Smart Contracts with Blockchain

Vidhi Patel

Student Number: C1524859

One Semester 40 credits Final year Project – CM3203

Supervisor: George Theodorakopoulos

Moderator: Philipp Reinecke

Project Description

Blockchain is the underlying technology used in cryptocurrencies, an invention by Satoshi Nakamoto. Blockchain is a distributed database which holds a series of shared records. The records are held publicly, and easily verifiable. The record series of transactions are grouped together as blocks. These records are called blocks, where each encrypted block has the history of earlier blocks and their timestamps. This is what creates the chain for the transactions to create the blockchain.

Blockchain primarily consists of a decentralised networking and verification of transactions. It is a network of nodes in which where all the computers connected to the Blockchain or a cryptocurrency have a copy of the blockchain, which is downloaded upon joining the network. Each entity who joins this network is an administrator of the Blockchain creating a peer-to-peer network. The distributed leger enables everyone to verify the transactions independently

Blockchains has many more application affecting the nature of large business, economies and governments. The most transformative application of Blockchain is Smart Contracts. Smart Contracts exploit the Blockchain Platform, conducting automated payments when the contractual conditions are met in the contract. The implication of this is that in certain types of organisation this results in less human interference reducing the cost for large organisations, maximising profitability to enable implementation of new business strategies and solutions.

In this project I am going to implement a smart contract prototype on the Blockchain platform. The project I am going to be working on is in collaboration with a company Equiniti which is financial services company which is heavily invested in researching and exploiting the Blockchain Technology.

Recently one application of Blockchain has captured my interest is the implementation of Blockchain Smart Contracts in the online e-Voting. Meanwhile, the main concern with developing an e-Voting system is that it can easily manipulated then the current system in place, with Blockchain providing us immutable series of transactions manipulation of data becomes a very problematic task.

Core Functionalities of the project is dependent on developing the smart contract where and individual can vote using the blockchain platform and have confirmation of the vote they casted. The identity of the user stays anonymous, thus only the individual will know his identity.

Desirable features, I want to implement will be data encryption to ensure data security, so it stops data modification and ensures the data integrity. I will also develop a web platform to demonstrate, how the user will be able to cast their votes.

I plan to make my program as modular as possible so that I can ensure the extensibility of the program.

Aims and Objectives

For my project, I will be using Go as my programming language to construct the prototype of Smart Contract. The Blockchain I will be using is Fabric which is part of Hyper ledger as well as, writing the Smart Contract by using ChainCode. The underlying database infrastructure I am using is Couch DB.

My Aim in this project is to be able to implement e-voting system using the Blockchain and Smart Contracts. I hope to see the feasibility of Blockchain Smart Contracts in the voting system to analyse whether it can be useful or not.

Objectives

- Outline and development of the web platform that allows the user to login to vote.
- Testing the developed Blockchain smart contract with artificial data sets which will be generated for testing purposes.
- Develop and Structure the Smart Contract using ChainCode.
- Implement the Blockchain and develop the communication protocols.
- Integrate security measures using hashes or data encryption.
- Design and develop the database to link to the Blockchain.

Assumptions

I am assuming that the system where the user registers to votes has already been developed. In this instance I am assuming that when the user registers to vote they are issued with the logging and authentication details, which they can use to verify their identity. For this system to work there needs to be a good internet connection.

Essential Functionality

- The person who participates in e-Voting needs to be able to make sure that their vote is correctly accounted for.
- The potential for the individual to change their vote and confirm the change of vote.
- The individual should only be able to vote for a single entity.
- No-one but the individual should be able to identify themselves and see who they have voted for.

Additional Functionality

- To encrypt all the data on the Blockchain
- To create a Rest API as intermediary service between the interface and the Blockchain
- To create a Website which will be the interface for the Blockchain for demonstration purposes.

Work Plan

Furthermore, I have provided a really detailed workplan, I have also setup my weekly meeting with my supervisor George Theodorakopoulos to confer my plans and progress. I have decided to use agile development throughout this project as it encourages adaptation which I think could be very beneficial for this project as it would allow me to have define my goals weekly.

