# Blockchain-based vaccination certificates management

Charalampos Bampalas
Konstantinos Rantos
cbampalas@ihu.edu.gr
krantos@cs.ihu.gr
International Hellenic University
Thessaloniki, GREECE

## ABSTRACT

With the explosion of COVID-19 cases and the government's needs to control virus spreading, the development of effective and robust systems for managing vaccination certificates to restrict citizens' activities has been in the centre of many governments. This paper proposes a system that allows for the update of the status of certificates and bases its function on a specific form of logs stored on Blockchains and a set of rules for the interpretation of these logs. Also an outline of a proof of concept implementation of the system in Ethereum together with a cost and security analysis are provided in the paper. The proposed architecture provides several benefits with the most prominent one being the suspension of certificates in case an already vaccinated individual is found positive. In existing certificate management systems a vaccinated individual that is tested positive still holds a valid vaccination certificate during the self-isolation period. This vulnerability allows infected individuals to commute freely and thus facilitates the spread of the pandemic. The proposed solution is not limited to COVID-19 related certificates, but rather it could be deployed in any kind of digital certificate.

## CCS CONCEPTS

• **Computing methodologies** → **Distributed computing methodologies**; • **Security and privacy** → **Distributed systems security**; • **Computer systems organization** → *Peer-to-peer architectures.*

## KEYWORDS

Blockchain, Ethereum, vaccination certificates, Covid-19

**ACM Reference Format:**
Charalampos Bampalas and Konstantinos Rantos. 2022. Blockchain-based vaccination certificates management. In *26th Pan-Hellenic Conference on Informatics (PCI 2022), November 25–27, 2022, Athens, Greece.* ACM, New York, NY, USA, 8 pages. https://doi.org/10.1145/3575879.3576010

## 1 INTRODUCTION

Blockchain is a rapidly growing field that combines elements of several scientific disciplines such as cryptography, probability theory, information security and computer science. Owning to its inherent characteristics it has led to some of the most groundbreaking concepts such as the cryptocurrency. During the past decade blockchain has triggered the interest of many organisations, companies, governments and other entities that wanted to invest on it and benefit from this promising technology. Introduced through the well-known bitcoin in 2009 [5], blockchain is gaining ground every day and new potentials are emerging resulting in applications on a plethora of different areas.

Amidst a new pandemic such as COVID-19, the existing knowledge and means do not suffice to combat the new virus and the many unprecedented situations that emerge daily. Data that arises over time is the only trustworthy indicator that shapes our grasp of the pandemic and determines the best strategy to limit its further spread. On this ground, technologies, mechanisms and approaches related to the pandemic should be continuously adjusted to the new data in order to be more efficient and curb the virus as soon as possible.

Taking into account the data that we have up until now, there is no doubt that vaccination does not prevent individuals from getting infected by the virus. However, this does not decrease the importance of the vaccine at all since its main role is to act as a shield for humans against the virus and to protect human lives. Nevertheless, vaccinated individuals may still get infected and spread the virus, and even if the risk for them is minimised due to vaccination, the risk for unvaccinated people is growing further.

If a vaccinated individual tests positive, she/he is obliged by the law to self-isolate so as not to put the others at risk. Although there are severe consequences for those who might break the self-isolation, there are no adequate control mechanisms for detecting such cases. However, the most alarming issue is the fact that those individuals still have a valid vaccination certificate rendering them able to commute without any restriction.

The proposed solution aims to deal with this weakness of the current COVID-19 certificate management system. Namely, the insufficient ability to suspend periodically a vaccination certificate in case the individual tests positive at a later time. This may not only prevent infected-vaccinated people from breaking the self-isolation but also, it may act as an alarming mechanism for authorities in cases of law violation.

The potential of a system that supports the suspension of certificates is not limited just to the above use case. For instance, suspension or revocation of certificates could prove to be particularly useful in case of forged certificates. Incidents of counterfeit certificates are usually investigated and disclosed at a later time, thus, having been valid for a while should not prevent certificates from being suspended or revoked. As time passes, new weaknesses in the current


*PCI 2022, November 25–27, 2022, Athens, Greece*

ACM ISBN 978-1-4503-9854-1/22/11…$15.00
https://doi.org/10.1145/3575879.3576010

mechanisms emerge that highlight the need for more flexible systems taking into account the attribute of fluidity of testing results given the fact that someone may test negative today and positive tomorrow.

