

Blockchain Smart Contracts for Cervical check patients in Ireland

MSc in Science Cloud Computing
Cloud Computing

Vania Gehrman Schneider

Student ID: 19139438

School of Computing
National College of Ireland

Supervisor: Divyaa Manimaran Elango

National College of Ireland
Project Submission Sheet
School of Computing



| | |
|-----------------------------|---|
| Student Name: | Vania Gehrman Schneider |
| Student ID: | 19139438 |
| Programme: | Cloud Computing |
| Year: | 2021 |
| Module: | MSc in Science Cloud Computing |
| Supervisor: | Divyaa Manimaran Elango |
| Submission Due Date: | 20/12/2021 |
| Project Title: | Blockchain Smart Contracts for Cervical check patients in Ireland |
| Word Count: | 6168 |
| Page Count: | 22 |

I hereby certify that the information contained in this (my submission) is information pertaining to research I conducted for this project. All information other than my own contribution will be fully referenced and listed in the relevant bibliography section at the rear of the project.

ALL internet material must be referenced in the bibliography section. Students are required to use the Referencing Standard specified in the report template. To use other author's written or electronic work is illegal (plagiarism) and may result in disciplinary action.

| | |
|-------------------|-------------------------|
| Signature: | Vania Gehrman Schneider |
| Date: | 15th August 2021 |

PLEASE READ THE FOLLOWING INSTRUCTIONS AND CHECKLIST:

| | |
|--|--------------------------|
| Attach a completed copy of this sheet to each project (including multiple copies). | <input type="checkbox"/> |
| Attach a Moodle submission receipt of the online project submission , to each project (including multiple copies). | <input type="checkbox"/> |
| You must ensure that you retain a HARD COPY of the project , both for your own reference and in case a project is lost or mislaid. It is not sufficient to keep a copy on computer. | <input type="checkbox"/> |

Assignments that are submitted to the Programme Coordinator office must be placed into the assignment box located outside the office.

| | |
|----------------------------------|--|
| Office Use Only | |
| Signature: | |
| Date: | |
| Penalty Applied (if applicable): | |

Contents

| | | |
|----------|--|-----------|
| 1 | Introduction | 1 |
| 1.1 | Research Question | 2 |
| 1.2 | Motivation | 2 |
| 1.3 | Business use case | 2 |
| 2 | Related Work and Literature Review | 2 |
| 2.1 | Related work | 2 |
| 2.2 | Literature Review | 5 |
| 2.3 | Blockchain | 5 |
| 2.4 | Security and Hash | 7 |
| 2.5 | Ethereum network | 8 |
| 2.6 | Smart Contracts | 9 |
| 2.7 | Healthcare records systems | 10 |
| 2.8 | Cervical Checks in Ireland | 11 |
| 3 | Methodology | 12 |
| 4 | Design Specification | 12 |
| 4.1 | Flask and Python | 12 |
| 4.2 | Solidity/Truffle Suite | 14 |
| 4.3 | Ganache | 16 |
| 4.4 | Metamask | 16 |
| 5 | Implementation | 17 |
| 6 | Evaluation | 18 |
| 6.1 | Experiment /Testing blockchain with Spreadsheet | 19 |
| 6.2 | Experiment / Testing with Python Hashlib library in the command line | 19 |
| 6.3 | Discussion | 20 |
| 7 | Conclusion and Future Work | 21 |

Blockchain Smart Contracts for Cervical check patients in Ireland

Vania Gehrman Schneider
19139438

Abstract

The presented research aims to help on improving the patient's data storage for Cervical Check exams in Ireland. Many issues are related to poor data storing and use, causing many deaths and severe illness problems for hundreds of women. The main scope is to help through blockchain technology and Ethereum network using smart Contracts concept to contribute to a better and robust patient's data handling to avoid incorrect data storing and mistakes related to patients status or miss information. The healthcare system should be trusted and safe for everyone, especially dealing with serious diseases that can lead to death. The technology and new research solutions are out there to help to improve and avoid this type of situation in the future. Reports and numbers related to the incident that happened in Ireland will be discussed along.

1 Introduction

Technology advancements such as blockchain, smart contracts, and cloud computing can be a potent combination to contribute to better and more accurate data management and deal with the fast-paced life routine that most people face. Humanity and technology need to walk together, and sometimes this can be forgotten along the way with tight time frames, quick results, fast turnaround, and targets to be met.

To secure data integrity and avoid irreparable mistakes in the future, the proposed applications using blockchain technology to ensure that the data is protected and kept safe through smart contracts using Ethereum Network would benefit this work.

This research intends to help improve data storing and handling through the developed applications to obtain data from the patients, to be kept safe and with a unique ID (hash number) generated by Smart Contract technology.

The cancer scandal related to the Cervical Checks in Ireland initially occurred in 2018, after they obtained inaccurate smear test results for cervical cancer.

According to the HSE, at least 209 women were given incorrect smear tests, and all of them were eventually diagnosed with cervical cancer. Eighteen of those ladies had already passed away, unaware that their diagnoses had been incorrect. Since then, at least 221 women have been found to have been misdiagnosed. The Cervical Check screening program noted in a May 2018 statement that on reflection, the clinical trial

may have delivered a different result or a notification of elevated risk or evidence of developing cancer for those women. The screening program was soon the subject of a risk assessment probe by the government. Its findings, which were backed up by the lobbying and efforts of terminally sick women.(1)

Further along more details will be discussed regarding the Cervical Check in Ireland scandal and numbers related to the case.

1.1 Research Question

Can medical records for Cervical check patients in Ireland be improved by the blockchain technology?

1.2 Motivation

The motivation for this research is to help improve patients' experience and promote a better environment and relationship between patients, doctors, clinics, and institutions. The fact that happened in Ireland back in 2017 brought to light how important it is to be accurate and transparent with data handling and how precious it is to keep the technology aligned with the world's advancements.

With this situation exposed and learning more about blockchain technologies and the significant advancements towards solid data tracking and security throughout different business needs, the combination of blockchain technologies and healthcare systems has great potential to change and improve many gaps that are needed to promote a better system and trust for everyone's wellbeing.

1.3 Business use case

There are many ways and success stories cases that can bring investments and real benefits about implementing Blockchain technologies and Smart Contracts for the public use. For example, in a nation vast like Estonia, that already implemented blockchain technology for the benefit of its citizens is a huge success and a great example to follow. Many other business streams are being encouraged and positively impacted for the improvement and solid consistency that blockchain technology can bring.

Strong words as trust and reliability are challenging in today's pace of life and stand out when it comes to having a better and improved system that can highly impact people's lives. More importantly, in the healthcare systems that people's well-being and health depend on, it is highly critical that this kind of approach be researched, invested, and implemented to benefit businesses and the citizens of a nation.

2 Related Work and Literature Review

2.1 Related work

This designated space will be dedicated to exploring the most exciting and related work that has similar motivation and goals, that is, to improve the healthcare system, patients, doctors, and most importantly, the patient's experience and data handling.

