
Bitcoin Wallet

Donal McGahon

Conor Tighe

Stephen Murphy

B.Sc.(Hons) in Software Development

APRIL 16, 2018

Final Year Project

Advised by: Gerard Harrison

Department of Computer Science and Applied Physics

Galway-Mayo Institute of Technology (GMIT)



Contents

1	Introduction	7
1.1	Specifications	8
1.1.1	Web application:	8
1.1.2	Databases:	8
2	Context	10
2.0.1	Objectives:	10
2.1	Project Links	11
2.2	Chapters Review	11
2.2.1	Methodology	11
2.2.2	Technology Review	11
2.2.3	System Design	12
2.2.4	System Evaluation	12
2.2.5	Conclusion	12
3	Methodology	13
3.1	Sprint: one	14
3.2	Sprint: Two	14
3.3	Sprint: Three	15
3.4	Sprint: Four	16
3.5	Sprint: Five	17
4	Technology Review	18
4.0.1	MEAN	18
4.0.2	Mongodb:	18
4.0.3	Angular2/5:	18
4.0.4	ExpressJs:	19
4.0.5	NodeJS:	19
4.1	Other Technologies	19
4.1.1	Docker:	19
4.1.2	Github:	19

4.1.3	Bootstrap:	20
4.1.4	Blockchain:	21
4.2	Bitcoin	21
4.2.1	The rise of the first cryptocurrency	21
4.2.2	Bitcoin: What is a bitcoin?	21
4.2.3	Blockchain: What is the blockchain?	22
4.2.4	Applications interactions with the blockchain: API's	23
4.2.5	Adobe Photoshop:	24
4.2.6	Google Fonts:	24
4.3	JavaScript	24
4.4	Robo 3T	25
4.5	Postman	26
4.6	Social Media Research	26
5	System Design	29
5.1	User Registration	29
5.1.1	Overview	29
5.1.2	In-depth	30
5.2	User Login	32
5.2.1	Overview	32
5.2.2	In-depth	32
5.3	Security	33
5.3.1	JSON Web Tokens	33
5.3.2	Auth Guards	34
5.3.3	Displaying router links	36
5.3.4	Encrypted Passwords	37
5.4	App Utility and Navigation bar	38
5.4.1	Overview	38
5.4.2	Application routing:	38
5.4.3	Tool bar aesthetics:	40
5.5	Blog Posts	42
5.5.1	Overview	42
5.5.2	Create Post	42
5.5.3	Delete Post	44
5.5.4	Like and dislike posts	45
5.5.5	Mongo Database used to store blog posts	47
5.6	Profiles and user customization	47
5.6.1	Overview	47
5.6.2	Displaying user information	48
5.6.3	Friends and networking	50
5.7	Statuses and sharing with other users	51

5.7.1	Overview	51
5.7.2	General statuses and sharing user activity	52
5.7.3	Block-chain Statuses	53
5.7.4	Wallet balance Statuses	54
5.7.5	Mining Statuses	55
5.7.6	Donation Statuses	57
5.8	Global Map and tracking user activity	60
5.8.1	Overview	60
5.8.2	Building features over google maps	61
5.8.3	Connecting the map to the external server	64
5.9	User Wallets and bitcoin features	67
5.9.1	Overview	67
5.9.2	Blockchain client and Creating a new wallet	68
5.9.3	Transactions	69
5.9.4	Converting to FIAT	70
5.10	Mlabs integration and Online interaction	74
5.10.1	Overview	74
5.10.2	Creating an online community	74
5.11	Middle-ware and Angular Services	77
5.11.1	Overview	77
5.11.2	Interfaces and heterogeneous computing	77
6	System Evaluation	81
6.1	Testing	81
6.1.1	Back-End Testing	81
6.1.2	System Testing	81
6.1.3	Browser Compatibility Testing	82
6.1.4	OS Compatibility Testing	82
6.1.5	Performance Testing	83
6.1.6	User Acceptance Testing	83
6.1.7	Limitations	84
7	Conclusion	86
7.0.1	What we learned	86
7.0.2	Future Development	87
8	Appendix	88

About this project

Abstract This project attempts to combine the cryptocurrency bitcoin and the blockchain which it uses to perform decentralized operations with the networking features offered by social media platforms. After examining the popular bitcoin wallets available online the team noticed a lack in user friendly applications for sending and storing bitcoin. On noticing this gap in the market it was decided we would create an application that would focus on efficient bitcoin and blockchain interactions while keeping each operation as user-friendly, robust and secure as possible. This application offers the user an authenticated profile for managing wallets and sharing information with the world. The application allows users to connect with a whole online community and share their recent transaction and experiences with bitcoin through a post system. Users can add friends and instantly send bitcoin to them, or use the maps feature to locate them. As bitcoin by its nature is volatile, the application pulls a range of up-to-date statistics to provide that user with complex charts, FIAT currency conversion, blockchain performance, miner activity and more.

Authors This project has been developed by fourth year students: Conor Tighe, Donal McGahon and Stephen Murphy. We developed this project for our Bachelors of Science Honours Degree in Software Development. We divided up the work into sections. Conor worked on "Bitcoin wallet integration, Blockchain utility tools, Social Media features and User connectivity". Donal worked on the authentication and security of the project. Also he worked on created a blog post feature and a cryptocurrency news feature to the application. Stephen worked on "Say what you work on here". We all collaborated on the look of the application as well as the dissertation.

Acknowledgements

We would like to acknowledge our team supervisor Gerard Harrison for support and understanding as well as all GMIT teachers for helping us to get this far.

Chapter 1

Introduction

This chapter will outline the objectives of the project along with the scope which we plan to complete those objectives in. An analysis of each of the chapters found in this dissertation along with a summary Github repository containing the project can be found below. This application will aim to satisfy the standards for a Software Development Level 8 project by surpassing the expectation of cryptocurrency wallets currently offered online. Bitcoin has received vast media coverage in the recent months because of its record high price. This brought a lot of new attention towards the technology, but to invest in or use this decentralized currency a benchmark of software and economic knowledge must be met. The members of this group have taken it upon themselves to create an application that not only allows users to use the cryptocurrency in a practical sense, but will also educate the users about the coins and offer feature relevant to members of the bitcoin community allowing them to easily interact with other owners of wallets and share blockchain statistics among each other. Proper authentication and login will be applied to the app to allowing users to easily assess there coins securely and associate relevant information to an address that will be stored in a NoSql database. Gloabal user infromation will be leased out to a server online hosted by Amazon Web Service, this is to create a complete physical separation between the vulnerable financial data stored locally and the profile data that is intended to be shared. Most of the technologies discussed here are emerging technologies that are not taught in the Software Development in GMIT.

1.1 Specifications

1.1.1 Web application:

- Receive bitcoin from external wallets at any time.
- Send bitcoin to external wallets easily and efficiently.
- Allow users to see their balance displayed clear and aesthetically.
- Represent address with QR Code.
- Google maps page show related bitcoin posts and user locations.
- FIAT conversion of major currencies to bitcoin.
- Create new user.
- Register and login system.
- Customize user profile.
- Display related bitcoin news.
- Display Bitcoin price on charts.
- Blog post feature to inform fellow users about latest cryptocurrency news or updates.
- Provide secure and robust routes for users.

1.1.2 Databases:

- Separation of wallet data from profile data.
- Local MongoDB for storing users local data.
- Local database stays true to bitcoin decentralized ideology/ doesn't expose wallet information to 3rd party.
- Local database stores status post for google maps.
- Local database stores friends list.
- Local database stores blog posts.
- Passwords encrypted on back end before stored.

- Mlabs integration to host online community.
- Mlabs can be searched with seacrh bar at top of app.
- Mlabs provides global status posts.

Chapter 2

Context

The general context of this project is a system that provides several but relative services to users of Bitcoin to help them store their Bitcoins and interact with fellow users of the cryptocurrency. Users of the bitcoin wallet will be able to store their bitcoins in our system and send and receive bitcoins to and from other users. They will be able to see their friends uses of their bitcoins through the google maps integrated solution in the project. Users can also be sure, due to the steps taking with security, that their bitcoins will be safe as the application has a strong authentication service. Users will also be able to interact through a blog post style feature that allows users to keep each other up to date with the latest news and information about bitcoin or other cryptocurrency news. Users will also be able to find the value of bitcoin in their own currency with the bitcoin currency converter feature. Users will be able to keep up to date with the latest news about cryptocurrencies with the cryptocurrency news feature and also keep the user up to date with the latest stocks and trading of cryptocurrencies with the trading feature. Each user will have their own profile page which will contain information about themselves, status's relating to their bitcoin activity and a twitter feed about cryptocurrency.

2.0.1 Objectives:

- Create a system capable of hosting interactions between members of the bitcoin community.
- Integrate a feature allowing users to have multiple wallets stored on one account, make these wallets easy to use and share.
- Strong authentication that's simple to use yet secure so users will trust us with their coins.

- Google Maps integration that will allow users to share there location or make posts on the map related to bitcoin.
- Blog post feature to allow users to interact and educate each other about the latest cryptocurrency news and information.
- News feature to keep users up to date with the latest news in the world of cryptocurrencies.
- Allow each user to easily add other users to a friends list to make transactions easier.
- Utility tools feature that allows users to complete common bitcoin tasks like currency conversion or sending bitcoin.
- Keep users up to date with the latest stocks and trading of cryptocurrencies.

2.1 Project Links

Links to this dissertation and the project repository can all be found below via the URL links:

Project Source Code Link: <https://github.com/Smurfgalway/Final-Year-Project-Applied-Diss>

Project Documentation Link: <https://github.com/Smurfgalway/Final-Year-Project-Applied-Diss/blob/master/FYP/FYP.pdf>

2.2 Chapters Review

2.2.1 Methodology

In this chapter we will cover the different development methodologies we used to develop this project, including weekly project meetings, collaboration tools used, application testing and weekly meetings with the project supervisors.

2.2.2 Technology Review

The different technologies used to design and implement the project from start to finish. The software development approaches to the tools used to create our application and the reasons for choosing the specified technologies.

2.2.3 System Design

This chapter will provide detailed information about the application system itself along with how it functions. This chapter also gives insight to code used in our project by providing code snippets explaining how we created certain features of our application.

2.2.4 System Evaluation

This chapter describes how we believe that our application is secure and robust through testing techniques that were used to test the application. We also discuss our initial objectives compared to our achieved goals, and highlight any of the limitation or opportunities in the technologies used.

2.2.5 Conclusion

This chapter summarises all we have learned and what we would have done differently throughout the whole process of our final year project. It also outlines possible future developments we could interpret into the application.

Chapter 3

Methodology

The following chapter will discuss how the development of the project was approached. Along with taking a view of how the team worked together and interacted over the course of development. Looking at chose methodology for problem solving, testing, communication and development tools utilized. This will give a keen insight into how the project was formed and came together over the development period. The methodology used for this project was a mix between Scrum and Extreme programming which are both agile ways of handling and developing a project. This mix of methodologies involved sprints where each of the team would take a task and work on it in short burst till completion while determining the best approach and practice for each of the team. Some tasks would be larger and take more time than others this is why it was not traditional Scrum or Extreme Programming but a mix of the two. As planned tasks are divided and carried out, each task contributes to the project coming together as a whole. The process was continuous with new versions of the project being delivered one after the other. The initial meeting or sprint consisted of the team meeting as a group for the first time and discussing the brief of the project that was given. Ideas were discussed technologies, Bitcoin stood out and it was decided that the project would center around it. Though following a Scrum methodology no one scrum master was chose but a idea to split the work and keep in constant contact with each other via a messaging service group chat. It was decided to meet weekly one to several times a week and discuss ideas and features for the project. When given a project supervisor the team had formed the idea to have the project be a Bitcoin wallet with more features and aims to be thought out and formed later. It was agreed with the project supervisor to meet weekly and discuss progress. The following is a Breakdown of a compilation of sprints given the reader an insight into the development of the project.

3.1 Sprint: one

The first sprint and initial project meeting after setting a main object and idea for the project, was to discuss and select the architecture that would be used going forward to develop this project. The Architecture of any project is crucial to the outcome and functionality of the project. Choosing the right architecture was a process that could not be rushed. Initially it was propose possibly to make the project using the flask framework and coding in python as the team had previous experience due to a past module. The idea was debated but it was decided due to the scale of the project and security issues it there would be other languages and frameworks better suited for developing the project.

Following this Conor introduced the team to a MEAN(MongoDB, Expressjs, Angular2/5, Nodejs) Stack having previously worked with one. The MEAN Stack offered the perfect structure and framework for the project. Each of the technologies of the MEAN giving vast amounts of scalability and room for agile development. Having a MEAN Stack set up meant that having a skeleton of the project to build off, meaning more time to develop idea's and solidify the project aims. This also offered the perfect format for group development as each member could take a component and work on developing and them separately but also working alongside each other to form the overall project. The use of API's and widgets were also crucial to the project. Widgets such as trading prices and twitter feeds. API's such as google maps and the blockchain API, in which the team had to contact those at blockchain to get permission and access to use the API.

3.2 Sprint: Two

Meeting regularly in the library and having the architecture figured out gave room discuss ideas and aims for the project. The initial idea was a Bitcoin wallet but it was felt there need to be more expansion on the idea. Instead of offering a simple Bitcoin wallet for storing the users crypto-currencies, the team saw a niche in market when it came to crypto-currencies. In most case's crypto-currencies were a jarring task for people new to the technology to get involved. There is also a very strong focus of anonymity in crypto currencies so the team wanted to offer something different. It was decided that there would be a focus put on offering a social media and community driven experience with the application. Functionality of being able to share crypto-currencies with your friends and offering non-bias educational information on Bitcoin. Another thing the team discussed during these meetings

was how there was a lack of easy to use Bitcoin wallets with intuitive UI. So it was decided to also adopt the aim of a Bitcoin wallet that could be used by anyone with a strong UI. As part of the module there was a short presentation that each group had to make in front of the class and lecturer. For this the team met in the library and did out a PowerPoint presentation detailing the technologies used and objectives of the project. Each member took a section of the presentation that they would present. Each group presenting was given 5 minutes to present along with time given afterwards to answer any questions the lecturer or peers may have. The presentation had to have a cover slide, a introduction, objectives, discuss the architecture and give a outline project plan for how this project would be achieved. Donal started the presentation introducing the audience to the project and what it would be along with the objectives that the team aimed to achieve. Stephen discussed the technologies that would be used to develop the project. Conor discussed the project plan for the development of the project and how the team was going to accomplish its goals. Finally the team answered any questions asked and why they were choosing this project.

3.3 Sprint: Three

The team continued to meet regularly and divide the work. The next plan of action was to layout the design, look and feel of the project. Stephen offered to take on some of the front end and the primary load of the aesthetics/ overall look of the project. Stephen had previous experience in graphic design. He photo-shopped mock designs and thumbnails for the project as development went on. Familiarizing himself with how the mean stack controlled its colour scheme and look through bootstrap, CSS and HTML components. A lot of research was done looking into different style-sheets and components to make the projects UI(user interface) stand out and be intuitive. The team had a working design that they wanted to achieve, sharing the creative input on how this application should look. Initially the aesthetic of the home page was chosen first. Making a 2 by 2 grid with 4 thumbnails that linked to different components of the project. To make this grid and to centre it the use of CSS sheet for the home component HTML page was employed. It was necessary for each of these thumbnails to highlight and portray exactly what they were linking to. To do so Adobe Photoshop was used for editing and graphic design.

