
Bitcoin Wallet

Donal McGahon

Conor Tighe

Stephen Murphy

B.Sc.(Hons) in Software Development

APRIL 13, 2018

Final Year Project

Advised by: Gerard Harrison

Department of Computer Science and Applied Physics

Galway-Mayo Institute of Technology (GMIT)



Contents

1	Introduction	8
1.0.1	Objectives:	8
1.1	Specifications	9
1.1.1	Web application:	9
1.1.2	Database:	9
1.1.3	Server:	10
1.1.4	The rise of the first cryptocurrency	10
1.1.5	Bitcoin: What is a bitcoin?	10
1.1.6	Blockchain: What is the blockchain?	11
1.1.7	Applications interactions with the blockchain: API's	12
2	Context	14
2.1	Filler	14
2.1.1	More filler	14
2.2	Filler	14
3	Methodology	15
3.1	Platform Design	15
4	Technology Review	17
4.0.1	MEAN	17
4.0.2	Mongodb:	17
4.0.3	Angular2/5:	17
4.0.4	ExpressJs:	18
4.0.5	NodeJS:	18
4.1	Other Technologies	18
4.1.1	Docker:	18
4.1.2	Github:	18
4.1.3	Bootstrap:	19
4.1.4	Blockchain:	20
4.1.5	Adobe Photoshop:	20

4.1.6	Google Fonts:	20
4.2	JavaScript	20
4.3	Social Media Research	21
5	System Design	23
5.1	User Registration	23
5.1.1	Overview	23
5.1.2	In-depth	24
5.2	User Login	26
5.2.1	Overview	26
5.2.2	In-depth	26
5.3	Security	27
5.3.1	JSON Web Tokens	27
5.3.2	Auth Guards	28
5.3.3	Displaying router links	30
5.3.4	Encrypted Passwords	31
5.4	Blog Posts	32
5.4.1	Overview	32
5.4.2	Create Post	32
5.4.3	Delete Post	33
5.4.4	Like and dislike posts	35
5.4.5	Mongo Database used to store blog posts	37
5.5	Profiles and user customization	37
5.5.1	Overview	37
5.5.2	In-depth	38
5.6	Statuses and sharing with other users	39
5.6.1	Overview	39
5.6.2	In-depth	41
5.7	Global Map and tracking user activity	43
5.7.1	Overview	43
5.7.2	In-depth	44
5.7.3	In-depth	44
5.8	User Wallets and bitcoin features	48
5.8.1	Overview	48
5.8.2	In-depth	48
6	System Evaluation	52
7	Conclusion	53
7.0.1	What we learned	53
7.0.2	What we would change	53

<i>CONTENTS</i>	4
7.0.3 Future Development	53
8 Appendix	54

List of Figures

1.1	Design pattern.	11
1.2	Blockchain.	12
5.1	Data stored in MongoDB.	24
5.2	Registration interface.	24
5.3	Blog-Post Database.	37

About this project

Abstract The aim of this project is to allow users the ability to have a user friendly bitcoin wallet to store their bitcoins. We want to have a secure wallet that allows the users to register and log in to the application with their information safely storing to a database.

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 "Say what you work on here". 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. 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. Most of the technologies discussed here are emerging technologies that are not taught in the Software Development in GMIT.

1.0.1 Objectives:

- Make the UI user friendly and appealing to new users of Bitcoin.
- Educate user on the technology bitcoin and how it works, display real time value.
- Strong authentication that's simple to use yet secure so users will trust us with their coins.

- Google Maps integration to show users bitcoin related locations like exchanges or stores that accept the currency.
- 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 users to add one another as friends with the bitcoin wallet.

1.1 Specifications

1.1.1 Web application:

- Receive bitcoin from external wallets at any time.
- Send bitcoin to external wallets at a fast and efficient rate using.
- Allow users to see their balance displayed clear and aesthetically.
- Google maps page show related bitcoin locations.
- Bitcoin price display showing the current value and related stats.
- Create new user.
- Log in.
- Log out.
- Update user details.
- Display related bitcoin news.
- Information pages to educate different bitcoin users.
- Blog post feature to inform fellow users about latest cryptocurrency news or updates.

1.1.2 Database:

- Should store user details.
- Should store bitcoin address.
- Should store contacts.

1.1.3 Server:

- Provide secure routes for users.
- Authenticate users.
- Send requests received from web app to database.
- Receive and forward database responses to web app.

1.1.4 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 blockchains 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 blockchains 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.

