THE UNIVERSITY OF SYDNEY

School of Information Technologies
Faculty of Engineering & IT

ASSIGNMENT/PROJECT COVERSHEET - GROUP ASSESSMENT

Unit of Study: COMP5703 Capstone Porject

Assignment name: An Online Web-Streaming Service for Bitcoin-Exchanges

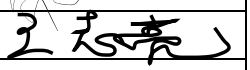
Tutorial time: Wednesday, 16:00 **Tutor name:** Martin

DECLARATION

We the undersigned declare that we have read and understood the *University of Sydney Academic Dishonesty and Plagiarism in Coursework Policy*, an, and except where specifically acknowledged, the work contained in this assignment/project is our own work, and has not been copied from other sources or been previously submitted for award or assessment.

We understand that failure to comply with the *Academic Dishonesty and Plagiarism in Coursework Policy* can lead to severe penalties as outlined under Chapter 8 of the *University of Sydney By-Law 1999* (as amended). These penalties may be imposed in cases where any significant portion of my submitted work has been copied without proper acknowledgement from other sources, including published works, the internet, existing programs, the work of other students, or work previously submitted for other awards or assessments.

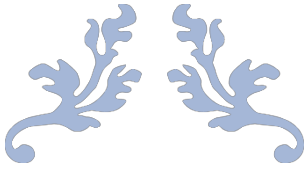
We realise that we may be asked to identify those portions of the work contributed by each of us and required to demonstrate our individual knowledge of the relevant material by answering oral questions or by undertaking supplementary work, either written or in the laboratory, in order to arrive at the final assessment mark.

Project team members				
Student name	**Student ID**	**Participated**	**Agree to share**	**Signature**
1. Lida GUO	460269052	~~Yes~~ / No	~~Yes~~ / No	
2. Jiyang Li	460061928	~~Yes~~ / No	~~Yes~~ / No	
3. Zhaohui CHANG	460477129	~~Yes~~ / No	~~Yes~~ / No	
4. Zhiliang WANG	460094203	~~Yes~~ / No	~~Yes~~ / No	
5.		Yes / No	Yes / No	
6.		Yes / No	Yes / No	
7.		Yes / No	Yes / No	
8.		Yes / No	Yes / No	
9.		Yes / No	Yes / No	
10.		Yes / No	Yes / No	

SIT Building, J12
The University of Sydney
NSW 2006 Australia

T +61 2 9351 3423
F +61 2 9351 3838
E sit.info@sydney.edu.au
sydney.edu.au/it

ABN 15 211 513 464
CRICOS 00026A



COMP5703

CAPSTONE PROJECT

An Online Web-Streaming Service for Bitcoin-Exchanges

Group No. 1

Lida GUO	460269052
Jiyang LI	460061928
Zhaohui CHANG	460477129
Zhiliang WANG	460094203

Table of Contents

I. ABSTRACT

The project is about a web application for collecting and visualize the information of cryptocurrency trading among different exchange websites. The application provides the visualization of real-time data based on the real trade information over the globe cryptocurrency market, and users can use the visualized charts and tables to analyse the most critical aspect of the cryptocurrency market performance. It can help users make the investment decisions more efficiently and accurately.

II. INTRODUCTION

i. Overview

A blockchain can be thought of as a distributed database across many nodes. The transactions can be reconciled and be recorded even when a few nodes on the network in various order. The blockchain technology has combined three features of the previous general and mature technologies, which are peer-to-peer networking, asymmetric cryptography, and cryptographic hashing. The first cryptocurrency, bitcoin, which is created based on these features by the pseudonymous Satoshi Nakamoto in 2009.

Token deals (likewise is called ICO) have stood out as genuinely newsworthy this year as a feature of enormous cost increments in the digital currency space. They convey a decentralised type of crowdfunding to the blockchain which means that it will not be controlled by an outsider, which is like the business model of Kickstarter but without the centralised manager. The prices of well-known digital coins, for example, Bitcoin and Ethereum have been raised dramatically in the period of mid-2017. A massive amount of investment has owed into the market. The enthusiasm if the investors have also influenced the popularity of the cryptocurrency exchange platform, such as GDAX, Bitfinex, Binance, etc. This move in the raising money scene has happened similarly as the Australian government has at long last managed and allowed crowdfunding for open organizations. Subsequently, the digital coin is being perceived by an ever-increasing number of individuals over the world.