Week 1 - 29/01/18 Background Research & Initial Plan

- Meeting with the supervisor to discuss the proposals for the project.
- After deciding on a proposal then to start writing up the initial Plan.
- Conduct Background Research on the technologies.

Target: Submission of the Initial Plan, completion of the background technologies and to meet with Supervisor.

Week 2 - 05/02/18 Researching Blockchains Smart Contract

- Start to investigate how to implement the Blockchain and How to initialise them.
- To explore the implementation and development of front-end development and the REST API as an intermediary service.
- Meeting with the supervisor
- To research and learn about the legal, social ethical issues with this system.
- Risk Assessment

Target: To select the resources that can aid in the implementation and support essential functionality and to have a general idea of creation of front-end development and the API.

Week 3 - 12/02/18 Prototype of User-Interface and Database Infrastructure

- Develop the Prototypes of the User Interface to better visualise the functionality of the application front-end.
- Start to learn GO programming language.
- Meeting with the supervisor.

Target: Generate the GUI prototype and the design of the API then to have a design for the database and to download and implement the Blockchain.

Week 4 - 19/02/18 Front-end development of the Blockchain and API

- Start to develop web application too add all the key features.
- Start to design the database Infrastructure and the API.
- Continue to learn Go.
- Meeting with the supervisor.

Target: To include the key features in the web application such as logging in starting to develop the database and the API design.

Week 5 - 26/02/18 Database & Blockchain development.

- Implement the database design into Couch DB.
- Research the encryption systems implementation in Blockchain.

- Meeting with the supervisor.
- Start to Implement the Blockchain
- Research about ChainCode and how to implement Smart Contract on to them.

Target: To have Blockchain partially implemented and to research of data encryption of Blocks.

Week 6 - 05/03/18 Develop the Database & Blockchain

- Meeting with the supervisor.
- Finished database implementation for the Blockchain.
- Start to develop the Blockchain.
- Start to implement the Data encryption.
- Start to implement to implement the Smart Contract

Week 7 - 12/03/18 Implement the Smart Contract using ChainCode

- Implementation of smart contract using ChainCode using Go language.
- Implement Docker into the Blockchain.
- Finish Blockchain development.
- Meeting with the supervisor to review progress.

Target: To have the API ready and the Blockchain run from the Docker container.

Week 8 - 19/03/18 Easter break (25/03/18) Implement the Smart Contract using ChainCode

- Complete the implementation of the Smart Contract.
- Populate the Blockchain with some test data.
- Start the development of the web platform & API.
- Meeting with the supervisor to review progress.

Target: complete the development of the web platform & the Smart Contract and add in the test data.

Week 9 - 26/03/18 to Week 10 – 2/04/18 Link the database to Blockchain to API to the front-end

- Finish the development of the API and the web application.
- Use the API to link the blockchain to the web application.
- Connect the database to the blockchain.
- Start to add data encryption to blockchain.

Target: To have partially encrypted and functional system.

Week 11 - 9/04/18 Testing Stage One & Start Final Report

- Start to develop the Test cases for the application
- Start to test the application using some data you generate.
- Start to write the Final report.

Target: Finish writing up the testcases, user testing for the front-end and testing for the Blockchain. Start to structure the report.

Week 12 - 16/04/18 Easter Ends Testing Stage two & Final Report

- Supervisor meeting to review the progress
- Continue the Final report.
- Meeting with the supervisor to review progress.
- Test all the core functionality is implemented and it works as it is intended to. Extend the testing the desirable features or work on developing them.

Target: Review the progress with the supervisor and make sure I am on track to finish my report and to get guidance on the system in general.

Week 13: 23/04/18 Final Report

- Finish the Final report
- Contingency

  Run the final the test and check the requirements.
  If all the functionality is added, then look to add other features.