There is no doubt that Blockchain technologies, Smart Contracts, empower the development of solutions to meet the increasing demand in the Healthcare sector regarding data handling, security, and robust systems that allow a better trust between the system and the patient daily.

Further below will be presented some other researches that also implemented ideas and projects with blockchain technologies to help to improve the healthcare systems, data handling, and security.

According to the author Sheng Cao, a secure cloud-assisted eHealth solution leveraging blockchain technology is proposed to protect outsourced Electronic Health Records from unlawful change. The core concept is that only authenticated participants can outsource Electronic Health Records and that each operation on outsourcing Electronic Health Records is recorded as a transaction on the public blockchain. The proposed work is a secure cloud-assisted eHealth system that ensures the secrecy, accuracy, and truthfulness of outsourced Electronic Health Records without introducing any trusted entity, in which Electronic Health Records generated by one doctor throughout a treatment period are integrated into a blockchain-based currency transaction. To build secure channels between patients and doctors, Electronic Health Records uses a user-friendly password-based key agreement, which can withstand password guesswork attacks without demanding significant investments on patients' devices.(2)

The work that was carried out by Sheng Cao et al.(2) seems to be very positive and effective in terms of confidentiality and security. The paper is very interesting to read, and even when a doctor would like to act maliciously, the system would protect against this kind of action.

Leila's proposed blockchain-based framework for health records management (BlockHR) is presented as a medical support system for medical professionals to improve diagnosis, treatment, and patient updates. Patients can utilize BlockHR to submit medical and lifestyle data that can be used to forecast their risk of chronic disease. Electronic Health Records should be exchanged and transmitted often among hospitals, clinics, health systems, medical drug manufacturers, pharmacists, health coverage providers, researchers, and patients to deliver correct health care. However, this presents a significant problem in regards to keeping sensitive patient data secure and up to date. In addition, during the treatment lifecycle, a patient may visit multiple hospitals or be transferred from one to another. A blockchain-based system for health record-keeping (BlockHR) is offered to improve the medical support network for practitioners and better diagnosis and treatment for the patient to pursue. Patients can submit their medical and lifestyle data to forecast their risk of developing chronic diseases using BlockHR's tools.(3)

It is interesting to see the approach and points that were explored by Leila(3), especially that the system proposed is to allow the doctors and patients be able to upload the data, helping to prevent the risk of diseases to develop, acting as a follow up for a better diagnosis.

Mischa brings a solid example exploring The Estonian e-Health program, which is the best

processed out of the other seven different exposed work scenarios. The Estonian e-Health effort, as per the author, leverages a blockchain-based Keyless Signature Infrastructure to protect the integrity of Estonian people's medical data.

The KSI blockchain is implemented in the e-Health initiative to safeguard Estonian people's medical data integrity. Even though this was a government-led initiative in collaboration with the commercial company Guardtime, technical specifics about the blockchain implementation were challenging to come by, and figuring out how blockchain was implemented in Estonia's e-Health use scenario took longer than planned. (4)

The topic is fascinating, and Estonia has been increasingly investing in different technologies and solutions for its citizens. The E-services that are provided online are indeed unique and revolutionary.

Innovative e-solutions have revolutionized Estonia's healthcare system. Not to mention hospitals and the government, patients and doctors benefit from the convenient access and savings that e-services have delivered.

The citizens in Estonia that have visited a doctor have an online e-Health record that can be tracked. Identified by the electronic ID card, the health information is kept completely secure and at the same time accessible to authorized individuals. In addition, KSI Blockchain technology is being used to ensure data integrity and mitigate internal threats to the data.

Patients can see their records, as well as those of their minor children and others who have permitted them. The patient can check doctor visits and current prescriptions and see which doctors have had access to their files by logging into the e-Patient portal with an electronic ID card.¹

Indeed, this is one of the most inspiring cases of enormous success and investments towards the healthcare system revolution and a unique system that cares for patients' well-being, respect, and right to data.

Asma describes a healthcare smart contract system that can handle medical data and simplify complex medical processes. The author addressed cutting-edge blockchain research in the health sector and created an Ethereum based healthcare management platform. This article aims to highlight how blockchain could be used in healthcare and the challenges and future directions of blockchain research. The implementation of smart contracts, which are embedded multipurpose protocols that streamline processes, minimize bureaucratic hassles, and eliminate intermediaries, can assist lower transaction costs. Other blockchain based initiatives aim to improve the collecting, utilizing and exchanging health data from patients, researchers, and data subprocessors. The author suggested solution employs blockchain technology to establish an innovative, flexible, safe, available, and decentralized health system. (5)

The author explores the concept of allowing the patients to exchange their medical records e a safe and transparent way, including the doctors and hospitals involved. And is essential to highlight the concern and importance of data handling for the patient's safety and well-being in the healthcare life cycle.

Analyzing the cases above and many others that were explored during the research and investigation on the subject of healthcare systems, patients, doctors, medicines, hospitals and all the ecosystem that involves the well being and safety for all patients, is indeed

¹<https://e-estonia.com/solutions/healthcare/e-health-record/>

increasing the interest and investigation exponentially to explore robustly and trusted technologies that can handle safety, privacy and security. Opening up for innovative ideas and technologies is undoubtedly the way to go. But, further, more investigation and studies will make more ground to make the safety grow and, most importantly, people's health and trust with the health care systems of each country and nation. It is very positive and rich material to read and find out that many studies and efforts are being taken into consideration and actions resulting in an excellent patient experience and dynamics of the system.

In the below section it will be focused on main concepts of the core subjects of the research and specific understanding about each technology explored throughout the research work:

2.2 Literature Review

2.3 Blockchain

The blockchain is a network that operates with extremely secure chained blocks that continually hold content along with a fingerprint, and this content is a financial transaction.

Blockchain is a data structure, a chain of connected lists of unique blocks. Every block is a list of transactions that points to the preceding one. The major innovation that blockchains have given us is built on top of relatively simple lists data structure, a technique for adding blocks to the chain without a centralized authority. Blockchains were created to run on decentralized networks. For example, people and businesses run nodes on the web, and all nodes are peers in many ways. This is possible as every node on the blockchain stores the complete history of every transaction that has ever taken place.

Transactions are validated by all nodes and transmitted to their peers. Furthermore, specific nodes engage in the block formation process and are rewarded by earning a block reward in the blockchain's native coin. Unlike the database example, a decentralized network allows any node to join or drop as the user wishes. No specific permission or rights are required to read or write to the blockchain as long as the protocol is respected.(6)

How does blockchain works in a nutshell:

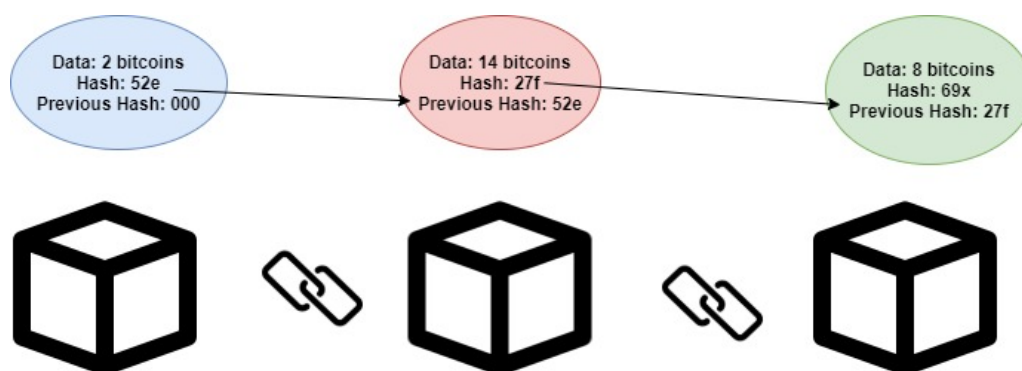


Figure 1: Simplified blockchain mechanism.

