Blockchain Digital Test Certificates for COVID-19

Ioannis Karamitsos\textsuperscript{a} and Maria Papadaki\textsuperscript{b}

\textsuperscript{a}Rochester Institute of Technology, Dubai, UAE
\textsuperscript{b}British University in Dubai, Dubai, UAE

Abstract. COVID-19 is a pandemic outbreak for each country worldwide. Each government needs to monitor every citizen and the COVID-19 test becomes an essential evidence for people who are travelling. This gives rise to the necessity of disruptive technologies such as Blockchain. In this paper, we provide an overview of the Hyperledger and Ethereum platforms and present how healthcare organizations can control and monitor digital health test certificates with citizens or other stakeholders. We also present a smart contract structure and implementation for COVID-19 test certificates in both blockchain platforms.

Keywords. Blockchain, COVID-19, Ethereum, Hyperledger, Health Certificate, Smart Contract

1. Introduction

Coronavirus Disease (COVID-19) \cite{1} is an outbreak pandemic infectious disease which has appeared in 2019 from a Chinese city, named Wuhan. In few months, the COVID-19 moved from being an epidemic to a pandemic infectious disease. Infectious diseases are diseases that spread rapidly among large numbers of people within a short period of time, and they can be caused by several organisms such as viruses, bacteria or parasites. Naturally, those organisms live in human bodies harmlessly, but due to certain factors or drivers, they become harmful to the body. The transmission of infectious diseases can occur by humans, insects, or animals, and each infectious disease differs in terms of the causing factors, symptoms, the transmission approach and prevention control.

According to the World Health Organisation (WHO) \cite{2}, 14 million confirmed cases, including 607781 deaths globally, have been reported. Due to the high number of infected people, many countries locked down all the activities affecting negatively the economy and the organisations. The main purpose of the lockdown was to limit the mobility of the people in order to keep the dispersion of the disease low. On the other hand, governments are now phasing the next day for the economy and reshaping their countermeasures in our daily activities. One of the first releases was the mobility of the people travelling inside or outside of their country. Each government needs to monitor every citizen and the COVID-19 test becomes an essential evidence for people who are travelling. These rapid changes are having a serious economic effect on governments and healthcare institutions. This drives the necessity of new digital technologies. It is

\textsuperscript{1} Ioannis Karamitsos, Rochester Institute of Technology- Dubai Campus, Silicon Oasis, 341055 Dubai, United Arab Emirates; E-mail: ixkcad1@rit.edu.
anticipated that new technologies such as blockchain will increase effectiveness, transparency, and trust of data sharing and will shake the policies, health protocols and procedures of the government.

The digital transformation and digital technologies produced a paradigm shift in the healthcare industry. The outcome of digitalization produces benefits for the healthcare systems and electronic medical test records improve the access to the health records both for patients and health practitioners. On account of the huge demand for the COVID-19 tests and the prevention of disease dispersion there is a clear demand for a new blockchain decentralized global healthcare approach. A COVID-19 test result is the health digital certificate of each person, and it is available to all responsible parties inside or outside countries. The availability of these health certificates is provided using Blockchain technology decentralized platforms.

Blockchain technology is considered as one of the major breakthroughs since the invention of the market. A forecast done by Gartner revealed that the business value-added of blockchain will reach $176 billion by 2025 and $3.1 trillion by 2030 [3]. The blockchain technology allows the exchange of a value without the need of a central authority [4]. A number of studies have found that blockchain is a new disruptive technology within the digital era [5] and avoiding the middleman. This make the technology quite cost effective [6] and minimize the risks and conflicts developing between the actors during the transaction execution. In addition, blockchain keeps a digital copy of the COVID-19 test certificates owners with an encrypted signature (hash key) into a local database for each node.

These digital certificates that are stored on blockchain storage hold plenty of advantages over the “ordinary” digital certificates in the following ways:

- **IMMUTABILITY:** COVID-19 certificates cannot be forged, and their content cannot be altered by external parties. The correctness of the data can be checked by the test certificate owner.
- **DECENTRALIZED:** COVID-19 certificates were approved by different actors who have read and write access to blockchain nodes. In consequence, there is no need for any intermediary and the centralized approach is eliminated.
- **VALIDATION:** COVID-19 test certificates maintain their validity status without any third party’s intervention.

The hash is a secret key associated to the original document that the citizen/user keeps. This means that you can publish the signature of a document without publishing the document itself, thus protecting the privacy of the document. Another method is used to issue COVID-19 certificates directly to blockchain network for validation and verification. One advantage of the direct issuance of COVID-19 certificates is that it avoids the problem of double verification. The main disadvantage of this method is that the scalability problem, thus effecting the low performance and high usage of the blockchain. Therefore, opting for a blockchain platform is an issue and depends on several parameters.