For inspiration and templates/base images vast research via Google images was employed. Using unique key words to locate base and template images that fit the theme. Research into various crypto-currencies wallets, stock

websites and angular apps was carried out to get a feel for how this project should look. The idea was to take the best aspects from each and improve on areas where it was felt these other platforms could have done so. Conor informed Stephen about Google fonts. Google fonts is a font hub offered by Google offering a free download of a endless amount of varying fonts. This service was used to find multiple fonts to suit the projects aesthetic and varying sections and areas that needed styling. The process for picking a correct font was visibility, context, styling and how it fit for the specified section it was being used in.

3.4 Sprint: Four

Functionality of the application was the next phase of the project. Having working components that tied in together was integral for the success of the project. A divide and conquer strategy was implemented with this, with each member taking a main component of the application and working on it. Each of the team took on different sections such as security, trading/finance, blockchain/Bitcoin functionality, user interaction, user support and news. Github was a intricate part of this type of developing. Github allowed for each of the team to work on their specified work load adding to the project while hosting the whole project in a group repository. The repository was one of the first thing set up when starting the project and each of the collaborates would pull and push their changes each time progress was made. Github offered a safe place to host the code of the project along with a smart system of keeping track of changes through commits. Another advantage of Github was if there was any crossover in the sections and members of the team had changed similar parts of the project, Github would inform them to pull the changes made before pushing their new changes. There was strong communication throughout these developments helping each other with similar errors that were encountered along with sharing research and easier ways to do things that were discovered. Resources from the web such as stack overflow and docs for bootstrap, angular and the other technologies were used. While development continued it was also decided to start documenting and writing the process in the dissertation and Github project repository readme. The dissertation was being written using sharelatex and the team also hosted it on project repository for easy access. Meaning any of the members could write their changes to the dissertation and push the changed to the repository.

3.5 Sprint: Five

The final sprint saw the finalization of the development process. Each of the sections had come together with strong functionality and the application was working smoothly as a whole. Rigorous testing had been carried out frequently through the whole development of the project. This final stage was used for user acceptance testing, the team shared the project with peers, friends and family letting them use the application and taking their feedback. The feedback provided keen insight into what needed to be modified in the project and what could be improved on. Taking this feedback into the UI was updated to provide a more friendly experience using the application. The friendlist and profile options were updated to offer the best community experience for users. Testing on different platforms and hardware was carried out for scope of deployment and availability of the application. The team demoed the fully working project to their project supervisor and explained why they chose to code and develop certain functions in the way they did. Due to time constraints and lack of resources certain stretch goals/aims of the project had to be eliminated. The time remaining until the deadline was used for writing and finalizing parts of the dissertation along with polishing the application both aesthetically and functionally. Further testing was carried out on different browsers and OS' to document any differences and examine if there was a optimum build environment for the application.

Chapter 4

Technology Review

About seven to ten pages.

4.0.1 MEAN

the following four technologies are the fundamentals of a MEAN stack(Mongodb,Express,Angular,]

4.0.2 Mongodb:

MongoDB is a free, open source cross-platform database program. It is document-oriented which means it is designed for storing, retrieving, and managing document-orientated information. This is also known as semi structured data. MongoDB is a NoSQL database program and uses JSONlike documents with schemas. MongoDB is a distributed database and is designed for ease of development and scaling it also possesses satisfying scalability and flexibility. The document model maps to the objects in your application code which makes data easy to work with. Ad hoc queries, indexing, and real time aggregation provide powerful ways to access and analyse your data[1].

MongoDB provides a wide range of beneficial features for users. For file storage, large objects or files are easily stored within MongoDB. MongoDB supports an easy to use protocol for storing large files and files metadata. Incredible performance is a major goal for MongoDB and has therefore shaped much of its design[2].

4.0.3 Angular2/5:

This is a Typescript framework for JavaScript and HTML that was developed by Google. We built our front-end using Angular2 by using creating Angular

components to represent part of HTML that can be served dynamically resulting in a high performance and reliable UI, any version of angular can be used with the MEAN stack but we decided to use Angular2 as it offers new features since the first version. Angular2/5 is a complete framework and is not to be confused with its predecessor AngularJS a JavaScript library.

4.0.4 ExpressJs:

This is a web application framework used by NodeJS that allows JavaScript to communicate with a database, this is what we will be using to get the data in our app from the front-end to the database.

4.0.5 NodeJS:

This is a run time environment for executing server-side JavaScript. This allows us to easily install libraries and add-ons using the node package manager with the command line.

4.1 Other Technologies

4.1.1 Docker:

Docker allows developers to use containers to ship and deploy their applications to system and users worldwide without having to worry about performance varying from each individual operating system or machine that the application runs on. A container can be thought of as a small virtual machine with a low resource demand that allows the application to run in an environment it has been tested and trialed on allowing the application to run in an optimized state and reducing the chances of software bugs and errors appearing.

4.1.2 Github:

GitHub is a web-based Git or version control repository and Internet hosting service that was founded in 2008. GitHub provides both public and private repositories which are used to host open-source software projects. Public repositories are free to use but private repositories come at a fixed monthly cost. GitHub also provides a graphical user interface for Windows and Mac, GitHub Desktop App to help eliminate the use of the command line tools for managing project uploads and commits, but many others prefer using the

command line tool Git for this. In addition to code, Github supports the following formats and features: Documentation, issue tracking, wikis, graphs, integration directories, email notification and PDF document viewer[3].

Some sample git commands used are as follows:

- `git clone path/to/repo`
This command allows to clone any project from your github account or any publicly available project for that matter.
- `git clone path/to/repo`
This command allows to clone any project from your github account or any publicly available project for that matter.
- `git status`
Checks the status of project once it has been cloned it shows added deleted and modifies files as well as indicates which files are tracked.
- `git add .`
Add folders or files to be tracked by github so later they can be committed and pushed on to github account.
- `git commit -a`
Makes local commit of all the changes done in folder added by previous command `git add .`
- `git push origin master`
Pushes commit (`git commit -a`) to users github account on his/her account
- `git push origin +'COMMIT ID':master`
Reverts back to the state of the repo at the desired commit

4.1.3 Bootstrap:

Bootstrap is an open-source front-end framework which allows users to generate efficient UI components fast. We decided to use Bootstrap as it lets us create a dynamic application UI that will work on mobile, tablets, desktop etc.

4.1.4 Blockchain:

This application will be closely tied to the bitcoin blockchain, a technology created by an individual or group called Satoshi Nakamoto. we will use an API to directly interacted with this decentralized public ledger allowing users to receive and send bitcoin from the application.

4.2 Bitcoin

4.2.1 The rise of the first cryptocurrency

On the October 31, 2008 by a computer scientist, programmer or group of programmers under the name of Satoshi Nakamoto published the first digital currency also known as the first 'cryptocurrency'. This technology attracted the attention of many because of its decentralization, meaning governments or organizations could not intervene with the blockchain's distribution of bitcoins or control the currency that is bitcoin. Satoshi Nakamoto also published a research paper titled [?]'Bitcoin: A Peer-to-Peer Electronic Cash System' that explained how the system operates and functions. It explained how the miners power the system by solving a complicated mathematical equation using an input provided by the previous block and an input provided by the miners CPU. The miners would then announce the solution to the rest of the network so other miners could validate the new block and assuring the blockchain's integrity. Users of bitcoin did not have to rely on outside intervention from a 3rd party for their online transactions as this mathematical proof-of-work approach eliminated the need for each person involved to give their identities to the 3rd party, allowing them to send bitcoin to other addresses or freely exchange bitcoin for goods and services and allowing the exchange of value to be taken care of by the system.

4.2.2 Bitcoin: What is a bitcoin?

A bitcoin can be thought of as a digital receipt, it's really a list of locations starting at the block that generated the coin. Currently when a block is solved the miner is rewarded with a transaction fee collected from each transaction within the block along with newly generated bitcoin. This is the start of a bitcoin's lifespan and each new address the bitcoin gets sent after being generated will be recorded. Validation of the bitcoin's history and location are done using a private key and public key. When someone sends a bitcoin from one address to another the user uses their public and private key to sign the transaction and then the receiver of the bitcoins compares

the public key to the address listed on the transaction. Once everything is in place the transaction is placed in a block to be validated on the blockchain. If this process was to be represented as a design pattern it would look like the following.

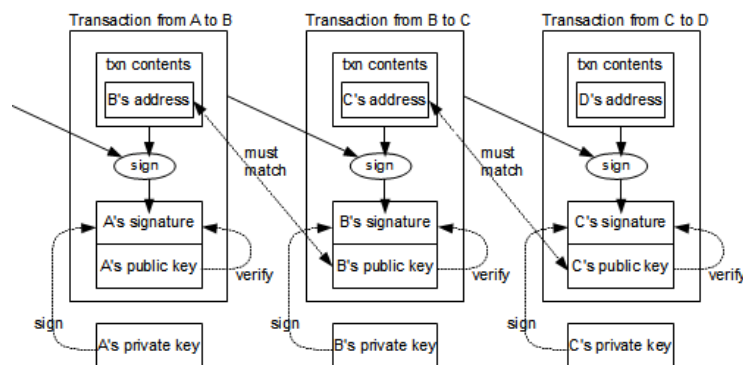


Figure 4.1: Design pattern.

If we were to represent a bitcoin as a design pattern like the above and included the first transaction of a bitcoin from the address that generated the value all the way to the most recent exchange from the previous address to the current address would be a good representation of what a bitcoin looks like. Representing value in this digital record approach appeals to many as it doesn't require overhead administration to work along with no enforcing of policy's or rules of use by an administrator. There is no physical copy of the value meaning it is a lot harder to steal or go missing, it also does not take up space in the physical world. No validating of the exchange by a 3rd party or outside source means transactions can be a lot faster compared to there fiat counterpart. The autonomous method for creating bitcoins at a set rate until a certain amount exist gives a scarcity and value to the coin as more cannot be printed.

4.2.3 Blockchain: What is the blockchain?

The block-chain is a design pattern that came about with the creation of bitcoin, this design pattern solved a problem that plagued computer scientists during the early years of the internet. The problem was how can we have people exchange services and things of value on the internet without a middleman or overseeing power having to get involved. The blockchain works by combining the collective processing power of computer systems worldwide in order

to process transactions. These machines vary from high performance computers to groups of less effective computers known as mining pools. About every 10 minutes these computers, also known to the cryptocurrency community as "miners" will collect a bunch of pending transactions and create a unsolved block. To solve the block we take the address of the previous block and combine it with a nonce which is provided by the miner's CPU power, this this is just a newly generated hash similar to the one from the previous block. Saoshi mentions in the published paper that the two hash strings are used in a series of calculations based on Adam Back's Hashcash, a algorithm created to stop denial-of-service attacks using cryptographic hashes such as SHA1, SHA256 or SHA3. The hash that is taken as the solution is the first miner to produce a SHA256 hash that has a header starting with a specified number of 0's set by the block-chains difficulty. The block-chain difficulty fluctuates depending on the rate of blocks being produced. Below is a simplified representation of what the blockchain looks like.

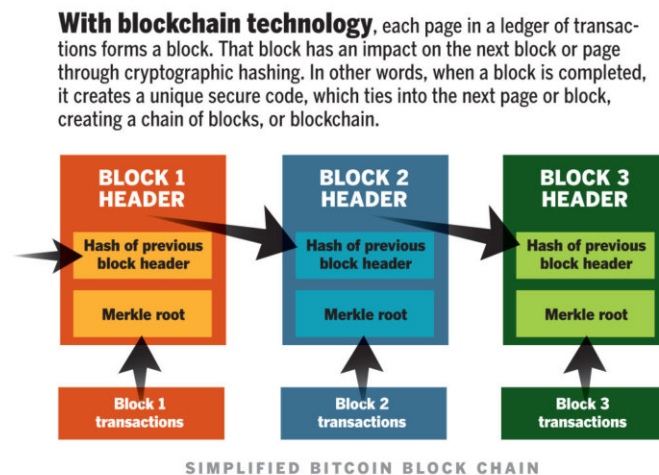


Figure 4.2: Blockchain.

4.2.4 Applications interactions with the blockchain: API's

Blockchain.info: This is a website that can be used to examine transactions and blocks that have been validated on the blockchain. You can also use this site to create an online wallet for storing your own bitcoins. You can apply for an API which will grant you the ability to integrate the blockchain into your application allowing you to create a wallet, send and receive bitcoins and get information on transactions. The API uses POST and GET calls to return JSON to the application which can be then used.

BlockCypher: This is another API that returns JSON to the application. BlockCypher is for interacting with blockchains, accessed over HTTP or HTTPS from the `api.blockcypher.com` domain. One of the major pros of using this service is that it does not only offer just the bitcoin blockchain but also Ethereum, Litecoin and Dogecoin.

Coinbase API: This API is offered by the one of the most popular exchanges coinbase. This is a well established site with an API that allows you to create wallets along with sending and receiving bitcoin. This API allows you to add widgets to your application allowing users to buy bitcoin.

4.2.5 Adobe Photoshop:

Adobe Photoshop is a photo editor developed by Adobe System for Mac and Windows operating systems. Its initial release was in 1990. Adobe Photoshop is the premier photo editor used all over the world by graphic designers. From small one man teams to huge corporations Photoshop is prolifically used. This is why I chose Photoshop when choosing something to give a custom aesthetic to our application. Photoshop offers a dynamic way to customize the looks of the icons, thumbnails and profile pictures.

4.2.6 Google Fonts:

Google Fonts is a font library API that offers over eight hundred fonts for use. It is also a interactive website that is easily browsed for finding the right font for your application or website. It helps create a dynamic UI and works across multiple platforms from mobile devices, desktop and many other devices.

4.3 JavaScript

JavaScript is a high-level, dynamic, programming language widely used alongside HTML and CSS employed by the majority of websites and supported by all modern web browsers. It is a small and lightweight language. It contains a standard library of objects, such as Date, Array, and Math and a core set of language elements such as operators, control structures, and statements[4]. The following is an example of JavaScript[5]:

```
1 // Function is called, return value will end up in x
2 var x = myFunction(4, 3);
3 // Function returns the product of a and b
4 function myFunction(a, b) {
```



```

5   return a * b;
6 }

```

4.4 Robo 3T

Robo 3T is a free open source tool used to interact with the contents of Mongo databases[6]. During the creating of the authentication and blog post feature, this tool was used a lot. It helped understanding how the mongoDB was working and what was in the databases. Below in figure 4.1: Robo 3T, an example of the applications MongoDB being viewed using Robo 3T.

