MAIN PROJECT

Project Guide:
Anitha Jose
Assistant Professor
Department of CSE

Group Members

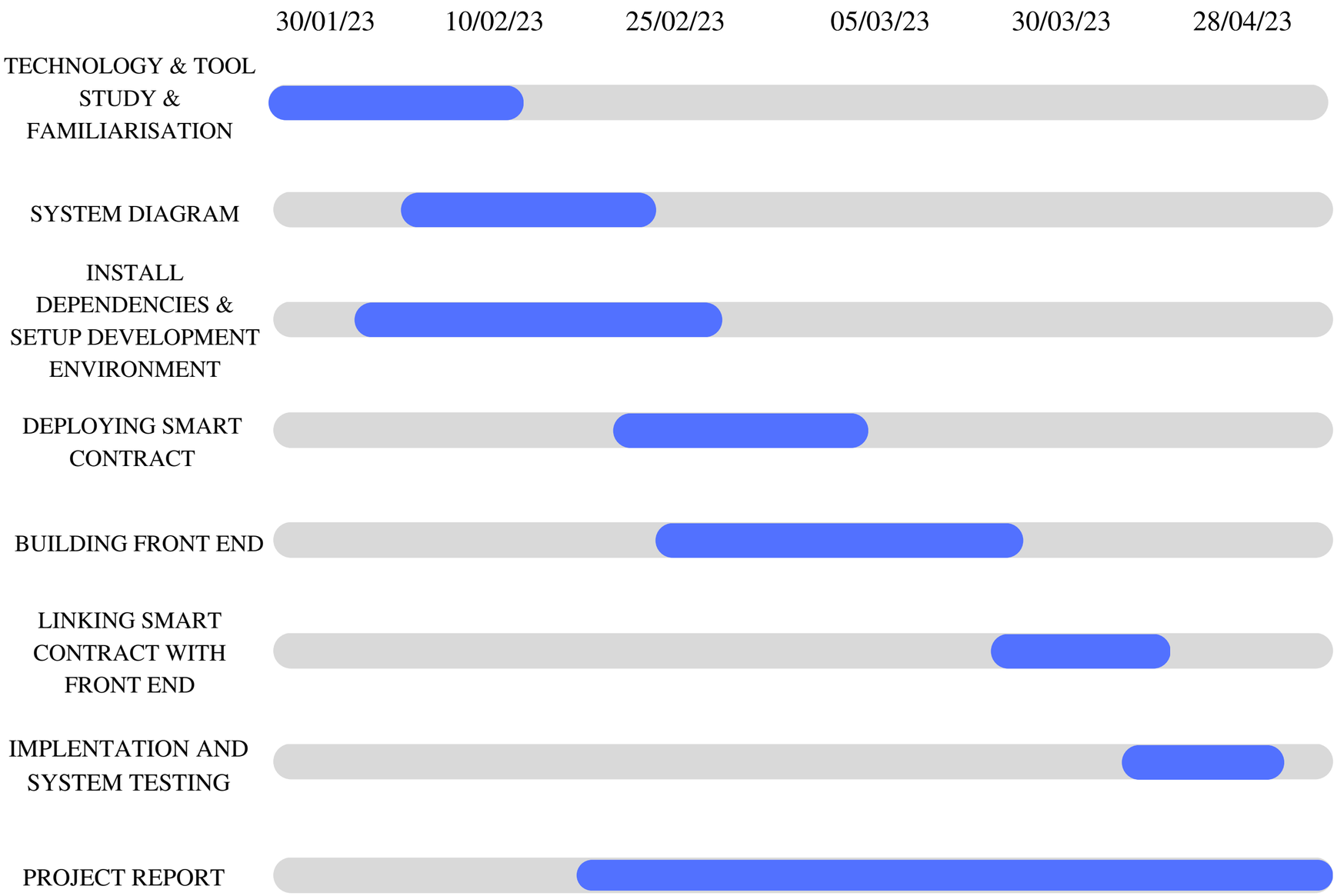
- Abel T Varghese
- Aju Sebastian
- Alan Francis Jose
- Sona Chacko
- Tinsu Mariyam Thomas

MediChain:

A User Controlled eHealth sharing system in blockchain.

