*School of Electronic Engineering and Computer Science*
*Queen Mary University of London*

# FINAL YEAR PROJECT DEFINITION
# 2019-20

***This project definition must be undertaken in consultation with your supervisor. The feasibility of the project should have been assessed and the project aims should be clearly defined.***
***Submission of this document implies that you have discussed the specification with your supervisor.***

**Project Title: BlockMail – A Blockchain based Email System**

**Supervisor: Professor Steve Uhlig**

**Student name: Thomas Daniel Herring**

**Student e-mail: t.d.herring@se17.qmul.ac.uk**

**Student phone number: 07960460647**

**PROJECT AIMS**:
*State the design, development or research challenge (problem) that the project aims to solve.*

To pull upon the foundations of Blockchain technology in order to create a decentralized email system which provides traceability and security through design. The primary aim is to take the processing away from a single party (such as Google or Yahoo) whom we place large amounts of trust to not misuse our data. Instead, we rely on the inherent security of Blockchain.

As Blockchain is a very new and emerging technology (circa 2008 with the release of *Bitcoin, Nakamoto, S. (2008) [online], Bitcoin: A Peer-to-Peer Electronic Cash System, Available at: https://bitcoin.org/bitcoin.pdf [Accessed 8 Oct. 2019]*. Therefore, a large amount of research will be required so that the best approach for development can be ascertained.

This also means that the project will primarily serve as a proof-of-concept that, in the future, such a system could be feasibly implemented in a secure environment, for example: communication between banks or government organizations which require a provable paper trail.

**PROJECT OBJECTIVES**

*List a series of objectives you need to achieve in order to fulfil the aims of your project.*

Mandatory**:**

- Operations which involve cryptographic functions (for example: key generation) should take place on the client-side as to ensure private keys are not exposed to any server at any time.
    - Users will sign in with their ECDSA Public and Private keys.
- A series of master nodes will be created. These will be hardcoded into the BlockMail node client and will be responsible for processing emails, or passing the emails on to other nodes for processing if they are not selected to do so. There will be 8 of these, to begin with, although this is easily expandable.
    - Each email will select a node to handle its processing. This will initially be random, but may be through a load balancing system later on in the projects life cycle.
- Emails (transactions) will be separated into “Blocks”. Blocks will be generated at a fixed time interval. This interval will start low and will increase as network usage expands.
    - Each email is broadcast to the entire network. At the end of the interval, each node will measure the size of all other nodes block (size being the number of emails in the block) and will elect the block with the biggest size to be added to the BlockMail Blockchain. In the event two have the same size, the first will be added.
- Every node on the network will know 8 other nodes.
    - Upon connecting to the network, the new node will contact master nodes in order to be directed to other nodes which will become the new nodes “neighbours”.
    - This leads to exponential email broadcasting.
- Anybody may download the BlockMail node client and contribute to the network.
- Emails to be encrypted with RSA-2048.
    - After logging in with their ECDSA Private key, they will then have to use the RSA Private key to decrypt the mail.
- Wallets (email addresses) will be using elliptic curve cryptography. Specifically, ECDSA SECP256K1, as this is what Blockchain uses, so there is already quite a lot of information available regarding it.
- The user interface will be web-based, therefore meaning that any device with a web browser with JavaScript compatibility will be able to use the system.
- The first transaction of every address on the network is to be that which contains its public key.

    - When sending an email to an address, the first thing to be looked up will be the public key of the recipient address in order to encrypt the email with their appropriate key so only they may view it.

Optional**:**

- A load balancing system which will ensure that less powerful nodes do not get overwhelmed with emails from the network.
    - A page which allows the user to see the load on each network node.
- A page which allows the user to view the live Blockchain.
    - Every email on the network.
        - Will be encrypted thus unviewable.
    - The number of times each node has been "awarded" the win for largest block.
    - Each email within the blocks.
    - Every email sent and received from each address.
- A "confirmation" system. This would report the number of blocks which have passed since each email. With each block passed, the validity of the email becomes more so.
    - An option upon sending the email to choose the number of required confirmations.

**METHODOLOGY**

*Describe the various steps that you intend to follow in order for you to achieve your project aims.*

1. The initial gathering of modules to use with the project.
2. Testing of modules. Understanding the use of these modules and how to implement them in a working system.
    a. *Sockets in JavaScript in Python and appropriate protocols.*
    b. *Elliptic Curve Cryptography.*
    c. *RSA asymmetric key encryption.*
3. Development of basic user interface to understand how to structure data for easy importation and formatting within the interface.
4. Implementation of the Blockchain system in Python.
    a. *Transaction broadcasting and communication with other nodes.*
    b. *Receiving emails ready for processing.*
    c. *Block election consensus protocol.*
5. Development of user interface.
    a. *Key authentication (login).*
    b. *Mail decryption.*
    c. *Wallet (address) generation.*
    d. *Other miscellaneous pages.*
        i. *Become a Node.*
        ii. *View Blockchain.*
        iii. *About Us.*
        iv. *Contact Us.*
6. Finalization of connections between frontend and backend.
7. Testing.