The proposed solution is meant to provide a mechanism that allows for the update of the vaccination certificate's status (valid, invalid, revoked, suspended) utilising blockchains. It is designed and implemented in Ethereum, a public permissionless blockchain which, in contrast to private/ consortium blockchains, provides a more secure, decentralised and robust environment. The core concept of the architecture of the solution can be likened to an independent ledger inside Ethereum's ledger. This independent ledger includes logs which are interpreted according to specific rules. Through these logs certificates can be exchanged between the entities of the system while the status of certificates varies based on the current owner at a given time. The challenging inherent property of immutability of blockchains is surpassed through a mechanism that sorts Ethereum logs in chronological order with the latest one acting as the current state. The code of the developed application is available in Github[1].

The rest of the paper is structured as follows: Section 2 deals with related work. Section 3 presents the architecture of the proposed solution. Section 4 summarises the main implementation components and Section 5 discusses cost, security, limitations and considerations regarding the proposed solution and depicts our future work objectives.

## 2 RELATED WORK

Several works have been proposed in the literature for managing vaccination certificates. However, they do not cover all the requirements set in this paper which are satisfied by the proposed architecture.

Justice Odoom et al. [7] proposed a decentralised solution utilising blockchain along with the IPFS (Interplanetaly File System). This is the only solution that takes into account the changing health status of individuals and is designed to permit updates on individuals' records. This solution requires that vaccination centres, medical professionals and individuals who want to get vaccinated or tested have blockchain addresses. Upon vaccination/ testing of individuals their blockchain address is generated. The created health record (test result or vaccination) is encrypted with the individual's public key and before it is pushed to the IPFS it is signed by the healthcare professional who operated the vaccination/ test. Then the IPFS returns a hash that is signed by the person and then via a smart contract it is stored in the blockchain. The individual's record can then be updated in any medical centre if needed.

Sanjib K. Deka et al. [1] have proposed a solution for storage and retrieval of immunity certificates that utilises the Ethereum blockchain in combination with the IPFS. Its function relies on two smart contracts, one for vaccination centres in order for new vaccination records to enter the blockchain and one for individuals in order to get their vaccination status. All documents related to vaccination are stored on the IPFS in a decentralised manner and individuals can access their data at any time without the need for a central storage system. Records are stored in smart-contracts on the blockchain and include information such as the name of the vaccination, the date of the vaccination and the IPFS ID hash. An estimation of the costs of the different functions is also presented according to which the solution is cost-efficient.

Peng Nie et al. [6] developed a traceability system for COVID-19 vaccines with the use of blockchain and smart contracts. The system provides the ability to track information related to the production and transportation of the vaccine to the medical centre and also enables individuals to view their vaccination history and the government to monitor the overall picture of the vaccination process. There are five interfaces which support the system's function: an input interface for the manufacturer, an input interface for the transportation company, an input interface for the hospital, and two query interfaces for citizens and the government. A unique number for each entry to the blockchain is generated and then stored in a database. Upon a query from the user or the government, the database is used to locate information and present it in the front-end. Personal data is stored only in the database and not in the blockchain for privacy reasons, so it is retrieved directly from the database. The production and transportation data is retrieved from the blockchain following the retrieval of the transactions' information from the database.

Madhwal Y. et al. [9] focus on the development of managing entities related with vaccination such as Health Ministry and vaccination centres. They have developed a decentralised application on Ethereum utilising smart contracts. According to the paper, the Health Ministry deploys the contract and registers medical centres. Registered centres can then vaccinate people. Information about registered centres and certificates is stored on the blockchain and can be retrieved for validation. Finally, researchers provide benchmarking results of the developed application as regards the time consumption.

Monafin Afif Fiquaro et al. [2] proposed a system for storing vaccination records using permissioned Blockchain. A complementary cloud storage area is used as a database to store credentials. Hospitals can apply for registration to the blockchain system and then the administrator can approve or reject them. Only the approved ones can register vaccination records in the blockchain. Also, the implementation of the project is based on Hyperledger Besu as a private blockchain and ReactJs for the creation of the front-end interfaces.

Ch. Rupa et al. [8] proposed a blockchain based solution for securing medical evidence. The system has a regulatory authority which registers both users and hospitals and provides to each one a unique ID. These ids together with hashes and signatures are used as inputs to functions such as Issue certificate(), Revoke certificate() and Validate certificate(). An implementation of the system is also developed in Ethereum.

