A picture containing graphical user interface

Description automatically generated

Singapore Institute of Technology - University of Glasgow  
Joint Degree in Computing Science Degree Programme

CSC3001 Capstone Project

Please complete the following form and attach it to the Capstone Report submitted.

**Capstone Period:**   **07/09/2022 to 22/07/2022**

**Assessment Trimester: Final Trimester**

**Project Type: Academic**

**Academic Supervisor Details:**

**Name: Purnima Murali Mohan**

**Designation: Assistant Professor**

**Email Address: purnima.mohan@singaporetech.edu.sg**

**Contact Number: +65 6592 2064**

**Student Particulars & Declaration:**

**Name of Student: Tay Meng Yao Arthur**

**Student ID: 1901824 / 2508403T**

I hereby acknowledge that I have engaged and discussed with my Academic Supervisor on the contents of this Capstone Report (Literature Review) and have sought approval to release the report to the Singapore Institute of Technology and the University of Glasgow.

|  |  |
| --- | --- |
| *Signature Shape  Description automatically generated with low confidence* |  |
| **Date:** | |

**END OF FORM**

|  |
| --- |
| A picture containing graphical user interface  Description automatically generated  Singapore Institute of Technology - University of Glasgow Joint Degree in Computing Science Degree Programme |
| Final Capstone Report  Telemedicine Platform with Blockchain NFT  For **Final Trimester** from **07/09/2022 to 15/04/2022**  *Tay Meng Yao Arthur*  *Student ID: 1901824*  *GUID ID: 2508403T* |
| Academic Supervisor: Purnima Murali Mohan |
| Submitted as part of the requirement for CSC3001 Capstone Project |

**Contents**

[List of Tables 1](#_Toc108889669)

[List of Figures 1](#_Toc108889670)

[Actknowledgement 2](#_Toc108889671)

[1. Introduction 3](#_Toc108889672)

[1.1 Problem formulation 3](#_Toc108889673)

[1.2 Project Objectives 4](#_Toc108889674)

[2. Literature Review 4](#_Toc108889675)

[2.1 Telemedicine and Information Access 4](#_Toc108889676)

[2.2 Blockchain 4](#_Toc108889677)

[2.3 Database vs Blockchain Comparison 6](#_Toc108889678)

[3.Methodology/Proposed Design 8](#_Toc108889679)

[3.1 Solution Architecture 9](#_Toc108889680)

[3.2 Distribution of Token 10](#_Toc108889681)

[3.3 Prototype 13](#_Toc108889682)

[3.4 Minting and Transaction Sucess 18](#_Toc108889683)

[4. Result and Analysis 20](#_Toc108889684)

[4.1 Cost Result 20](#_Toc108889685)

[4.2 Cost Analysis 20](#_Toc108889686)

[4.3 Hash Result 22](#_Toc108889687)

[4.4 Hash Analysis 22](#_Toc108889688)

[5. Conclusion 24](#_Toc108889689)

[5.1 Summary 24](#_Toc108889690)

[5.2 Future Work 25](#_Toc108889691)

[6.References 26](#_Toc108889692)

[7. Knowledge and Training Requirement 29](#_Toc108889693)

[7.1 Applicable Knowledge from the Degree Programme 29](#_Toc108889694)

[7.2 Additional Knowledge,Skillsets, or Certifications Requireds 29](#_Toc108889695)

[Appendix: Result and Analysis 30](#_Toc108889696)

# List of Tables

[Table 1 Comparison Public and Private Blockchain 5](#_Toc109166104)

[Table 2 Blockchain vs Database Comparison [29] 6](#_Toc109166105)

[Table 3 Etheruem tokens [40] [41] 10](#_Toc109166106)

[Table 4 ETH Exchange Rate [44] 21](#_Toc109166107)

[Table 5 Cost Analysis 22](#_Toc109166108)

# List of Figures

[Figure 1 Existing ECO system for blockchain EHR [36] 8](#_Toc109297966)

[Figure 2 Proposed Architecture 9](#_Toc109297967)

[Figure 3 Example of NFTExisting Distribution [42] 11](#_Toc109297968)

[Figure 4 Token Transfer Process 12](#_Toc109297969)

[Figure 5 Node Api Set Up 13](#_Toc109297970)

[Figure 6 Blockchain Set Up 13](#_Toc109297971)

[Figure 7 Deployment of Smart Contract Command 14](#_Toc109297972)

[Figure 8 Smart Contract Deployment Sucessful 14](#_Toc109297973)

[Figure 9 User Connecting to Application 15](#_Toc109297974)

[Figure 10 User connected 15](#_Toc109297975)

[Figure 11 User registering 16](#_Toc109297976)

[Figure 12 User’s information store in database 16](#_Toc109297977)

[Figure 13 Admin View on Token to mint 16](#_Toc109297978)

[Figure 14 Signing and Confirming Transaction 17](#_Toc109297979)

[Figure 15 Smart contact interaction sucessful 18](#_Toc109297980)

[Figure 16 Recorded Transaction of Minting 18](#_Toc109297981)

[Figure 17 Recorded Transaction of Approval 19](#_Toc109297982)

[Figure 18 Recorded Transaction of Creating Account information to track 19](#_Toc109297983)

[Figure 19 Recorded Transaction of Transfering Token to User 19](#_Toc109297984)

[Figure 20 Minted Status 19](#_Toc109297985)

[Figure 21 Eth Used Per Transaction 20](#_Toc109297986)

[Figure 22 Current Eth to SGD [43] 21](#_Toc109297987)

[Figure 23 User’s Token Received 22](#_Toc109297988)

[Figure 24 Original Data 23](#_Toc109297989)

[Figure 25 Data Altered 23](#_Toc109297990)

[Figure 26 Transaction Eth Used Dataset 31](#_Toc109297991)

[Figure 27 Min Max Mean Value 32](#_Toc109297992)

[Figure 28 Latency for Eth Used 32](#_Toc109297993)

[Figure 29 Latency per transaction 33](#_Toc109297994)

# Actknowledgement

I would like to thank my academic supervisor, Professor Purnima Murali Mohan for her guidance,encouragement and constructive feedback on my work progresss. Professor Purnima has provided assistance on getting started with blockchain and has given input on her experitise with blockchain for this project. Professor Purnima has provided meaningful insights on various different ways on analyzing a Blockchain.