In the project, the information about the cryptocurrency market over the world can be refined to graphs, tables or charts. It will aggregate the market information of different cryptocurrencies, as well as the market trends across different cryptocurrency exchanges. Users can analyse the investment strategy based on this visualised information. It provides the real-time currency rate between different cryptocurrencies. Also, the historical trade details and price records can be shown to the users after the different forms of data visualisation.

ii. Background

The cryptocurrency is a recent phenomenon with a bright future. In the past, from 1944 to 1973, most countries in the world joined the monetary system using the U.S. dollar as an international monetary centre. At that time, the United States accounted for one-quarter of the world's total economic output and more than two-thirds of its gold reserves. It naturally became the centre of the international monetary system.

The US dollar is linked to gold, and the United States is a reserve currency issuer. The Fed guarantees that the dollar will be exchanged for gold at official prices. Therefore, there are

three characteristics of the credit system of the currency. First, gold mining is limited and scarce and has the certain value. Second, the United States has a significant amount of gold and loud volume of the economy. Finally, the United States issues currency in circulation and links the US dollar with gold, become a circulating medium for the payment of international currency. Similarly, in the blockchain economy, bitcoin mining is limited and scarce, so it has a certain value. Most blockchain projects are raised in Ethereum and Bitcoin, so the two digital currencies are strong endorsements in the blockchain system, and many new projects issue Tokens in the process of crowdfunding, that means Token has become the payment distribution medium for blockchain investments.

Currently, there are four principal profit-making methods in the blockchain economy. The first is mining, users need to provide machines, and then they receive system rewards by helping to prove the transfer process. The second is to trade the same amount of currencies across exchanges to earn the difference. The third type is short-term trading, which is to buy lows and sell highs on the exchange to make a difference. The last one is to do blockchain business through ICO crowdfunding. It is clear to see that these actions are closely related to the market information of digital currency exchanges. Therefore, how to allow users obtain more effective digital currency market information has become a very meaningful service.

Current exchanges provide two of main features to the user, which are coins and tokens exchange and margin trading. Some exchange websites provide the exchange service between popular cryptocurrencies (Bitcoin, Ethereum, EOS, etc.) and legal tender (USD, AUD, CNY, etc.), which is called OTC (Over-The-Counter) market. For example, In the Bitfinex, Bitstamp, Huobi.pro, they provide both OTC trading and exchange between cryptocurrencies. In the OTC market, users can use fiat currencies to buy cryptocurrencies by either directly placing an order or posting a purchase offer. However, some other exchange websites only provide the exchange service between cryptocurrencies, such as GDAX, Binance, etc.

The exchange section of the cryptocurrency market is similar to the exchange market of stock. The exchange website offers the different client types of orders, such as Limit order (buy or sell at a given price or better price), Market order (buy or sell at current market price immediately), Stop order (sell or close the position when it arrive a specific price), Full or fill (limit order which can make sure the position is entered at a configured price), OCO (One cancels others, the combination of stop order and limit order, which means cancel the other orders after one of them has been fully or partially executed), etc.

The exchange website also provides the margin trading, which means the exchange website allow users to trade with up to 20x (huobi.pro) leverage by borrowing short-life assets from the exchange websites themselves or the peer-to-peer margin funding platform. In Bitfinex, Users can place the order on peer-to-peer margin funding platform to borrow the desired amount of cryptocurrencies at an appropriate rate and duration, or the Bitfinex can help the users complete the orders at the best available price and time.

For assisting users to take the order, the exchange website provides the real-time market information and also the trading platform to the users. However, the price of the same cryptocurrency from different exchange websites is different. If a user owns cryptocurrency assets in multiple exchange websites, an information comparison website that covers multiple mainstream digital currencies in multiple transaction exchange websites can provide such users with useful help.

For achieving the aim of helping users making decisions on cryptocurrency investment, there are four main features have been considered in the web application, which are the real-time exchange feed, bubble chart of private investment profit trend, K-line of live trades and depth

chart of real-time orders. All these markets information are not from one same exchange websites but the difference. The details of these features will be described in the methodologies part.