Agam Bansal et al. [3] proposed a system based on blockchain for vaccination certificate sharing. It is based on a permissioned blockchain that consists of nodes designated by each EU country. Citizens, medical centres and certificates are verified and identified with the use of Verifiable Credentials and decentralised Identifiers. The designated node of each country is responsible to register national medical centres so they can operate vaccinations. After vaccination, information is logged on the Blockchain through the state's Blockchain node. The verification is done through application that interacts with the blockchain. Also, a detailed performance

[1](https://github.com/HarrisB92/Blockchain-based-vaccination-certificates-management)

evaluation is included that analyses the systems behaviour as regards the network, time and CPU usage.

A lot of research has been done on COVID-19 certificates and how blockchains could be deployed so as to produce a system that can manage certificates sufficiently, though only the work of Justice Odoom et. Al. [7] approaches the need of a more flexible system that allows certificate status updates. However, their solution substantially differs from the proposed one as regards its architecture while it lacks a mechanism that prevents the arbitrary update of certificates' status without the user's knowledge and authorisation. The proposed solution allows for the suspension of certificates and approaches the certificate's status update through a different logic that leverages Ethereum event logs together with an interpreting mechanism so as to add extra utilities to the logged information. Also, focus has been placed on reducing the control and authorisation that privileged entities of the system have upon the users certificates. As to our knowledge, the is no other proposal that addresses these issues in the same manner.

# 3 BLOCKCHAIN-BASED VACCINATION CERTIFICATES MANAGEMENT

The proposed solution utilises a distributed ledger to manage COVID-19 certificates. The system imitates the way cryptocurrencies are stored and exchanged through a distributed ledger and attempts to create logs of certificate hashes (and some other information) that will be treated in a similar manner as cryptocurrencies. The two basic components of the system are a specific form of logs for the storage of certificates in the blockchain and a mechanism for the interpretation of these logs. Once a certificate enters the blockchain, it can belong either to an individual or a medical centre or to the administrator. It cannot be deleted, it can only change ownership as with cryptocurrencies. This ownership will determine the certificate's status and thus its validity. Each one of the stored certificate hashes can be searched in the blockchain, and as with transactions and cryptocurrencies, the full history of the previous owners of the specific hash will be available to everyone. This is one of the main reasons why a certificate's change of status was chosen to be demonstrated by the change of ownership as opposed to using a simple field in the certificate for this purpose.

## 3.1 Requirements

Two of the main requirements that our system is meant to fulfil and are missing from other solutions is the certificate's suspension as well as the prevention of arbitrary updates on citizens certificates by the administrating entities. Several other requirements have been taken into consideration for the development of the solution and stem from the current best practices and the studied literature. All the requirements of the system are listed below:

- Only approved entities (e.g. medical centres or the administrator) should be able to issue, revoke or suspend certificates.
- All participating entities should be able to see the transactions and logs in the blockchain.
- All participating entities should be able to validate a certificate at no cost.
- No technical knowledge on blockchains or interference with it (e.g. create transactions) is required by the user.
- The user should not be charged for the use the services.
- Transaction costs should burden only the administrating entities of the system.
- Integrity, authenticity, availability and non-repudiation of the information stored in the blockchain should be provided by the system.
- The validation process should rely only on the information stored in the blockchain.
- The system should provide functionality for certificate revocation.
- The system should permit the suspension of certificates at any time.
- Suspension of a certificate should not be allowed without the acquiescence of its owner.
- A suspended certificate should automatically become valid again after the current self-isolation period.

## 3.2 Architecture

The proposed solution is based on a public permissionless blockchain network where medical centres and citizens participate in and interact with each other so as to store data to the ledger. Consequently, both medical centres and individuals need to have addresses on the blockchain network. As a result, each participant has a unique public-private pair of cryptographic keys. Undoubtedly, the fact that individuals need to have addresses on the blockchain network induces some privacy concerns that will be analysed in the following sections. However, since the user is not dealing with transactions and there is no need for them to possess funds, the risk is limited. Note that since the solution is based on the Ethereum blockchain, in the rest of the section the terms "Blockchain" and "Ethereum" are used interchangeably.

One of the basic characteristics of the proposed system is the way the certificate is stored in the blockchain. Like the majority of existing solutions, only the hash of the certificate along with the required digital signatures enter the blockchain. Since in a public permissionless blockchain transactions are visible to anyone, publishing personal information on it is avoided for privacy reasons. However, in contrast to the existing solutions, the hash of the certificate can be transferred between parties of the system using Ethereum events to control certificate ownership and validity as we will see in the following section. All the possible transactions that can be performed in the system, are triggered either by a medical centre's or the system administrator's address which in this case act as the "from" address of the transaction, while the "to" address of the transaction is always the smart contract. Since in Ethereum the address that is charged with the transaction fees is the one that initiates the transaction , citizens can participate in the system without any financial burden.