The data in the blockchain pursues a model to be verified and validated at any time, creating a chain of information that needs to be linked with each one of them systematically.

In this way, it is impossible to trespass the data chain due to the data that has to be validated in the previous data and the following data.

Blockchain is well known as a distributed database that is updated and shared across a network of computers. The term block alludes to the notion that data and structure are kept in chunks or blocks. The term chain implies how every block has a cryptographic reference to its predecessor. The information contained within a block can't be modified without affecting all following blocks, necessitating network unanimity. Every computer in the network needs to agree with each new block and the chain as a whole before it can be used. Nodes are the machines that make up the network. This ensures that everyone has access to the same information.².

The main key benefits that stand out in terms of the healthcare industry are:

Decentralized information kept between patients, doctors, and clinic/hospitals:

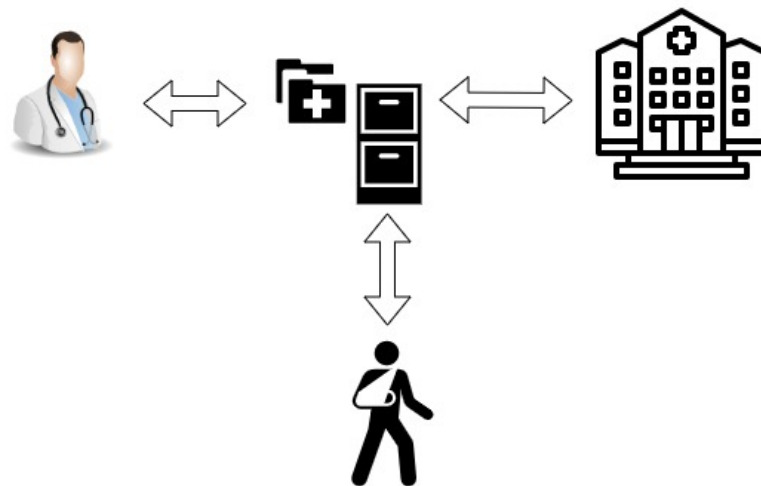


Figure 2: Demonstration of decentralized information.

Medical records are kept in a secure and electronic system:



²<https://ethereum.org/en/developers/docs/intro-to-ethereum/what-is-a-blockchain>

Figure 3: Demonstration of the safe records.

Doctors and other streams of the health care ecosystem are linked in one platform:

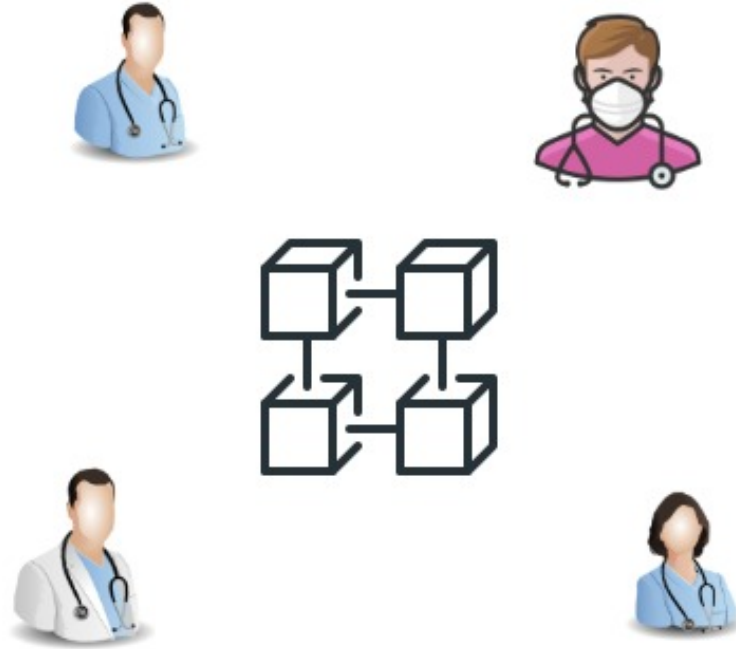


Figure 4: Decentralized information available to all staff registered in the system.

Secure data storage and handling:



Figure 5: Safer healthcare ecosystem.

2.4 Security and Hash

The hash is a mathematical function that gets a message or file and generates a code with letters and numbers that embodies the data the user has registered for any purpose.

In Essence, the hash holds a large amount of data and turns it into a small quantity of information. It is the file's fingerprint, and in regards to a blockchain, a block. The fingerprint is the essential key in the system of linked blocks.

If any information changes in the block, the hash will flag the difference and will be able to see this new information in the block's contents.

When the user generates a new block that similarly contains the hash of the previous one, a new kind of stamp is created. The user can verify and indicate if any of the blocks have been changed and decide whether it is valid or invalid.

Each blockchain network also has nodes, which gathers users who perhaps have the same interest for this kind of process; for example, in bitcoin interest, it is the fact that the users/owners can be transferring money for any needs. These nodes can be transactional, which write or generate blocks, or miners, who check if the written blocks are valid in that circumstance.

Even if someone thinks that it can be possible to forge a transaction, it would be almost impossible nowadays because if anything changes, the hash will also change, then that will make the transaction illegitimate, making all the efforts to make this forgery happen a failure.

In this way, it makes it much more difficult, or almost impossible, for a hacker to tamper with a transaction because each block has the hash of the previous block, and if anything is different or not according to the expected will have a domino effect on the whole chain, exposing the attempt to forgery or theft.

Blockchain technology includes several security features to increase its applicability and adoption in a broader range of applications. For example, if one chooses to build and use blockchain-based apps, patient records, including domestic or international identity numbers, personal connections, and account information, will be accessible through third-party platforms.(7)

2.5 Ethereum network

Ethereum serves as the foundation for a worldwide decentralized computing model. This platform enables users to run decentralized applications and smart contracts with no single point of failure or control and connect to a payment network and operate on an open blockchain.(8)

Ethereum is a public, open-source blockchain that works in a similar way to the Bitcoin network. The primary distinction between Bitcoin and itself is that it delivers a programming platform on top of the blockchain called Smart Contract and a cryptocurrency called Ether, which is identical to Bitcoin.(9)

Ethereum allows developers to create any program they need for any business and run it on the basic features of Blockchain technology, using smart contracts to perform any required actions. Smart contracts are generated automatically based on predetermined

conditions built into the algorithm.