III. METHODOLOGIES

In this section, we would like to analyse it from two aspects, practical and theoretical. In terms of a practical part, this is a general requirement for our potential customers and contains several updating or advanced functions after comparing with GDAX exchange website. From the technology perspective, it shows what we are maybe going to use and program, that should include the framework, programming language, front end, back end, database and essential functions.

i. Practical

a. Users

We suppose our users or clients are interested in cryptocurrencies exchange and do want to get profits by exchanging websites and organizations. Generally, consumers can go through four approaches to exchange cryptocurrencies. Use bitcoin here as a sample to introduce.

1. The first method is exploring bitcoin also called “Mining coin” by some algorithms and special machines, which have a high capacity for calculation. The total bitcoin is like a “Mining Farm”, according to the blockchain, the total volume is a fixed number

2. The second one is trading bitcoin in one exchanging organization; buying at lower and selling at higher.

3. Then the transferring bitcoin from one exchanging organization to another one, because of different current prices.

4. The last way is “Initial Public Offering (ICO)”, which is a third public party that aims to help you to manage your cryptocurrencies. This has its risks and saves time for their clients.

In the short terms, our target users are from No.2 and No.3 above. They do not need to “Mining”, however, what they only need to do is decide which exchanging websites can give them lowest/highest price and increasing trends.

In the long terms, we hope we can provide our analysis of the trend or prediction in cryptocurrencies. We can also attract No.4 customers above.

b. Demands

This web service focus on customers’ needs. What we contribute effort to do is to make data more visually and easily to read. So, the data, which collected from other websites, is our most important sources to show. Customers want to compare the different information among the various exchange organizations, such as the current prices and trading volumes in different organizations showing below like figure 1.

Figure 1. Index page mock-up.

In figure 1, the top four blocks we want to show the different exchange websites' current price compared with USD or USDT, which is legal currency or cryptocurrency. General trends can show the trend in different organizations.

The second division is Line chart can show as "Candle chart". Users also need to check the trend of public data, which can easily show the increase and decrease in this chart. Several integrators and tools can help users to get more accurate prediction.

On the right of second division, it will be a login section for users' registration and log in, which can check their private data after login.

The foundational function is checking the exchange rate about each cryptocurrency and currency, such as Bitcoin, Bitcoin cash, Ether and Litecoin exchanging with USD, EUR and GBP. We will display this part as a real-time block, changing at any time.

Moreover, the depth chart is a basic diagram to show the public volume and expected price. The area of depth chart can easily show the public trend and clients' psychology.

Furthermore, a global map is also required by some of our customers, which can show the volume and position of exchange lively during this time showing below like figure 2.

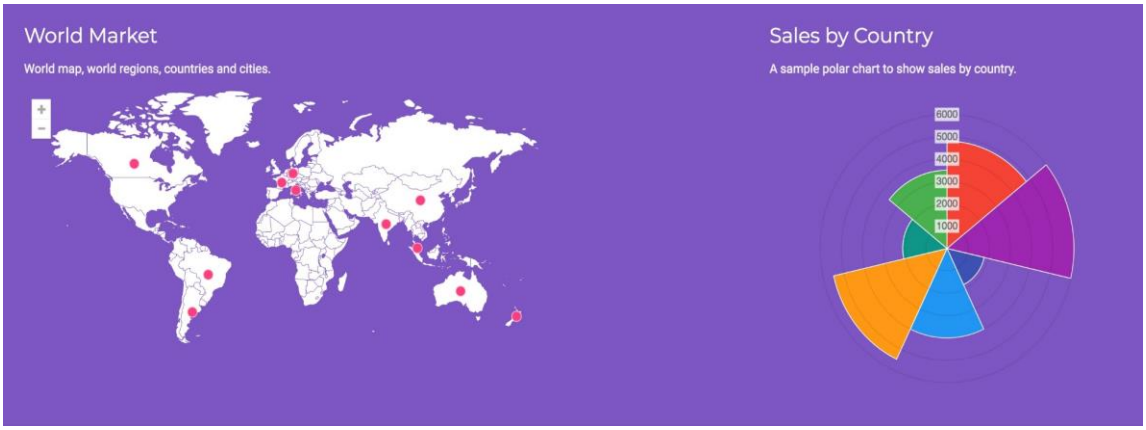


Figure 2. Global trading map.

In term of the practical situation, we consider it from two aspects in short term, one is Individual part and the other is a public part. Based on what problems we find from other exchange websites; we will use several methods to solve them.

c. Problems

Compared with GDAX, we find some problems need to be solved.