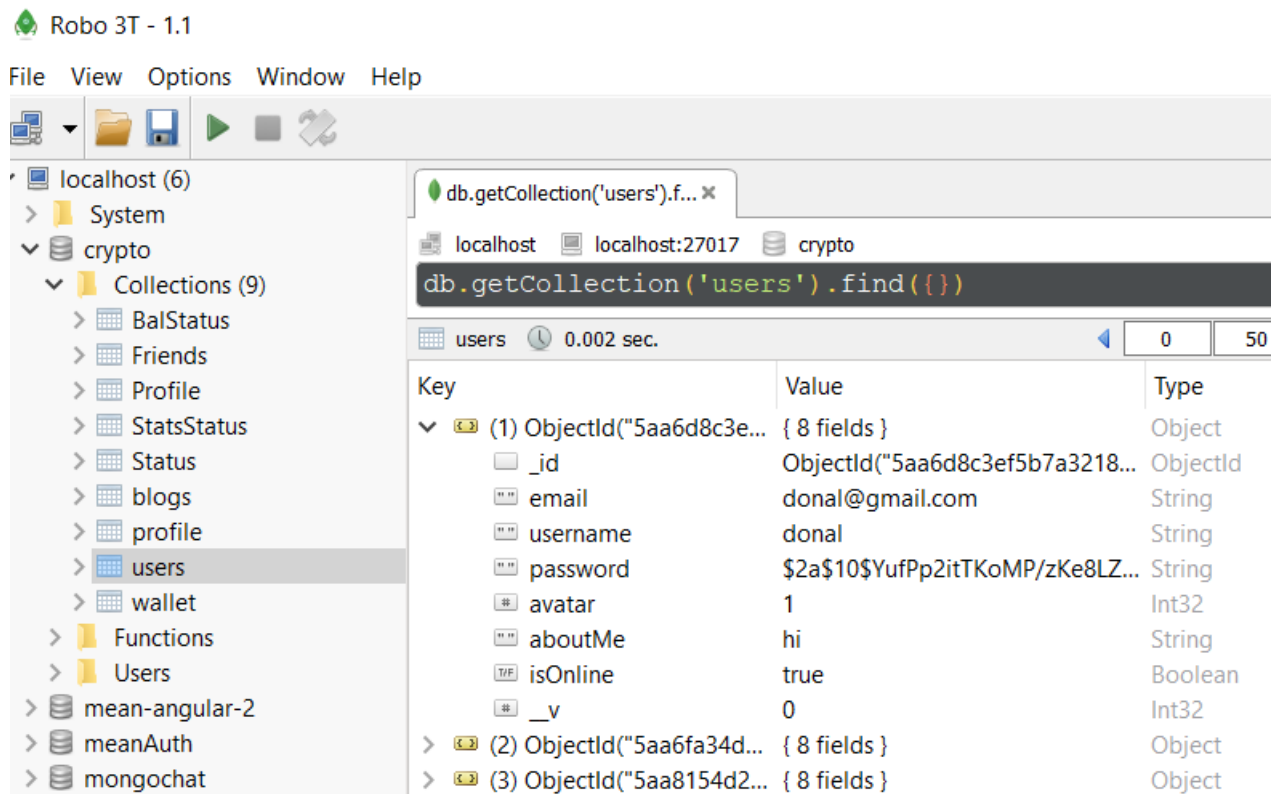


Figure 4.3: Robo 3T.

4.5 Postman

Postman is a Google Chrome app for interacting with HTTP APIs and it also has some powerful testing features. It presents you with a friendly GUI for constructing requests and reading responses[7]. Throughout many features of the application we used postman to test out parts of our application. For example, for the login feature of the application, postman was used to test the username and password would work. Below in figure 4.2: Robo 3T, shows postman testing a username and password and responding that the password is invalid.

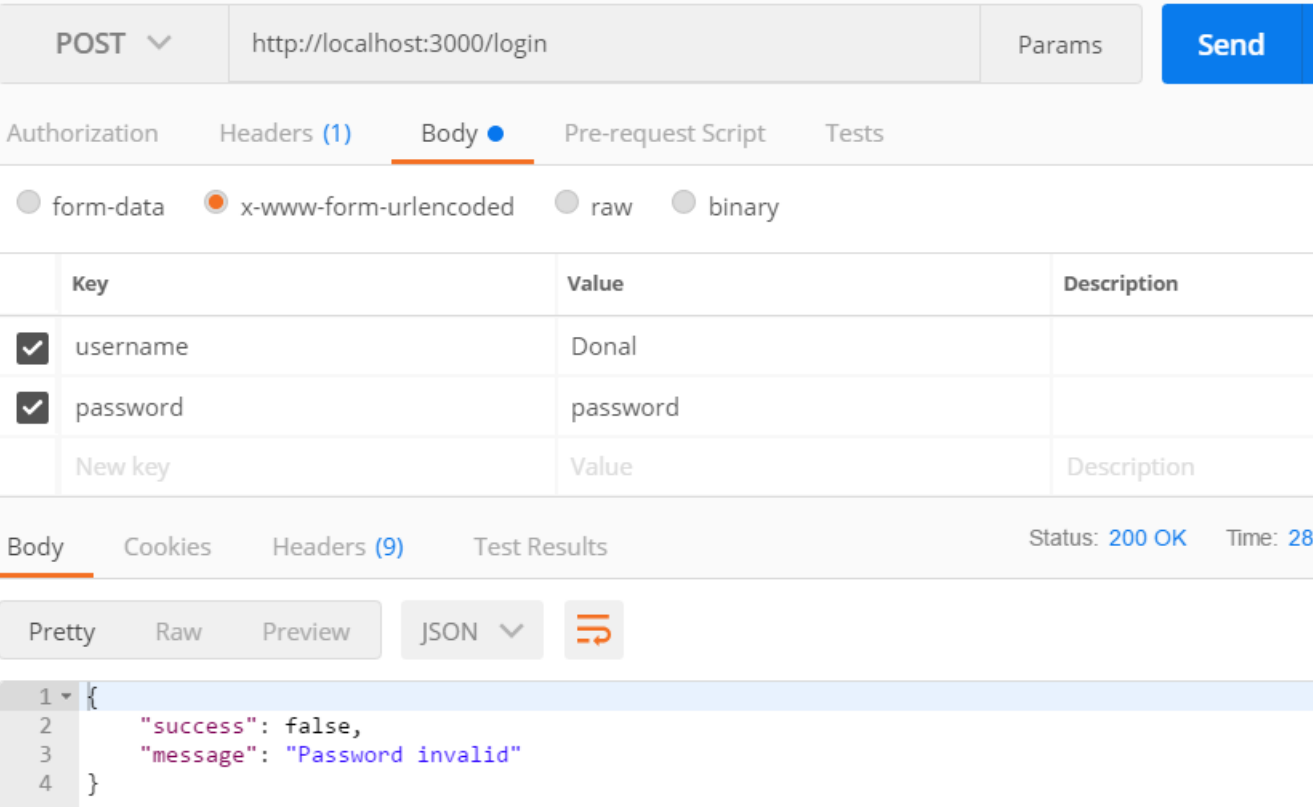


Figure 4.4: Robo 3T.

4.6 Social Media Research

Social media plays a crucial part in our everyday lives. Whether we like to give it that much importance it is the most prominent and hugely influential factors in our world right now. Whole business have been set up and

run off the back off these social media platforms, with new revenue streams being offered thanks to their existence. More and more each day people are dependant on social media for their news instead of news outlets which then informs the users views on certain topics and products. A products reception on the social media giants like Twitter or Facebook can be make or break. A couple bad tweets, posts on Facebook or rants on YouTube can result in PR nightmares for companies and loss in revenue and stock. Social media can also be used to document users trends and habits giving vital information on what the user wants to see and where the platform is heading. Facebook and Twitters ability to document users information and habits has helped them stay on top and stick with whats trending and not fall by the way side like many other social media platforms. This also leads to targeted advertisements a users search history and likes and viewings are used to inform what else they will see on a platform. For example a common thing you may have come across is: you have searched or liked something relating to a particular television show then you open up Instagram and scroll and the first advert that pops up is merchandise relating to that television show. This happens every day and with social media AI being trained to handle your own social sphere better and better your platform and overall experience can wind up completely different to those around you.

So taking of this into account and to bring a educational crypto-currency platform to the market it is necessary to research the information and trends out there in the market and on social media. As discussed previously Social Media influences the market. Public opinion will influence the success of your product and in this day and age social media is public opinion. To Launch any sort of app these days, there Has to be some sort of social media interaction or built in functionality. Every app these days lets you follow your friends and informs you what they are doing. Each app has a communication/messaging service between its users. FAQ services and support between the user and the developer is of the up most importance a lot of this is done through social media. Take air line's social medias often people can complain to these accounts and the issues will instantly be resolved. No company wants a negative image on social media as they know people will be swayed.

Public opinion on the topic that informs the app or the platform is based on is also hugely important. Taking this into account we can't just observe how our platform is interacts with social media and what people say about it on social media. We in fact have to look at the subject matter of our application, Bitcoin a violate crypto currency that everyone in the past year has an opinion on and has been talking about. Social media can literally affect the price of any crypto currency. From celebrities and social media personalities talking about and announcing their support or investment into

a currency to people talking about the negative affects or downside of Crypto-Currencies. Bitcoin and Crypto-Currencies are a new wave and almost controversial topic. The information is out there but people aren't very well informed on the topic. With differing opinions and news flooding in on social media platforms it gets very confusing for the average person to know who to listen to and what to follow..

Chapter 5

System Design

In this section, we will cover the overall design and implementation of the application with help from screenshots, code snippets and a UML diagram to visualize the structure.

5.1 User Registration

5.1.1 Overview

The user can register and create an account with the application through the register page. The register page is accessible through the opening page of the application by pressing the register button. This will bring you to the register page and will ask you for the necessary details in order to create an account. The information that's needed to create an account are as follows: Username, Email address, Password and user will be asked to reenter their password to confirm it. The user must provide this information and it is then stored to our MongoDB database. When the users password is stored to MongoDB, their password is encrypted to make the application more secure. The users information that is stored to MongoDB can then be used to Login to the application. Below is a sample of the Registration interface and user information stored in MongoDB which is being viewed through Robo 3T.

Key	Value	Type
▼ (1) ObjectId("5aa6d...	{ 8 fields }	Object
_id	ObjectId("5aa6d8c3ef5b7a...	ObjectId
email	donal@gmail.com	String
username	donal	String
password	\$2a\$10\$YufPp2itTKoMP/zK...	String

Figure 5.1: Data stored in MongoDB.

Register Page

Username

- Username is available

Email

- E-mail is available

Password

Confirm Password

Figure 5.2: Registration interface.

5.1.2 In-depth

In the HTML of the register page, I created inputs that take a type text for the users username, email address, password and confirmed password. The submit button is unusable until the user has entered all the correct information. I have ngIf statements that give back errors or success information

when the user is entering information. For example if a username is already taken, the application will return and tell the user that this username is already taken by accessing the information stored in the MongoDB database. In the `register.component.ts` file, I created validation functions to insure the correct information was being inputted by the user. For example for the password I wanted to make sure the user created a complex password, so there has to be a capital letter, small letter and a symbol. Below is the code used to achieve this:

```
1  validatePassword(controls) {
2    const regExp = new RegExp(/^(?=.*?[a-z])(?=.*?[A-Z])
   (?=.*?[\d])(?=.*?[\W]).{8,35}$/);
3    if (regExp.test(controls.value)){
4      return null;
5    } else {
6      return { 'validatePassword': true }
7    }
8  }
```

I used a similar concept for the users email and username. I also created validators to insure a correct length was applied to the username, email and passwords. I made a minimum length of 3 characters and a max length of 15 characters for the username. A minimum length of 5 characters and a max length of 30 characters for the email address. Finally a minimum length of 8 characters and a max length of 30 characters for the password. Below is the code I used to achieve this:

```
1  createForm () {
2    this.form = this.formBuilder.group({
3      username: ['', Validators.compose([
4        Validators.required,
5        Validators.minLength(3),
6        Validators.maxLength(15),
7        this.validateUsername
8      ])],
9      email: ['', Validators.compose([
10       Validators.required,
11       Validators.minLength(5),
12       Validators.maxLength(30),
13       this.validateEmail
14     ])],
15     password: ['', Validators.compose([
16       Validators.required,
17       Validators.minLength(8),
18       Validators.maxLength(30),
19       this.validatePassword
```

```
20 |         ]]],
21 |         confirm: ['', Validators.required]
22 |     }, { validator: this.matchingPasswords ('password' , '
    | confirm' )}})
23 |     }
```

5.2 User Login

5.2.1 Overview

Once a user has registered, they are navigated to the login page and can use their credentials to sign into the application. On the login page the user is greeted with two textboxes to enter their username and their password. When the user enters their information into these fields, the application checks to see if there is a registered user with these credentials in the database. If the user provides the correct credentials, a "Success" message is displayed and the user is navigated to the home page. Otherwise, if there is not, there is an error displayed at the top of the page. The error that gets displayed is based on what incorrect information the user has provided. For example, if the user has entered the incorrect username, "Username not found" will be displayed. If the username is found, but an incorrect password was given, "Password invalid" will be displayed back to the user. When a user has successfully logged into the application, they can easily logout of the application again, by clicking the Logout button on the top right hand corner of the applications nav-bar. This will log out the current user and return them to the welcome page of our application.

5.2.2 In-depth

In the HTML of the login page, I created inputs that take a type text for the users username and password. The submit button is again unusable until the user has entered all the correct information. I used ngIf statements in the HTML to inform the user that each field is required to login. In the login.component.ts file I created a form that takes in the username and password. I also have a submit function for when the user has entered their information, this submit function creates a const called user and logs the user in. Below is the function:

```
1 |     onLoginSubmit() {
2 |         // Create user object from user's input
```



```
3     const user = {  
4       username: this.form.get('username').value, // Username  
        input field  
5       password: this.form.get('password').value // Password  
        input field  
6     }
```

I have also a function that will store the user data to the local database. This function uses a function in the authservice.ts file that stores the user data. It stores the user information in the local database of the browser so I can use this information for other functions, for example displaying the logged in user in the application or checking whether or not there is a valid token in the system. The function is displayed below.

```
1   storeUserData(token, user, email) {  
2     localStorage.setItem('token', token); // Set token in  
        local storage  
3     localStorage.setItem('user', JSON.stringify(user)); //  
        Set user in local storage  
4     localStorage.setItem('email', JSON.stringify(email)); //  
        Set email in local storage  
5     this.authToken = token; // Assign token to be used  
        elsewhere  
6   }
```

5.3 Security

5.3.1 JSON Web Tokens

I used JSON web tokens to validate that a legitimate user is logged into the application. A JSON web token is an open standard that defines a compact and self-contained way for securely transmitting information between parties as a JSON object. The most common use of JSON Web Tokens is for authentication which is how I used them for this application[8]. To install JSON web tokens into our project, I had to install it using the following command in root directory of the project: `npm install jsonwebtoken --save`. I defined the `jsonwebtoken` in the `authentication.js` file where I used it. To create the token I followed instructions from the official JSON web token website [9], where it explains how to create a JSON web token and how to have the token expire after 24 hours. Below is the code used to create the web token for this application:

```
1 const token = jwt.sign({ userId: user._id }, config.secret, {  
    expiresIn: '24h' }); // Create a token for client  
2     res.json({ success: true, message: 'Success!',  
    token: token, user: { username: user.username }, email: {  
    email: user.email } }); // Return success and token to  
    frontend
```

5.3.2 Auth Guards

Angular's route guards are interfaces which can tell the router whether or not it should allow navigation to a requested route. They make this decision by looking for a true or false return value from a class which implements the given guard interface[10]. The purpose of the Auth guards for this application is to stop unregistered users accessing routes that they should not be able to. The Auth guards are used to stop unregistered users from accessing a route by using a url link or by accessing routes through the navbar of the application. For this project I created a auth.guard.ts file which is used to create the auth guards. To ensure a legitimate user is logged into the application I first have to check for this, and if they are logged in return true. Otherwise, if the user is not logged in, I return them to the login page and return false. Below is the code used to achieve this:

```
1 // Check if user is logged in  
2 if (this.authService.loggedIn()) {  
3     return true; // Return true: User is allowed to view  
    route  
4 } else {  
5     this.redirectUrl = state.url; // Grab previous url  
6     this.router.navigate(['/login']); // Return error and  
    route to login page  
7     return false; // Return false: user not authorized to  
    view page  
8 }
```

If the user is logged into the application, there is certain routes that we do not want to be able to access, for example the login or registered routes. To stop this I also created a noauth.guard.ts file. This works the same way as the auth.guard.ts file works except it does the opposite. When a user is logged in and tries to access a route they should not I check to see if the user is logged in and if they are I return them to the home page of the application

and return false. Otherwise they I return true and they can access these routes which means the user is not logged in. Below is the code used to achieve this:

```
1 if (this.authService.loggedIn()) {  
2     this.router.navigate(['/']); // Route to home  
3     return false; // User not allowed to view route  
4 } else {  
5     return true; // Return true: user is allowed to view  
    route }
```