The components of the system can be categorized in two types: *interacting entities* and *technical infrastructure*.

**Interacting entities:**

- Administrator – It is the entity that deploys the contract and controls the most privileged account (e.g.

the top-level health body at a state or European level).
- Medical centres – Places like hospitals and clinics that are authorised by the administrator to operate vaccinations and issue/ suspend certificates.
- Medical centre's representative – The physical person who performs vaccinations, NAAT (Nucleic Acid Amplification Test) and rapid tests under the authority of an authorised medical centre.
- Citizen (or individual) – Any physical person who wants to get a vaccination certificate, NAAT or rapid test.
- Validator – The physical person who wants to verify a citizen's certificate or test result e.g. an airport employee. This should not be confused with the term "Validator" that is used in Proof of Stake-based blockchains.

**Technical Infrastructure:**

- Blockchain network – This is the core infrastructure of the proposed system. It is the peer-to-peer network upon which the Ethereum blockchain is built.
- Centralised server – A centralised server supports a small part of the back-end and the front-end of the application.
- Off-chain database – It is used as an off-chain storage of certificates and test results. Every record in the off-chain database is encrypted and only the authorised parties can access them. Information stored in the off-chain database is not used in the validation of certificates or in any of the core functions of the system thus, compromising the off-chain database does not affect the functionality of the system. The role of this database is mainly to allow the re-issuance of certificates in case of loss.
- Smart contract – The system utilises a smart contract that provides functionalities to the parties interacting with it such as: certificate issuance, certificate suspension, certificate revocation and some more.

*3.2.1 The functions of the proposed solution.* The proposed solution allows for the issuance, the verification, the suspension and the revocation of certificates. It also allows the administrator to set the suspension period, and to update it in order for the system to adapt to the current scientific directives. Another functionality available for the administrator only is to give permission to a medical centre to issue or suspend certificates. Through the external database where copies of the issued certificates are stored, re-issuance of certificates or test results in case of loss is also allowed. Below is a detailed list of the functions of each entity of the system.

- Administrator
  - Sets suspension period (it equals the current self-isolation period)
  - Gives permission to a Medical centre (to issue/ suspend certificates)
  - Revokes certificates issued before a certain date according to the current expiration timespan of certificates
- Medical centre
  - Generates Ethereum addresses [1]
  - Issues certificates [2]
  - Suspends certificates
- User
  - Signs a message (in particular the timestamp of the latest block on the chain which represents the current time). Users' signatures are used as a requirement for certificate suspension to ensure that no administrative entity can arbitrarily suspend users' certificates.
- Validator
  - Scans the QR-code and verifies the validity of the certificate

Figure 1 provides an overview of the participating entities and the relations between them. In particular, we can see all the participants and the components of the system while the arrows indicate all the possible interactions between them. In the following part of this section these functions and procedures are described step-by-step.

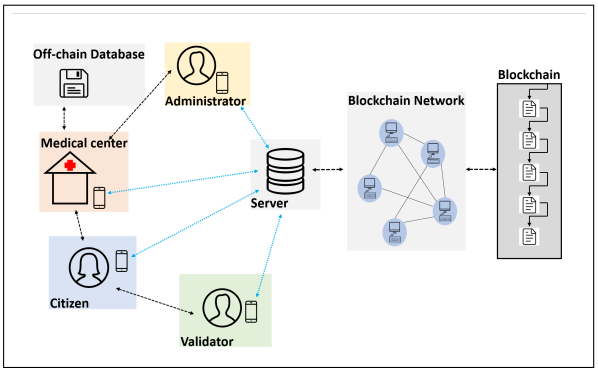


**Figure 1: Participating entities in the proposed architecture**

*Certificate issuance.* This process typically involves the following steps:

(1) The citizen visits a medical centre, shows their ID and gets vaccinated.
(2) The medical centre generates a unique Ethereum address for the citizen and issues the digital certificate with the vaccination details. In case a citizen already possesses an address there is no need for a new one to be generated. The medical centre can verify if someone has not been vaccinated yet, and thus does not possess an Ethereum address through typical citizen identification and authentication and information stored on the off-chain database.
(3) The hash of the certificate is calculated and the authorised medical personnel signs the hash with their personal digital signature. This signature could act as a security and traceability mechanism. For example, in case a fraud is disclosed at a later phase, this mechanism could provide information that leads to the responsible medical centre's employee.