1. Clients cannot exchange with other currencies like AUD or SGD, which limits our customers' choices and loses several potential customers. Users should consider the exchange rate firstly and exchange then operate it. Popular currencies can attract more customers.
2. After we selling and buying such bitcoins in a sandbox of GDAX, we can only find a list or a table to show the history of transferring and ordering. We cannot get some direct information about what we bought before, such as a diagram or a line chart. Customers should compare each price, which was exchanged before by themselves, in order to know each action's profits or losses.
3. K-line, which is also called "Candlestick chart", is a great analytics tool to show the trend of commercial currencies. However, in the short term, k-line cannot help users to analyse the trend with the recent trends, compared with five days, ten days or more. This is useful for those short-term operators. What GDAX has is the Exponential Moving Average.
4. Depth chart, which can show the volume of exchange, is also a good chart to show some information about bitcoin exchanges. However, users cannot find an accurate number to set as a threshold. If the number is higher than this threshold, users should take care of bitcoin operation.

d. Solutions

For the first issue, we add multiple currencies' options about cryptocurrencies' exchanges, such as CNY, AUD and SGD in real-time exchange rate.

The second issue requires us to make an individual part to show the trend or more visualized methods to display the revenue of users. In the beginning, we try to use "Bubble chart" to deal with that showing like figure 3.

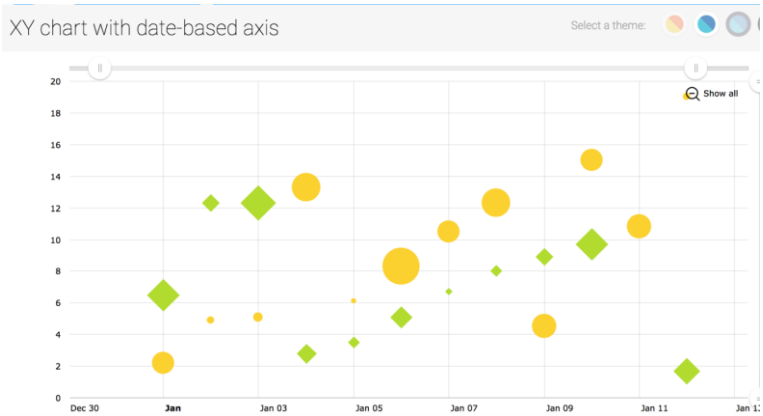


Figure 3. Individual investment trend in bubble chart (XY chart with date-based axis – amCharts, 2018).

For the third issue, based on the experience of stocks, we combine the k-line with average lines together, such as Moving Average (MA) line. If a user wants to operate bitcoin within only three days or shorter, MA5 (Moving Average 5 days) can help him/her to know the recent trend showing in figure 4 below.

Figure 4. K-line / Candlestick chart (ECharts Demo, 2018).

For the fourth issue, we will also add depth chart on our website, however, we also provide a quantity relative ratio R, which has a calculation function. According to the relational knowledge, it defines that the total volume of trades is $V1$; the total minutes from opening time till now is $T1$; the average daily rate in each minute over past 5 days is Ro. So, the function is shown below formula 1.

$$R = V1 \div T1 \div R0 \qquad \text{[Formula 1]}$$

The depth chart will be shown as below figure 5.

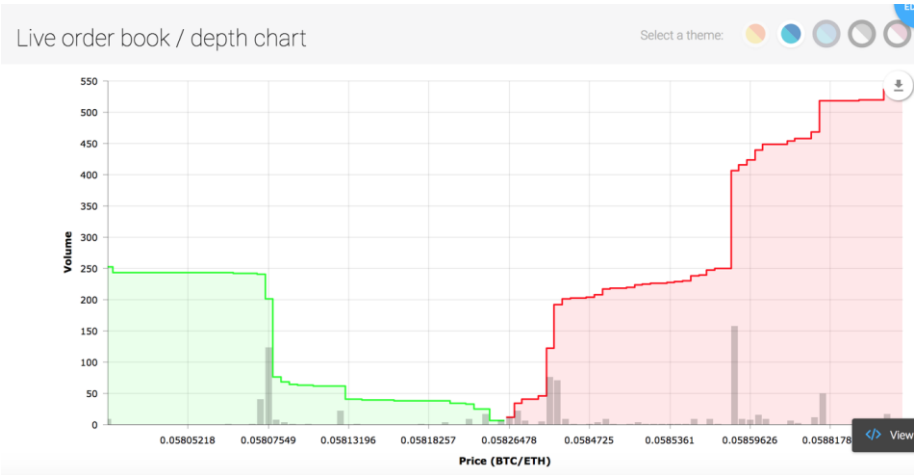


Figure 5. Depth chart (Live order book / depth chart – amCharts, 2018).