# 1. Introduction

## 1.1 Problem formulation

With the COVID-19 pandemic, women could not attend their pregnancy check-up appointments, affecting their access to antenatal care and health services, increasing constant fear and anxiety [1]. Everyday,Pregnant women are at risk of getting gestational diabetes mellitus(GDM), also known as GDM short, and it is a disease caused by high blood sugar levels present during pregnancy [2]. This disease may cause complications to the health of both mother and baby, such as birth injuries and respiratory distress syndrome, increasing the risk of high blood pressure [3] . However, there are ways to prevent or reduce the chances of gestational diabetes through healthy eating habits, exercising, and weight management, which pregnant women should be informed of [3].

Currently, this is also a problem that is trying to be solved by Gloobe Pte Ltd on the open innovation network portal, where the company states there is a lack of all-in-one platforms for gestational diabetes. There was also a concern about ensuring PDPA for users utilizing the digital platform. [4]. It’s essential to ensure PDPA for the health-related system, as noted. In 2018 there was a health data breach within SingHealth [5]. This incident caused severe damage to Singhealth, both finically and in privacy, with a considerable large amount of fines and leakage of 160,000 health records [6]. About 59% of records breaches were in healthcare in the US, and 28.8% of these records are due to unauthorized access and disclosure incidents. [7]

Globe is looking for a digital platform solution; however, people have had concerns over data leakage of telemedicine due to data security and privacy concerns for telemedicine platforms where there is no trust in the technology. Most of these concerns were how the patient data was used and afraid of data leakage from unauthorized personnel [8]. A survey paper published online in September 2021 shows that e-health data concern is due to unauthorized access, data disclosure, tampering, and forgery. Data forgery could impersonate a service provider or doctor by data tampering, leading to data disclosure and unauthorized access to sensitive data. [9]. All this Data tampering and breaches can have a high consequence on an organization, in which attackers insert malicious files that could modify user credentials to gain access to sensitive data, which needs to be prevented [10].

## 1.2 Project Objectives

The project's aim includes researching the feasibility of implementing architecture with blockchain to add security properties to healthcare data or user credentials in a Telemedicine platform created for gestational diabetes patients. Furthermore, access control is also an indispensable security solution to protect e-health data by restricting unauthorized access. [9]. The solution will target adding security properties for data integrity and protection by integrating technology such as blockchain to protect and verify data on atelemedicine platform for its access control. Additionally, implementing blockchain to protect health data. Blockchain will also act as decentralised storage, increasing the difficulty of hackers penetrating the database and ensuring data privacy [11]. While possibility includes healthcare features such asinformative consulting from doctor, which digitally provides healthcare from a distance, allowing pregnant women to easily safety access GDM information to improve awareness and care for all similar to all Telemedicine platform

# 2. Literature Review

Further study is conducted to identify the feasibility of blockchain to be used as a database, the type of blockchain and the feasibility of creating a digital platform that acts similarly to telemedicine to interact with soon-to-be mothers.

## 2.1 Telemedicine and Information Access

Currently, telemedicine is an option for pregnant women to receive care in the pandemic, and it’s expected to reduce the risk of infection [12] and telemedicine platforms are expected to be the leading industry trend in 2021 due to the COVID-19 pandemic. [13] The amount of monthly active of telemedicine platforms grew by 272% from 2019 to 2021, and registered users have seen a 65% increase over the years [14]. Essentially shows the potential of a digital platform solution providing care and consultation at a distance. It’s also noted that most pregnant ladies obtained information from health care providers in GDM clinics, and at least 60% of GDM data were obtained from websites. [15]

## 2.2 Blockchain

Blockchain is distributed ledger technology (DLT) that stores information electronically on nodes in a network, maintaining a decentralized set of records. The information in blockchain technology allows data to be recorded and distributed, and it's immutable [16]. This Blockchain technology is used across various sectors such as healthcare, financial services, supply chain, etc. For example, blockchain targets healthcare by managing and protecting electronic health data [17].

There are mainly two types of Blockchain Permissionless and Permissioned Blockchain. The Permissionless Blockchain allows any user to participate on the node, known as the public blockchain. On the other hand, the permissioned type Blockchain is restricted and governed by single or multiple entities, also known as private Blockchain [18] [19]. The comparison between the two types of blockchains is seen in Table 1.

Table Comparison Public and Private Blockchain

|  |  |  |
| --- | --- | --- |
|  | **Public Blockchain** | **Private Blockchain** |
| **Available Fabric** | **Ethereum** | **HyperLedger Fabric** |
| **Algorithm** | **Proof of Work** [20] | **Pluggable** [20] |
| **Smart Contract** | **Yes** | **Yes** |
| **Language** | **Solidity (JavaScript)** [20][21] | **ChainCode (JavaScript, Golang, and Java)** [20][21] |
| **Type** | **Permissionless** | **Permissioned** |
| **Applications** | **MedCredits** [22] | **MedicalChain** [23] |

Both Ethereum and Hyperledger Fabric utilized smart contracts; for Ethereum, it's known to be solidity, and for Hyperledger fabric, its chaincode [21]. This smart contract is a form of digital agreement that executes automatically after fulfilling a set of pre-programmed conditions [24] [25].

Compared to Hyperledger fabric and Ethereum on latency and throughput, the private Blockchain Hyperledger shows higher performances and consumes fewer resources [26]. Hyperledger fabric adopts a micro-services-based architecture with permissioned based capability to ensure privacy and provide flexibility for different modes of consensus such as Raft and Kafta [20]. In contrast to Ethereum's framework, Ethereum does not offer the flexibility of consensus algorithms solely utilizing proof of work, and transactions are publicly accessible, which will cause privacy flaws. However, Ethereum uses cases mainly involve financial and asset trading and verification of transaction [20]. An Example of an Ethereum based healthcare application is Medcredits, used to automate the payments and validate the patients' transactions [27]. On the other hand, an example of Hyperledger fabric is Medicalchains, which are mainly used to support access control policy and securely share health data within the organisation [27]. Public Blockchain may seem to be better used for public verification purposes due to its transparency properties to gain trust of users who are concerned about how the data is being used. Private blockchains are meant for a private organization to other organizations' data consistency. Notability, there is also hybrid blockchain such as Dragonchain, a hybrid blockchain design consisting of a private blockchain network linking to a public network [28].