It is feasible to build private Ethereum networks, identical to how a private internet is an intranet. These private networks use ether the same way that the public Ethereum network does, but their ether has no value on the open market. The public Ethereum network's ether is referred to as ETH, and it has actual value. Developers refer to the public Ethereum network as the main-net. The industry also employs public test networks or test nets as staging environments. These test networks usually contain "faucets," or systems that provide free ether to developers so they may test their smart contracts.(10)

The development and possession of a secret cryptographic key, part of a public or private key, is used to establish an identity on a blockchain. On a blockchain, keys are used to sign transactions digitally. Although the key's owner is unknown, the identity of the person who holds it is reliable. (6)

In computer science, Ethereum is a consistent yet essentially limitless state machine consisting of a globally accessible single state and a virtual machine that implements its changes.

Ethereum is a worldwide, open-source, decentralized computing platform that makes executing innovative contract applications far more practical. It uses a blockchain to track and control execution resource costs and a cryptocurrency called ether to integrate and maintain state changes in the system. The Ethereum platform allows developers to create powerful decentralized applications with built-in economic features. It reduces or removes censorship while also reducing or eliminating some counterparty risks.(8)

2.6 Smart Contracts

The Smart Contract is a program that executes on the Ethereum blockchain. It is a set of code and its functions and data and its related states that is found at a speci-

fic address on the Ethereum blockchain. Smart contracts are used to display the Ethereum accounts. This means they have reached a state of equilibrium and can send events across the network. As a result, they are not controlled by a user. They can also be deployed to the network and function according to a set of rules. The user accounts can then communicate with a smart contract by sending transactions instructing the smart contract to complete a task. Smart contracts, like regular contracts, can create rules and enforce them automatically by the blockchain.³

The concept of smart contracts can be defined as a set of contractual clauses transcribed in the form of a code written in a computer language, the execution of which is programmed to be automatic when the conditions are met.

A smart contract is a computerized algorithm that carries out the contract's terms. On the other hand, this approach does not distinguish smart contracts from other well-known contractual forms that incorporate automated functionality, like vending machines. Vending machines are self-contained automatic machines that provide products or give services in exchange for cash or, in some instances, credit card payment. Vending machines are programmed with specific rules that they follow. If the only difference between vending machines and smart contracts is their age, smart contracts are as old as Roman law.(11)

³<https://ethereum.org/en/developers/docs/smart-contracts/>

How smart contract works:

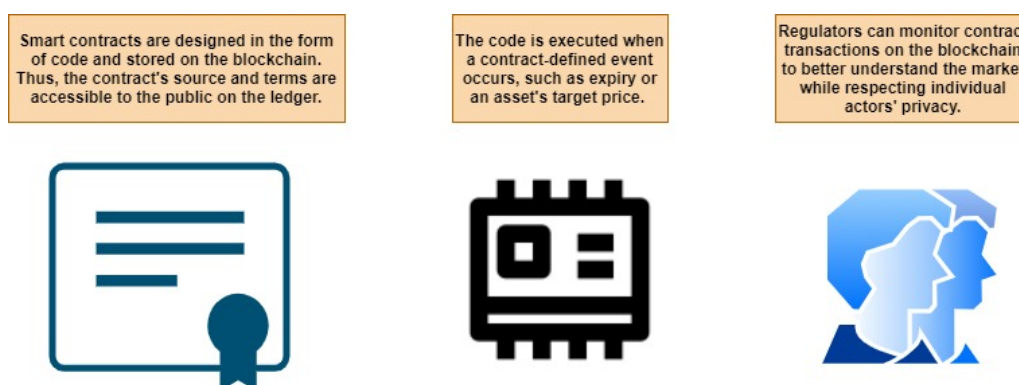


Figure 6: Smart contract overview.

Nick Szabo proposed the concept of intelligent contracts based on cryptographic protocols in the 1990s. Smart contracts integrate protocols, user interfaces, and promises conveyed via those interfaces to codify and secure interactions over public networks, Szabo concluded in a 1997 article. This opens new possibilities for formalizing digital relationships that are significantly more practical than their lifeless paper-based forerunners. Smart contracts lower transaction costs enforced by owners, third parties, or their instruments in terms of both cognitive and computer processing.(12)

Smart Contracts are one of the most widely used blockchain applications. One of the great promises of the digital market is that it has enormous development potential, with implementation and use growing even faster in recent years.

Smart contracts are generated by using the Solidity programming language. Therefore, the development can depend on different IDE platforms if they are operating on Ethereum and Hyperledger blockchains.

2.7 Healthcare records systems

Blockchain offers a robust way to control patient data management. It provides a structured approach to store data that can be accessed by authorized professionals who are part of the system's network that is adopted. Patient data can be stored on the blockchain, and the accessibility to the data will be given to the patient, the doctor managing the case. Access to the data can be withdrawn at any time, certifying that the patient has full permission over their medical reports.

Many procedures are involved in the healthcare system, including handling funds, staff, patients, legal challenges, logistics, inventory, and many others. Medical processes frequently comprise a series of conditional phases that can be described as repetitive chores connected to the actual patient treatment. Among hospitals and other healthcare service providers, these are aimed to provide more robust internal controls, enhanced efficiency, compliance, and productivity, as well as minimize risk, work cycles, and expense. Managing funds, personnel, patients, legal challenges, logistics, inventory, and

other operations are components of health care management. In addition, medical workflows frequently include a series of conditional phases that can be laid out as repetitive chores connected to patient treatment. Within hospitals and other healthcare service providers, these are aimed to provide more robust internal controls, increased efficiency, accountability, and efficiency, as well as minimize risk, work cycles, and expense.(5)

Each hospital and clinic keeps its database in the current healthcare data record management systems, which uses a client-server mechanism to communicate, store patient data, and saves it in various formats and database systems. Standardization across different healthcare providers and hospitals create roadblocks to effective data sharing, administration, and, as a result, precise healthcare delivery. Furthermore, patient data housed in a centralized database is more likely to be insecure, as it would be lost in the event of a single point of failure.(3)

2.8 Cervical Checks in Ireland

Cervical Check is a nationwide cervical cancer screening program that is implemented in Ireland. The program offers free cervical screening tests to women and men between the ages of 25 and 65 who have a cervix. An HPV cervical screening test is a quick and painless process that takes only a few minutes to complete. It is the most reliable method for detecting HPV Human Papilloma Virus and alterations in cervix cells. ⁴.

The main news about the scandal of the Cervical Checks in Ireland started with the patient Vicky Phelan, who has two children from Annacotty, County Limerick, who had a cervical cancer smear test in 2011. Even though her test results were average, she was diagnosed with cervical cancer in 2014. According to an internal CervicalCheck study, the original finding was wrong, but Phelan was not notified until 2017. Consequently, she filed a lawsuit towards Clinical Pathology Laboratories Inc in Austin, Texas, for performing the false test. Without admitting liability, the case was resolved for 2.5 million. In the 2014 analysis, 14 more women were discovered to have false-negative test results. On April 26, 2018, the HSE reported that 206 women had developed cervical cancer due to a misread CervicalCheck smear test. Of those, 162 had not been informed that the preliminary findings were wrong. CervicalCheck's clinical director, Dr. Grainne Flannelly, resigned down on April 28. It was reported a week ago that Dr. Flannelly told a gynecologist in 2017 not to say to women about the re-evaluated test findings but to file them instead.