ii. Technological

From the technological perspective, according to building an online web-streaming service, we are going to build a web application for bitcoin-exchanges to our customers. After considering the demands and requirements of this project, the next step is to collect the fundamental information required for the web app development (IT Outsourcing India, 2018).

a. Framework & Programming Language

The first things we need to confirm are the frameworks and programming languages. We will use MVC framework in our web service, which is good at multi-workers cooperating and efficiently controlling, furthermore, the details about how we build this framework and what the responsibilities of each block take will be showed in framework section.

Asynchronization means computer multithreading asynchronization processing. Relative to synchronization processing, asynchronization processing doesn't need to wait for current thread finish. It allows the subsequent task start at the same time until the all other threads complete their task. Then it will use the call-back function to announce the current thread.

The node.js used a single thread to avoid multithreading, state synchronization problems. Of course, the asynchronization I/O feature can help single thread to avoid the block and use CPU more efficiently. Of course, the asynchronization will bring some problems, like call-back function nest too deep. But the Promise, Generators and Async function will deal with it.

b. Front End & Back End

In the web application, separated by front-end and back-end, we choose HTML/CSS and Embedded JavaScript (EJS) templates in front-end; Node.js is the best choice for the back-end, which we can use it to build MVC and finish the request/response actions with web browsers. In the front end, we need to draw several charts using amchart.com and echart.com, which are convenient for us to offer many templates using node.js.

In the back-end, we use Application programming interface (API) to get the data from several bitcoin-exchange websites, such as GDAX, Coinbase, Binance and Bitcoin Ticker; and cryptocurrency analytics websites, such as Coinmarket, Coingecko and Fei Xiao Hao. Bitcoin-exchange websites can provide the public data, but the private data can be used in a sandbox of GDAX. In the future work, we will contribute much effort into other websites exploration. The bitcoin analytics website is an organization to collect and analyse public data, then give a trend or sort, which can mention users to notice which exchange organization is popular and the size is large. We can use this information to make a better one.

After getting data from outside, we need a database to store data. Based on the format of data using in node JavaScript and MVC framework advantages, we choose MongoDB as our database, which can also save users' registration and private information, such as, personal information, account details, passphrase, API keys and secrets.

c. Basic Functions

Finally, some essential functions we will also add in our web service, for instance, automatic edit management, update management, revenue reporting, user tracking and billing management.

IV. CONFIGURATION

i. Hardware

The website can be shown in all operating systems, and it is compatible with both 32bit and 64bit. We suggest that the Windows OS version should upper than Windows 98 for fluent performance. The RAM is recommended to be larger than 1GB. The Hard Disk is proposed to be larger than 3GB. The video memory of integrated graphics and standalone graphics are advised to be larger than 1GB. All mobile devices of Android and IOS are compatible.

ii. Software

a. WebStorm

We use WebStorm as the integrated development environment. This IDE will bring us six advantages. First, it can display image attributes when we test the code. Second, it provides automatically reconstitution for a label, file name, CSS file and JavaScript file. Third, build-in SASS, Node.js, CoffeeScript and Jade are supported. Fourth, a user can customize the template of code. Fifth, the setting item can be searched. Sixth, the WebStorm has a built-in version control.

b. MongoDB

We use MongoDB as a database. The MongoDB has six advantages. First, it has Document-oriented feature, that means it doesn't need a strict data structure. Then, High performance and High availability and High usability are their advantages of MongoDB. The Easy scalability brings PB level storage space. Of course, it supports ShardingRich query language. The perfect build-in Java API and supporting JSON object are the major advantages of MongoDB.

c. Robomongo

The Robomongo is a GUI of MongoDB, using this software will convince to set and operate the MongoDB.

d. Git

By using Git, we will bring us four capabilities of version control. First, the local version warehouse will help us go back to the last version in anytime. Second, it is easy to establish a branch for multi-user working together. Third, the Git is very fast to switch branch and submit modification that will improve our efficiency. Fourth, the Git can interact with multi-far-end.

e. GitKraken

GitKraken is a GUI tool for Git. It convinces us to operate Git and do the version control.

f. Chrome

We use Chrome browser for running, testing and display our website project. Because of the V8 engine, the Chrome is very fast and stable. The Check function of Chrome is an important reason for us because we can find error and bug in the Chrome console directly, that is convincing and efficient for us to run and test the code.

g. Slack

Slack is an online community platform, and we use that to discuss the details of the project. The fast file transmission has saved much time for us.

iii. Framework

a. Overview

We used the Express framework which supported by node.js. The Express framework implement the MVC framework shown like figure 6 below. All the data communication is based on routers that provide by Express.