## 2.3 Database vs Blockchain Comparison

Table Blockchain vs Database Comparison [29]

|  |  |  |
| --- | --- | --- |
|  | **Blockchain** | **Database** |
| **Authority** | **Decentralized** | **Centralized** |
| **Architecture** | **Peer to Peer** | **Client- Server Model** |
| **Data Handling** | **Read and write** | **Create, Read, Update, Delete** |
| **Data Integrity** | **Yes** | **No** |
| **Transparency** | **Transparent** | **Non-Transparent** |
| **Cryptography** | **Yes** | **No** |
| **Transaction Performance** | **Low** | **High** |

The main difference between blockchain and a database is the Authority; Blockchain is decentralized while the database is centralized. [29] Blockchain relies on Proof-of-work to write into the blockchain, which is necessary to prevent Sybil while writing into a database is immediate [30].In terms of performance, an average centralised database query speed is much faster compared to blockchain as database storage [31]. Databases are generally customizable to meet business requirements and have the stability of handling large volumes of data and processing thousands of transactions per second. In comparison to Blockchain, It has security properties such as hashing and data immutability to ensure data integrity. It provides the decentralization properties to ensure a fault-tolerant way to store and verify critical data, which is immutable, preventing tampering [30] [32] [33]. In addition, it’s transparency to the public adds trust value to a system [30] [32] [33] Furthermore, blockchains prevent external and internal attackers from forging and tampering with data utilizing the time stamping method, which overwrites the tampered data to the original data [35]. This could prevent issues attackers from modifying user credentials to modify user credentials gain access to sensitive data.

However, data being transparent could lead to problems with storing sensitive data on the blockchain. But with, the combination of utilizing the immutability property of blockchain with the use of Crypto-privacy methods such as encryption ensures data privacy preservation and possibility resolves data being misused [34].

Databases examples are best for enterprise networks due to their stability in handling a large volume of data. Ideal for keeping confidential information and fast data processing [32] [35]. While use case examples for blockchain are establishing trust and transparency while providing security properties for transactions. Blockchain can be used for monetary transactions, verification of trusted data, essential verification, etc. [32] [35]. The data verification aspect may be used to ensure the data accuracy of the telemedicine platform shared between patients to reduce errors. This could be used to verify the user’s access role to ensure that there to ensure that only authorized healthcare roles can have access to particular data possibility reducing the likelihood of data breach of unauthorized access and disclosure incidents.

# 3.Methodology/Proposed Design

A picture containing timeline

Description automatically generated

Figure Existing ECO system for blockchain EHR [36]

Figure 1 shows an existing ECO system for blockchain on how it’s used for electronic health records. The author interacts with the smart contracts, which create the health electronic record, and create a block, and this block is distributed to the patient peer or family member. The members will then verify that the information is accurate and correct before approving the transaction to be written into the blockchain. [36]

Based on the existing example with blockchain implemented it prevents data tampering and data forgery however, patients are still concern on the privacy of the data being used. For our solution approach differs by implementing NFT. However one of the problems for Patient was how the health record data was used which the existing solution did not cover as a technical or staff can read the blockchain data without the user being notified.

## 3.1 Solution Architecture

Graphical user interface, application

Description automatically generated

Figure Proposed Architecture

To improve the current ecosystem to target patient data tracking, as described in figure 1. The solution will be based on the existing blockchain ecosystem but with the implementation of NFT, also known as Non-Fungible Token. With NFT implemented, it will come with an inherent feature for tracking data [37].This is based on how the smart contract/program is designed, allowing patients to specify who can access their personal health records [38].In addition, u would not have to worry about their information being used without their permission, as NFT has the potential and extend complex uses cases to assign rights to those who can access token data [39] [38]. The implementation of NFT will use the openzeppelin library, which will be described in the later section of this report on how this token is distributed and utilized.

Additionally, It’s essential for webpage data processing to be fast; however, based on the above research in the literature review, blockchain is slower than a database in terms of transaction speed, as shown in Table 2, which may not be ideal for to be used for an entire application data processing. To resolve this, the proposed solution adopts a hybrid database design approach for faster data processing and security properties from the blockchain to aid validation.

As seen in Figure 2, the SQL database will act as an off-chain database for other purposes, while the blockchain would verify specific data, such as access control.

Client

On the client side, the Ether Api library would allow the client side application to interact with the etherum blockchain and the ecosystems easily. The browser extension metamask allows users to interact with the Ethereum blockchain and the application to manage their account keys and transactions. The application will be developed with react as this framework has unique properties of virtual dom, allowing only components that change to rerender and do not render everything making the website more efficient in terms of loading.

Backend

Node express is used to create a rest API for the client to interact with the centralized PostgreSQL database as an off-chain data storage. Solidity is used to develop the smart contract as a digital agreement that executes automatically after fulfilling a set of pre-programmed conditions. The contract will be compiled using hardhat to the local simulated blockchain created by hardhat itself. All smart contract data interactions will be stored in the local Ethereum blockchain for validation purposes for the actual data in the centralized SQL database.

## 3.2 Distribution of Token

For the access control portion of the telemedicine website. The solution will be using Ethereum NFT tokens to allow users to access certain website features based on their roles. In the telemedicine system, we have three roles. The Patient will seek consultation, the Doctors will provide the consultating and perform their expertise, and lastly, Admin will enrol the users.

Table Etheruem tokens [40] [41]

|  |  |  |
| --- | --- | --- |
|  | **ERC20** | **ERC721** |
| **Token** | **Fungible** | **Non-Fungible** |
| **Interchangeable** | **Interchangeable** | **Non-Interchangeable(Unique)** |
| **Use Cases** | **Service vouchers, Governance token,etc** | **Artwork, Digital assets, Property,** |

The blockchain token in the solution will be utilizing ERC721 standard, also known as a non-fungible token(NFT). NFT is usually represented as artwork, digital asset or property; in this case, the NFT would be used to represent the user account as an account token. In addition, each token has a tokenID,unique properties, and owner’s information. It uniquely identifies and differentiates itself from other token to help uniquely identify each user [41].

As NFTs are part of the public blockchain implemented, owners of the NFT can easily verify token ownership as all transactions are transparent. Moreover, the NFT data are immutable, such as metadata, token id and transaction of the tokens are recorded in a distributed ledger or database, which makes it impossible to change the information, which is part of the blockchain tamper-proof aspect.This can aid fraud prevention for a user to impersonate a role to get access to sensitive records [41].