[1] These are general-purpose addresses. They do not have special permissions. This functionality is mostly used to generate addresses for the users upon their vaccination.
[2] Certificate issuance actually means storing the certificate's hash on the blockchain.

(4) The hash of the certificate is sent to the individual's blockchain address through an Ethereum event. The emission of the event is a transaction where the sender is the authorised medical centre and the "to" address is the smart contract.
(5) The QR-code is generated and printed on the certificate. This can be scanned by anyone who wants to validate the certificate.
(6) The certificate is stored in the off-chain database.

*QR-code.* The QR-code is used for the validation of the certificate. It contains information such as the citizens name and surname, the Ethereum address of the citizen, the type of the vaccine, the date of vaccination and a unique certificate ID. The unique certificate ID makes the certificate's hash unpredictable. Without a unique certificate ID, it would be easy for a malicious user to regenerate some valid certificate hashes through trial and error. This could lead to retrieving citizen's personal information and mapping hashes to certificate owners.

*Testing against Covid-19.* The citizen visits a medical centre and before getting tested against Covid-19 they provide a digital signature to the operator generated by their private key. In particular the key that is used for this signature is the private key of the citizen's Ethereum address created upon their vaccination. This signature is valid for a limited time only, and is used by the responsible medical personnel to suspend user's certificate in case of positive results. Signatures can be produced through the application. If a citizen does not already have an Ethereum account, it means that they have not been vaccinated so there is no certificate to be suspended.

*Certificate validation.* Let's assume that Bob wants to validate Alice's certificate.

(1) Bob scans the QR-code of Alice's certificate and retrieves the information stored in the QR-code. Then Bob cross-checks the name from the retrieved data with Alice's ID.
(2) The hash of the retrieved data is automatically calculated and the application scans the blockchain's records against the hash.
(3) Validation is based on the following set of rules:

    a) if the hash is found in the blockchain and belongs to the citizen's address retrieved by the QR-code upon validation, it is considered valid. Note that the ownership is determined after chronological ordering of Ethereum logs.
    b) if the hash is found in the blockchain and belongs to the administrator's or a medical centre's address, the certificate is revoked or suspended respectively. In both cases it is invalid.
    c) if the hash does not exist in the blockchain logs, the certificate is not valid and potentially forged.

*Certificate suspension.* Certificate suspension involves the following steps:

(1) A citizen who has already been vaccinated and holds a vaccination certificate, tests positive for COVID-19 after a rapid or NAAT test. Note that before testing, the citizen has provided a signature which is valid only for a limited time, for example 6 hours (details of this signature are discussed in the following sections), enough for the test results to be issued.
(2) The medical representative after the positive test result should suspend the vaccination certificate of the citizen which, up until now, is valid. In order to perform the suspension he/ she needs the following details:
    - User's Ethereum address
    - The hash of the certificate that is going to be suspended
    - The users signature
(3) The hash can be calculated from the copy of the user's certificate that is stored in the off-chain database.
(4) After these details are filled in a form, the suspension is submitted and several validation mechanisms take place. Note that this process should be performed withing the timespan that the citizen's signature is valid.
(5) After the validation, these details are stored in the blockchain. This action changes the ownership of the certificate which until now belongs to the user's address and after the suspension is transferred to the medical centre's address. This automatically renders the certificate invalid.
(6) After the predefined self-isolation period (e.g. 5 days), another transaction is automatically triggered (by the medical centre's address) that emits an event through which, the hash of the certificate is sent back to the citizen's address, thus the certificate becomes valid again.

*Certificate revocation.* The revocation of certificates occurs when the expected validity period of the vaccination has passed and the individual is no longer considered "protected" against the virus. Due to insufficient scientific data and owning to the liquidity of the course of the pandemic, the validity period of vaccination and immunity certificates is not fixed but rather fluctuates according to the current scientific guidelines.

In the proposed solution the Administrator of the system can set a date and time and revoke all the vaccination certificates issued before this date. This function could also run periodically as a service (e.g. once a day) and revoke all the "expired" certificates automatically without the need for human interaction. However, in the decentralised application developed in the context of this work, this function is triggered manually.

## 4 REFERENCE IMPLEMENTATION

As previously mentioned, the system is built on Ethereum and the generated by the authorised entities logs are stored in the blockchain through Ethereum events. Note that the developed application does not include the external database since it is a well established concept and easy to be integrated in any application. Also, it is important to clarify that the application is designed and developed only as a proof of concept. Web development, web security, network stability and efficiency are out of the scope of this work.