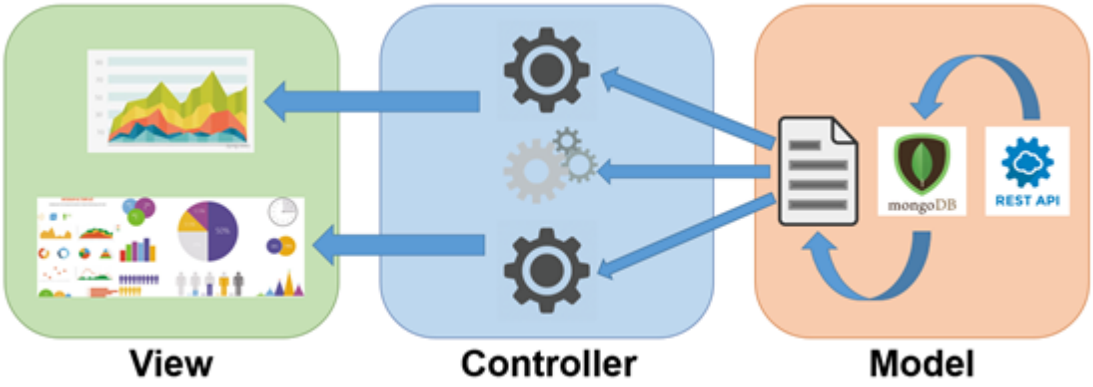


Figure 6. MVC framework overview.

b. Model Block

The model block used for acquiring data from exchange website and cryptocurrency exchange platform, like GDAX, Huobi, etc. And reconstitute data from MongoDB. The role of the model block is labour working between controller and data source. The raw data which comes from an external data source via Rest API will be translated into a new structure by many processors or functions in the model block. Then the processed data will be delivered to controllers.

c. View Block

The view block used for displaying the processed data in a reasonable way which acquired from controllers. The data will be shown like, Candlestick Line, BTC-History Trend Line, etc. The role of the view block is a screen of deliverable information. It used CSS and JavaScript class library to complete the render task. The view block doesn't need to translate or transform the data but show them.

d. Controller Block

The controller block used for communicating with a model block and view block. The role of a controller is a middleware which orders the model block to process expecting raw data and delivers the processed data to view model for giving the reasonable information.

V. MILESTONES & REPORTING

Milestone	Tasks	Reporting	Date
Week-1	**Definition:** Orientation **Mission:** Participate Orientation and know members in our group **Risk:** None	**Deliverables:** None Team members' express individual statements on the project. (State: Completed)	14-03-2018
Week-2	**Definition:** Define framework and purpose **Mission:** Figure out the purpose of web program and the necessary functionalities in this project. Decide to use which type of MVC framework and development platform. **Risk:** The unsuitable purpose and framework will delay the delivery time.	**Deliverables:** Designed Framework **Description:** Design a framework (State: Completed)	21-03-2018
Week-3	**Definition:** Deploy framework and APIs **Mission:** Complete the MVC framework design, and finish at least one module, for example, we can download data from third-party organisations by using RESTful API method. **Risk:** If the deployed framework is unsuitable, that will delay the delivery time.	**Deliverables:** Framework directory and one executable work line. **Description:** Develop framework and finish the draft framework. The executable work line is completed. (State: Completed)	25-03-2018