This study provides an exciting opportunity to advance our knowledge of understanding how blockchain and health digital certificates can interwork to allow this technology to be successfully implemented in healthcare institutions.

The paper offers a background information about the importance and the surprise of the blockchain technology followed by the description of the health COVID-19 test certificates and the implementation in smart contracts. The readers will have the opportunity to see how this solution operates in practice and how the health digital COVID-19 tests are fully utilised using Hyperledger and Ethereum platforms. The
selection of the platforms depends on the health protocols that each government has applied.

The remaining of the paper proceeds as follows: Section 2 presents the literature review using bibliometric techniques. Section 3 begins by developing COVID-19 digital test certificates using the Hyperledger platform. Section 4 presents the Ethereum platform, focusing on the smart contract implementation. Section 5 draws the citizen registration process as part of the whole healthcare pipeline. Finally, the conclusion gives a brief summary of the findings and recommendations for future research in this area.

2. Related Work

The study uses a systematic review in order to search the literature review and identify gaps by using different keywords: digital certificates, blockchain and COVID-19. We used a bibliometrix tool developed by Aria Massimo [7] to search for conference papers and journal articles using the scopus database. A number of 245 papers were identified for further analysis. After collection, the papers were examined on the basis of a degree of homogeneity of their title and abstract and the papers were reduced to 59 papers. The results in this literature review indicate that blockchain technology can help the pandemic minimizing the infections rates and the economy optimistically. There is an unambiguous relationship between blockchain, COVID-19 and healthcare transmission stages. It is interesting to note that the distribution and access of electronic medical records (EMR) are becoming essential after the COVID-19 pandemic. Yang et al. [8] concludes that healthcare management information is far most cost effective, and therefore better value-added to the healthcare processes. Previous research has indicated that smart contracts have a positive impact on the automatic execution of transactions and information exchange (Karamitsos et al., [9]). In addition, there was a significant positive association between smart contracts and COVID-19.

Christ et al., [10] stated that current medical and healthcare providers are insufficient. Health problems seem to be becoming more complex, necessitating a sufficient healthcare system. Instead of availability and traceability of data, IT in health industry is improving electronic medical records, biomedical databases, and public health. Due to privacy concerns, most healthcare institutions keep archives of patient records that are unavailable to other institutions despite the fact that studies have shown that EMR exchange can help resolve healthcare issues. Health care institutions keep these essential data private [10]. Implementing blockchain in health industry benefits in multiple ways to the patients as well as the institution i.e., accessing their health records, granting permissions to institution to get access to the patient’s data, enhanced pharmaceutical supply chain management processes, and patients’ data can be analyzed for medical innovations and research results. However, there is a gap for the verification and ownership of the electronic medical records [11].

Ting et al. [12] investigated the differential impact of digital technologies on public health administrations. By drawing on the concept of blockchain (Ting et al. [12]) have been able to show a collaborating system between different stakeholders such as patients, pharmacists, and hospitals for accurate tracking.

One study of Chamola et al. [13] examined the usage of disruptive technologies such as artificial intelligence (AI) and blockchain in order to minimize the impact of the pandemic. The development of mobile applications has been widely investigated for storing health medical data in immutable records. In their research study, Chamola et al.
[13] identified two mobile applications which include MiPasa and CIVITAS. MiPasa application was designed in Hyperledger fabric platform in order to gain insights into the patient personal information. CIVITAS application used for filling the healthcare records capturing citizen’s ID personal information. The healthcare records were transferred and loaded into the blockchain storage providing ownership to citizens [13].

Mashamba et al. [14] provided an in-depth analysis of the tracking system showing its relevance to infectious diseases using both blockchain and artificial intelligence. The tracking system development is based on Geographic Information System (GIS) installed in smartphones enabling tracking between positive tested.

Vaishya et al. [15] draw our attention to disruptive technologies for combating the COVID-19 pandemic disease. In their review of blockchain processes presented the benefits of traceability and real-time information [15].

In summary, these studies show that blockchain is a disruptive technology providing secure verification regarding the citizen information [12-14]. The citizen information is stored at every blockchain node in a decentralized topology providing tamper-proof and immutability. Further investigation is required to determine the blockchain limitations such as performance, legal regulation and limited technology awareness.