For the simulation of the Ethereum network we used Ganache. Solidity is used for the development of the smart contract and Python tools such as web3.py and Flask are

used for the building of the users' interfaces for the interaction with the blockchain. Several other Python libraries are utilised such as hashlib, qrcode, schedule, time and math.

### 4.1 Example of a log

As described above, the whole system is based on Ethereum event logs. Next, we can see an example of such a log in our implementation.

sender:
0x6EF4880eC1956b3Fbf35158f55c4A34d59fe0385
receiver:
0x3c5D1D5655076DF9B51D3e6969FD106E2A63e1E4
cert_hash:
e1f6ec4ec90154c6c17491d907c797811fe5402849f45f3a9d
e070eb76236199

The above log is interpreted by the system as follows:

**0x...385** sends the certificate **e1...199** to **0x...1E4**

If this is the latest log relevant to the certificate e1...199 then the current owner of the certificate is the address 0x...1E4. If this address belongs to an individual it is valid, if it belongs to a medical centre it is suspended (invalid), and if it belongs to the administrator it is revoked (invalid).

At this point, it is crucially important to clarify that the "sender" and "receiver" addresses in the logs should not be confused with the "from" and "to" addresses of the transaction. The former is simply a terminology used in the proposed system's logs while the latter is the actual transaction that stores the logs in the Blockchain. Transactions that store logs in the Blockchain are always initiated either by a medical centre's address or the administrator's address, and the "to" address of any transaction is always the smart contract's address.

## 5 COST AND SECURITY ANALYSIS

### 5.1 Cost Evaluation

One of the most demanding areas when it comes to Ethereum DApps and blockchain applications in general, is the cost minimisation. However, the developed application is not designed with cost efficiency in mind. There are ways to reduce its cost by amending and optimising the smart contracts code, however, this is out of the scope of this work. This does not imply that the costs are prohibitively high. As we will see in this section, even with no efficiency amendments, the application does not consume too much gas, however, the current increased Ethereum prices make the application quite costly.

For the cost calculation, the standard gas price provided by ethgasstation.info has been used which, by 3/4/2022, was 30 gwei. This means that we have to multiply the gas that each function in the application consumes by 30. Then, we convert the gwei to ether and finally to USD. Below we can see a table which includes all the available functions of the DApp and their respective costs.

At first glance, the above costs seem to be quite high. However, this is not a consequence of the gas usage but rather it is affected by the high prices of Ethereum at the time of writing. For instance, a trivial transaction in Ethereum consumes 21.000 units of gas which, at the time of writing, corresponds to 2,18$, which is a considerable fee for a simple ether transfer transaction.

**Table 1: The cost of the system's functions. Gas consumption and USD prices (3/4/2022)**

| Function | Gas usage | USD |
|---|---|---|
| contract deployment | 1066801 | 110,53 |
| set suspension time | 42558 | 4,41 |
| medical centre's authorisation | 43711 | 4,53 |
| certificate issuance | 30479 | 3,16 |
| certificate suspension | 37443 | 3,88 |
| automatically abrogate suspension | 31895 | 3,3 |
| certificate revocation | 28064 | 2,91 |
| certificate validation | 0 | free |

### 5.2 Security

The architecture of the proposed solution allows for several security mechanisms to be developed as we will discuss in this section. Some of the most crucial security features related to the design of the solution as well as the smart contract that supports most of its functions are described below.

*5.2.1 Medical centre's authorisation.* As we have already discussed, there are several entities in the system, each of whom is authorised to perform specific functions of the application. Medical centre's authorisation is the system administrator's responsibility. That is, there is a transaction that authorises a medical centre and can only be initiated by the administrator's address, which is the address that has deployed the contract. This is implemented with the use of Solidity modifiers which are pieces of code that usually define prerequisites for functions.

*5.2.2 Validation before Certificate issuance.* Certificate issuance is meant to be performed by authorised by the administrator medical centres only. The code that validates the authorisation of medical centres runs in the smart contract. The smart contract utilises solidity mappings to manage the authorised medical centres. In particular, there is a mapping that matches Ethereum addresses with a Boolean variable. For an address to be treated as an authorised medical centre, the corresponding Boolean value of the mapping should be "true". Through a solidity modifier, it is ensured that the address that performed a certificate issuance belongs to an authorised medical centre.