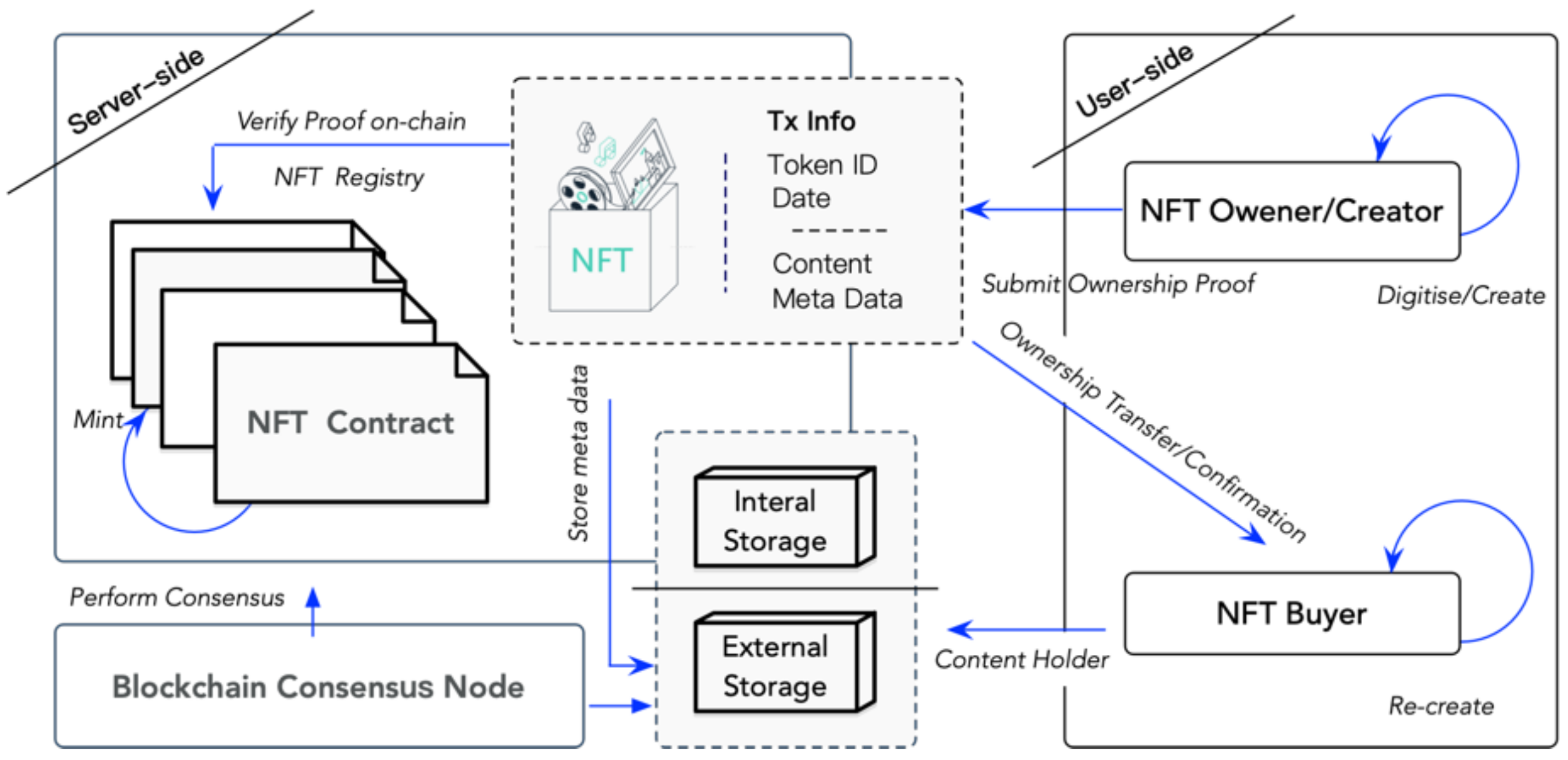


Figure Example of NFTExisting Distribution [42]

Currently, an example of a general model of NFT being distributed can be seen in Figure 3 above from a paper. A typical process consists of two roles: the NFT owner and the NFT buyer. As NFT can be represented as an Artwork, the original NFT owner would create and digitize the raw data and mint it into the blockchain. The metadata of the token is then stored in external storage. During the process, the owner would also sign the transaction with a cryptographic signature to mint into the blockchain, which cannot be changed. If the NFT buyer buys the token, the ownership will be transferred to the NFT buyer. The NFT Buyer would then possess the right to do anything to the token that was brought based on their wallet address [42].

Text

Description automatically generated with medium confidence

Figure Token Transfer Process

The token distribution process for the telemedicine solution can be seen in Figure 4. This is done using openzepplin’s library. Similar to what is described in Figure 2, where there is a creator and a requester. The NFT buyers' roles would be Doctor and Patient, and the NFT Creator would be the organisation's Admin. However, in this aspect, the Doctor and Patient would not pay the gas fee and Eth, where the organization will bear the cost of these tokens. For the process, the Doctor/Patient would connect to the meta mask and register an account which will be stored in PostgreSQL database. This database aims to ensure that we can retrieve the registered user’s unique wallet address as part of transferring an NFT token requirement that requires the receiver wallet address.

Additionally Doctor and Patient would not want to pay the gas fee, which this distribution method resolves it. Once registered, the Admin will be the decision maker to view and verify if it’s a valid doctor or Patient before minting the token on the admin view. Once minted, the token will be transferred to the registered user’s unique wallet address and gain access to features tied to their role.

## 3.3 Prototype

To showcase the distribution process, a prototype is developed with various steps shown below.

Setup Phase



Figure Node Api Set Up

Text

Description automatically generated

Figure Blockchain Set Up

The node js server app would be set up to allow the interaction of the PostgreSQL database seen in Figure 5, where the application will interact with port 3001. The blockchain is set up using a hardhard console, which creates a simulated local blockchain environment for the application to interact with. By running the “npx hardhat node”. With the local blockchain up, a list of test accounts is displayed in the figure above in Figure 6.

Smart contract Deployment

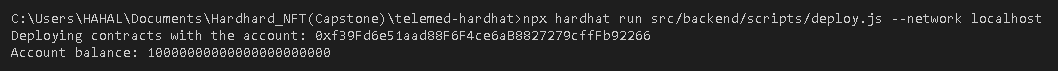


Figure Deployment of Smart Contract Command

Text

Description automatically generated

Figure Smart Contract Deployment Sucessful

With the blockchain and databased up. The telemedicine organization can then compile and deploy the smart contract to the blockchain, enabling the token's minting and transferring. The smart contract is deployed using a written javascript with the command

”npx hardhat run src/backend/scripts/deploy.js --network localhost” seen in figure 7

There are two smart contracts for interaction:

* User - Keep track of the accounts minted
* NFT - Minting the NFT to the blockchain

For the smart contract owner that owns and deploys the contract owns the unique wallet address “0xf39fd6e51aad88f6f4ce6ab8827279cfffb92266” from the test account created. From Figure 8 it can be seen the successful deployment of the smart contract.