Week-4	**Definition:** MongoDB creation and CRUD function development **Mission:** Make sure that the database could connect with local service, and CRUD operation could be run smoothly when using RESTful API (request GDAX public data and private data successfully get response); Finish the proposal draft. **Risk:** None	**Deliverables:** A connectable MongoDB and one executable work line. **Description:** Connect the database and finish at least one completing work line. (State: Completed)	28-03-2018
Week-5	**Definition:** Proposal Report **Mission:** Totally familiar with APIs in GDAX, Huobi and Binance.; Could store public and private data into the database; Could run frontend demo successfully; Proposal Report Due. **Risk:** Unsuitable API invoking may delay the delivery time.	**Deliverables:** Proposal Report **Description:** Finish two of three APIs invoking (GDAX and Binance). The frontend framework demo has been finished. Finish the proposal report	13-04-2018
Week-6	**Definition:** Cooperate work **Mission:** Front-end and back-end program will cooperate with each other smoothly; the visualisation of test data the development of main page (Navigate bar, menu, main page charts, exchange rate feed) should be completed. **Risk:** None	**Deliverables:** An executable work line between frontend and backend **Description:** Complete front-end first demo version and the development of main page template.	13-04-2018
Week-7	**Definition:** Integrate all the parts of project **Mission:** Complete the integration of different components and subpages, the major functionalities of backend and frontend should be implemented. **Risk:** Some parts may not work well, that will cost time to fix it.	**Deliverables:** A project can do the demo **Description:** Complete the demo project and start to optimize the performance.	25-04-2018

Week-8	**Definition:** **Mission:** All the development of features and functions complete, begin the project beta V1.0 testing process **Risk:**	**Deliverables:** **Description:** Testing the website performance by a series of processes	09-05-2018
Week-9	**Definition:** Progress Report **Mission:** Progress Report Due. And finish the work that may be delayed. **Risk:** None	**Deliverables:** Progress Report **Description:** Finish the progress report	11-05-2018
Week-10	**Definition:** Remote host testing **Mission:** Remote host testing; Multiple-platform testing (Chrome browser, Safari browser, iOS and Android browsers). **Risk:** If the remote host testing failed, that we will use local host to do the demo.	**Deliverables:** The project deployed on the real webserver. **Description:** Complete the remote host deployment and multi-platform test.	16-05-2018
Week-11	**Definition:** Documentation **Mission:** Complete all the documentations written. (user manual, Git readme, project report) **Risk:** None	**Deliverables:** Documentation **Description:** Finish the written of relative documentations.	23-05-2018
Week-12	**Definition:** Final Report **Mission:** Final Report (thesis) **Risk:** None	**Deliverables:** Final Report **Description:** Prepare and finish the final report	08-06-2018
Week-13	**Definition:** Final Presentation **Mission:** Final Presentation **Risk:** None	**Deliverables:** Final Presentation **Description:** Prepare and finish final presentation	22-06-2018

Table 1. Milestones and Reporting

VI. WEB TESTING UNIT

i. Functionality Testing

This unit test will focus on links, button click and scrolling within web pages, database connection between backend and frontend in running state, Cookie testing and so on.

ii. Usability testing

Usability testing is the process of which the interaction between human and machine. Though this process we can identify the problems and weakness when users, especially those who are not IT technicians, using our web application.

iii. Compatibility testing

The main components in compatibility testing consisted of browser compatibility, operating system compatibility, mobile browsing, printing options.

iv.Performance testing

Web performance testing should include Web Load Testing and Web Stress Testing. Test application performance on different internet connection speed.

v. Security testing

The potential vulnerabilities in a web application includes network Scanning, vulnerability scanning, password cracking, log review, integrity checkers, virus detection (Security and Penetration Testing, 2009).

Thanks for reading and comments.

VII. REFERENCE

Dannen, C. (2017). *Introducing Ethereum and Solidity. [S.l.]: Apress.*

XY chart with date-based axis - amCharts. (2018). *amCharts*. Retrieved 3 April 2018, from https://www.amcharts.com/demos/xy-chart-date-based-axis/

ECharts Demo. (2018). *Ecomfe.github.io*. Retrieved 3 April 2018, from https://ecomfe.github.io/echarts-examples/public/editor.html?c=candlestick-brush

Live order book / depth chart - amCharts. (2018). *amCharts. Retrieved 3 April 2018, from* https://www.amcharts.com/demos/live-order-book-depth-chart/

IT Outsourcing India. (2018). *Web Applications Development Methodology - Pillars of strength, IT Outsourcing India*. Retrieved 28 Mar 2018, from http://www.itoutsourcingindia.com/about/web

Security and Penetration Testing. (2009), Retrieved 10 April 2018, from The Official 360 logical Blog website, from https://www.360logica.com/blog/security-and-penetration-testing/