To specify which Auth guards are to be used on which routes, I had to provide this information to the app.routing.ts file of the application. I had to go through each route of the application and check when a user is logged in, which routes they have access to and when they are logged out, the routes they have access to. An example of a user that has access to a route when logged in and logged out are seen below:

```
1 {  
2     path: 'login',  
3     component: LoginComponent,  
4     canActivate: [NotAuthGuard] // User can only view this  
    route if they are logged out  
5 },  
6 {  
7     path: 'cryptonews',  
8     component: CryptonewsComponent,  
9     canActivate: [AuthGuard] // User must be logged in to  
    view this route  
10 }
```

When a user requests a route through a URL, normally they are redirected back to the login page where they can login and then instead of returning the user to the route they originally requested they are returned to a default route, for example the home page. I changed this and instead of returning the user to a default page, I redirected the user to the page they originally requested. I done this by using the RouterStateSnapshot import from angular which allows you to take the url the user tried to access. I created a variable called redirectUrl which stores the previous URL the user tried to access. On the login component I check to see if the user was redirected and if they were, I display an error message 'You must be logged in to view that page.', and make the user log in. Once they do, they are then redirected to the saved route in the variable redirectUrl (which is saved as previousUrl in the

login.component.ts file) and sent back to that route. I also make sure to erase the content of the redirectUrl. Below is some code snippets used to achieve this in our application:

```
1  if (this.previousUrl) {
2      this.router.navigate([this.previousUrl]); //
    Redirect to page they were trying to view before
3      } else {
4          this.router.navigate(['/home']); // Navigate to
    home view
5      }
6
7  ngOnInit() {
8      // On page load, check if user was redirected to login
9      if (this.authGuard.redirectUrl) {
10         this.messageClass = 'alert alert-danger'; // Set
    error message: need to login
11         this.message = 'You must be logged in to view that
    page.'; // Set message
12         this.previousUrl = this.authGuard.redirectUrl; // Set
    the previous URL user was redirected from
13         this.authGuard.redirectUrl = undefined; // Erase
    previous URL
14     }
```

5.3.3 Displaying router links

To make sure that unwanted users could not gain access to router links they should not see, I had to ensure they were not being displayed on the applications navigation bar or elsewhere. To ensure this I had to make sure that a legitimate user was logged into the application. I created a function called `loggedIn()` in the `auth.service.ts` file. This function searches for a legitimate token in the database which is created once a user has logged into the application. The function returns true if a token is found, otherwise it will return false. Below is the function:

```
1  loggedIn() {
2      //return tokenNotExpired();
3      if (this.authToken = localStorage.getItem('token')) { // if
    there is a user token in the storage
4          return true; // return true
5      } else { // otherwise
6          return false; // return user to page } }
```

Within the applications HTML files, I went through each of the router links that are to be displayed when a user is logged in and when a user is logged out. I used ngIf statements that use the function above to check if the user is logged in or not. Below is an example of both when a user has logged in a route they can use and when the user has logged out a route they can not use.

```

1 <li *ngIf="authService.loggedIn()"><a routerLink="/global"><
    span class="glyphicon glyphicon-globe"></span> Users</a></
    li>
2 <li *ngIf="!authService.loggedIn()"><a routerLink="/register"
    ><span class="glyphicon glyphicon-user"></span> Sign Up</a
    ></li>

```

5.3.4 Encrypted Passwords

One of the most crucial parts of security is the users details. To insure maximum security I created encrypted passwords that are created when a user creates a password. These encrypted passwords are stored in the mongo database. To create these encrypted passwords I used a middleware called bcrypt-nodejs. Bcrypt is a password hashing function. Its slowness and multiple rounds ensures that an attacker must deploy massive funds and hardware to be able to crack a passwords. In addition to that per-password salts which is random data that is used as an additional input to a one-way function that "hashes" a password, an attacker will not be able to break into this without a massive amount of funds or hardware[11]. Below is some code snippets used to encrypt the passwords with also how I matched up the encrypted passwords to the passwords stored in the database:

```

1 const bcrypt = require('bcrypt-nodejs');
2
3 // Middleware to encrypt passwords
4 userSchema.pre('save', function(next) {
5   // Apply encryption
6   bcrypt.hash(this.password, null, null, (err, hash) => {
7     if (err) return next(err);
8     this.password = hash; // Apply encryption to password
9     next(); // Exit middleware
10  })
11 });
12
13 // Matching up Encrypted Passwords
14 userSchema.methods.comparePassword = function(password) {

```

```
15 |     return bcrypt.compareSync(password, this.password); //  
    |     Return comparison of login password to password in  
    |     database (true or false)  
16 | };
```

5.4 App Utility and Navigation bar

5.4.1 Overview

Easy navigation around any web service or mobile application has become more and more important in recent years with companies like Apple or Facebook dominating the market and a lot of that success being credited to their products being easy to use plus learn. The navigation bar is designed to allow users to not just move through the routes easily but to be able to access key features of our application fast regardless if they are viewing bitcoin statistics or reading friends posts. On the left side of the tool bar the focus is navigation, from left to right you can go to the welcome page, home page, your wallets, your friends list, your profile setting and then there is a drop down for support options. In the middle of the toolbar we have the search bar for searching through users. Then beside the search bar we have a navigation option to a blogs post feature between users. Following this is the two utility features allow us to convert from a choice of 20 FIAT currencies to bitcoin or send bitcoin to an address. There is the global users button to show all the users online followed by who is currently logged in.

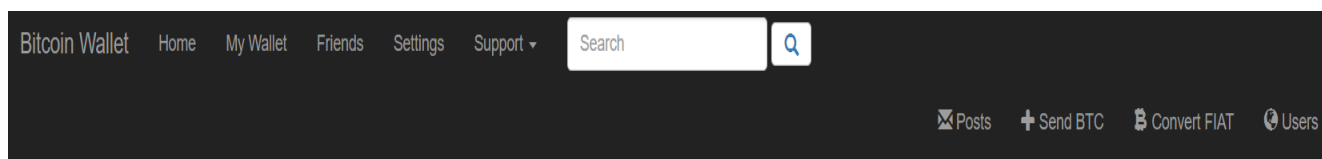


Figure 5.3: Utility bar.

5.4.2 Application routing:

The routing system available to angular2 offers a great deal of flexibility allowing us to create a reliable light-weight navigation system while still having consistent and fast system performance. Our application routing is managed by the app.routing file, here we can import our built components and then assign them to a route on the localhost. This is all made available through

the Angular2 Route and RouterModule objects in '@angular/router'. Once the routes are defined the ForRoot constructor is set for the Angular Module by passing them to it. In the app,main file we define a platformBrowserDynamic() object and set it up in a way to assure that when a user holding a authentication token refreshes the page the app will return to its last state without crashing or losing data of the current session.

```
1 const appRoutes: Routes = [  
2   {  
3     path: '',  
4     component: WelcomeComponent  
5   },  
6   {  
7     path: 'home',  
8     component: HomeComponent,  
9     canActivate: [AuthGuard] // User must be logged in to  
10    view this route  
11  },  
12  {  
13    path: 'profile',  
14    component: ProfileComponent,  
15    canActivate: [AuthGuard] // User must be logged in to  
16    view this route  
17  },  
18  {  
19    path: 'flaglocation',  
20    component: FlagComponent,  
21    canActivate: [AuthGuard] // User must be logged in to  
22    view this route  
23  },  
24  ...  
25  {  
26    path: 'cryptonews',  
27    component: CryptonewsComponent,  
28    canActivate: [AuthGuard] // User must be logged in to  
29    view this route  
30  },  
31  {  
32    path: 'blog',  
33    component: BlogComponent,  
34    canActivate: [AuthGuard] // User must be logged in to  
35    view this route  
36  },  
37  {  
38    path: 'delete-blog/:id',  
39    component: DeleteBlogComponent,  
40  },  
41  ]
```

```

37 |         canActivate: [AuthGuard] // User must be logged in to
    |         view this route
38 |     }
39 | ];

```

5.4.3 Tool bar aesthetics:

The tool bar is created by using the NavBar component from bootstrap as a starting point and then expanded on using HTML and CSS. The profile currently logged in to the app is tracked and displayed using Angular data binding. The NavBar Component contains the setting file which allows us to edit profile information and also includes the code for a FAQ page. The icons used for the navigation buttons are bootstrap glyphs, icons offered in bootstraps library that are easy to recognize symbols, increasing usability. Below are some protected buttons on right of tool bar followed by more code from the tool bar front-end:

```

1 | <ul class="nav navbar-nav navbar-right">
2 |     <li *ngIf="authService.loggedIn()"><a
    | routerLink="/blog"><span class="glyphicon glyphicon-
    | envelope"></span> Posts</a></li>
3 |     <li *ngIf="authService.loggedIn()"><a
    | routerLink="/sendbtc"><span class="glyphicon glyphicon-
    | plus"></span> Send BTC</a></li>
4 |     <li *ngIf="authService.loggedIn()"><a
    | routerLink="/convert"><span class="glyphicon glyphicon-
    | bitcoin"></span> Convert FIAT</a></li>
5 |     <li *ngIf="authService.loggedIn()"><a
    | routerLink="/global"><span class="glyphicon glyphicon-
    | globe"></span> Users</a></li>
6 |     <li *ngIf="!authService.loggedIn()"><a
    | routerLink="/register"><span class="glyphicon glyphicon-
    | user"></span> Sign Up</a></li>
7 |     <li *ngIf="!authService.loggedIn()"><a
    | routerLink="/login"><span class="glyphicon glyphicon-log-
    | in"></span> Login</a></li>
8 |     <li *ngIf="authService.loggedIn()"><a
    | routerLink="/profile"><span class="glyphicon glyphicon-
    | user"></span> {{ user.username }}</a></li>
9 |     <li *ngIf="authService.loggedIn()"><a href="#"
    | " (click)="onLogoutClick()">Logout</a></li>
10| </ul>

```


Search bar in center:

```

1 <div class="col-sm-3 col-md-3">
2   <form class="navbar-form" role="search">
3     <div class="row">
4       <input #search type="text" class="form-control"
placeholder="Search" name="q">
5       <button class="btn btn-default" type="submit" (click)
="goToSearch(search.value)"><a class="glyphicon glyphicon-
search"></a></button>
6     </div>
7   </form>
8 </div>

```

Protected buttons and dropdown on left:

```

1 <div class="navbar-header">
2 <a class="navbar-brand" routerLink="/">Bitcoin Wallet</a>
3 </div>
4 <ul class="nav navbar-nav">
5   <li *ngIf="authService.loggedIn()"><a routerLink="/home"
>Home</a></li>
6   <li *ngIf="authService.loggedIn()"><a routerLink="/
linkwallet">My Wallet</a></li>
7   <li *ngIf="authService.loggedIn()"><a routerLink="/
friends">Friends</a></li>
8   <li *ngIf="authService.loggedIn()"><a routerLink="/
settings">Settings</a></li>
9   <li class="dropdown">
10     <a *ngIf="authService.loggedIn()" class="dropdown-
toggle" data-toggle="dropdown" href="#">Support
11     <span class="caret"></span></a>
12     <ul class="dropdown-menu">
13       <li *ngIf="authService.loggedIn()"><a href="https://
github.com/Smurfgalway/Final-Year-Project-Applied-Diss/
issues">Report Issue</a></li>
14       <li *ngIf="authService.loggedIn()"><a routerLink="/
FAQ">FAQ and help</a></li>
15       <li *ngIf="authService.loggedIn()"><a href="https://
github.com/blockchain/service-my-wallet-v3">blockchain.
info API</a></li>
16     </ul>
17   </li>
18 </ul>

```

Display avatars that user can change to:

```
1 <h2>Change avatar:</h2>
2   <ul id="thumbnailsList">
3     <li *ngFor="let image of imagePaths; let i = index" >
4       
7     </li>
8   </ul>
```

5.5 Blog Posts

5.5.1 Overview

We wanted to have a way of allowing the users to interact with each other through the application. We also wanted to have a way for them to share and inform each other on the latest news or information relating to different cryptocurrencies. A good way to allow this was to create a blog feature to the application. This would allow users to interact while also informing each other about cryptocurrencies. The blog feature grants the users to create a blog post title related to any topic they wish, and to post a relatively short paragraph about the topic. Their topic is then displayed in a list from the newest to oldest blog posts on the blog post page. The user will be able to view their posts and information related to it. Other users can see these posts and interact with them by liking the post or disliking the post. By allowing the users to like and dislike posts it lets the author of the post know whether or not their post was useful to other users. If a user who has posted a blog post wants to delete their post, they can easily do so by pressing the delete button under the post they wish to delete. It will prompt the user to ensure they are sure they want to delete this post, and the user can simply press yes or no.

5.5.2 Create Post

For the user to create a post, they can simply click the new post button at the top of the blog post page. This button will navigate them to a new form that asks the user to enter a title of their blog post and then the blog post itself in the body section. Once the user has entered the information and are happy with it, the submit button and the blog post is saved and displayed on the blog post page. The user is redirected back to the blog page and

will be able to see their new post. Restrictions were added to the length of the post the users can have on the title and the body of their blog posts. This was to avoid any spanning of the blog post feature. The minimum title length is five characters and the maximum is fifty. For the body of the post the maximum is five hundred characters long and the minimum again is five characters long. To achieve this I created a form with validators. The code can be seen below:

```
1 // Function to create new blog form
2 createNewBlogForm() {
3   this.form = this.formBuilder.group({
4     title: ['', Validators.compose([
5       Validators.required,
6       Validators.maxLength(50),
7       Validators.minLength(5)
8     ])],
9     body: ['', Validators.compose([
10      Validators.required,
11      Validators.maxLength(500),
12      Validators.minLength(5)
13    ])]
14  })
15 }
```

Once the title and body of the post have been written and meet the requirements of the validators, the user then presses the submit button. The submit button works as follows, it creates a new const called blog that contains the content of the users post, which is the title and body and also it takes in the name of the logged in user of the application so we can tell which user has posted this blog. The submit button also disables the button after it is pressed and locks the form. The code is below:

```
1 // Function to submit a new blog post
2 onBlogSubmit() {
3   this.processing = true; // Disable submit button
4   this.disableFormNewBlogForm(); // Lock form
5   // Create blog object from form fields
6   const blog = {
7     title: this.form.get('title').value, // Title field
8     body: this.form.get('body').value, // Body field
9     createdBy: this.username // CreatedBy field
10  }
```

5.5.3 Delete Post

When a user wants to delete a post they can do so very easily. The user can press the delete button which is displayed directly under their post. This button will navigate them to a new page. On this page the post they wish to delete will be displayed with a confirmation, "Are you sure you would like to delete this post?". The user then has two options, they can press the yes button and delete their post or press the no button and they will be navigated back to the blog post page. To grab the post the user wants to delete and display it on the delete blog page, I create a function that takes the users post. It first checks to see if it has successfully grabbed the users post and if not it will display an error. Otherwise the function creates a blog object that can be used in the HTML of the delete page. The code can be seen below:

```

1  this.blogService.getSingleBlog(this.currentUrl.id).subscribe(
    data => {
2      // Check if request was successful
3      if (!data.success) {
4          this.messageClass = 'alert alert-danger';
5          this.message = data.message;
6      } else {
7          // Create the blog object to use in HTML
8          this.blog = {
9              title: data.blog.title,
10             body: data.blog.body,
11             createdBy: data.blog.createdBy,
12             createdAt: data.blog.createdAt
13         }
14         this.foundBlog = true;
15     }
16 });