The most recent case of a terminally sick mother receiving compensation due to the CervicalCheck dispute occurred in January 2021, when a 46-year-old woman agreed.⁵

It is critical and delicate when it comes to lives and their health records, data handling has to be looked at with closed eyes, and more investments in technologies and resources have to be available for the whole system to progress and make things better and with solid results and in the end to offer everyone the right to be able to trust in the system that each one has their accurate and trusted record in hands.

⁴https://www.citizensinformation.ie/en/health/health_services/cancer_services/cervical_screening_programme.html

⁵https://en.wikipedia.org/wiki/CervicalCheck_cancer_scandal

3 Methodology

The methodology waterfall was the one chosen to plan and develop the software lifecycle. The waterfall is a sequential software development model in which the process is understood as a cascade; this way, it was easier to identify the gaps, the steps to be taken during the developing process, and how to adjust with the time constraints. With this method, it was easier to visualize and to have a clear plan of the project’s ideas and main pillars, which are explained in more detail in the image below:

Below is the process:

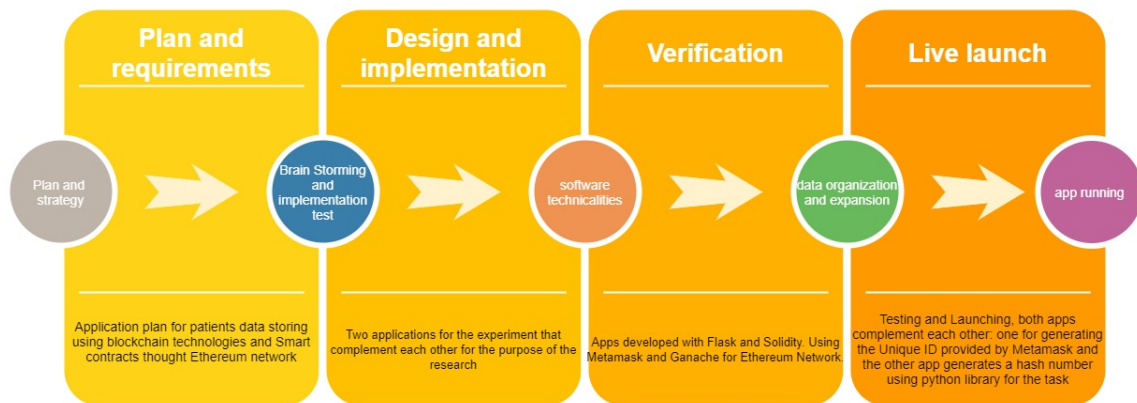


Figure 7: Methodology plan and development.

The steps that were taken to carry the research was:

- research about technologies that are used to develop blockchain technologies;
- research papers with similar content study and investigation to gather as much information as possible to enrich the application and the concept of the research;
- books and tutorials for guidance to implement different technologies.

4 Design Specification

Regarding design and technologies, the proposed work had its main streams of research to use blockchain technology, smart contracts, and Ethereum network as robustly and straightforwardly as possible, so the users would feel comfortable enough to have the applications up running without complicated and expensive resources.

Below will be expanded more about each technology involved and the main concepts about them:

4.1 Flask and Python

The chosen technologies to build the application and to generate the unique hash number were Flask and Python. Flask is a web framework written in Python and is a great tool to start building an app and learn from it.

Flask was built from the bottom to be an extendable framework; it provides a solid core with essential services, and extensions provide the rest. It is a lean stack with no weight and does exactly what the user intends to do with the application. For example, one application was used to collect data from each patient using Flask and Python and the hash library to use the provided requirements.(13)

The library used to provide the unique hash value was the import hashlib. The hashlib hashing function in Python turns a variable-length sequence of bytes into a fixed-length sequence. This is a function that only works in one direction. When the user hashes a message, the user obtains a sequence of a set length. However, those set length sequences will not yield the original message. If the original message cannot be deciphered from the hash message, a hash algorithm is better in cryptography. Changing one byte in the original message also affects the message digest value significantly. In order to save passwords in encrypted form, Python safe hash values are utilized. Passwords are verified when the user enters the password again, and the hash value is calculated and compared with the stored value, so even the program owner does not have access to the user password. ⁶.

The hashlib module provides a standard interface to a variety of secure hash and message digest algorithms. The secure hash algorithms SHA1, SHA224, SHA256, SHA384, and SHA512, are included and RSA's MD5. Secure hash and the message digest are two interchangeable words. Message digests were the name of an older type of algorithm. Secure hash is a more contemporary word.

For each type of hash, there is a separate constructor method. All of them provide a hash object with the same straightforward interface. To build an SHA-256 hash object, for example, use sha256(). The update() method can now feed this object bytes like objects that are usually bytes.⁷

Flask/Python web app:

Patients

Patient's name
Full name

Date of birth
DOB dd/mm/yyyy

Address
Address:

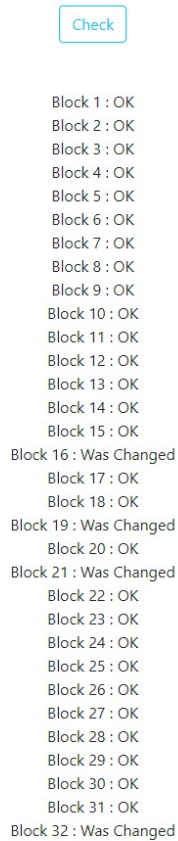
Cervical check Number
Cervical check number:

Figure 8: Main page of the flask platform system.

⁶<https://www.journaldev.com/16035/python-hashlib>

⁷<https://docs.python.org/3/library/hashlib.html>

Checking data integrity: OK= for data that still the same as before
Was Changed= for data that changes was applied



```
Check

Block 1 : OK
Block 2 : OK
Block 3 : OK
Block 4 : OK
Block 5 : OK
Block 6 : OK
Block 7 : OK
Block 8 : OK
Block 9 : OK
Block 10 : OK
Block 11 : OK
Block 12 : OK
Block 13 : OK
Block 14 : OK
Block 15 : OK
Block 16 : Was Changed
Block 17 : OK
Block 18 : OK
Block 19 : Was Changed
Block 20 : OK
Block 21 : Was Changed
Block 22 : OK
Block 23 : OK
Block 24 : OK
Block 25 : OK
Block 26 : OK
Block 27 : OK
Block 28 : OK
Block 29 : OK
Block 30 : OK
Block 31 : OK
Block 32 : Was Changed
```

Figure 9: Result output after clicking the button "check".

Data JSON format inside the app(code):



```
blockchain > 28
1 {
2   "patient": "Mark Wiens",
3   "dateofbirth": "1980-08-25",
4   "address": "89, Thai road",
5   "cervical": null,
6   "prev_block": {
7     "hash": "fc9e8fb8baf5b060bcad2e3bfbcb22fd2",
8     "filename": "27"
9   }
10 }
11 |
```

Figure 10: Piece of code from the application with the JSON information data.