INDEX

Gantt Chart


30/01/23
10/02/23
25/02/23
05/03/23
30/03/23
28/04/23
TECHNOLOGY & TOOL STUDY & FAMILIARISATION
SYSTEM DIAGRAM
INSTALL DEPENDENCIES & SETUP DEVELOPMENT ENVIRONMENT
DEPLOYING SMART CONTRACT
BUILDING FRONT END
LINKING SMART CONTRACT WITH FRONT END
IMPLENTATION AND SYSTEM TESTING
PROJECT REPORT

Introduction

- People like to travel and may visit different doctors across different jurisdictions (such as countries).
- eHealth data of individuals is managed by the diverse health service providers and stored in different locations. Often, sharing is not even allowed within the same country between different healthcare providers.
- There are several reasons but, as a general theme, it is due to a lack of trust or data disclosure considerations stemming from compliance and regulations.
- There is a consensus that healthcare data is sensitive personal information that must be well protected.

Abstract

- There exists a problem in sharing eHealth data across different jurisdictions.
- As a general rule, and due to the sensitive nature of the information, different national regulations impose severe limits on what can be exchanged, even in case of emergencies.
- Furthermore, different systems in different jurisdictions do not communicate.
- We propose a system that allows eHealth data to be securely exchanged, with the data subject always in the position of mediation.

Problem Statement

There is an absence of a trusted, decentralized system that allows secure transaction of eHealth data without third party involvement and often there are a lot of regional restrictions and regulations that slows the data exchange.

Terms used

- Requesting Party: The person or entity that is requesting the data of a patient.
- Data Subject: The patient whose data is being requested.
- Authorization Server: The local server in which verification is done and data is downloaded.

Literature Survey

[1]“User-Controlled, Auditable, Cross-Jurisdiction Sharing of Healthcare Data Mediated by a Public Blockchain”-Xiaohu Zhou, Vitor Jesus, Yonghao Wang and Mark Josephs-2020

- This paper tackles the problem of eHealth data that is managed by diverse health service providers with an agreement between different jurisdictions not to share the data externally due to lack of trust or data disclosure considerations by introducing a decentralized scheme known as BRUE.
- The above paper propose a BRUE scheme:-(i)centering all information exchange and control on data subject,(ii)combine a set of technologies and standards(Blockchain, Receipts, UMA for eHealth data sharing).