Registering

Graphical user interface, application

Description automatically generated

Figure User Connecting to Application

Graphical user interface, application

Description automatically generated

Figure User connected

Graphical user interface, application, website

Description automatically generated

Figure User registering

Table

Description automatically generated

Figure User’s information store in database

For the user to use the application, metamask would be required to connect their wallet address and use the application. The connection can be seen in figure 9 and 10 above. Once connected, the user can begin registering and requesting the token based on the desired role and nickname seen in figure 11 above once the form has been submitted successfully. It will be stored in the centralized database seen in figure 12.

Admin Distributing Token

Graphical user interface

Description automatically generated with low confidence

Figure Admin View on Token to mint

With the user’s info registered, the Admin can view the account request and help them enrol the telemedicine website by minting the token for them by selecting the “Mint Token” button seen in figure 13. In this case, the Admin would be the owner of the contract owner, which deploys the smart contract. For the data minted, the data would be hashed, which will be used to verifty the integrity of the database's data if it’s tampered with.

Graphical user interface, text, application, email

Description automatically generated

Figure Signing and Confirming Transaction

There are a total of 4 interactions of the smart contract function and transaction confirmation to mint and distribute the token for each interaction it has to be confirmed. For each transaction, the user would have to pay a gas fee which is a certain amount of ETH, to conduct the transaction. An example is seen in Figure 14 above.

1. **Mint token** – This function mints from the openzepplin library the NFT token into the blockchain based on the user’s credentials
2. **SetapprovalForAll** – This function from the openzepplin library, as the token owner, would have to call this function from the ERC721 standard, which will allow the token to be transferred.
3. **CreateAccount** - this function is from the User smart contract, which tracks an account that has been created.
4. **DistributeToken** - this function is from the User smart contract, which is used to transfer the token to the user based on the user’s wallet address

## 3.4 Minting and Transaction Sucess

The completion of Admin minting and transferring the token and successful transaction can be seen below in Figures 15 to 19.

Graphical user interface, application

Description automatically generated

Figure Smart contact interaction sucessful

Text

Description automatically generated

Figure Recorded Transaction of Minting

Text

Description automatically generated

Figure Recorded Transaction of Approval

Text

Description automatically generated

Figure Recorded Transaction of Creating Account information to track

Text

Description automatically generated

Figure Recorded Transaction of Transfering Token to User

For the 4 interactions of the smart contract function and transaction, it can be seen that its written to the blockchain where all transaction block’s hash is computed from Figure 16 to figure 19 above. It tracks the interactions of the sender and the smart contract itself.

Admin View

A picture containing graphical user interface

Description automatically generated

Figure Minted Status

On the Admin view, with the transaction completed, the centralized database would update the minted column to true, indicating to the Admin that the token has been created and minted to the blockchain and transferred to the user.

# 4. Result and Analysis

In this section, analysis was done based on the result obtained from the prototyping. This consists of analysing the distribution process's cost and the scenario of hash data being tampered with to verify the integrity and changes. Based on the distribution process of the token, an experiment was conducted to monitor the average price of minting and distributing the token to the user. Thirty consecutive transactions were executed and recorded as a minimum of 30 observations is sufficient to conduct significant statistics. Additionally, the computed hash value of the user’s registered data was analysed in this section to showcase the scenario if data has tampered

## 4.1 Cost Result

Chart

Description automatically generated

Figure Eth Used Per Transaction

The results' hypothesis is that gas fees increase as the blockchain network gets busy and congested. One transfer consists of the four smart contract interactions and the four functions described in the prototype section. The actual gas fee was collected by converting gwei to eth, and thirty mintings and token transfers were executed consecutively; this can be seen in Figure 21 above. The observation is that after the 23rd transaction, the amount of Ethereum used to mint and transfer the token increases exponentially.

## 4.2 Cost Analysis

Chart

Description automatically generated

Figure Current Eth to SGD [43]

Based on the current ETh market in the month of July 2022, 1 Eth is estimated1680.44 SGD from the coin-based market website in Figure 22. Therefore, the average cost of minting and distributing the token was 0.000506 Eth. Therefore, on average, converting to SGD will be 0.85 SGD for the organization to mint and transfer a token to a user. However, the average cost amount is solely based on the experiment's results, and this cost will continue to fluctuate even more and increase exponentially, as seen in Figure 21.

Table ETH Exchange Rate [44]

|  |  |  |  |
| --- | --- | --- | --- |
| **Eth Exchange Rate** | **Past 1 Year** | **Past 3 Year** | **Past 5 Years** |
| **Maximum Rate**  **(Per 1 Eth)** | **4732.48 SGD** | **4732.48 SGD** | **4732.48 SGD** |
| **Minimum Rate**  **(Per 1 Eth)** | **1048.71 SGD** | **132.20 SGD** | **105.96 SGD** |

Table Cost Analysis

|  |  |  |
| --- | --- | --- |
| **Average Gas (0.000506Eth)** | **Mnimum Cost** | **Maximum Cost** |
| **Mint and Distribute Single Token** | **0.05 SGD** | **2.40 SGD** |

Based on the table above, the exchange rate of the maximum and minimum values of the past five years is analysed and collected. Based on the tables, if the exchange rate were to vary over time, the maximum cost of minting and distributing a token after converting to ETH to SGD estimated would be 2.40 SGD, and the lowest would be 0.05 SGD per token.

## 4.3 Hash Result

Receive Token

Shape, rectangle

Description automatically generated

Figure User’s Token Received

With the token minted, on the token requester end, once the token has been transferred to the requester, it will display on the application once the user logins in seen in Figure 21.This will allow them to access features of the appropriate roles. The token created and transferred to the user will consist of the registered information and a computed hashed utilizing the name, role and user’s unique wallet address for other users or the system to verify against the blockchain that the data has not be tampered and ensure the data is not fake

## 4.4 Hash Analysis

As the data are hashed, anyone can verify the data based on what the database reads against the blockchain. Each transaction that occurred is written in the block and with a hash computed seen in figures 15 to 18 earlier. This ensures that blockchain is tampered-proof where if someone tries to tamper with the data, the entire block’s hash will change making it invalid additionally, many sources have also claimed that blockchain is tampered-proof [30] [32] [33]. With blockchain being tampered proof, the hash data stored on the blockchain can be used to verify the data in the centralized database giving it the validation properties.