*5.2.3 Validation before Certificate suspension.* Certificate suspension is the function with the most requirements to be satisfied. Except for the already mentioned validation of the medical centre's authorisation the following should also be met.

First of all, the ownership of the certificate that is to be suspended is verified. Since the architecture of the system is based upon the exchange of certificates between participating entities, a certificate should have only one owner at a given time. The action of suspension actually means that a certificate will temporarily be transferred from a user A to a medical centre B, so it is mandatory that the certificate exists and the owner of the certificate prior to suspension is A. Internally, this is validated by scanning though the past Ethereum events on the blockchain and checking:

a) **if the certificate exists**
There is no point in suspending a non-existing certificate.
b) **if the owner of the certificate is A**
The certificate cannot be transferred from A to B if it does not belong to A. This process is analogous to the balance check that is performed by Ethereum before each transaction to ensure that the sender possesses more funds than the amount to be transferred.

The smart contract's code provides also time validation as regards suspension. This is an internal mechanism that ensures that the suspension cannot be reverted unless the "suspension time" has passed. The smart contract validates the time that the reversion of suspension is attempted and if not enough time has passed since suspension, the action cannot be performed.

Another crucially important condition that needs to be satisfied for the successful suspension of a user's certificate is the usage of a valid signature that should have been generated by the user no more than a fixed timespan enough for the test results to be issued but not too long so as to prevent administrating entities to use the same signature more than once.

This utility is based on a special precompiled function available in Solidity called **ecrecover**. This function takes the hash of the message wich was signed together with the signature as inputs and returns the address that this hash was signed by. This functionality is used by the system to determine if the provided signature is actually the user's signature meaning that it has been produced by the user's private key according to the ECDSA elliptic curve digital signature scheme.

To conclude, it is worth noting that all the above security mechanisms and validations are based on the smart contract's code which runs on the blockchain. This enhances the security of the application since on-chain code leverages the security and stability that blockchain technology provides to decentralised applications.

## 5.3 Considerations and Limitations

*5.3.1 Cost.* A considerable limitation as regards the cost of the specific implementation, is the liquidity of Ethereum fees that might drive the cost of the application too high. This fluctuation depends on factors such as the congestion of the network. On the other hand, if Ethereum fees slump, the costs will fall accordingly.

*5.3.2 Considerations regarding privacy.* Unlike solutions that do not require citizens to participate on the blockchain network, the privacy of the proposed solution is heavily relied upon the anonymity-pseudonymity of the blockchain. In other words, everyone will be able to see that a specific address on the network possesses a hash and that hash originated from a transaction signed by a medical centre so, in order to preserve privacy, it should be practically infeasible for someone to know who owns a specific address on the network. This is theoretically achieved through the inherent architecture of blockchains.

Addresses on the Ethereum network derive from their respective public keys. In particular, an address derives from the rightmost 20 bytes of the Keccak-256 hash of the public key[1]. Due to the fact that anyone can see the balance of an address but cannot link this address to the identity of its owner, blockchains like Bitcoin and Ethereum are considered pseudo-anonymous. Theoretically, given an address or a public key, no information can be derived about its owner. However, anonymity in blockchain networks is a particularly controversial topic with a considerable part of the community maintaining that any wallet could possibly be tracked back to its owner's identity.

Possible user mistakes or cyber attacks to the blockchain can reveal information that can link an address to a physical person[2]. Also, gathering information about an address can lead to the further disclosure of information about other addresses through "taint" analysis. There are many techniques that can expose information regarding the identity of the owner of an address on a blockchain network. Most of them usually leverage some extra off-chain information such as IP addresses, geo-location information and inner network information [4]. Further analysis of the privacy in blockchain is out of the scope or this paper.

*5.3.3 Security considerations.* Building a user-friendly environment for decentralised applications poses a great challenge for developers. However, user-interfaces are necessary for a solution that addresses the general public and does not require them to have any technical knowledge on blockchains, which is one of the proposed solution's requirements. Integrating a centralised server that supports user-interfaces in a blockchain applications could reduces the security and solidity that blockchain provides. Since our implementation utilises a centralised server security risks may arise that could affect the stability of the system. However, with the core functionalities running on the smart contract the threat is minimised.

*5.3.4 Future work.* A possible future amendment of the proposed solution would be the expansion of it in order to cover immunity certificates too. Another possible improvement is the design of a function that allows the revocation of a single certificate. As described in the previous section, the revocation function of the developed system is designed to revoke all certificates issued before a certain date. However, in some cases such as frauds, it would be particularly useful to be able to revoke only the fake certificates.