4.2 Solidity/Truffle Suite

An intense research was done to find the best and simpler way to build a blockchain app, and truffle suit is one of the most popular framework for Ethereum, with rich documentation and guidance through the documentation.

How truffle suit works along with Ganache and Smartcontracts:

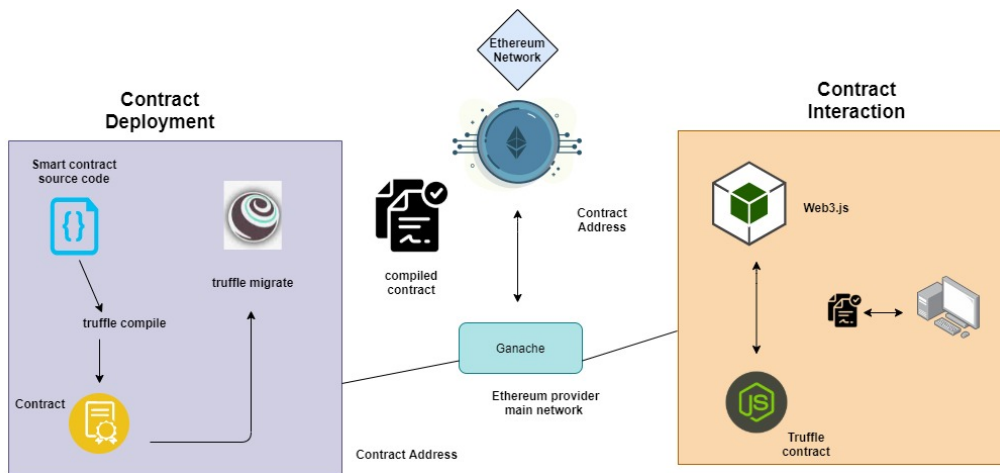


Figure 11: Details of the development cycle with Truffle, Ganache and JS.

The first base part of the project was built with the truffle suite, for the healthcare system for the Cervical check patients.

Main page for the Solidity application:

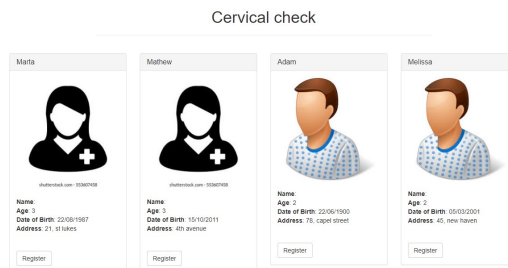


Figure 12: Main web page from the Solidity application.

JSON data app(code):

```
{
  "id": 0,
  "name": "Marta",
  "picture": "images/patient3.jpeg",
  "age": 3,
  "address": "21, st lukes",
  "dateofbirth": "22/08/1987"
},
```

Figure 13: Main webpage from the Solidity application.

Solidity is a programming language high-level object-oriented that may be used to create smart contracts. In the Ethereum state, smart contracts are programs that control how accounts behave. Solidity’s language is written in curly brackets. It was made with the Ethereum Virtual Machine and was inspired by C++, Python, and JavaScript.

Solidity is statically typed, and it supports inheritance, libraries, and advanced user-defined types, among other things. In addition, solidity allows users to create contracts for voting, crowdfunding, blind auctions, and multi-signature wallets. ⁸

4.3 Ganache

Ganache is a personal blockchain that enables the building of Ethereum and Corda distributed applications quickly. Ganache may be used throughout the development cycle, allowing the user to develop, deploy, and test the dApps in a secure and predictable environment. Ganache is available in two types: user interface and command-line interface. Ganache UI is a desktop program that is compatible with both Ethereum and Corda. ⁹

Ganache UI:

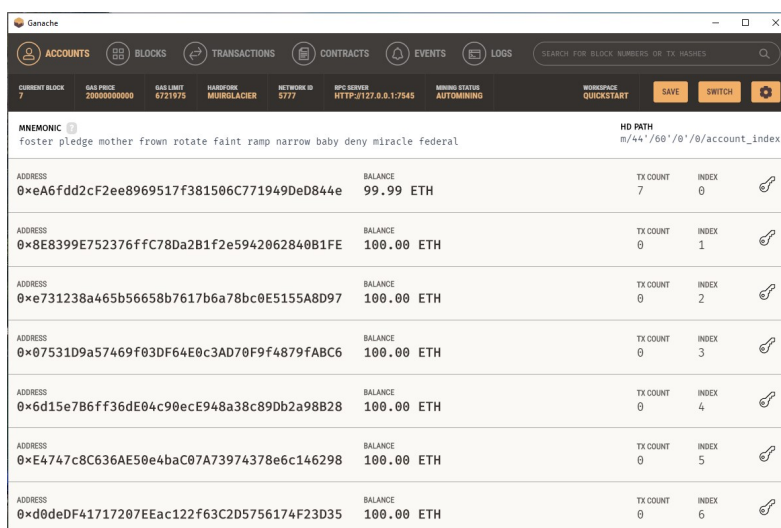


Figure 14: Ganache application development.

4.4 Metamask

MetaMask is a tool that allows users to handle their accounts and keys in several methods, including hardware wallets while keeping them separate from the site’s context. This is a significant security enhancement over storing user keys on a single central server or even locally. In addition, MetaMask will alert the user clearly and understandably. This maintains consumers awareness, and attackers are forced to phishing individual users instead of mass hacking. ¹⁰

⁸<https://docs.soliditylang.org/en/v0.8.6/>

⁹<https://www.trufflesuite.com/docs/ganache/overview>

¹⁰<https://docs.metamask.io/guide/why-metamask>

MetaMask implementation in the application:

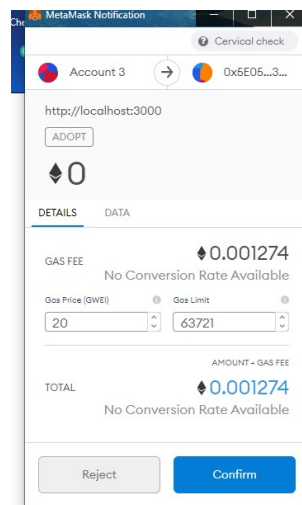


Figure 15: MetaMask prompt when a transaction happens, in the case of the application is for the patients registration.

MetaMask transaction details in the application:

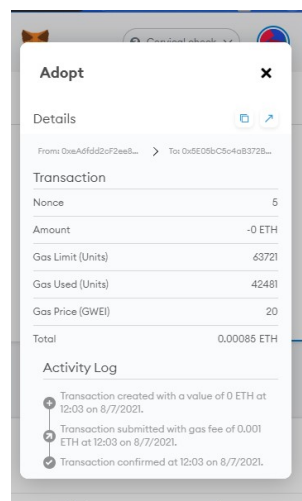


Figure 16: MetaMask prompt when a transaction happens, the full details of the background information.

5 Implementation

The proposed solution for the purposes of safer data storing and handling was done through two applications that complement each other.