```

To display the users posts in the HTML I simply used the object that was created, for example to display the blog post body I can use " blog.body ". The below code is the HTML that displays the users blog post on the delete page:

```

1  <div class="panel panel-primary">
2      <div class="panel-heading">
3          <h3 class="panel-title">{{ blog.title }}</h3>
4      </div>
5      <div class="panel-body">
6          {{ blog.body }}
7      </div>
8  </div>

```

```
9     <div class="panel-footer">
10     <strong>Posted by: </strong> {{ blog.createdBy.username
    }}
11     <br />
12     <strong>Date: </strong> {{ blog.createdAt | date: 'MMM dd,
    yyyy' }}
13     </div>
14 </div>
```

When the user clicks the yes button and confirms they wish to delete their blog post, the post is deleted from the blog post page and is also deleted from the database. The code used to achieve this is shown below:

```
1 deleteBlog() {
2   this.processing = true; // Disable buttons
3   // Function for DELETE request
4   this.blogService.deleteBlog(this.currentUrl.id).subscribe(
    data => {
5     // Check if delete request worked
6     if (!data.success) {
7       this.messageClass = 'alert alert-danger';
8       this.message = data.message;
9     } else {
10      this.messageClass = 'alert alert-success';
11      this.message = data.message;
12      // After two second timeout, route to blog page
13      setTimeout(() => {
14        this.router.navigate(['/blog']);
15      }, 1500);
16    }
17  });
18 }
```

5.5.4 Like and dislike posts

Each blog post has a feature that allows other users to like and dislike a post. A user cannot like or dislike their own blog post but they can like and dislike others. The number of likes and dislikes are displayed under the the logged in users blog posts. Other blog posts that do not belong to the user that is logged in, they're likes and dislikes are displayed on the corresponding buttons under there own posts. The likes and dislikes are saved to the MongoDB database and keeps track of the amount of dislikes and likes on a post. Each time the like or dislike button is pressed its amount is

increased by one. To achieve this a created two functions, one called likeBlog and the other called dislikeBlog with their number of like or dislikes being stored in the id. Below are the functions:

```

1 // Function to like blog
2 likeBlog(id){
3   this.blogService.likeBlog(id).subscribe(data => {
4     this.getAllBlogs();
5   });
6
7 }
8 // Function to dislike blog
9 dislikeBlog(id){
10  this.blogService.dislikeBlog(id).subscribe(data => {
11    this.getAllBlogs();
12  });
13 }

```

In the HTML, there is two buttons that represent the likes and another that represents the dislikes. Both of these buttons when clicked, call their corresponding function in the typescript file. For example, when the like button is clicked it calls the likeBlog(id) function displayed above and adds a like to the database and displays the new amount of like to the page. These buttons are only displayed under posts that do not belong to the user logged into the application. To achieve this I used ngIf statements that compare the name of the user logged in and the name of the user that created the blog post. If these comparisons are the same, the buttons are not displayed but if not, the buttons are displayed. Below is the code used to achieve this:

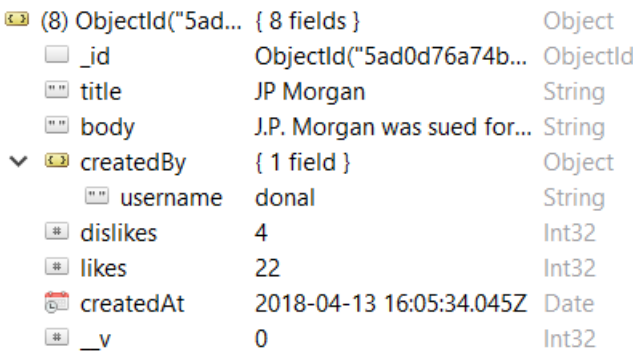
```

1 <!-- Like Button -->
2 <button type="button" name="button" class="btn btn-sm btn-
  success" (click)="likeBlog(blog._id)" *ngIf="user?.
  username !== blog.createdBy.username"><span class="
  glyphicon glyphicon-thumbs-up">&nbsp;</span>Likes: {{ blog
  .likes }}</button>
3
4 <!-- Dislike Button -->
5 <button type="button" name="button" class="btn btn-sm btn-
  warning" (click)="dislikeBlog(blog._id)" *ngIf="user?.
  username !== blog.createdBy.username"><span class="
  glyphicon glyphicon-thumbs-down">&nbsp;</span>Dislikes: {{
  blog.dislikes }}</button>

```

5.5.5 Mongo Database used to store blog posts

To store all the blog posts from all users of the application I used MongoDB. This was the best database to store the users blog posts and because I already used MongoDB to store the users account details I had experience using it. The title, body, user who created the blog post, the amount of likes and dislikes and also the time and date when the blog post was created are all stored in the mongo database. Using the application Robo 3T, you can see an example blog post that was saved to the database.



The screenshot shows a MongoDB document in Robo 3T. The document has 8 fields: `_id` (ObjectId), `title` (String), `body` (String), `createdBy` (Object), `dislikes` (Int32), `likes` (Int32), `createdAt` (Date), and `_v` (Int32). The `createdBy` field is expanded to show a `username` field with the value `donal`.

Field	Value	Type
<code>(8) ObjectId("5ad...</code>	<code>{ 8 fields }</code>	Object
<code>_id</code>	<code>ObjectId("5ad0d76a74b...</code>	ObjectId
<code>title</code>	<code>JP Morgan</code>	String
<code>body</code>	<code>J.P. Morgan was sued for...</code>	String
<code>createdBy</code>	<code>{ 1 field }</code>	Object
<code>username</code>	<code>donal</code>	String
<code>dislikes</code>	<code>4</code>	Int32
<code>likes</code>	<code>22</code>	Int32
<code>createdAt</code>	<code>2018-04-13 16:05:34.045Z</code>	Date
<code>_v</code>	<code>0</code>	Int32

Figure 5.4: Blog-Post Database.

5.6 Profiles and user customization

5.6.1 Overview

The goal of the profile and social media aspects of this project was to create a system that would allow some individuality among users along with all the benefits of a typical social media platform like networking and maintaining contact with other people. While designing with this intent we also didn't want to expose too much personal information that could make the profile venerable to an extent for security reasons as the application does involve dealing with financial assets. Each profile displays a user-name, an about me section, shows a custom image, the number of statuses they have posted, friends count, if there online there main bitcoin address, and there email. All of the details are displayed in a rich GUI for the user so the can easily see a users details and information while navigating the status posts. Profiles can be easily connected together in order to send bitcoin from on address to another, users can navigate to there friends lists in order to easily see their information.

5.6.2 Displaying user information

The profile and social interaction features are separated into multiple components as they are a major aspect of the application. If you navigate to the profile component in the Angular2 app folder you will in the app see a list of HTML, Typescript and Javascript files stored inside. This profile component uses the information entered by the user during registration and displays it on a modern GUI. The profile component reaches into the different status collections stored in mongodb and lists them on the profile page using a ngFor loop combined with status and profile services imported using the providers feature of angular2. From here they can be deleted if the user decided they no longer want that post publicly displayed on the page.

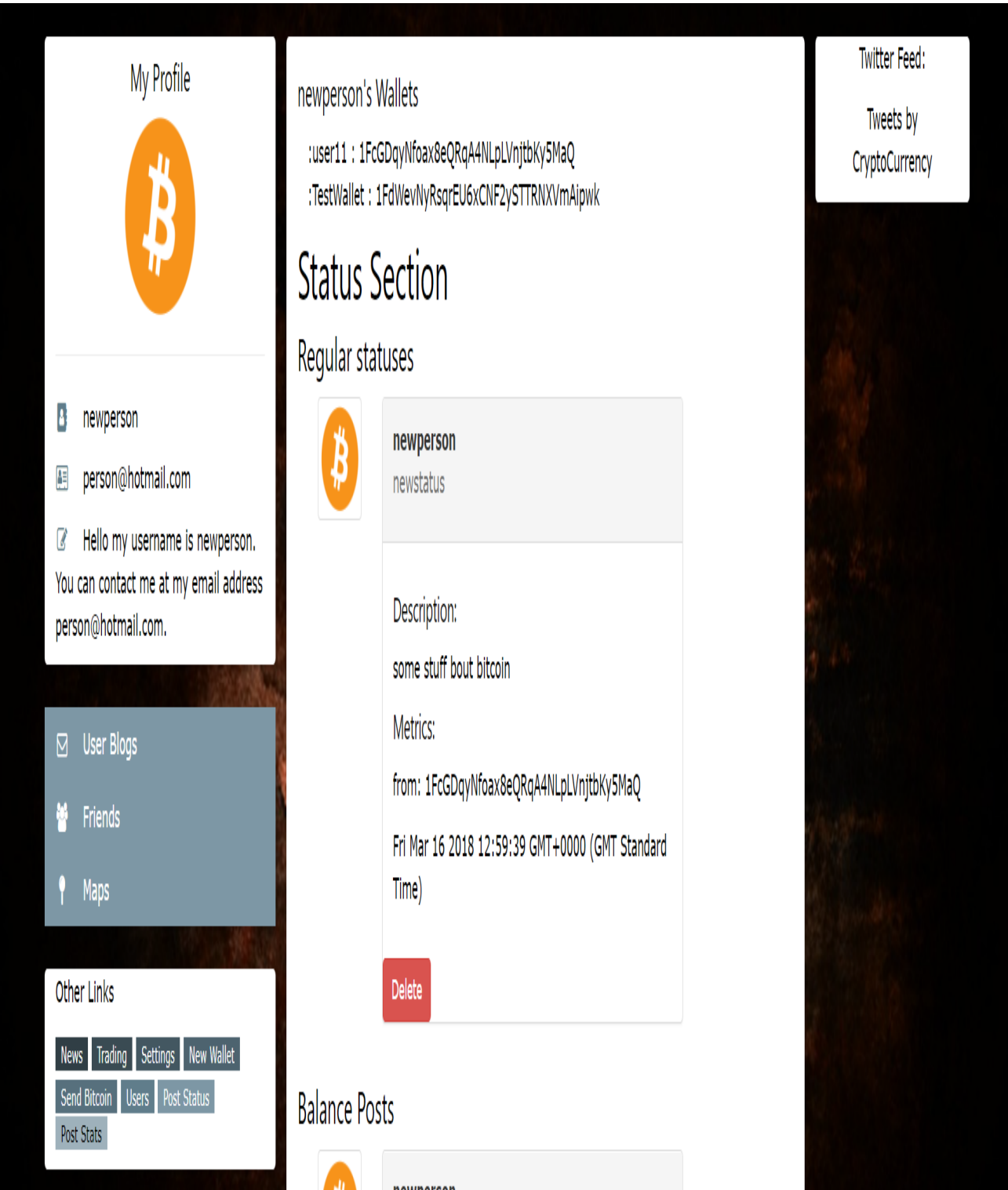


Figure 5.5: Profile.

5.6.3 Friends and networking

The friends components take all the users added to the collection of the profile friends lists and displays them with ngFor and an accordion list to expose information the logged in user cannot see about the account before they added them. The benefits of adding a user to your friends list is that there address can easily be selected for a action in another part of the app, like sending bitcoin or inspecting there address.

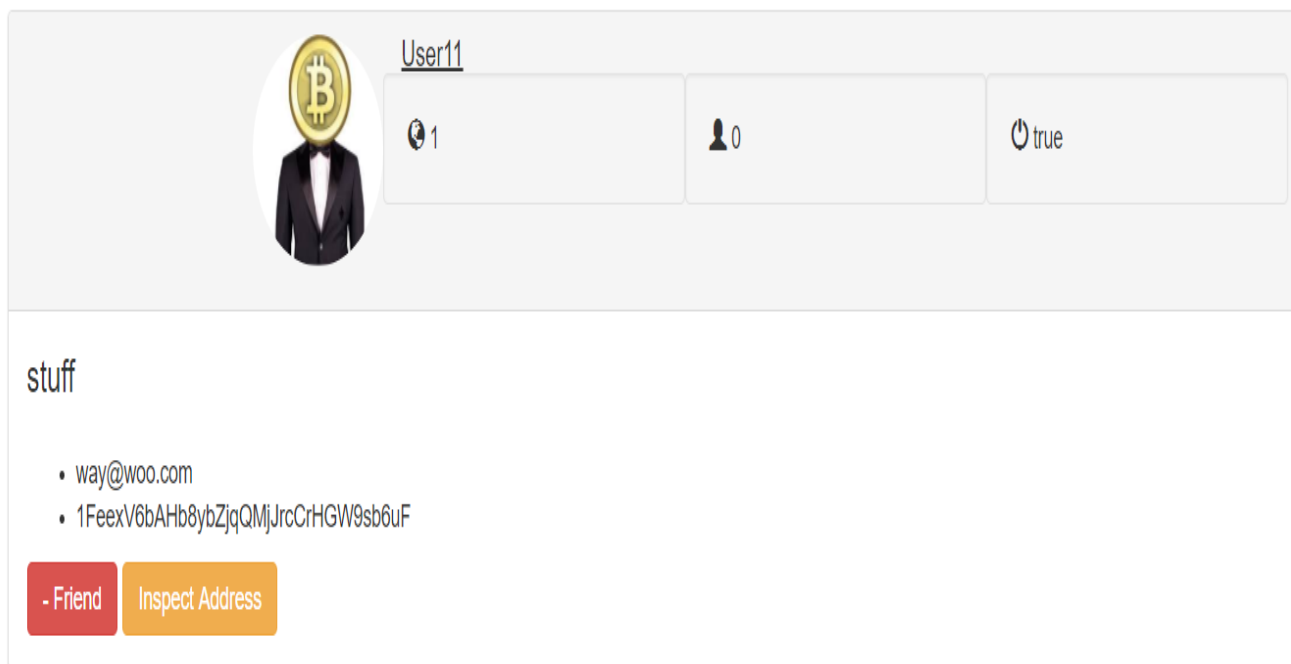


Figure 5.6: Friend list.

This service gets the logged in users profile:

```

1  this.profileService.getProfileByUsername(this.username)
2  .subscribe(
3    profiles => {
4      this.profile = profiles;
5      console.log("GET this users profile");
6    },
7    error => console.error(error)
8  );

```

This service gets the logged in users profile:

```

1      onDeleteStatus(title: string) {
2          var proceed = confirm("Do you want to continue ?");
3          if( proceed == true ){
4              this.statusService
5                  .deleteStatusWithTitle(title)
6                  .subscribe(
7                      result => alert('DELETED ' + title),
8                      error => console.error(error)
9                  );
10             }else{
11                 alert("Delete canceled!");
12                 return false;
13             }
14     }

```

This service gets the the users friends:

```

1      this.profileService.getFriends()
2          .subscribe(
3              res => {
4                  this.profiles = res;
5                  console.log("results: " + this.profiles);
6              },
7              error => console.error("error:" + error)
8          );

```

How we convert the timestamp values coming from mongodb:

```

1      Timestamp(date: number){
2          var d = new Date(date);
3          return d;
4      }

```

5.7 Statuses and sharing with other users

5.7.1 Overview

The status system is very similar to other social media feeds someone would see one twitter or facebook, except since the feature is designed around sharing information the blockchain,bitcoin and the cryptocurrency community.