1.1.5 Bitcoin: What is a bitcoin?

A bitcoin can be thought of as a digital receipt, its 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 bitcoins lifespan and each new address the bitcoin gets sent after being generated will be recorded. Validation of the bitcoins history and location are done using a private key and public key. When someone sends a bitcoins 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.

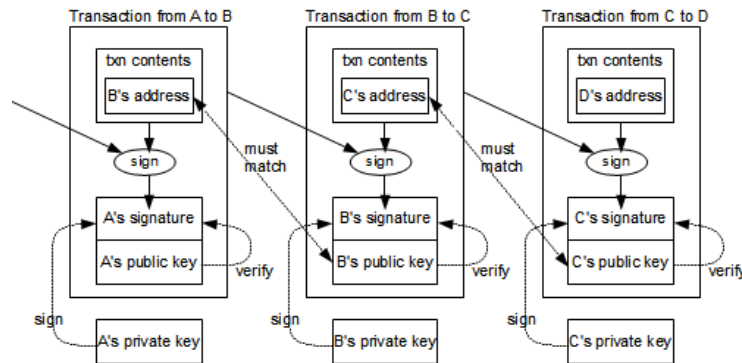


Figure 1.1: Design pattern.

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.

1.1.6 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.

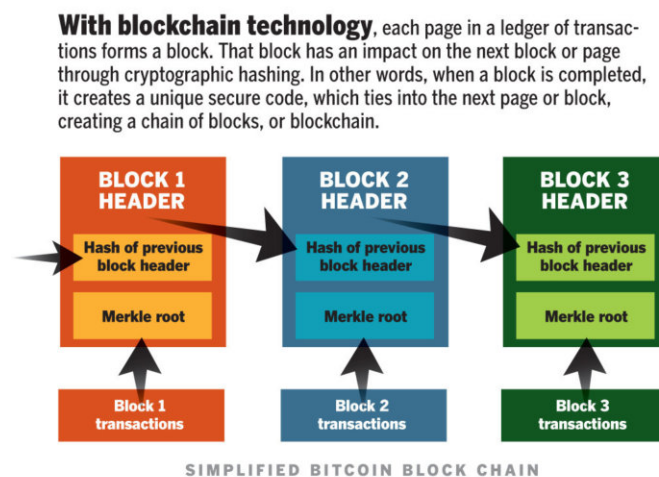


Figure 1.2: Blockchain.

1.1.7 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.

Chapter 2

Context

- Provide a context for your project.
- Set out the objectives of the project
- Briefly list each chapter / section and provide a 1-2 line description of what each section contains.
- List the resource URL (GitHub address) for the project and provide a brief list of the main elements at the URL.

2.1 Filler

2.1.1 More filler

2.2 Filler

Chapter 3

Methodology

About one to two pages. Describe the way you went about your project:

- Agile / incremental and iterative approach to development. Planning, meetings.
- What about validation and testing? Junit or some other framework.
- If team based, did you use GitHub during the development process.
- Selection criteria for algorithms, languages, platforms and technologies.

Check out the nice graphs in Figure ??, and the nice diagram in Figure ??.

3.1 Platform Design

As a group Conor, Donal and I(Stephen) met regularly each week and our first plan of action was to divide the work and objectives between the 3 of us. I offered to take on some of the front end and the primary load of the aesthetics/ overall look of the project. I had previous experience in graphic design so I photo-shopped mock designs and thumbnails for the project as we went on. I familiarized myself with how the mean stack controlled its colour scheme and look through bootstrap, CSS and HTML components. I researched a lot of different style-sheets and components to make the projects UI(user interface) stand out and be intuitive. I had working design in my head that I wanted to achieve, along with receiving creative input from Conor and Donal.

I started with the aesthetic of the home page 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 I used a CSS sheet for the home component HTML page. I wanted each of these thumbnails highlight when hovered on and portray exactly what they linked to. To do so I used Adobe Photoshop for editing and graphic design. For inspiration and templates/base images I used Google images with key words to find exactly what I was looking for. I looked at various crypto-currencies wallets, stock websites and angular apps to get a feel for how this project should look. I want to take the best aspects from each and improve on areas where I felt these other platforms could have.

Conor informed me about Google fonts. Google fonts is a font hub offered by Google offering a free download of a endless amount of varying fonts. I browsed through the website and found multiple fonts I felt would fit the idea for the look of the app. My criteria for picking a font was

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.

4.1.5 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.

4.1.6 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.