Week 14: 30/04/18

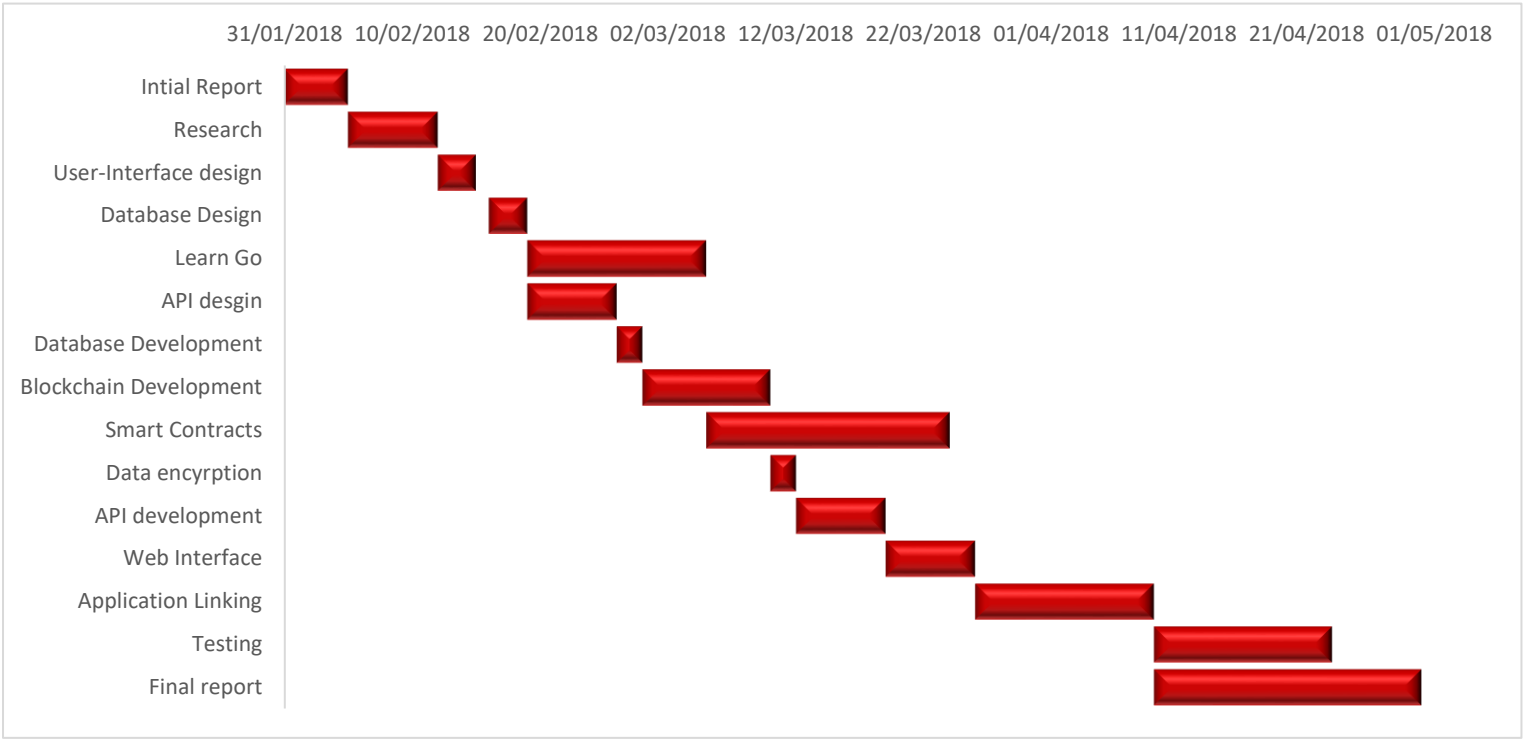
- Contingency week
- Finish the report and proof read.

Target: To have the definitive version of the report ready to submit.

Week 12: 7/05/18 Deadline

- Upload the final draft of the report.

To give a better visual representation I have created a Gantt chart of my workplan.



References

https://hbr.org/2017/01/the-truth-about-blockchain

http://uk.pcmag.com/amazon-web-services/87703/feature/blockchain-the-invisible-technology-thats-changing-the-world

https://blockgeeks.com/guides/what-is-blockchain-technology/