People who own bitcoin or follow the technology know there is a major focus on the most recent blockchain statics and bitcoin price down to the milliseconds. This is because bitcoins price by nature is volatile and the blockchain grows at a rapid pace everyday as a result of the miners contribution and the transactions of bitcoin owners. This was the reason behind creating a feature in the application that would allow a user to post updates about there spending, bitcoin metrics, miner metrics, bitcoin value, their wallet balance, bitcoin related locations, blockchain performance and donation requests. Depending on the type of post you make the app will record your location or have you click a location on the the map to set the latitude and longitude to show the status post on the map later. These components use the blockchain.info API to pull the most recent data on bitcoin and the blockchain, these are the most up to date metric and highest quality metrics available to the public right now and they can be easily shared with friends and family thanks to this system in the wallet.

5.7.2 General statuses and sharing user activity

In the Angular 2 app folder if you navigate to the StatusComponent folder you will see all the HTML, Javascript and Typescript files that make up the status system for users. The poststatus files allow just a general post with no metadata tied to the post. All the addresses are time-stamped from the date the user posts them. The profile service is what allows the status component to access the users addresses or the friends addresses using the providers. The Angular GeoLocation is what we use to retrieve the the device latitude and longitude.

Status title

Status text:

Amount sent:

Choose a wallet

SET ADDRESS	Address	Wallet label
<div>Set</div>	1FcGDqyNfoax8eQRqA4NLpLVnjtbKy5MaQ	:user11

SET ADDRESS	Address	Wallet label
<div>Set</div>	1FdWevNyRsqrEU6xCNF2ySTTRNXVmAipwk	:TestWallet

Enter a receiving address or select an address from friends list

Receiving address:

Set target address

Figure 5.7: Status Post General.

5.7.3 Block-chain Statuses

The blockchainActivity files provide the current price values for bitcoins on the blockchain in different currency’s. The blockstats provide all the main metadata of the blockchains recent performance like blockchain mining difficulty, bitcoins mined so far and more which are shown below. This is a user-friendly way of creating discussion o the current blockchain performance and state, something commonly talked about on cryptocurrency forms.

Post about blockchain activity

Status title

Status text:

Post status

Most recent blockchain activity

Price in USD: 7946.208333333333

Hash rate: 23963896084.35904

Total fees BTC: 2884906026

BTC Mined: 196250000000

Transactions: 189392

Total BTC: 1697737500000000

Total block: 518190

Trans vol716112754.0566669

Block size: 115325941

Figure 5.8: Status Post Metrics.

5.7.4 Wallet balance Statuses

The postbal files allow users to share the balance of a particular address assigned to the user. This requires the users pin just like any other interaction with the wallet on our system and involves doing a GET request to the blockchain-client service on port 4000.

Status title

Status text:

GUID	Address	Wallet label
<div>Set</div>	1FcGDqyNfoax8eQRq44NLpLVnjtkYj5MaQ	:user11
<div>Set</div>	1FdWewNyRsqrEU6xCNF2ySTTRNXVmAipwk	:TestWallet

Click the button below to get the value of the selected address using its guid:

Wallet Password:

Wallet Password validation:

Retrive Balance

Figure 5.9: Status Post Balance.

5.7.5 Mining Statuses

The are posts about the most recent miner activity and what miner pools are currently contributing the most to that blockchain and helping solve blocks. Users can upload a post with the miner statistics below.

Post about blockchain activity

Status title

Status text:

Post status

Most recent blockchain activity

Price in USD: 7946.208333333333

Hash rate: 29963996084.35904

Total fees BTC: 2884906026

BTC Mined: 196250000000

Transactions: 189392

Total BTC: 1697737500000000

Total block: 518190

Trans vol716112754.0566669

Block size: 115325941

Figure 5.10: Status Post Location.

Status title

Status text:

Name of location:

Related phone/email/website etc.

Click to set location of intrest




Figure 5.11: Status Post Location.

5.7.6 Donation Statuses

The requestbitcoin is for donation requests to certain addresses. This could be used by a charity or a way of a shared group of individuals could raise money for a cause. It could also be used for fund raising something like a start up.

Status title

Status text:

Amount requested:

Choose a wallet

SET ADDRESS	Address	Wallet label
<input type="button" value="Set"/>	1FcGDqyNfoax8eQRqA4NLpLVnjtbKy5MaQ	:user11
<input type="button" value="Set"/>	1FdWevNyRsqrEU6xCNF2ySTTRNXVmAipwk	:TestWallet

Custom address:

Figure 5.12: Status Post Donation.

```

1  this.blockchainService.getCurrentPrice()
2    .subscribe(
3      res => {
4
5          console.log('GET from ticker');
6          console.log(res);
7          for(let price in res){
8              let value = res[price];
9              console.log("p: " + value.last);
10             this.prices.push(new Ticker(value.last, value
11             .buy, value.sell, value.symbol));
12         }
13         error => console.error("error:" + error)
14     });

```

How we get the device location:

```

1  getLocation() {
2      if (window.navigator && window.navigator.geolocation) {
3          window.navigator.geolocation.getCurrentPosition(

```

```

4         position => {
5             this.geolocationPosition = position,
6             console.log(position),
7             this.setPosition(position)
8         },
9         error => {
10             switch (error.code) {
11                 case 1:
12                     console.log('Permission Denied');
13                     break;
14                 case 2:
15                     console.log('Position Unavailable');
16                     break;
17                 case 3:
18                     console.log('Timeout');
19                     break;
20             }
21         }
22     );
23 };
24 }

```

Submit a status post example:

```

1     onStatusBalSubmit(){
2         // set current date
3         this.date = Date.now();
4         //console.log(this.username,this.date,this.title,this
5         .text,this.balance,this.lat,this.long)
6         // create new balance modal
7         const newStatusPost = new BalStatus(this.username,
8         this.date,this.title,this.text,this.balance,this.lat,this.
9         long);
10        // send modal to service
11        this.statusService.saveBalPost(newStatusPost)
12        .subscribe(
13            () => console.log('POST from status'),
14            error => console.error(error)
15        );
16    }

```

Posting a status to MongoDB:

```

1     onStatusBalSubmit(){
2         // set current date
3         this.date = Date.now();

```

```
4      //console.log(this.username,this.date,this.title,this
      .text,this.balance,this.lat,this.long)
5      // create new balance modal
6      const newStatusPost = new BalStatus(this.username,
      this.date,this.title,this.text,this.balance,this.lat,this.
      long);
7      // send modal to service
8      this.statusService.saveBalPost(newStatusPost)
9      .subscribe(
10         () => console.log('POST from status'),
11         error => console.error(error)
12     );
13 }
```

Posting a status to MongoDB:

```
1      onStatusBalSubmit(){
2          // set current date
3          this.date = Date.now();
4          //console.log(this.username,this.date,this.title,this
      .text,this.balance,this.lat,this.long)
5          // create new balance modal
6          const newStatusPost = new BalStatus(this.username,
      this.date,this.title,this.text,this.balance,this.lat,this.
      long);
7          // send modal to service
8          this.statusService.saveBalPost(newStatusPost)
9          .subscribe(
10             () => console.log('POST from status'),
11             error => console.error(error)
12         );
13     }
```

5.8 Global Map and tracking user activity

5.8.1 Overview

The inspiration of this feature was snapchats map feature which shows the users latest activity. I wanted to integrate a way so that the user could not just post about bitcoin but also use there location in the post or set a location using google maps. The map can also be used to show your friends locations depending where they set it to. All the status posts have a latitude and longitude tied to them so the appear on the map. At the bottom of the map

there is a map legend that shows users the status icons and what they mean. This feature could be used for anything from post reviews of transactions of services to events that accept bitcoin and many more as the abstract design puts the power in the users hand.

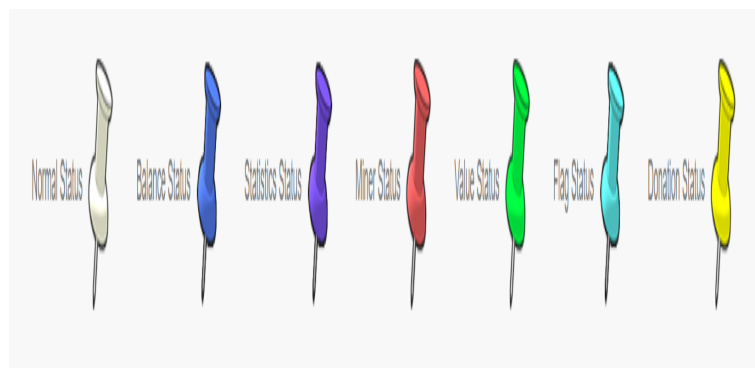


Figure 5.13: Map icons.

5.8.2 Building features over google maps

The MapsComponent folder consists of the components that makes up the status and friends location display feature of the wallet by using google maps. The menu for viewing the maps and navigating to a status post is made up by the cryptomap component files. The viewMap and viewGlobalMap components decide what is displayed on the map with viewMap using just your status posts and viewGlobalMap showing everyone online. The peopleMap component then shows the locations of people on your friends list. All the .ts files mentioned use the viewMap.component.html and the view for the map. The reason behind this design is to reinforce the concept of re usability that is so important when designing large applications or working on embedded systems. The Google maps object is what I used to generate the map within in the html files, then this is bind-ed to my own custom maps object within in the typescript files. The showmap variable is the typescript controller used to hide the status footer when on the people map by using a ngIf data binding statement.

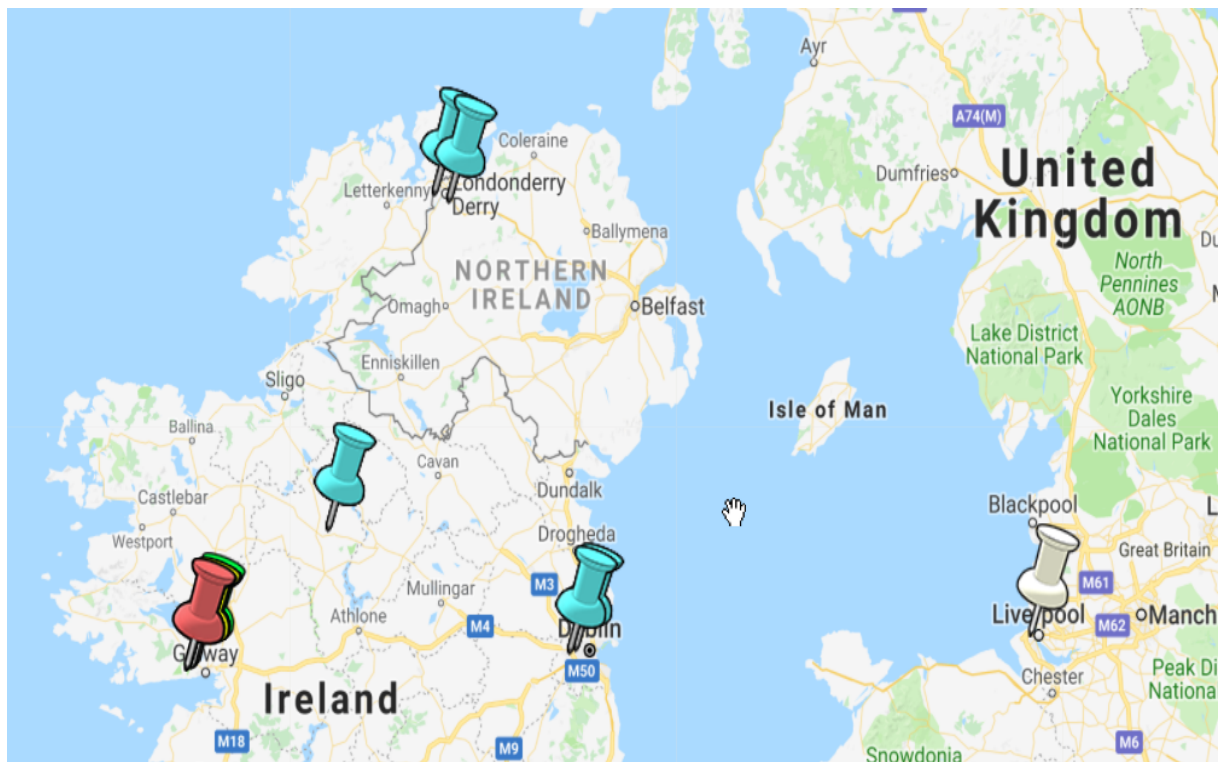


Figure 5.14: Your statuses mapped.



Figure 5.15: Global statuses.



Figure 5.16: Friends mapped.

5.8.3 Connecting the map to the external server

The Profile and Status services and what provide the vieMap component with the user's personal status posts for display and information, the PeopleMap and GlobalMap use the Profile combined with the Mlabs service to retrieve data from the mongo server hosted on amazon web service to plot online user data on those maps like the user location, their status posts or display their custom avatar. Below is the HTML and typescript object that we use to create the map. The maps used the latest lat and longs written to the user's online profile to represent them on the map.

```

1   <div id="cryptoMap" style="clear:both; height:700px;"></div>
2   </div>string}
3
4   \begin{lstlisting}
5       declare var google: any;
6
7       ...
8   
```



```

9      this.map = new google.maps.Map(document.getElementById('
cryptoMap'), {
10          zoom: 4,
11          center: {lat: 53.1424, lng: -7.6921}
12      });

```

Footer for status icon legend:

```

1      <nav *ngIf="showmap" class="navbar navbar-default sidebar
" role="navigation">
2          <div class="container-fluid">
3              <div class="collapse navbar-collapse" id="bs-sidebar-
navbar-collapse-1">
4                  <ul class="nav navbar-nav">
5                      <li><a href="#">Normal Status</a
></li>
6                      <li><a href="#">Balance Status</a
></li>
7                      <li><a href="#">Statistics Status</a></li>
8                      <li><a href="#">Miner Status</a
></li>
9                      <li><a href="#">Value Status</a
></li>
10                     <li><a href="#">Flag Status</a></
li>
11                     <li><a href="#">Donation Status</a
></li>
12                 </ul>
13             </div>
14         </div>
15 </nav>

```

Get the users we have save from the online database and added to our friends list:

```

1      this.profileService.getFriends()
2          .subscribe(
3              res => {
4                  this.profiles = res;

```

```

5           // Unpack friends profile modals
6           for (let p of this.profiles){
7               console.log(p);
8               this.plotFriends(p);
9           }
10        },
11        error => console.error("error:" + error)
12    );
13 }

```

How we plot the users avatar onto the map:

```

1 plotFriends(friend: Profile){
2     // log lat and long
3     console.log("friend location:" + friend.lat + friend.long
4 );
5
6     // create icon from friends avatar
7     var icon = {
8         url: "/app/avatars/" + friend.avatar + ".png", // url
9         scaledSize: new google.maps.Size(50, 50), // scaled
10        size
11        origin: new google.maps.Point(0,0), // origin
12        anchor: new google.maps.Point(0, 0) // anchor
13    };
14
15    // Create objects to mark on map
16    var location = {lat: friend.lat, lng: friend.long};
17    var marker = new google.maps.Marker({
18        position: location,
19        map: this.map,
20        icon: icon,
21        title: friend.username,
22    });
23    // add listener to marker that shows profile about me
24    section
25    marker.addListener('click', ()=> {
26        alert(friend.aboutMe);
27    });
28 }

```

Get the global general status posts from the online service:

```

1 this.mlabsService.getGlobalStatus()
2 .subscribe(
3     res => {
4         res.forEach(status => {

```

```
5         console.log("normal status:" + status.lat +
6         status.long);
7         var location = {lat: status.lat, lng: status.long
8         };
9         var marker = new google.maps.Marker({
10        position: location,
11        map: this.map,
12        icon: 'http://maps.google.com/mapfiles/kml/
13        pushpin/wht-pushpin.png',
14        title: status.title,
15        });
16        marker.addListener('click', ()=> {
17        alert("title:" + status.text + "\n" + status.
18        text);
19        });
20    });
21    },
22    error => console.error(error)
23  );
```

5.9 User Wallets and bitcoin features

5.9.1 Overview

One of the main features of this wallet is the ability to create and manage bitcoin address form the application. You can access the social elements of the system without needing to run the blockchain client, but to assure maximum security all exchanges of assets or interactions with wallets must pass through the blockchain-wallet-service which runs in a separate command line process. Once in operation the user can create wallets and store the GUID in mongo along with the address and a label which will be used as a ID for the wallet. We made the design decision to keep all this information on the local database only as bitcoin is a decentralized technology so all variable information should be kept on the users hard drive and only there for maximum security. We don't save the users password as this is typically a standard when creating bitcoin wallets to enforce cryptography standards. We would prefer that a user must enter their pin every time to ensure they do not leave their device vulnerable to others around them or simply accidentally sent the wrong amount by entering a typo in the BTC value box/send to the wrong person. The user has a password to the social media features that is stored and encrypted through the client, this is separate from the login password

that donal created with the user login system covered in the authentication section. Access to the pin allows users to request a new wallet, check the balance of an existing wallet and sent bitcoin to another address that is or isn't on our platform.