**PROJECT MI LESTONES**

*Indicate what measurable/tangible components you will produce as part of this project. This may take the form of deliverable document(s) or developmental milestones such as a working piece of software/hardware.*

| Component | | Description |
|---|---|---|
| **Implementation** | **Blockchain Network** | The primary foundations of the BlockMail network. This is to be the “distributed” part of the system. Developed in Python. |
| | **Frontend** | The user interface for the system. This is the only part of the system to be hosted at one location (rather than distributed) – although will not be problematic as secure operations will happen on client-side with JavaScript. |
| **Documentation** | **Project Definition and Plan** | This document. Provides an outline of the project and goals. |
| | **Interim Report** | A progress report on the project. Accompanies slides and a presentation to supervisor. |
| | **Draft Report** | A first try at the report for the project. Submitted to supervisor in order to gather feedback for improvement prior to final report submission. |
| | **Poster** | To be used on demo day. Summarizes BlockMail in a presentable format. |
| | **Final Report** | The primary submitted document. Gives an overview of the project, explains how all parts of it work together to give a final system. |
| | **e-Portfolio** | Weekly summary of progress on the project. |

**REQUIRED KNOWLEDGE/ SKILLS/TOOLS/RESOURCES:**

*Indicate as far as possible the skills that are required for you to undertake this project. Also include any software, hardware or other tools or resources that you believe you will need.*

Knowledge of the following languages, and associated modules to provide elliptic curve cryptography and sockets:

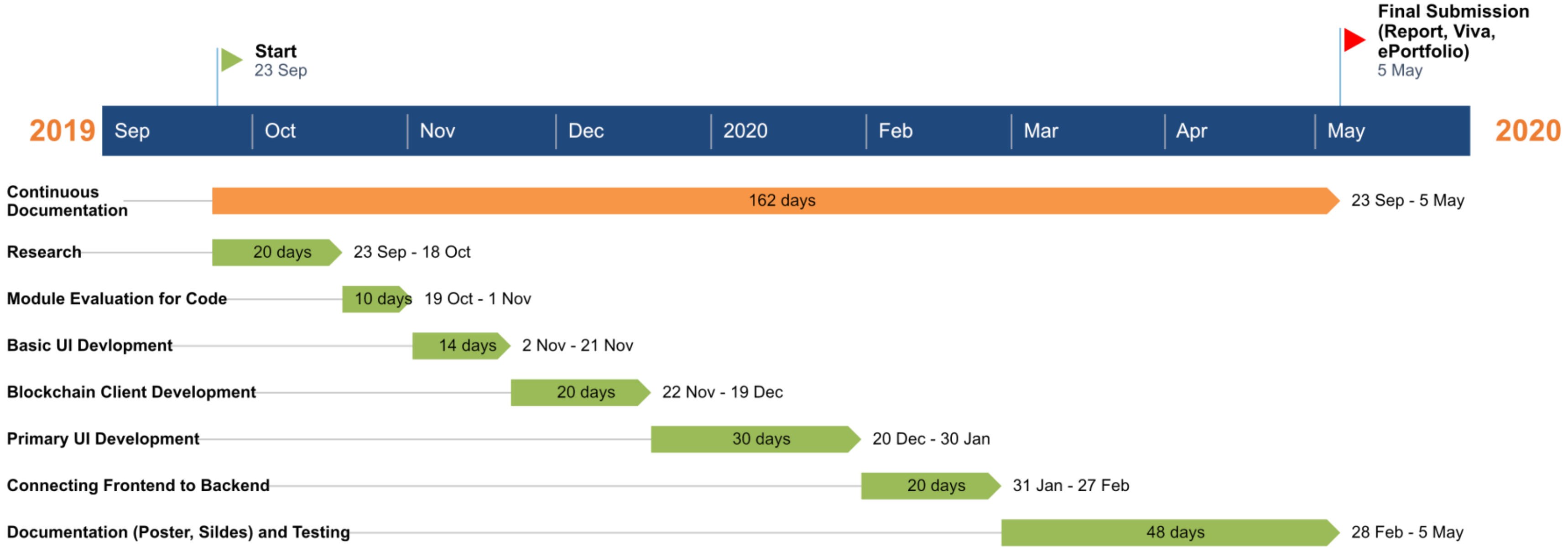
- HTML / CSS with Bootstrap.
- JavaScript.
- Python.

Some base servers will be required for the master nodes of the network. These will be virtualized in the demonstration.

As this is a software-focused project, no specific hardware is required.

## TIME PLAN

*This can be a GANTT chart submitted with this document or a list of tasks, milestones and deliverables with timings.*



BlockMail - Final Year Project Timeline