A picture containing graphical user interface

Description automatically generated

Figure Original Data

Graphical user interface, website

Description automatically generated

Figure Data Altered

Figure 24 shows the original data of the user’s token computed using SHA256, and figure 25 shows the altered data. This indicates that even a slight data tampering would drastically change the computed hash. In the scenario of data computed from the centralized database and the hash value in the blockchain does not match. The organization could immediately tell if the data has been tampered with and revert the changes to the blockchain’s data. This would also aid in recovering the data that was tampered.

However, there are flaws and room for improvement in this distribution process, which is currently before minting to the blockchain; the data might be tampered with before minting, which would require a way to secure the centralized SQL database itself. However, once minted, the validation could be done and securing the data. Additionally, currently, the Admin has to identify if the person registering is a Doctor or a Patient. There should be ways to prove a doctor’s identification, such as medical certification.

# 5. Conclusion

## 5.1 Summary

With the COVID-19 pandemic, women could not attend their pregnancy check-up appointments, affecting their access to antenatal care and health services and increasing constant fear and anxiety [1]. This, in turn, allow people to seek Telemedicine platforms, and these digital platforms have been trending and rising since the pandemic, showing the potential success of creating a digital platform providing care from a distance. However, there were concerns over data leakage of telemedicine due to data security and privacy concerns for telemedicine platforms, such as how the data is being used or incidents of data breaches and tampering.

To resolve and improve on this issue, research was conducted on the potential of using blockchain to prevent data breaches and tampering in a telemedicine platform. Through research, although blockchain may not seem ideal to store a large amount of data compared to a regular database, blockchain could still be used to ensure the role and access control with its tampered proof and verification aspect.

Based on the existing blockchain solution ecosystem in a healthcare scenario, the solution implemented utilizes the current blockchain ecosystem with improvement, including an additional component with the utilization of NFT, also known as Non-Fungible Token. Showcasing the potential of data protection and ownership. A prototype was completed to showcase this token's distribution process to a User who wants to enrol on the telemedicine platform.

The distribution process of the NFT to the user successfully shows another way of distributing NFT tokens. The combination of storing the computing hash on the blockchain and using it as validation storage will help to ensure data forging is prevented. Additionally, using NFT helps to strengthen access control where no one could impersonate a role to cause a data breach using forged roles and access sensitive data once the data has been minted. And from the above results, it can be seen if there is slight data tampered with in the centralized database, the hash will change drastically, which differs from the actual blockchain stored hash. Therefore, the organization would be able to revert the tampered data immediately. This has helped to strengthen the issue with access control and prevents the attacker from storing data to impersonate a specific role to gain access to sensitive health records. Furthermore, Patient who is concerned about data being misused would no longer be an issue as the controls are within the Patient through NFT security

However, after implementing and analysing the solution, there were flaws in certain areas that requires improvement. For instance, a user registering for an account, the SQL centralized database record may still be tamper before the token was minted to the blockchain. So improvement will be required to encrypt the data in the database to secure it. Additionally, blockchain can be costly for each transaction conducted to the blockchain; the gas fee fluctuates based on how busy the blockchain network is, which possibly gets very expensive sometimes. Our experiment has already shown that gas fees increase exponentially, which can be a huge gap as the network gets more congested to mine for blocks.

## 5.2 Future Work

Although it’s mentioned with NFT implemented patients to specify who can access their personal health records [38]. The prototype does not showcase and has not implemented a function for users to edit data reading permission of their NFT. However, this can be done through openzepplin using Role-Based Access Control functionality to configure the permission of the NFT tokens for future work [45].

Furthermore, as seen in the cost analysis experiment, gas prices used for minting and transferring token fluctuates and increase exponentially. Improvements to the blockchain can be made in areas such as scaling. An example would be to implement layer 2 scaling where transactions are combined into a single transaction and sent to the blockchain, which will increase the transaction per second greatly and reduce network congestion on the mainnet leading to a reduction in gas price [46].

Additionally, with blockchain implemented, ERC20 tokens, also known as fungible tokens, can act as consultation vouchers,can be implemented in future. For example, a Patient could buy a consultation voucher based on ERC20 standard and redeem a doctor’s consultation session as a form of payment. At the same time, the doctor can receive ETH in exchange. Lastly, the centralized database could be better secured with a form of encryption possible to be explored to patch the flaws of the current design.