3. Hyperledger Blockchain Platform

Hyperledger [16] is an open source software under the Linux Foundation. The use of Hyperledger platform is a well-established approach in blockchain and consists of infrastructure, frameworks and tools. Hyperledger fabric framework is selected as the primary platform for the COVID-19 digital test certificate. The Hyperledger, unlike the bitcoin and Ethereum did not require any mining process for the validation of their transactions. The benefits of the selection of the Hyperledger fabric platform are presented as follows:

- Hyperledger Fabric issues transactions with derived certificates that are unlinkable to the owning participant.
- Relies on a smart contract system (Chaincode), runs in Docker containers by any peer of the network.
- All participants must register proof of identity to membership services in order to gain access to the system.
- Each transaction content was secured using an encryption mechanism to ensure that the content is available only to the intended participants.
- Hyperledger fabric contains only secure, private, and confidential transaction. Only peer members can modify the content of Hyperledger fabric.
- Transactions are executed without a mining validation.
- The events are structured as transactions and are exchanged between the different participants.

The Hyperledger fabric application has three main components. First, the model file which contains the definition of each class of assets, transactions, participants and events. Table 1 shows an overview of roles and responsibilities for each participant.
Table 1. Hyperledger Fabric Participants/Actors

| Hyperledger Participants | Roles /Responsibilities |
|--------------------------|-------------------------|
| Healthcare Institutions (Blockchain Developer/Architect) | Application Design & Development/Big data Storage for Covid19 tests/ Issuance of COVID-19 test certificate template |
| Healthcare Regulator | Monitoring the health protocols |
| Government Institutions | Issuance of COVID19 test certificate at country level |
| Citizens/Users | Provide personal information and ownership of Covid-19 Test Certificate |

Second the script file: It is also called the transaction processor function file and it houses the JavaScript logic to execute the transaction explained in the model file. The two transactions performed in this paper are the publication of COVID-19 certificates by the healthcare institutions and the issuing of a certificate by the citizen to a beneficiary. Third, the ACL file: This contains the data within a business network which defines an asset or groups of assets as well as the participants that can conduct operations that affect those assets. The asset for this research is the certificate that contains the citizen details and the test results of COVID-19.

3.1. Hyperledger Implementation

The chaincode [16] component plays the role of the smart contract within the Hyperledger platform. The healthcare developers shall design and develop an application and the smart contract (chaincode) as presented in the following Figure 1. Chaincode [16] is distributed inside the blockchain network and control the ledger’s status. The application handles user interface and submits chaincode named transactions to the network.

Therefore, the blockchain network emits transaction block events which enable applications to integrate with other systems.
4. Ethereum Platform

Ethereum [17] is a technology for smart contract development. Smart contracts are complex set of software code with components designed to automate execution on the blockchain and are capable of imposing rules, consequences and computation over any transaction that happens in the blockchain. The study of the smart contract was first carried out by Nick Szabo (1997) [18]. Smart contracts may take any type of data as input, as the COVID-19 test certificate in our study. In addition, smart contracts based on the protocols defined in the smart contract perform input computation and can implement decisions based on the prevailing output production conditions. Functions and state machine are the main components of the transactions. Smart contracts are implemented by Turing complete programming languages which can translate the contract into bytecode and execute it using Ethereum Virtual Machine (EVM) [9] as depicted in Figure 2.

![Figure 2. Ethereum platform Implementation](image)

The Ethereum architecture and implementation are completely independent of the bitcoin cryptocurrency. Solidity (Java-like) [19] and Serpent (Python-like) [20] are currently available programming languages which support the Ethereum platform. Smart contracts and decentralized applications (Dapps) are written with a high-level programming language. The developer will create the format of transactions, the functions of events and state transitions, and the rules of ownership. Ethereum Virtual Machine (EVM) is a virtual machine in which the software code is executed. [9].

4.1. Ethereum Implementation

The design and development of the smart contract was carried out over the Ethereum platform for the implementation of COVID-19 digital certificates. COVID-19 smart contract architecture is comprised of the following steps:

First, the Ethereum node setup with actors and roles is required for every citizen/user and healthcare institutions; second, the business services/functions are
specified and finally, the collaboration among the users and services/functions is implemented. The above steps are discussed in detail in the following sections.

4.1.1. Ethereum Node Setup
The setup of the Ethereum node was based on actors, business services and Ethereum processes.

4.1.1.1. Actors and Roles
Actors and roles were identified using the COVID-19 smart contract developed in Ethereum node as follows:
- Smart contract owner is typically healthcare government or private institutions that are responsible for creating the smart contract and have a digital certificate from COVID-19 test.
- Citizens/users are responsible for building their Ethereum wallets in the public/private blockchain and have access to P2P nodes.

