario context that the application fits in, a solution can be developed in a permissioned blockchain network. Hyperledger Fabric is an example of permissioned networks that offer confidentiality and privacy. Membership Service Provider (MSP), channels, and groups are ways that those permissioned networks use to capture identities and engage only the needed participating entities together. Therefore, only the authorized entities can communicate together privately. To summarize, IPFS and Blockchain provide guaranteed protection and security to the vaccination records stored in a decentralized manner over the network. This concludes that the solution provided in this paper is safe, secure, and has the utmost integrity.

As it can be seen from the discussions and results the proposed model can be used in a feasible manner to be used in real world and there are scopes for changes to be made as per needs of the authorities.

VI. CONCLUSION

Need for an efficient and standardized system to maintain vaccination records which can provide the records quickly on need has been since long and various solutions have been suggested with introduction of new technologies. This paper presents a detailed study of a model to store vaccination records in a blockchain network and discusses various aspects like design, cost and feasibility of the proposed solution. Solution proposed by this paper aims to provide a standardized efficient solution for storing vaccination records on blockchain in a safe and cost-effective manner. The results from analyzing the solution and transaction logs show that proposed solution is feasible and efficient enough to open the way for mass adoption of blockchain based vaccination record management.

REFERENCES

[1] Anderson, R. M., & May, R. M. (1985). Vaccination and herd immunity to infectious diseases. *Nature*, *318*(6044), 323–329. https://doi.org/10.1038/318323a0

[2] Edridge, A., Kaczorowska, J., Hoste, A., Bakker, M., Klein, M., Jebbink, M., Matser, A., Kinsella, C., Rueda, P., Prins, M., Sastre, P., Deijs, M., & Hoek, L. (2020). Coronavirus protective immunity is short-lasting*medRxiv*

[3] F. M. Benčić, & I. Podnar Žarko (2018). Distributed Ledger Technology: Blockchain Compared to Directed Acyclic Graph. In 2018 IEEE 38th International Conference on Distributed Computing Systems (ICDCS) (pp. 1569-1570).

[4] World Health Organization. (1971). Vaccination Certificate Requirements for International Travel. *Weekly Epidemiological Record= Relevé épidémiologique hebdomadaire*, *46*(01-02), 02-02.C. J. Kaufman, Rocky Mountain Research Lab., Boulder, CO, private communication, May 1995.

[5] Maurer, W., Seeber, L., Rundblad, G., Kochhar, S., Trusko, B., Kisler, B., Kush, R., & Rath, B. (2014). Standardization and simplification of vaccination recordsExpert Review of Vaccines, 13, 545-559.

[6] Groom, M. (2015). the Community Preventive Services Task Force Immunization Information Systems to Increase Vaccination Rates Journal of Public Health Management and Practice, 21, 227-248.

[7] Chen, Y., Ding, S., Xu, Z., Zheng, H., & Yang, S. (2019). Blockchain-based medical records secure storage and medical service framework. *Journal of medical systems*, *43*(1), 5.

[8] Chen, Y., Ding, S., Xu, Z., Zheng, H., & Yang, S. (2018). Blockchain-Based Medical Records Secure Storage and Medical Service Framework *Journal of Medical Systems, 43.*

[9] Resiere, D., Resiere, D., & Kallel, H. (2020). Implementation of Medical and Scientific Cooperation in the Caribbean Using Blockchain Technology in Coronavirus (Covid-19) Pandemics *Journal of Medical Systems, 44.*

[10] Khatoon, A. (2020). A Blockchain-Based Smart Contract System for Healthcare Management. *Electronics*, *9*(1), 94. doi:10.3390/electronics9010094

[11] Bansal, A., Garg, C., & Padappayil, R. (2020). Optimizing the Implementation of COVID-19 "Immunity Certificates" Using Blockchain *Journal of Medical Systems, 44*, 140.

[12] Naz, M., Alzahrani, F., Khalid, R., Javaid, N., Qamar, A., Afzal, M., & Shafiq, M. (2019). A Secure Data Sharing Platform using Blockchain and IPFS*Sustainability, 11.*

[13] G. A. Pierro, & H. Rocha (2019). The Influence Factors on Ethereum Transaction Fees. In *2019 IEEE/ACM 2nd International Workshop on Emerging Trends in Software Engineering for Blockchain (WETSEB)*