The proposed solution could be expanded and elaborated with a traceability and security mechanism to detect self-isolation violations. Due to its architecture that is designed to provide full history of each certificate upon validation, it could be possible to develop an alarming mechanism that notifies authorities in case a citizen violates the self-isolation. Since during the self-isolation certificates are suspended according to the proposed solution, it will be easy for the system to detect violations through the blockchain logs.

Research for ways to maximise the extent that the function of the application is based on smart contracts will be considered as a future expansion in order to make the system even more decentralised. Since our implementation relies both on code that runs on the blockchain and code that runs on a centralised server an updated implementation that would minimise the server's role could significantly enhance

[1] https://ethereum.org/en/developers/docs/accounts/#account-creation/
[2] https://www.mcafee.com/blogs/other-blogs/mcafee-labs/staying-anonymous-on-the-blockchain-concerns-and-techniques

the security of the system. Finally our follow up efforts will focus on system's cost reduction to ensure its sustainability.

## 6 CONCLUSIONS

This paper proposed a blockchain-based solution to support the management and circulation of vaccination certificates providing security mechanisms and utilities to adapt to the emerging needs of the health sector in the view of the pandemic. The system is based on Ethereum events and a logic mechanism to handle and interpret the event logs related to certificate management. The potentials of this idea are not restricted to those presented in this work. Event logs can be further explored so that more functions could be added. For example, the user's interface could be enhanced with a function that displays all the authorised medical centres, or the non-respect of the self-isolation could be easily detected through the event logs which could trigger an alarm to relevant authorities. Also, the system could incorporate the IPFS instead of the centralised database and user's identification could be enhanced by self sovereign identities.

The implementation of the concepts and ideas of the developed solution is not restricted to vaccination certificates only but it could be expanded to cover any kind of certificate. The decentralised application is developed only as a proof of concept and for a real world implementation many amendments would be needed. Perhaps the core limitation of the system is that its cost depends on the fluctuating Ethereum prices. However, this paper presented an architecture which, among others, satisfies the strong requirement for a robust system that supports certificate suspension despite the mutability challenges of blockchains.

## Acknowledgements

This work has been supported by the MSc in Cybersecurity program, School of Science and Technology, International Hellenic University.

## REFERENCES

[1] Deka, S. K., Goswami, S., and Anand, A. A blockchain based technique for storing vaccination records. In *2020 IEEE Bombay Section Signature Conference (IBSSC)* (2020), pp. 135–139.

[2] Fiquaro, M. A., Zahilah, R., Othman, S. H., Arshad, M. M., and Sheikh Saad, S. M. Vaccination system using blockchain technology: A prototype development. In *2021 3rd International Cyber Resilience Conference (CRC)* (2021), pp. 1–6.

[3] J.L., H.-R., G., K., D., G., T., M., G., K., and I.N., F. Sharing pandemic vaccination certificates through blockchain: Case study and performance evaluation. *Wireless Communications and Mobile Computing 2021* (2021). Cited by: 3; All Open Access, Gold Open Access, Green Open Access.

[4] Linoy, S., Stakhanova, N., and Matyukhina, A. Exploring Ethereum's Blockchain Anonymity Using Smart Contract Code Attribution. In *2019 15th International Conference on Network and Service Management (CNSM)* (Halifax, NS, Canada, Oct. 2019), IEEE, pp. 1–9.

[5] Nakamoto, S. Bitcoin: A peer-to-peer electronic cash system, 2009.

[6] Nie, P., Zhou, X., Wang, C., Zheng, H., and Zeng, Y. Design and implementation of coronavirus vaccines information traceability system based on blockchain. In *2021 International Symposium on Artificial Intelligence and its Application on Media (ISAIAM)* (2021), pp. 121–124.

[7] Odoom, J., Soglo, R. S., Danso, S. A., and Xiaofang, H. A privacy-preserving covid-19 updatable test result and vaccination provenance based on blockchain and smart contract. In *2019 International Conference on Mechatronics, Remote Sensing, Information Systems and Industrial Information Technologies (ICMRSISIIT)* (2019), vol. 1, pp. 1–6.

[8] Rupa, C., and Midhunchakkaravarthy, D. Preserve security to medical evidences using blockchain technology. In *2020 4th International Conference on Intelligent Computing and Control Systems (ICICCS)* (2020), pp. 438–443.

[9] Y., M., Y., Y., and I., C. Covid-19 vaccination certificate supply verification based on blockchain. p. 88 – 93. Cited by: 0.