# 6.References

|  |  |
| --- | --- |
| [1] | R. Aydin and S. Aktas, “An investigation of women’s pregnancy experiences during the COVID-19 pandemic: A qualitative study,” *The International Journal of Clinical Practice,* vol. 75, no. 9, 2021. |
| [2] | WebMD, “Gestational diabetes: Symptoms, causes, diet, diagnosis, and treatment,” 13 December 2019. [Online]. Available: https://www.webmd.com/diabetes/gestational-diabetes. |
| [3] | M. F. f. M. E. a. Research, “Gestational diabetes,” Mayo Clinic, 26 August 2020. [Online]. Available: https://www.mayoclinic.org/diseases-conditions/gestational-diabetes/symptoms-causes/syc-20355339. |
| [4] | G. P. Ltd, “Design Think-Tank 2021,” Design Think-Tank 2021, 29 September 2021. [Online]. Available: https://www.openinnovationnetwork.gov.sg/innovation-challenges/design-think-tank-2021?tab=problem. [Accessed 21 November 2021]. |
| [5] | Irene, “Personal info of 1.5m SingHealth patients, including PM LEE, stolen in Singapore's worst cyber attack,” The Straits Times, 20 July 2018. [Online]. Available: https://www.straitstimes.com/singapore/personal-info-of-15m-singhealth-patients-including-pm-lee-stolen-in-singapores-most. |
| [6] | M. Mohan, “PDPC fines IHiS, SingHealth combined S$1 million for data breach following cyberattack,” CNA, 15 January 2019. [Online]. Available: https://www.channelnewsasia.com/singapore/ihis-singhealth-fined-1-million-data-breach-cyberattack-906806. |
| [7] | R. Basen, “Medical News,” MedpageToday, 04 September 2020. [Online]. Available: https://www.medpagetoday.com/practicemanagement/telehealth/88469. |
| [8] | J. McKeon, “81% of telehealth providers are concerned about data leakage,” HealthITSecurity, 06 December 2021. [Online]. Available: https://healthitsecurity.com/news/81-of-telehealth-providers-are-concerned-about-data-leakage. |
| [9] | S.-R. Oh, Y.-D. Seo, E. Lee and Y.-G. Kim, “A Comprehensive Survey on Security and Privacy for Electronic Health Data,” *Int J Environ Res Public Health. ,* vol. 18, no. 10.3390/ijerph18189668, p. 18, 2021 . |
| [10] | C. D. D. RSS, “How to prevent data tampering in your business,” Cypress Data Defense RSS, 24 June 2020. [Online]. Available: https://www.cypressdatadefense.com/blog/data-tampering-prevention/. |
| [11] | J. Legrand, “The future use cases of blockchain for cybersecurity,” Cyber Management, [Online]. Available: https://www.cm-alliance.com/cybersecurity-blog/the-future-use-cases-of-blockchain-for-cybersecurity. |
| [12] | K. Nakagawa, T. Umazume, M. Mayama, K. Chiba, Y. Saito, K. Noshiro, M. Morikawa, M. Yoshino and H. Watari, “Survey of attitudes of individuals who underwent remote prenatal check-ups and consultations in response to the COVID-19 pandemic,” *Journal of Obstetrics and Gynaecology Research,* vol. 47, no. 7, pp. 2380-2386, 2021. |
| [13] | GlobalData, “Telemedicine expected to be a leading industry trend in 2021, with some telemedicine apps having reported whopping 8,270% increase in downloads in 2020, says GlobalData,” GlobalData, 29 January 2021. [Online]. Available: https://www.globaldata.com/telemedicine-expected-leading-industry-trend-2021-telemedicine-apps-reported-whopping-8270-increase-downloads-2020-says-globaldata/. |
| [14] | V. Kapur and A. Boulton, “Asia-Pacific telemedicine platforms will long outlast covid-19,” Bain, 22 April 2021. [Online]. Available: https://www.bain.com/insights/asia-pacific-telemedicine-platforms-will-long-outlast-covid-19-snap-chart/. |
| [15] | S. Hewage, J. Audimulam, E. Sullivan, C. Chi, T. W. Yew and J. Yoong, “Barriers to Gestational Diabetes Management and Preferred Interventions for Women With Gestational Diabetes in Singapore: Mixed Methods Study,” *JMIR Form Res.,* vol. e14486, no. doi:10.2196/14486, p. 4(6), 2020. |
| [16] | L. Conway, “Blockchain explained,” Investopedia, 04 November 2021. [Online]. Available: https://www.investopedia.com/terms/b/blockchain.asp. |
| [17] | P. Brody, “5 tips to successfully implement blockchain for businesses,” TechTarget, 11 June 2021. [Online]. Available: https://searchcio.techtarget.com/feature/Todays-blockchain-use-cases-and-industry-applications. |
| [18] | K. E. Wegrzyn and E. Wang, “Types of blockchain: Public, private, or something in between: Foley & Lardner LLP,” Foley & Lardner LLP, 19 August 2021. [Online]. Available: https://www.foley.com/en/insights/publications/2021/08/types-of-blockchain-public-private-between. |
| [19] | C. Parizo, “What are the 4 different types of blockchain technology?,” TechTarget, 28 May 2021. [Online]. Available: https://searchcio.techtarget.com/feature/What-are-the-4-different-types-of-blockchain-technology. |
| [20] | TharakaHewa, M. Ylianttila and M. Liyanage, “Survey on blockchain based smart contracts: Applications, opportunities and challenges,” *Journal of Network and Computer Applications,* vol. 177, 2021. |
| [21] | T. Wiesner, “What's the difference between JavaScript, solidity, Ethereum and chaincode?,” Vomtom.at, 29 May 2019. [Online]. Available: https://vomtom.at/whats-the-difference-between-javascript-solidity-and-ethereum/. |
| [22] | M. Protocol, “MedX Protocol,” MedX Protocol, [Online]. Available: https://medcredits.io/. |
| [23] | Medicalchain, “Medicalchain,” Medicalchain, [Online]. Available: https://medicalchain.com/en/. |
| [24] | M. G. Kukkuru, “Role of smart contracts on Blockchain explained,” Infosys, [Online]. Available: https://www.infosys.com/insights/digital-future/smart-contracts.html. |
| [25] | L. Mearian, “What's a smart contract (and how does it work)?,” Computerworld, 29 July 2019. [Online]. Available: https://www.computerworld.com/article/3412140/whats-a-smart-contract-and-how-does-it-work.html. |
| [26] | F. I. R., A. V. Pimenov, G. A. Panin and S. V. Bezzateev, “Blockchain in 5G Networks: Perfomance Evaluation of Private Blockchain,” *2021 Wave Electronics and its Application in Information and Telecommunication Systems (WECONF),* pp. 1-4, 2021. |
| [27] | R. W. Ahmad, K. Salah, R. Jayaraman, I. Yaqoob, S. Ellahham and M. Omar, “The role of blockchain technology in telehealth and telemedicine,” *International journal of medical informatics,* vol. 148, 2021. |
| [28] | “Blockchain Developers: Dragonchain SaaS,” Dragonchain, [Online]. Available: https://dragonchain.com/developers/. |
| [29] | 1. Blockchains, “Blockchain Vs Relational Database: What's The Difference?,” 101 Blockchains, 03 November 2021. [Online]. Available: https://101blockchains.com/blockchain-vs-relational-database/. |
| [30] | L. Martin, Blockchain or relational Database? How to choose the right technology for your application,” TechBeacon, 31 January 2020. [Online]. Available: https://techbeacon.com/security/blockchain-vs-relational-database-which-right-your-application. |
| [31] | 1. Blockchains, “101 Blockchains,” 2021 November 17. [Online]. Available: https://101blockchains.com/blockchain-vs-database-the-difference/. |
| [32] | V. Tabora, “Databases and Blockchains, The Difference Is In Their Purpose And Design,” HackerMoon, 4 August 2018. [Online]. Available: https://hackernoon.com/databases-and-blockchains-the-difference-is-in-their-purpose-and-design-56ba6335778b. |
| [33] | E. Keary, “Security Think Tank: Use blockchain for integrity and immutability checks,” ComputerWeekly , 06 September 2019. [Online]. Available: https://www.computerweekly.com/opinion/Security-Think-Tank-Use-blockchain-for-integrity-and-immutability-checks. |
| [34] | B. Bernabe, J. a. Canovas, J. L. a. Hernandez-Ramos, J. L. a. T. Moreno, R. a. Skarmeta and Antonio, “Privacy-Preserving Solutions for Blockchain: Review and Challenges,” *IEEE Access,* vol. 7, no. 10.1109/ACCESS.2019.2950872, pp. 64908-164940, 2019. |
| [35] | Chowdhury, Mohammad and Colman, Alan and Kabir, Ashad and Han, Jun and Sarda and Paul, “Blockchain Versus Database: A Critical Analysis,” in *Conference: 2018 17th IEEE International Conference On Trust, Security And Privacy In Computing And Communications/ 12th IEEE International Conference On Big Data Science And Engineering (TrustCom/BigDataSE)*, 2018. |
| [36] | Esposito, C. a. D. Santis, A. a. Tortora, G. a. Chang, H. a. Choo and K.-K. Raymond, “Blockchain: A Panacea for Healthcare Cloud-Based Data Security and Privacy?,” *IEEE Cloud Computing,* vol. 5, no. 10.1109/MCC.2018.011791712, pp. 31-37, 2018. |
| [37] | T. M. Futurist, “NFT in healthcare: How patients could monetise their health data,” The Medical Futurist, 12 January 2022. [Online]. Available: https://medicalfuturist.com/nfts-an-health-data/. |
| [38] | Leonid, “Non-fungible tokens in healthcare: Inevitable, promising, but unclear as yet,” CIFS Health, 15 March 2022. [Online]. Available: Non-fungible tokens in healthcare: Inevitable, promising, but unclear as yet. |
| [39] | Orchid, “Privacy & VPN Blog - Orchid,” Orchid, [Online]. Available: What do NFTS mean for privacy?. |
| [40] | A. Banerjee, “Difference disclosed: Erc20 vs. ERC721,” Web3.0 & Blockchain Certifications, 24 March 2022. [Online]. Available: https://www.blockchain-council.org/ethereum/erc20-vs-erc721/. |
| [41] | S. M. H. Bamakan, N. Nezhadsistani, O. Bodaghi and Q. Qu, “Patents and intellectual property assets as non-fungible tokens; key technologies and challenges,” *Scientific Reports,* vol. 12, no. 1, pp. 2045-2322, 2022. |
| [42] | “Betraying Blockchain: Accountability, Transparency and Document Standards for Non-Fungible Tokens (NFTs),” *Information,* vol. 12, p. 9, 2021. |
| [43] | Coinbase, “Ethereum (ETH) Price, Charts, and News: Coinbase: ethereum price, eth price, ethereum,” Coinbase, [Online]. Available: https://www.coinbase.com/price/ethereum. [Accessed 19 July 2022]. |
| [44] | Ethereum, “CoinDesk Latest Headlines RSS,” Ethereum, 19 July 2022. [Online]. Available: https://www.coindesk.com/price/ethereum/. |
| [45] | O. Docs, “Access control,” OpenZeppelin Docs, [Online]. Available: https://docs.openzeppelin.com/contracts/2.x/access-control. |
| [46] | ethereum, “Scaling,” ethereum, [Online]. Available: https://ethereum.org/en/developers/docs/scaling/. |
| [47] | E. Byakwaga, S. Musa and A. Nakimuli, “Level of and factors associated with awareness of gestational diabetes mellitus among pregnant women attending antenatal care at Kawempe National Referral Hospital: a cross sectional study,” *BMC Pregnancy and Childbirth ,* 2021. |
| [48] | L. A. Price, L. J. Lock, L. E. Archer and Z. Ahmed, “Awareness of Gestational Diabetes and its Risk Factors among Pregnant Women in Samoa,” *Hawaii J Med Public Health,* vol. 76(2), p. 48–54, 2017 Feb. |