Solution

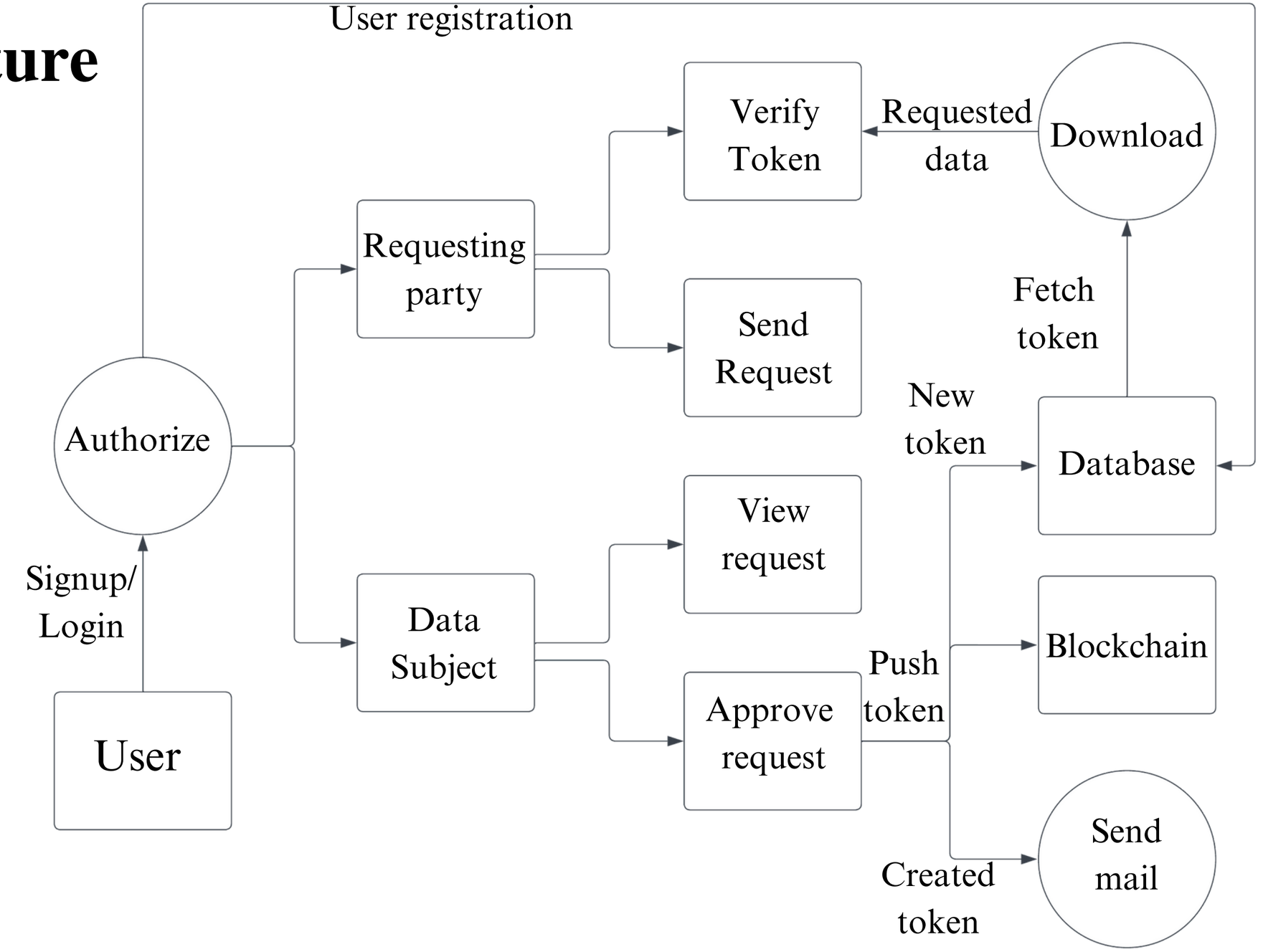
- We propose a system that allows eHealth data to be securely exchanged, with the data subject/patient always in the position of mediation.
- Tokens are issued to access data.
- Blockchain technology is used to implement a secure platform for the transaction of tokens.

