Student Number: 170146926 **Supervisor:** Professor Steve Uhlig

BlockMail

A blockchain-based Email System

by Thomas Daniel Herring

Problem Statement & Aims

Existing Solutions:

- **LedgerMail (2019)** A private blockchain-based email system. Costs money to use.
- **CryptaMail (2014)** Based on the NXTCoin blockchain. Inactive.

It is not possible to ascertain whether the systems are actually in use or just form proof of concepts. There is a gap in the marked for a free, public blockchain-based email system.

BlockMail aims to explore a new, unexplored alternative application of Blockchain, contrary to existing implementations (such as Bitcoin or Ethereum), which take a focus on cryptocurrency and smart-contracts respectively. It makes use of the benefits and characteristics of blockchain technology to provide a secure, traceable, & reliable method of communication between individuals.

About the Solution

The solution has two primary constituent elements:

- **Backend** Developed in Python3. Handles the operation of the blockchain data structure.
- **Frontend** Developed using HTML (with Bootstrap), and JavaScript (with JQuery). Provides an interface to the blockchain and allows users to create accounts and send mail.

Main Features:

- **RSA-2048** The RSA public-key cryptosystem provides the foundations of mail encryption in BlockMail. Every "email address" has a corresponding public and private key. The public key for an address is always its first transaction in the blockchain (see figure a).
- **TCP** The underlying protocol for communication between nodes. Ensures reliability of data transfer.
- **EC Keys** ECDSA SECP256K1 generates keys (email addresses) for each user. The chance of collisions is so small it's considered mathematically impossible. This is the also used by the Bitcoin network.

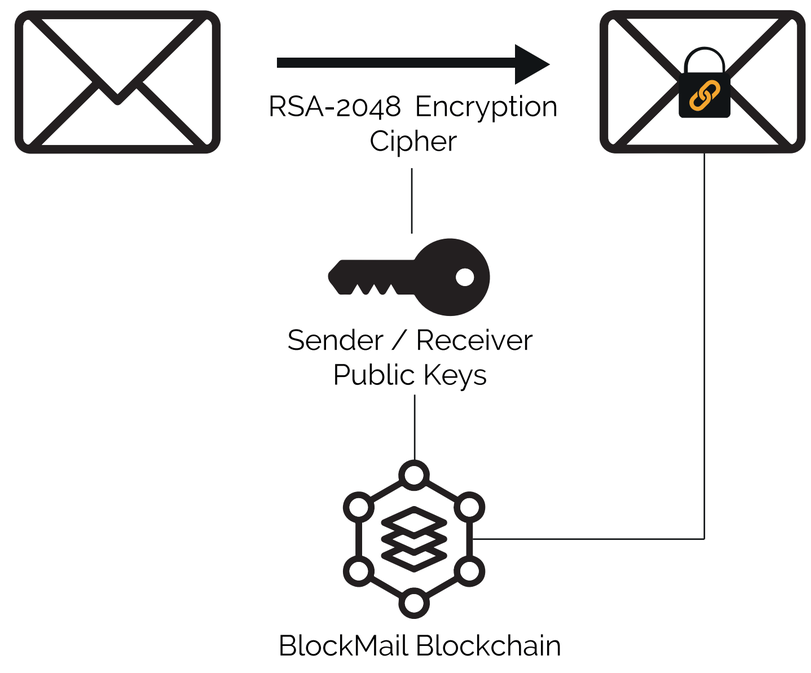
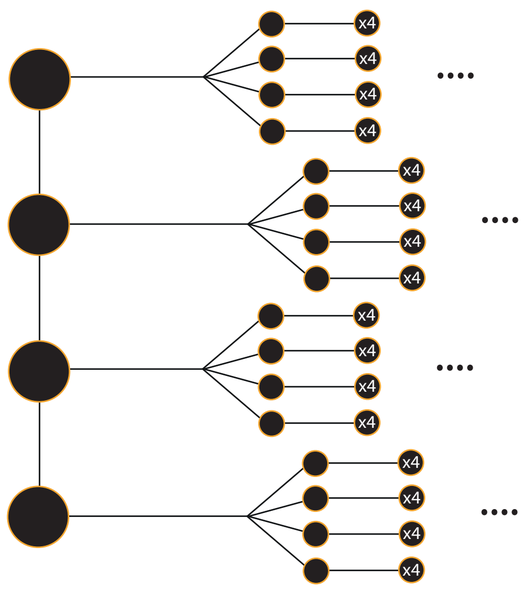


Figure a.



This figure demonstrates the BlockMail network node structure. The Master Nodes are shown on the left, which extend to regular nodes. As discussed above, each node has 4 neighbours, leading to exponential growth. That is:

If a node knows four nodes, it by proxy knows 16, 64, 256 ... 2^n.

Figure b.

Summary of Work

Throughout the development of BockMail, there were many challenges. The project was the first time I had applied many ideas which had remained purely theoretical until its conception, so required me to learn a range of new skills, both before and during development. This was achieved through a number of web tutorials, and primarily, experimentation; deciding which modules worked best for the application was something that could only be achieved by trying the plethora of options available.

The main challenge faced was the consideration of scalability. Since the BlockMail network could theoretically expand almost infinitely, certain design decisions had to be made in order to account for this. For example, exchange of node information upon initial connection is essential to node discovery, which ensures that emails are able to propagate throughout the network properly. Furthermore, considerations were made when working with the blockchain - specifically, it is handled progressively rather than being read in all at once, as to ensure the system doesn't crash as a result of RAM exhaustion.

Presentation of Results

The project has been a great sucess, meeting all of the mandatory objectives laid out in the initial report. Users can:

- **Send / Recieve Mail (to any other user on the network, securely, with RSA-2048 encryption).**
- **See a live overview of the network, including all mail flowing through it and active nodes.**
- **Generate new addresses at any time.**
- **Contribute to the network by downloading and hosting the node client on their machines.**

Among many other features...

References

World's first email service on Blockchain | Best Blockchain based Encrypted Email Service Ledgermail.io. (2019). World's first email service on Blockchain | Best Blockchain based Encrypted Email Service. [online] Available at: https://ledgermail.io/ [Accessed 25 Feb. 2020].

CryptaMail. (2019). CryptaMail. [online] Available at: http://www.cryptamail.com/ [Accessed 10 Nov. 2019].

Acknowledgements

Professor Steve Uhlig, Professor of Networks, of Queen Mary University of London. Thank you for your support throughout this project - it has proven invaluable.

For any questions, please see me at the demo day, or email me at *t.d.herring@se17.qmul.ac.uk*

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