# 7. Knowledge and Training Requirement

The section lists all the knowledge, skillsets and certifications from the degree programme and beyond that were necessary for successfully completing the capstone projects.

## 7.1 Applicable Knowledge from the Degree Programme

The prerequisite knowledge and skillsets from the degree programme that was necessary for the capstone projects are as follows:

|  |  |  |
| --- | --- | --- |
| **No.** | **Module(s)** | **Knowledge(s) Applied** |
| 1 | CSC2002: Team Project | I did not have much time to deal with learning how to create a web application during my Capstone project.However because of my experience in the Team project module where we were tasked to create an actual application for a client cloudplus. I have already obtained the set of skills to develop using react. Additionally I understand that reacts virtual dom properties makes it a unique framework for a application. Virtual dom enables efficient rendering of components in the web application where it only renders parts of the application that has changed. |
| 2 | CSC2008: Database Systems | In the Database module we were taught the basic of databases where applying SQL to query something from the database which was relatively straightforward making it ease to apply to my capstoneand additionally for group projects I have already self taught and learn on setting up and configuring databases. |
| 3 | CSC2005: Human Computer Interaction | The module teaches us about the basics of creating a better User Interface (UI) and User experience (UX). This has help me to style my prototype Telemedicine application. |
| 4 | CSC2001: Professional Software Development | In this module I learn the various type of architectures out there and was able to apply the concepts in my capstone, Additionally diagram such as activity diagram, flow diagram were taught and gave me insight in doing up my own diagram for this project. |
| 5 | CSC2901: Effective Communication | Effective communication module has prepared me on effective writing and taught the ways to cite a source properly. |

## 7.2 Additional Knowledge,Skillsets, or Certifications Requireds

The following are the additional requirements and knowledge that were required for for the capstone projects:

|  |  |  |
| --- | --- | --- |
| **No.** | **Additional Requirement(s)** | **Knowledge(s) Applied** |
| 1 | Blockchain Etherum | Knowledge required to understand how blockchain like etherum works. As blockchain has not really been cover in the other modules and research is required to look for the libraries that can interact with the Ethereum framework |
| 2 | Solidity | Knowledge of Solidity is required which is not taught in school. Solidity is a programming language that is use to implement smart contracts. This smart contracts is then compile and deployed into the blockchain. The smart contract written controls the functionally logic of what the user can do on the client side of the application |
| 3 | Hardhat | Knowledge Hardhat is required to setup a local blockchain which is not covered in school. Hardhat allows the simulation and showcase the interaction of the blockchain with the smart contract. |
| 4. | Ether.js | This library knowledge is required to create a Web3 application. Ether.js is a library that consist of functionally allowing the client to interact with the blockchain and it’s ecosystem which is essential to develop a telemedicine application with blockchain. |
| 5. | Openzeppelin | This library knowledge is required to create NFT and disitrbute the NFT to the users in the prototype. Openzeppelin is a extension of functions that was created using solidity. |

# Appendix: Result and Analysis

Table

Description automatically generated

Figure Transaction Eth Used Dataset

Graphical user interface, text, application, email, Teams

Description automatically generated

Figure Min Max Mean Value

Shape

Description automatically generated

Figure Latency for Eth Used

Shape

Description automatically generated with medium confidence

Figure Latency per transaction

**END OF REPORT**