5.9.2 Blockchain client and Creating a new wallet

The WalletComponet folder with-in the application is what controls the front end side of the features listed above. The walletrequest.component files allow users to create wallets by contacting the block-client by using a the blockchain service passed with the Angular2/5 component promises to activate a route on the server-side code which the passed the submitted wallet details to the block chain client process for ensure its a valid request for the blockchain. The blockclient performs a security check on the values and then contacts the API which will return a new address and GUID. The new wallet details mentioned are saved to the MyWallet collection in mongodb to be used later in the application. The user can easily share the address stored but the GUID cannot be shared as this is important information that needs to be protected. Users can navigate to myWallet.components which make up a page listing the users wallets and allows them to check there balance for a selected wallet by passing a pin the user must enter each time and using a GUID that is retrieved from the backed that matched the users selected label. Users can own as many wallets as the client will allow.

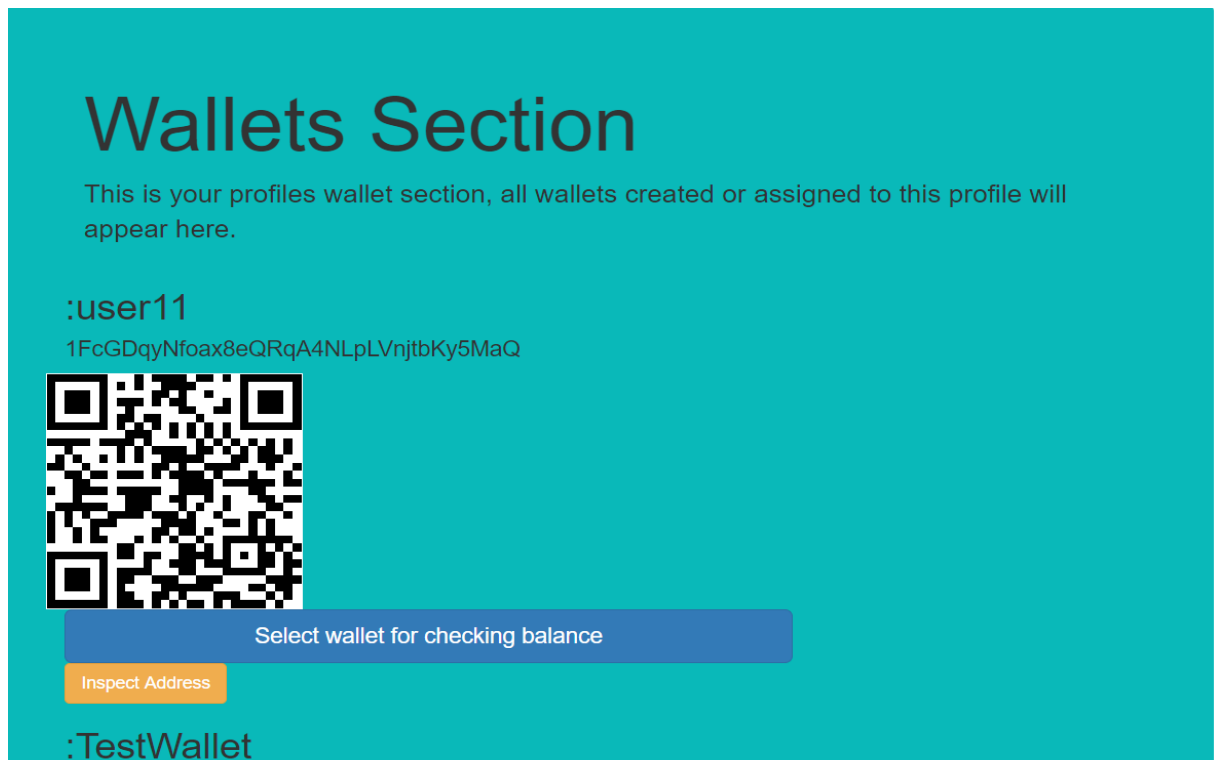


Figure 5.17: Wallets.

5.9.3 Transactions

Once the user has access to a wallet in there logged in profile they can then send BTC with the `sendbtc.components`. This is done by passing an entered pin to our block chain service along with a assigned GUID stored in mongodb that will be retrieve when the user selects the appropriate label(ID user gave to the wallet). If wallet does not have the appropriate funds to complete the transaction then the appropriate error will be returned. Linking a profile to a wallet allows you to easily send BTC to friends through the profile service after you've entered your pin twice and the validation has been complete on the front through a string comparison check.

Choose an address from your wallets

1FcGDqyNfoax8eQRqA4NLpLVnjtbKy5MaQ

Enter a target address or choose someone on your friends list

Use friends address

Enter another address below

Choose from a friends list or enter a address to send BTC to

SET ADDRESS	Address	Wallet label
<div>Set</div>	1FeexV6bAHb8ybZjqQMjJrcCrHGW9sb6uF	User11

Recieving address:

Set target address

Enter bitcoin below

BTC

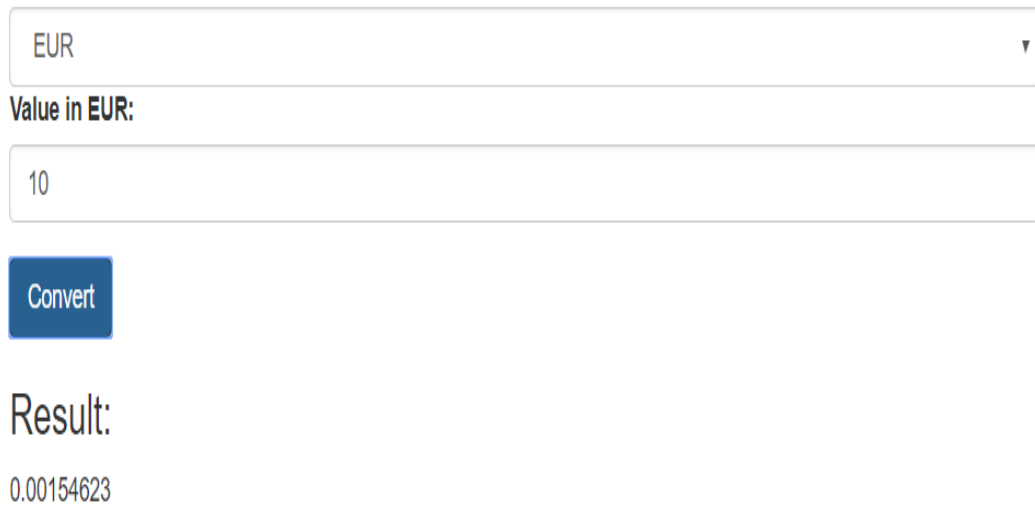
Password:

Password validation:

Figure 5.18: Send btc.

5.9.4 Converting to FIAT

The convert.components allow users to convert the value of a FIAT currency to bitcoin through the block chain service that contacts the blockchain service API which will return the latest value of the selected currency entered as a parameter when the user selects a current from the drop down.



EUR ▼

Value in EUR:

10

Convert

Result:

0.00154623

Figure 5.19: fiat conversion.

```
1  setTargetAddress(address: string){
2      console.log("address: " + address);
3      this.to = address;
4      console.log(this.to);
5  }
6
7  onSendBTC() {
8      if(this.password != this.passwordValid){
9          return alert("Passwords dont match");
10     }
11     this.blockchainService.sendBTC(this.guid,this.password,
12     this.amount,this.to)
13         .subscribe(
14             messages => this.wallets = messages,
15             error => console.error(error)
16         );
17 }
```

Initiating the stored user wallets and there friend wallets:

```
1 this.profileService.getMyWallets()
2   .subscribe(
3     response => {
4       this.wallets = response;
5       console.log(this.wallets);
6       console.log("got wallets");
7     },
8     error => console.error(error)
9 );
10
11 this.profileService.getFriends()
12   .subscribe(
13     res => {
14       console.log(res);
15       this.friends = res;
16       console.log(this.friends);
17     },
18     error => console.error("error:" + error)
19 );
```

Getting the value off an selected FIAT value:

```
1 fiatGroup: any[] = ["EUR", "USD", "JPY", "SGD", "HKD", "CAD", "NZD",
2   "AUD", "CLP", "GBP", "DKK", "SEK", "ISK", "CHF", "BRL", "RUB", "
3   PLN", "THB", "KRW", "TWD"];
4
5 onConvertFiat() {
6   if(this.fiat == null){
7     return alert("Select Fiat");
8   }
9   else if(this.value == null){
10    return alert("Enter value");
11  }
12  console.log(this.fiat);
13  console.log(this.value);
14  this.blockchainService.getValueAtTime(this.fiat, this.
15  value)
16    .subscribe(
17      message => this.result = message,
18      error => console.error(error)
19    );
20  }
21
22  updateFiat(val: string){
23    this.fiat = val;
24  }
25 }
```


Getting the balance of a selected wallet:

```
1  setGuid(gid: string){
2      console.log("guid: " + gid);
3      this.guid = gid;
4      console.log(this.guid);
5  }
6
7  onGetBal(){
8      if(this.guid == null){
9          return "GUID is empty please select an address"
10     }
11
12     if(this.pass != this.passvalid){
13         return "GUID is empty please select an address"
14     }
15
16     const balrequest = new BalanceReq(this.guid,this.pass);
17     this.blockchainService.getBalance(balrequest)
18     .subscribe(
19         messages => this.balance = messages,
20         error => console.error(error)
21     );
22 }
```

Event that creates a new wallet:

```
1  onCreateNewWallet() {
2      console.log("request triggered");
3
4      if(this.walletpass != this.passwordValid){
5          alert("pass not same");
6          return;
7      }
8
9      console.log(this.walletpass);
10     console.log(this.label);
11     const newWallet = new createWallet (this.walletpass,this.
12     label);
13
14     this.blockchainService.saveWallet(newWallet)
15     .subscribe(
16         messages => this.wallet = messages,
17         error => console.error(error)
18     );
19     console.log(this.wallet);
20 }
```

5.10 Mlabs integration and Online interaction

5.10.1 Overview

As social interaction is a major part of our application we allow the user to instantly move through out the current online profile by selecting the global option from the navigation bar, this lists all the users online. We can search through all the users on the Mlabs database from the navigation bar. you can add one of these users to your friends list by clicks this plus button. The will be added to your local database and listed on your friends list. Mlabs also provides all the online user status posts so you can view the most up to date posts from users around the world.

5.10.2 Creating an online community

Since there is a heavy focus the social aspects of this application it was important to put a lot of design and thought into the execution of user interaction. Since our applications local database was MongoDB we knew that using another NoSQL database would be a good move to ensure data integrity , system performance and minimize the middle ware used when passing the data from a local level to the online server. When looking at candidates I came across Mlabs, this is a MongoDB database that allows you to choose a cloud service provider to host the database. After talking to the others in the group(donal,stephan) we decided amazon web service would be the best option as we have experience with that provider from previous modules. Mabl's now would act as a global server for our application by storing all the online user details and post as JSON. Mlabs is conntated through the Mlabs service in Angular where that sends GET request to the appropriate ExpressJs URL route, that route then triggers this uses a process request method to prepare the information and then uses a MongoClient to contct Mblabs. The MongoClient that is uses is configured differently to the Mongoose client that we used to contact the local database and uses a login to interact with our online server. Below is and example of how I call to the service to diplay the online users along with other examples of executing tasks in code:

```
1   this.mlabsService.getGlobalUsers()
2       .subscribe(
3           res => {
4               this.profiles = res;
5               console.log("results: " + this.profiles);
```

```

6         },
7         error => console.error("error:" + error)
8     );

```

Adding a friend to your friends list:

```

1     onAddFriend(username: string, aboutMe: string, avatar:
2     number, statusCount: number,
3     friendCount: number, isOnline: Boolean, address: string,
4     email: string, lat: number, long: number){
5
6         // Create new friend modal
7         const newFriendPost = new Profile(username, aboutMe,
8         avatar, statusCount, friendCount, isOnline, address, email, lat,
9         long);
10        // Pass new friend modal to service
11        this.profileService.addFriend(newFriendPost)
12        .subscribe(
13            () => console.log('POST to friends'),
14            error => console.error(error)
15        );
16    }

```

Search users online:

```

1     this.route.queryParams.subscribe(params =>{
2         // Retrieve string from router parameters
3         this.value = params['word'];
4         console.log("Searched word: " + this.value);
5
6         // Contact MLABS service
7         this.mlabsService.searchUsers(this.value)
8         .subscribe(
9             res => {
10                 this.profiles = res;
11                 console.log("MLABS search results: " + this.
12                 profiles);
13             },
14             error => console.error("error:" + error)
15         );
16    })

```

Connecting to Mlabs

```

1     const MONGO_URL = 'mongodb://Conor:
2     softwaregroup10@ds145438.mlab.com:45438/globalusers';

```

```

2   var global = new MLABS();
3   var database;
4
5   MongoClient.connect(MONGO_URL, (err, db) => {
6       if(err){
7           console.error("Error! " + err);
8       }else{
9           console.log("Connected to online server");
10          database = db;
11      }
12  });

```

How we search MLabs from the back end:

```

1   router.get('/globalusers/:username', function(req, res,
2   next) {
3       console.log("gothere!!!");
4       var username = req.params.username;
5       console.log(username);
6
7       function processResponse(resp) {
8           console.log(resp);
9           res.json(resp);
10          console.log("process mlabs done");
11      }
12
13      var search = '.*' + username + '.*';
14      console.log(search);
15      database.collection("users").find({ username: {'
16      $regex': search, '$options' : 'i'}}).toArray(function(err,
17      result) {
18          if (err) throw err;
19          processResponse(result);
20      });
21  });

```

Get All users online from the back end:

```

1   router.get('/globalusers', function(req, res, next) {
2       console.log("gothere!!!");
3
4       function processResponse(resp) {
5           res.json(resp);
6           console.log("process mlabs done");
7       }
8

```

```
9 |     database.collection("users").find().toArray(function(err,
    |     result) {
10 |         if (err) throw err;
11 |         console.log(result);
12 |         processResponse(result);
13 |     });
14 | });
```

5.11 Middle-ware and Angular Services

5.11.1 Overview

As data and the way it is transferred to each respected component of the system is a major concern for us as protection of user information is crucial for development of a social media application given the controversy other top social media platforms have faced in the recent years. We wanted to keep the data intended to share online completely separate to the users wallet details so it seemed like a good idea to have two databases for both purposes. But in doing this we had to take into account the times we would need to display or exchange data from the respected databases or combine the two services for features in our application. This is why we have a folder known as DataModels. These are interfaces that allow us to convert objects and data from the cooperating technologies and APIs. These are used to make sense of the information received from the API requests in the Angular services and then send them to our local database or online server. They are also used to set a standard of required transaction data for sending a payment request or wallet request that the blockchain will accept while also allowing us to extend on the message variable we will use to track the transaction for the user on the machine so the response can be processed or saved. Angular2 Services are used to eliminate repetition from applications by taking care of small tasks for components, typically ones that involve retrieving or sending data.