4.2 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 }
```

4.3 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 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 volatile 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[6]. 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 [7], 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[8]. 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[9]. 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 Blog Posts

5.4.1 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.

5.4.2 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  }
```

5.4.3 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
9      <div class="panel-footer">
10         <strong>Posted by: </strong> {{ blog.createdBy.username
11     }}
12     <br />

```

```

12     <strong>Date: </strong> {{ blog.createdAt | date: 'MMM dd,
13     yyyy' }}
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(
5     data => {
6       // Check if delete request worked
7       if (!data.success) {
8         this.messageClass = 'alert alert-danger';
9         this.message = data.message;
10      } else {
11        this.messageClass = 'alert alert-success';
12        this.message = data.message;
13        // After two second timeout, route to blog page
14        setTimeout(() => {
15          this.router.navigate(['/blog']);
16        }, 1500);
17      }
18    });
19 }

```

5.4.4 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 // Function to dislike blog
8 dislikeBlog(id){
9     this.blogService.dislikeBlog(id).subscribe(data => {
10         this.getAllBlogs();
11     });
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:

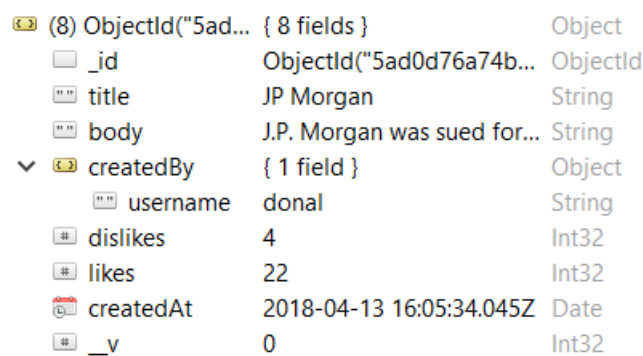
```

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>

```

5.4.5 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 is an Object with 8 fields. The fields are: _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 single field, username (String).

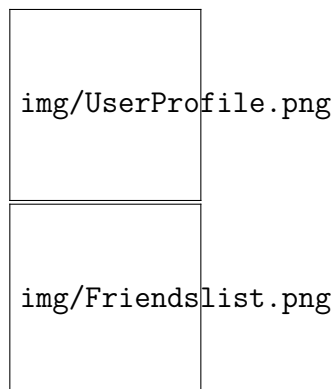
Field	Value	Type
(8) ObjectId("5ad... { 8 fields }		Object
_id	ObjectId("5ad0d76a74b...	ObjectId
title	JP Morgan	String
body	J.P. Morgan was sued for...	String
createdBy	{ 1 field }	Object
username	donal	String
dislikes	4	Int32
likes	22	Int32
createdAt	2018-04-13 16:05:34.045Z	Date
_v	0	Int32

Figure 5.3: Blog-Post Database.

5.5 Profiles and user customization

5.5.1 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.



5.5.2 In-depth

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. 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 total service calls to construct the profile and friend list pages is 17, below are some examples of how these are executed in typescript:

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      }

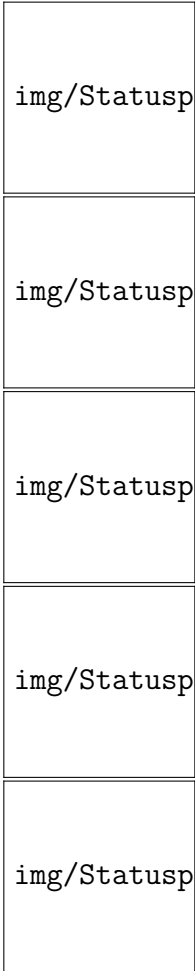
```

5.6 Statuses and sharing with other users

5.6.1 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 their 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 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.



img/Statuspost1.png

img/Statuspost2.png

img/Statuspost3.png

img/Statuspost4.png

img/Statuspost5.png

5.6.2 In-depth

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 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. The flag files allow users to mark bitcoin related places of interest using your location or a marked location using the map. The postbal files allow users to share the balance of a particular address assigned to the user. The poststatus files allow just a general post with no metadata tied to the post. The requestbitcoin is for donation requests to certain addresses. 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. Below we show how we get the prices for the price status posts followed by more code examples of tasks:

```

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
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.