4.1.1.2. Business Services and Functions
The business services and functions which the smart contract needs are as follows:
- Registration of citizens/users
- Design and develop Smart Contract
- Create functions/events
- Send messages/events
- Use cryptocurrency (Ether or BTC) for gas mining fee

4.1.1.3. Ethereum Processes
We have four processes for the Ethereum platform, which are:
- Block validation process
- Network discovery process: for a new node to join the P2P blockchain network
- The design of transactions enabling citizens and healthcare organisations to make transactions and enabling COVID-19 smart contract to generate events and messages.
- The transaction validation process (COVID-19 test certificate) into the block using mining approach.

4.1.2. Smart Contract
For the Ethereum framework, transactions were executed using a group of functions and state variables written in software programming languages. Each transaction contains input parameters which involve a smart contract function. Depending on the logic implementation the state variables changed status during the execution of a function.

Using the programming languages Solidity [19] or Serpent [20], both the functions and the state variables are translated into program code. The contract code is then submitted to the blockchain network until the compiler runs without any errors. The blockchain network will assign a unique address for each contract that is submitted. Any citizen/user or healthcare organization can submit events to contracts other than this. The event consists of the sender's address, the recipient's address, the transfer value, and a data field containing the receiver contract input data. There is a distinction between transaction and event where the smart contract generates the event while the transaction is generated by the External Owned Account (EOA) [9], as shown in Figure 3.
Healthcare organisations and citizens/users/government have been identified as external owned accounts (EOAs) for the smart contract. The external owned accounts were managed using security mechanism (private and public keys) and smart contract transactions were transferred data and value. Smart contract accounts (SCAs) management were performed using their software code. The smart contract messaging system executed in timely manner, provided read and write access to the internal database and communicated with other smart contracts. Miners validate the blocks and transactions. The transaction is enclosed in a block, and for this block, miners will validate the transactions using a consensus mechanism, for example proof of work (PoW). After the transaction is authenticated into the chain, miners are given a sum as a reward.

5. COVID-19 Test Certificates Pipeline

In any blockchain project, teams of developers and healthcare practitioners work to build state-of-art models using automatic driven processes. COVID-19 test certificates pipeline process is a convenient and frequently used tool in the study of COVID-19 use cases. The process is script-driven, and every step is automatic including generation, distribution, and verification stages. The COVID-19 test certificates pipeline process is composed of three stages as depicted in Figure 4.
From the abovementioned Figure 4 we select for further analysis the generation of the citizen registration process. This process is the most important step for the COVID-19 test certificates because we have the involvement of the healthcare institutions and the citizen.

5.1. Use case: Citizen Registration Process

This process can be used for both blockchain platforms. The two main actors are the citizen and the healthcare blockchain administration. Figure 5 demonstrates how blockchain can enhance mobility between healthcare institutions, government and citizens.

The citizen registers in the country healthcare platform introducing his personal data and the healthcare national number. Upon receiving an application submission context from a citizen, the healthcare national system produces a unique citizen ID. The system notifies the citizen by SMS or email. The citizen checks the correctness of the data file. If the data is correct, then the healthcare system generates a blockchain address with public and private keys. Then the citizen creates a blockchain wallet using public/private keys from the system. This information is stored safely in the citizen’s wallet. A blockchain synchronization is performed between the citizen and the healthcare system.
6. Conclusion and Future Work

The present study was designed to determine the effect of the blockchain platforms in healthcare sector. This research was undertaken to design a smart contract and implement a use case of COVID-19 test certificates. Healthcare organisations should assess whether and when blockchain can be used as a solution in their ecosystem.

The present work makes several noteworthy contributions to COVID-19 pandemic using smart contract and blockchain platforms. A variety of advantages are presented as follows:

- **Equitable access:** COVID-19 test results can access by different actors. In the healthcare ecosystem multiple actors such as healthcare organisations, regulator and citizen/user involve the management of the COVID-19 certificate. They have access to read/write or modify any information depending on the access rights provided by the blockchain owner, which is in our case healthcare organisations that are responsible for the ownership of the COVID-19 test results.

- **Low risk fraud:** Distributed ledgers were chosen for the storage of COVID-19 test certificates and copies of transactions are distributed among the nodes in the network. This gives the blockchain an attribute of making it almost impossible to alter the data by external parties. Therefore, the COVID-19 test certificates maintain the immutability property of the blockchain technology.

- **Privacy:** The smart contract for COVID-19 offers a secured privacy to citizens/users. The COVID-19 test results are under citizens’ control and not giving the privilege to a certain institution to use this data which may have value to another external party.

- **Security:** Blockchain platforms and decentralized ledgers use an encrypted database providing more resilience and less exposure to malicious attackers.