5.11.2 Interfaces and heterogeneous computing

If you look inside the DataModels folder and look at the files you will see that each file has one or more interfaces defined depending on the goal of that file. These are called at the appropriate time to mainly process or send JSON. An Angular 2 service is simply a javascript function, along with its associated properties and methods, that can be included (via dependency injection)

into Angular 2 components. An Angular 2 service in this application are mainly used to eliminate the tasks of retrieving or sending information from technology to technology and making calls for blockchain data, bitcoin value statistics or saving/posting new information. If you go to the service folder to see the defined service files you'll notice that have been abstracted to cover certain tasks for features of the application like blockchain tasks or Mlabs tasks. If you inspect one of the files you will see that the required data models for that task are imported at the top of the service along with the required components for building an angular2 service like the Observable object and the Http, Headers, Response modules for the requests. Once @Injectable is defined over the class and the Http module is passed in the constructor we are now ready to set up the service methods. Below are some examples how we used services to interact with the blockchain and the models paired with it:

```

1      saveWallet(wallet: createWallet): Observable<any> {
2          console.log(wallet);
3          const body = JSON.stringify(wallet);
4          console.log(body);
5          const headers = new Headers({'Content-Type': '
application/json'});
6          return this.http.post('http://localhost:3000/
newWallet', body, {headers: headers});
7      }
8
9      getCurrentPrice() {
10         console.log("contacting ticker");
11         return this.http.get('https://blockchain.info/
ticker')
12             .map(response => response.json() as Ticker[])
13             .catch(handleError);
14     }
15
16     getValueAtTime(fiat:string, val: string) {
17         console.log("contacting ticker");
18         return this.http.get('https://blockchain.info/
tobtc?currency=' + fiat + '&value=' + val)
19             .map(response => response.json() as Ticker[])
20             .catch(handleError);
21     }
22
23     getBlockchainStats() {
24         console.log("contacting stats");
25         return this.http.get('https://api.blockchain.info
/stats?cors=true')
26             .map(response => response.json() as Stats[])
27             .catch(handleError);

```

```

28     }
29
30     getPools() {
31         console.log("contacting pools");
32         return this.http.get('https://api.blockchain.info
/pools?cors=true&timespan=5days')
33             .map(response => response.json() as Pools[])
34             .catch(handleError);
35     }
36
37     getBalance(balreq: BalanceReq): Observable<any> {
38         console.log(balreq);
39         const body = JSON.stringify(balreq);
40         console.log(body);
41         const headers = new Headers({'Content-Type': '
application/json'});
42         return this.http.post('http://localhost:3000/
Wallet/balance', body, {headers: headers}).map( (data:
Response) => {
43             console.log(data.json());
44             const extracted = data.json();
45             const msgArray: Balance[] = [];
46             var message;
47             console.log("fixed: " + extracted.balance);
48             message = extracted.balance;
49             return message;
50         });
51     }
52
53     sendBTC(guid : string, pass : string, amount: string,
to: string) {
54         console.log("sending bitcoin");
55         return this.http.get('https://api.blockchain.info
/merchant/' + guid + '/payment?password=' + pass + '&
amount=' + amount + '&to=' + to)
56             .map(response => response.json() as Payment[])
57             .catch(handleError);
58     }
59 }

```

Data Model for blockchain value ticker interface and post ticker status interface:

```

1
2     export class Ticker {
3         constructor(
4             public last: string,
5             public buy: string,

```

```
6         public sell: string,  
7         public symbol: string) {}  
8     }  
9  
10    export class PostTicker {  
11        constructor(  
12            public username: string,  
13            public date: number,  
14            public title: string,  
15            public text: string,  
16            public last: number,  
17            public buy: number,  
18            public sell: number,  
19            public symbol: string,  
20            public lat: number,  
21            public long: number) {}  
22    }
```

Data Model for payment response:

```
1 export class Payment {  
2     constructor(  
3         public to: string,  
4         public from: number,  
5         public amounts: number,  
6         public fees: number,  
7         public txid: number,  
8         public success: number) {}  
9 }
```

Data Model create wallet request:

```
1 export class Wallet {  
2     constructor(  
3         public guid: string,  
4         public address: string,  
5         public label: string) {}  
6 }
```


Chapter 6

System Evaluation

The following chapter will talk through the testing and evaluation process of the project. Taking a look at the testing processes and steps taken while developing this project. Along with taking note of any constraint's or drawbacks on the project. Then looking at where improvements could have been made to better the finished product.

6.1 Testing

6.1.1 Back-End Testing

Back-end testing is hugely important while developing any kind of application. It is vital to know that anything from the front end that the user is interacting with that deals with storing data is being stored to the database. In the case of this project while working with MongoDB it was necessary throughout multiple stages of the project to check that data and information was being stored correctly in the database. Writing dummy data and post was important in this as it would give an idea of what was storing. To ensure it wasn't just session based storing. The use of Robo 3T a GUI application for MongoDB was utilized. This made it much easier to see if data was in fact being stored correctly to the Mongo database.

6.1.2 System Testing

It is important to carry out System Testing, ensuring each node of the system enters acts correctly together and the system as an entirety meets requirements. Having used a MEAN Stack for this project system testing was a regular part of the project. To even run the project correctly must ensure

that the MEAN stack is working correctly and each part is interacting correctly together. In doing this it meant having to run the MongoDB first in command line then in a separate command line run the node server instance on a local host. If there was any error in the Angular code the project would not run correctly and be stuck at a loading screen. If there were any errors or issues loading it would mean having to inspect the element and use the browsers console to see what was causing the errors. While the project was running HTML and CSS files within the project could be changed on the file and live tested. Whereas when anything was changed in a TypeScript file would mean having to kill the instance of the server running on the console and recompile the angular files. While compiling if there were any errors the console would save the new changes to the files but alert us to errors on the command line.

6.1.3 Browser Compatibility Testing

Having an app be available on multiple platforms and work across different browser is vital for user adoption of the app. This is why we carried out multiple test cases across the different browsers ensuring the application was capable of running on any the user desired. Running a local host on each of the browsers and documenting any differences or errors was a huge part of this. Selenium an automated suite of tools was chosen to test web browsers, in particular Firefox which has built in extension for selenium. Multiple test cases were run, such as pages loading correctly, link testing, data entry testing, correct loading of APIs and widgets etc. These test cases proved to be very useful as it identified any errors any of the pages might have. Along with this it was important to check that bootstrap was working correctly across the different browsers and if anything wasn't to scale or if visibility was poor.

6.1.4 OS Compatibility Testing

Like discussed in like discussed in the browser compatibility testing section, It is very important to offer as much choice to the user as possible when developing an application. The fewer systems an application can run on the correlates to fewer users. This is why it was important to test the application on different operating systems to insure the maximum amount of users for the application can be reached. Virtual machines were employed to achieve this. Having used VM Ware in the past for previous college assignments, it was decided it would be the chose virtual machine software for testing. Making instances of virtual machines of a macOS build and a Ubuntu(Linux) build.

After installing the MEAN Stack and other dependencies for the project to both virtual machines it was time to run test cases. All test cases that had been run on the windows build of the project where run on each of the separate os builds. It was important to ensure that the project is versatile enough to work across every platform it could.

6.1.5 Performance Testing

How well a application can perform is crucial as it will affect. If an application is sluggish, buggy and doesn't run correctly it will not be accepted by the wider market or have a user base. This is why it is very important to work out the minimum requirements to run a particular application. Minimum requirements such as:

- Minimum disk/install space.
- Connection to WIFI for API's and other web dependencies.
- A current browser: Microsoft Edge, Google Chrome, Firefox, Safari.
- Mouse, keyboard.

These would be basic requirements the user would need to run the application. Having better hardware or WIFI connections will always lead to better performance. When developing and testing the application many different machines of varying types were used. Mainly the three machines of varying specs used for development by each of the developers. Then Machines the application was installed on for user testing. This gave an scope of what hardware offered the best performance for the application. Performance testing also entailed of workload/stress testing the application from posting multiple posts one after the other to using products such as selenium to continually reload pages and send request to test how the application handled it.

6.1.6 User Acceptance Testing

An application being accepted by it user base is vital to the life and future of the application. When developing any application the focus is always on the user, making sure it is easy to use, has a intuitive UI and well be something they will use regularly. To meet all these requirements it was important to get an outside perspective from those that weren't developing the application. As developers it is very much see a problem and fix it. This means being so close to the project there can be things that can be missed. To get a fresh perspective each of the group got peers, friends and families to user test the

app at different stages, taking note of their feedback and general feelings on the application. Having such a wide pool of people to pick from gave a huge range of varying perspective and skills. With peers it gave the perspective from those with strong coding and software experience, their input was vital for many aspects of the app. Whereas from the perspective of family and friends it gave more of a general view from those with little to no coding or software experience. Their input was just as vital as it gave a fresh look on things. Along with seeing if the aim of introducing and educating those new to Bitcoin and crypto-currencies could be met. With those of varying age ranges and experiences it also gave useful information on who the target audience for the application could be. User acceptance was very positive from those who tested the application.

6.1.7 Limitations

Identifying limitations of any project is always important it isn't identifying failure but offering insight into the making of the project and what could have been improved upon. This project is no exception while developing there were many obstacles that had to be overcome and some that were insurmountable. When it came to the Trading section of the project the task was to get an API or widget that would display the current price of several crypto-currencies, along with graphing the falls and rises in each. This was done using a the Trading View web widget. The widget works perfectly and offers vast functionality but also limits the users navigation in the application. This is because the widget loads over the applications bootstrap navigation bar stopping them from easily cycling through the app unlike on all the other pages where the navigation bar remains. This means to get back to the rest of the app the user must press the back key in the URL bar and reload the page. This would not be up to industry or market place standard as the user should not have to do anything extra just to navigate through the app. The page does fulfill its function and offers unique and helpful information, but at the cost of easy navigation for the user.

Looking at another aspect of the project there is the problem of it not being a application that comes ready in the box. What is meant by this is there are quite a few dependencies the user must install to have this web application up and running correctly. As opposed to a mobile application you download on your phone that comes ready to go or a website you can just navigate to. The MEAN Stack has a lot of different technologies and nodes working together to produce this working web application. While this is also a strong point of the application as there is a lot of strengths and functionality offered by the MEAN technologies. It also can lead to some alienation of possible

user base, as some people will find problem with having to install and run multiple technologies for the purpose of one application. Another factor of this is if something would or is to go wrong in one of the components of the application or one of the MEAN technologies it can crash the whole application. If this is occur it can be damaging to the reputation of the application along with a unfortunate task for the developers to correct this this error. On the other side of thing the application does come with a section for users to submit problems they have encountered while using the application and a opportunity for the developers to be constantly improving the application and meeting the users needs.

Chapter 7

Conclusion

7.0.1 What we learned

Throughout the whole process of the final year project, we have learned a substantial amount about a whole range of subjects. From working as part of a team to learning, from scratch, new languages and programs to complete our project. We learned that working as part of a team can have some great benefits. As a team you get input and information from each member that other members may not have known before which can greatly help in succeeding. The greatest benefit of teamwork is by working efficiency together you can get a great amount of work done compared to if you were working on your own. If you can distribute work out evenly to each individual in the group it makes it fair and realistic. We learned that if we met up on a regular basis and worked on the project together it benefited us greatly as we were able to help one another out and got more work done due to this. We also learned a lot about the MEAN stack. This is what we used to build our application, and as we were never taught it in college we had to research it ourselves and how to use it in the most efficient way possible to create the best possible project. With the MEAN stack we learned how to have multiple technologies and databases interact with one another, for example the MEAN stack allows us to have angular 2, node.js, express.js and mongoDB all interact with each other. A major part as working as part of a team is using Github. We learned throughout the course of our final year project how to best use Github and all its features to our advantage as working as part of a team. Github allowed us to work on part of our project on our own time and when we each completed parts of the project we were able to commit them to Github where the rest of the members in the group could easily see the changes that were made and pull them down to their own machine. Github also allowed us to raise any issues we encountered to our

fellow team members by using the Github issues feature. This feature would allow a member to raise a problem they have encountered and allow for the other members in the group to provide solutions. We found this feature very useful and helped us work better as a team.

7.0.2 Future Development

For future development of the application we could add many new and exciting aspects. One feature we could add to the application in the future is an instant chat messenger. This feature would allow the users of the bitcoin wallet to talk to their friends on the application instantly. This would give the application even more social aspects which would benefit the application hugely and it would allow the users to keep in touch with each other effortlessly.

We could also introduce a questions and answers feature like stackoverflow, where the users can ask questions related to topics about the bitcoin wallet or other quires they may have. Other users would then be able to answer their questions and help them out.

Future development of the application could see us integrate notifications to the application. For example, when a user receives bitcoin from another user, they will be alerted about this. Also we could have notifications for when another user has liked or disliked their blog post or when a user receives a friend request.

Chapter 8

Appendix

Project Source Code Link: <https://github.com/Smurfgalway/Final-Year-Project-Applied-Diss>

Project Documentation Link: <https://github.com/Smurfgalway/Final-Year-Project-Applied-Diss/blob/master/FYP/FYP.pdf>

Bibliography

- [1] “What is mongodb? — mongodb.” <https://www.mongodb.com/what-is-mongodb>. (Accessed on 03/30/2018).
- [2] K. Chodorow, “usuaris.tinet.cat/bertolin/pdfs/mongodb_ the definitive guide - kristina chodorow_1401.pdf.” http://usuaris.tinet.cat/bertolin/pdfs/mongodb_%20the%20definitive%20guide%20-%20kristina%20chodorow_1401.pdf. (Accessed on 03/30/2018).
- [3] “What is github, and what is it used for?” <https://www.howtogeek.com/180167/htg-explains-what-is-github-and-what-do-geeks-use-it-for/>. (Accessed on 03/30/2018).
- [4] “Introduction - javascript — mdn.” <https://developer.mozilla.org/en-US/docs/Web/JavaScript/Guide/Introduction>. (Accessed on 04/11/2018).
- [5] “Javascript functions.” https://www.w3schools.com/js/js_functions.asp. (Accessed on 04/11/2018).
- [6] “Robo 3t - formerly robomongo — native mongodb management tool (admin ui).” <https://robomongo.org/>. (Accessed on 04/14/2018).
- [7] “Api testing with postman — sparkbox — web design and development.” https://seesparkbox.com/foundry/api_testing_with_postman. (Accessed on 04/14/2018).
- [8] “Json web token introduction - jwt.io.” <https://jwt.io/introduction/>. (Accessed on 04/10/2018).
- [9] “jsonwebtoken - npm.” <https://www.npmjs.com/package/jsonwebtoken>. (Accessed on 04/10/2018).

- [10] “Angular authentication: Using route guards – ryan chenzie – medium.” https://medium.com/@ryanchenzie_40935/angular-authentication-using-route-guards-bf7a4ca13ae3. (Accessed on 04/10/2018).
- [11] “What is bcrypt? - quora.” <https://www.quora.com/What-is-bcrypt>. (Accessed on 04/13/2018).