Description

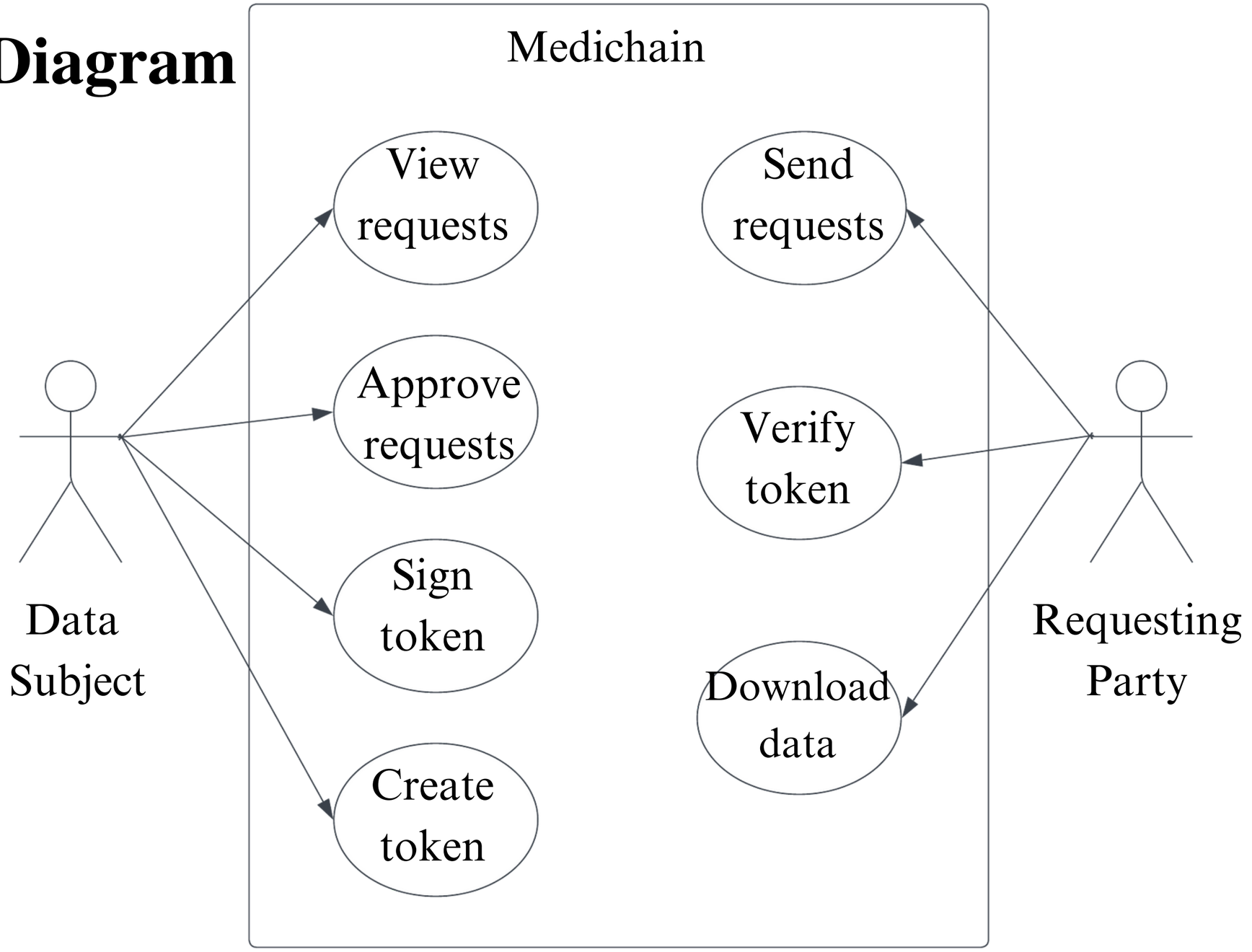
The System is divided into 4 modules/ apps:

1. Core: Used to define the base template for the frontend and also to serve as the landing page for the project.
2. Parties: Manages authentication and registration of users on the basis of user type (ie. Requesting party and data subject).
3. Chain: Contains the actions related to token creation, blockchain connection, mail sending etc.
4. Auth_server: Manages verification of token and downloading of data.

Architecture



Use Case Diagram



Testing

- Used unit testing in solidity to test the saveToken and getToken function in the solidity contract.
- Used mailtrap.io to check the mail sending functionality.

Conclusion

- Implemented a feasible system for eHealth data exchange using open protocols.
- Satisfies key requirements: auditability, confidentiality, non-repudiation, and cross-jurisdiction compatibility.
- User-friendly interface for non-technical users, facilitated by Django's built-in tools.

Future Scope

- Essential features for emergencies when timely consent is not possible such as a nominee.
- Define a data model for the stored data of the patient.
- The vulnerabilities of blockchain technology, including the Fork problem and scalability challenges, should be addressed to enhance the system's security and reliability.

References

- [1]“User-Controlled, Auditable, Cross-Jurisdiction Sharing of Healthcare Data Mediated by a Public Blockchain”-Xiaohu Zhou, Vitor Jesus, Yonghao Wang and Mark Josephs-2020
- [2]https://www.djangoproject.com/
- [3] https://dapp-world.com/course/introduction-to-blockchain-GuiT
- [4] https://dapp-world.com/course/ethereum-dapp-development-beginner-T2QL
- [5] https://www.dappuniversity.com/articles/the-ultimate-ethereum-dapp-tutorial
- [6]https://youtu.be/ZxMB6Njs3ck
- [7] https://dapp-world.com/course/introduction-to-solidity-Ynws

Thank You