```

```
    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  
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 }
```

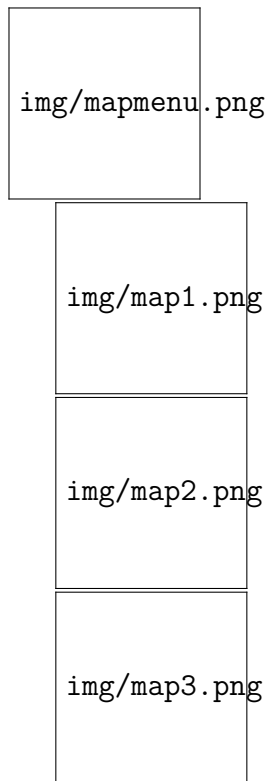
5.7 Global Map and tracking user activity

5.7.1 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. Below we show the menu that give the user the option to view the maps or post statuses that cant be plotted:

5.7.2 In-depth



5.7.3 In-depth

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 withing in the html files, then this is bind-ed to my own custom maps object

withing 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 statment. The Profile and Status services and what provide the vieMap component with the useres 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 dipslay there custom avatar. Below is the HTML and typescript object that we use to create the map, followed by more examples related to what I've covered here:

```

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('
10         cryptoMap'), {
11             zoom: 4,
12             center: {lat: 53.1424, lng: -7.6921}
13         });

```

Footer for status icon legend:

```

1      <nav *ngIf="showmap" class="navbar navbar-default sidebar
2      " role="navigation">
3          <div class="container-fluid">
4              <div class="collapse navbar-collapse" id="bs-sidebar-
5              navbar-collapse-1">
6                  <ul class="nav navbar-nav">
7                      <li><a href="#">Normal Status</a
9                      ></li>
10                     <li><a href="#">Balance Status</a
12                     ></li>
13                     <li><a href="#">Statistics Status</a></li>
16                     <li><a href="#">Miner Status</a
18                     ></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      // create icon from friends avatar
6      var icon = {
7          url: "/app/avatars/" + friend.avatar + ".png", // url
8          scaledSize: new google.maps.Size(50, 50), // scaled
size
9          origin: new google.maps.Point(0,0), // origin
10         anchor: new google.maps.Point(0, 0) // anchor
11     };
12

```

```
13 // Create objects to mark on map
14 var location = {lat: friend.lat, lng: friend.lng};
15 var marker = new google.maps.Marker({
16   position: location,
17   map: this.map,
18   icon: icon,
19   title: friend.username,
20 });
21 // add listener to marker that shows profile about me
section
22 marker.addListener('click', ()=> {
23   alert(friend.aboutMe);
24 });
25 }
```

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

5.8 User Wallets and bitcoin features

5.8.1 Overview

One of the main features of this wallet is the ability to create and manage bitcoin address from 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 was 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 send bitcoin to another address that is or isn't on our platform.

5.8.2 In-depth

The WalletComponent folder within 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 the blockchain service passed with the Angular2/5 component promises to activate a route on the server-side code which then passes the submitted wallet details to the block chain client process for processing. 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. Once the user has access to a wallet in their 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). 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. 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 which is used as a parameter. The send bitcoin feature is done using the sendbtc.component.ts files. This 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. Below is an example of how we execute this bitcoin transaction followed by other relevant code snippets:

```

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.
label);
12
13    this.blockchainService.saveWallet(newWallet)
14    .subscribe(
15        messages => this.wallet = messages,
16        error => console.error(error)
17    );
18    console.log(this.wallet);
19 }
```

Chapter 6

System Evaluation

As many pages as needed.

- Prove that your software is robust. How? Testing etc.
- Use performance benchmarks (space and time) if algorithmic.
- Measure the outcomes / outputs of your system / software against the objectives from the Introduction.
- Highlight any limitations or opportunities in your approach or technologies used.

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 you may have not know before which can greatly help in succeeding. The greatest benefit of teamwork is 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 teach ourselves how to use it in the most efficient way possible to create the best possible project. With the MEAN.

7.0.2 What we would change

7.0.3 Future Development

- Briefly summarise your context and objectives (a few lines).
- Highlight your findings from the evaluation section / chapter and any opportunities identified.

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] “Json web token introduction - jwt.io.” <https://jwt.io/introduction/>. (Accessed on 04/10/2018).
- [7] “jsonwebtoken - npm.” <https://www.npmjs.com/package/jsonwebtoken>. (Accessed on 04/10/2018).
- [8] “Angular authentication: Using route guards - ryan chenkie — medium.” https://medium.com/@ryanchenkie_40935/angular-authentication-using-route-guards-bf7a4ca13ae3. (Accessed on 04/10/2018).
- [9] “What is bcrypt? - quora.” <https://www.quora.com/What-is-bcrypt>. (Accessed on 04/13/2018).