Full proposal ecosystem:

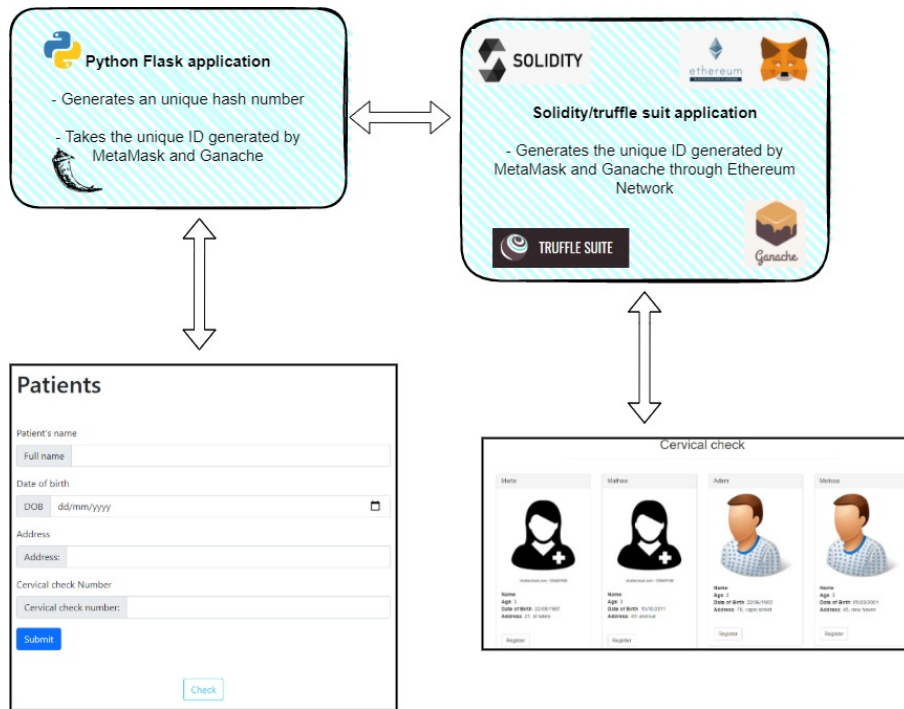


Figure 17: Full application design and technologies explained.

The final result in the JSON code verification is possible to locate the two unique IDs: JSON(code) in Flask application with both cervical and hash unique ID's:

```

blockchain > 34
1  {
2  "patient": "Desise Park",
3  "dateofbirth": "1990-08-25",
4  "address": "S, London road",
5  "cervical": "0x887570e81289ad3d81d1fa057f0fc1d870cab214dd141c380045df62a40e4d1",
6  "prev_block": {
7  "hash": "b3bd9b3a969af8e29916e045ca0ca5fc",
8  "filename": "33"
9  }
10 }
11

```

Figure 18: **cervical variable**: is the unique id generated by MetaMask and Ganache on the truffle/solidity application **hash variable**: is generated by the hashlib python library implemented in the Flask application.

6 Evaluation

To evaluate the process and obtain solid results, prior to the start of planning the application, tests and experiments, different variety of scenarios of testing were implemented prior to build the applications.

Down below will be explained in details the evaluation tests regarding hashing and blockchain concepts that was important for the foundation of knowledge and to aid in the methodology and design of the applications project.

6.1 Experiment / Testing blockchain with Spreadsheet

Hashing is a powerful way to identify the data, by giving a unique id of numbers and letters that are gathered together. It is interesting to see this formula in action and how it interacts within the blocks. Analysing the highlighted black boxes in the image below is possible to see how they are connected with each other. The MD5 algorithm generates a 128 bit hashing number.

| Block #5 | | | Block #6 | | | Block #7 | | |
|---------------|----------------------------------|---------|---------------|----------------------------------|---------|---------------|----------------------------------|---------|
| Transactions | | | Transactions | | | Transactions | | |
| From | To | Amount | From | To | Amount | From | To | Amount |
| | Miner | £ 12.50 | | Miner | £ 12.50 | | Miner | £ 12.50 |
| Vania | Gaga | £ 15.12 | Schneider | Glesias | £ 31.40 | Lady | Tom | £ 21.26 |
| Henrik | Vania | £ 75.35 | Gaga | Cruise | £ 19.00 | Vania | Henrik | £ 17.82 |
| Schneider | Cruise | £ 31.51 | | | | Gaga | Schneider | £ 02.13 |
| Lady | Tom | £ 99.00 | | | | | | |
| Metadata | | | Metadata | | | Metadata | | |
| Previous Hash | 2e6e504e147d1f5e4c7c9d7109073a24 | | Previous Hash | 4e97332ec76c0c56ec449d5732da7064 | | Previous Hash | b678e88b414d63c74e39a908e0dd13aa | |
| Timestamp | 2019-05-05 17:46 | | Timestamp | 2019-05-05 17:46 | | Timestamp | 2019-05-05 17:46 | |
| Junk | ABC123456 | | Junk | 012ABC1234123456789Ea212 | | Junk | ABC1234abda | |
| Hash | 4697332ec76c0c56ec449d5732da7064 | | Hash | b678e88b414d63c74e39a908e0dd13aa | | Hash | a521e50e277304a420f83bae399b494 | |

Figure 19: Firts testings with blockchain technologies using Spreadsheet and MD5 hashing algorithm.¹¹

6.2 Experiment / Testing with Python Hashlib library in the command line

Commands used to perform this test:

- python
- import hashlib
- contract = open('contract', 'rb').read()
- contract
- h = hashlib.md5(contract).hexdigest()
- h

```
PS C:\Users\vania\OneDrive\Documents\test_block> python
Python 3.8.2 (tags/v3.8.2:7b3ab59, Feb 25 2020, 23:03:10) [MSC v.1916 64 bit (AMD64)] on win32
Type "help", "copyright", "credits" or "license" for more information.
>>> import hashlib
```

Figure 20:Importing the hashlib library into the Python-Flask App test.

```
>>> contract = open('contract', 'rb').read()
>>> contract
b'DRAFT AGREEMENT FOR SALE\reference to the Standard Commercial Property Conditions (2nd Edition)\PARTICULARS\n1. (i) Vendor THE MAYOR AND BURGESSES OF THE LONDON\BOROUGH OF HARINGEY of the Civic Centre, Wood\Green, N22 8LE acting by its Principal Lawyer\n(ii) Selling Full Title Guarantee\n2. Purchaser\n3. Price \xc2\xa3\n4. Description of\nProperty and\ninterest sold\nThe freehold title of the property known as 1-12\nArchway Heights 16-20 Archway Road London N19\nand for the purposes of identification only shown edged\nred on the plan attached to this Agreement\n5. Vendor\enabling\npower\n[Housing Act 1985]\n6. Completion Date On the day of 200 at the office of\nthe Vendor\995 Principal Lawyer, Alexandra House, 10\nStation Road, Wood Green N22 7TR\nThe Standard Commercial Property Condition s (Second Edition) are deemed to be\nincorporated in this Agreement as far as they are not inconsistent with the following\nspecial conditions.\n\nThe Vendor agrees to sell and the Purchaser agrees to purchase the Property\ndescribed in the Particulars and on the terms of this agreement.\nSPECIAL CONDITIONS\nA. Title is deduced and consists of as shown in Part I of the Schedule to this\nAgreement (\xe2\x80\x9cthe Schedule\xe2\x80\x9d).\n\nB. The property is sold subject to and with the benefit of the entries in the\nRegisters of the Vendor's Title and the Purchaser having been supplied with\ncopies of the entries is deemed to purchase with full knowledge of the entries "\n>>> h = hashlib.md5(contract).hexdigest()
>>> h
'de859a4eda27811c6d18af2ba538d7ae'
>>> contract = open('contract', 'rb').read()
>>> h = hashlib.md5(contract).hexdigest()
>>> h
'ee4d0c471bffa9071b4e67004a4a8502'
```

¹¹<https://medium.com/@vanflymen/learn-blockchains-using-spreadsheets-b97ad92b9b4d>

Figure 21: contract commands run in the terminal and output.