- **Efficiency:** COVID-19 certificates were generated a common version for all the transactions across the network, blockchain platforms provide instant visibility.

A smart contract structure for Hyperledger and Ethereum platforms is presented in detail. Further studies, which take these blockchain platforms into account, will need to be undertaken before the application of healthcare protocols applied in different countries. Also, a common healthcare COVID-19 test template is required to design and develop a smart contract.

References

[1] Mayo Clinic, USA. Retrieved on 12 July 2020 from: https://www.mayoclinic.org/diseases-conditions/coronavirus/symptoms-causes/syc-20479963

[2] World Health Organization Coronavirus 2019 (COVID-19) situation report-51. World Health Organization (2020). Retrieved on 22 July 2020 from: https://www.who.int/docs/default-source/wha-70-and-phe/20200721-covid-19-sitrrep-183.pdf?sfvrsn=b3869b3_2

[3] Gartner Research (2017). Forecast: Blockchain Business Value. Worldwide, 2017-2030.

[4] Niranjanamurthy, M., Nithya, B. N., & Jagannatha, S. (2018). Analysis of Blockchain technology-pros,cons and SWOT. Cluster Computing

[5] H. Kakavand, H., N. Kost De Serves, N., & Chilton, B., (2017). The Blockchain Revolution:An Analysis of Regulation and Technology Related to Distributed Ledger Technologies. SSRN Electron. J.
[6] Kosba, A., Miller, A., Shi, E., Wen, Z., & Papamanthou, C. (2016). Hawk: The Blockchain Model of Cryptography and Privacy-Preserving Smart Contracts, in Proceedings-2016, IEEE Symposium on Security and Privacy, SP 2016.

[7] Aria, M. & Cuccurullo, C. (2017). bibliometrix: An R-tool for comprehensive science mapping analysis, Journal of Informetrics, 11(4), pp 959-975, Elsevier, https://doi.org/10.1016/j.joi.2017.08.007

[8] Yang, H., & Yang, B. (2017). A Blockchain-based Approach to the Secure Sharing of Healthcare Data. Norwegian Information Security Conference.

[9] Karamitsos, I., Papadaki, M., & Barghuthi, N. (2018). Design of the Blockchain Smart Contract: A Use Case for Real Estate. Journal of Information Security, vol.9, pp.177-190.

[10] Christ, M.J., Nikolaus Permana Tri, R., Chandra, W., & Gunawan, W. (2019). Exploring Blockchain in Healthcare Industry. In 2019 International Conference on ICT for Smart Society (ICISS), pp. 1-4, https://doi.org/10.1109/ICISS48059.2019.8969791.

[11] Al-Jaroodi, J., & Mohamed, N. (2019). Blockchain in Industries: A Survey. IEEE Access, 7, pp. 36500–36515

[12] Ting, D. S. W., Carin, L., Dzau, V., & Wong, T. Y. (2020). Digital technology and COVID-19. In Nature Medicine. https://doi.org/10.1038/s41591-020-0824-5

[13] Chamola, V., Hassija, V., Gupta, V., & Guizani, M. (2020). A Comprehensive Review of the COVID-19 Pandemic and the Role of IoT, Drones, AI, Blockchain, and 5G in Managing its Impact. IEEE Access. https://doi.org/10.1109/ACCESS.2020.2992341

[14] Mashamba-Thompson, T. P., & Crayton, E. D. (2020). Blockchain and artificial intelligence technology for novel coronavirus disease-19 self-testing. In Diagnostics. https://doi.org/10.3390/diagnostics10040198

[15] Vaishya, R., Haleem, A., Vaish, A., & Javaid, M. (2020). Emerging Technologies to Combat the COVID-19 Pandemic. In Journal of Clinical and Experimental Hepatology. https://doi.org/10.1016/j.jceh.2020.04.019

[16] Linux Foundation, About Hyperledger Fabric. Retrieved on 22 July 2020 from: https://www.hyperledger.org/projects/fabric

[17] V. Buterin, “On public and private blockchain,”. Ethereum blog, crypto, (2015). Retrieved on 22 July 2020 from: https://blog.ethereum.org/2015/08/07/on-public-and-privateblockchains/.

[18] N. Szabo, “Formalizing and securing relationships on public networks,” First Monday 2(9),1997. Retrieved on 22 July 2020 from: https://doi.org/10.5210/fm.v2n9.s269

[19] Solidity documentation. Retrieved on 15 July 2020 from: https://solidity.readthedocs.io

[20] Serpent documentation. Retrieved on 15 July 2020 from: https://ethereumclassic.org/blog/2017-02-10-serpent