After changing one letter on the contract: hashes are different:

```
>>> h
'de859a4eda27811c6d18af2ba538d7ae'
>>> contract = open('contract', 'rb').read()
>>> h = hashlib.md5(contract).hexdigest()
>>> h
'ee4d0c471bffa9071b4e67004a4a8502'
>>>
```

Figure 22: Hashes differences shown by the red boxes.

After undo the change on the document the hash is the same:

```
'de859a4eda27811c6d18af2ba538d7ae'
>>> contract = open('contract', 'rb').read()
>>> h = hashlib.md5(contract).hexdigest()
>>> h
'ee4d0c471bffa9071b4e67004a4a8502'
>>> contract = open('contract', 'rb').read()
>>> h = hashlib.md5(contract).hexdigest()
>>> h
'de859a4eda27811c6d18af2ba538d7ae'
```

Figure 23: Hashes are similar again as previous test.

6.3 Discussion

This research intends to promote a better solution for cervical check patients in Ireland, and the main goal was to have the data storage and handling kept safely and with a unique ID.

The technique and methods used in this study were created and applied to ensure a reliable and user-friendly application of technology. Once the tests and experiments with data were completed, a straightforward way to see the theory in practice led to a greater comprehension of the concept's foundation. The first experiment using spreadsheet and MD5 formula had a very positive and a great starting point to have a different scope on how the hashing works and how it relates between each block connected.

The other approach with python library Hashlib was an important test to be done before building the application, as the logic of the library itself demonstrated to have a clear and straightforward approach in testing and seeing results in the prompt command line output.

The challenges and difficulties surround the learning curve that blockchain technology demands, as well as investments and, most of all, to be open for new solutions that can contribute to a better health care system.

For future work, the integration of both applications would be helpful and also expand the concept for more areas in the healthcare systems.

The tests and results reported in this study were favorable and helped the project's development; as a result, it was feasible to observe that this strategy can positively impact data handling concerns for patients who have cervical screening exams in Ireland in the near future.

7 Conclusion and Future Work

Situations and disruptions can highly impact the trust that people used to have in the healthcare system, especially with misinformation, lack of accuracy, and the list can go on. The ability to rely on medical systems and ensure that all the information is well kept and handled is crucial in this relationship between patients, hospitals, doctors, nurses, and clinics. The information about patients' health status in totality should be as accurate as possible because a minimal error, a missing information/communication can lead to many problems like sickness, chronic diseases, and even death. Sometimes it feels like the Healthcare system is more likely to be driven as a business side of things, instead of seeing at what the institution should be about, having people's lives and well-being in the first place as a priority, and not just profits and business expansion.

Learning about the situation in Ireland about the Cervical checks that have negatively affected hundreds of women in the country due to poor data handling led to deaths and many complicated cases is unacceptable and has to be taken seriously so this would never happen anymore. Failure to improve and advance with technology, high quality on data storage, and security should be highly prioritized in health technology systems.

Many great approaches are being explored, as the above-related work can prove that many researchers worldwide are investing and investigating better solutions that can bring to society the best way possible to make people feel and be safe in terms of the healthcare system. The change is happening slowly but is growing steadily for brighter and safer days ahead.

References

- [1] C. Kara Fox. (2019) A scandal over cervical checks is a sign of a bigger problem in ireland. [Online]. Available: <https://edition.cnn.com/2019/10/05/europe/ireland-cervical-check-scandal-intl/index.html>
- [2] S. Cao, G. Zhang, P. Liu, X. Zhang, and F. Neri, “Cloud-assisted secure ehealth systems for tamper-proofing ehr via blockchain,” *Information Sciences*, vol. 485, pp. 427–440, 2019. [Online]. Available: <https://www.sciencedirect.com/science/article/pii/S0020025519301471>
- [3] L. Ismail, H. Materwala, and Y. Sharaf, “Blockhr – a blockchain-based healthcare records management framework: Performance evaluation and comparison with client/server architecture,” in *2020 International Symposium on Networks, Computers and Communications (ISNCC)*, 2020, pp. 1–8.
- [4] M. van Reede, “Evaluating the practicality of using blockchain technology in different use cases in the healthcare sector,” *Radboud Universityt*, p. 54, 2020.
- [5] A. Khatoon, “A blockchain-based smart contract system for healthcare management,” *Electronics*, vol. 9, p. 94, 2020.
- [6] G. Leeming, J. Cunningham, and J. Ainsworth, “A ledger of me: Personalizing healthcare using blockchain technology,” *Frontiers in Medicine*, vol. 6, p. 171, 2019. [Online]. Available: <https://www.frontiersin.org/article/10.3389/fmed.2019.00171>
- [7] A. Kumar, R. Krishnamurthi, A. Nayyar, K. Sharma, V. Grover, and E. Hossain, “A novel smart healthcare design, simulation, and implementation using healthcare 4.0 processes,” *IEEE Access*, vol. 8, pp. 118 433–118 471, 2020.
- [8] G. W. ”Andreas M. Antonopoulos, ”*Mastering Ethereum*”. ”O’Reilly Media, Inc”, 2018.
- [9] A. M. K. ”Wei-Meng Lee, ”*Beginning Ethereum Smart Contracts Programming*”. ”O’Reilly Media, Inc”, 2019.
- [10] D. H. H. Kevin Solorio, Randall Kanna, *Hands-On Smart Contract Development with Solidity and Ethereum*. Frontiers, December 2019. [Online]. Available: <https://www.frontiersin.org/articles/10.3389/fmed.2019.00171/full>
- [11] K. I. R. M. S. L. M. W. ”Joseph J. Bambara, Paul R. Allen, ”*Blockchain: A Practical Guide to Developing Business, Law, and Technology Solutions*”. ”O’Reilly Media, Inc”, 2018.
- [12] M. Quiniou”, ”*Blockchain, The advent of Disintermediation*”. ”O’Reilly Media, Inc”, 2019.
- [13] M. Grinberg”, ”*Flask Web Development, 2nd Edition*”. ”O’Reilly Media, Inc”, 2018.