SCHOOL OF
ELECTRICAL AND
ELECTRONIC ENGINEERING

THE UNIVERSITY of ADELAIDE

Modelling the Dynamics of the Cryptocurrency Market

Nikolaos Flabouris
(Partner: Jeremy Abbot)

ELEC ENG 4068 Honours Project

Each student at Level IV in the School of Electrical and Electronic Engineering is required to complete a final-year design or honours project. The course involves approximately 300 hours of project work over the whole academic year. Students are assessed on their performance in the project, the quality of their outcomes, two progress reports, a final report, two seminars and a project exhibition.

Date submitted: 1st June 2018
Supervisors: Derek Abbott, Azhar Iqbal, Matthew Sorell

Acknowledgments

I would like to thank my partner Jeremy Abbot for working alongside me to complete this project. Thank you to our three supervisors Derek Abott, Azhar Iqbal and Matthew Sorell for their guidance throughout the development of this project. This project was also supported by the School of Electrical and Electronic Engineering at the University of Adelaide.

Executive Summary

As the relevance of cryptocurrencies grows so does the need to better understand the cryptocurrency market. This project aims to develop a model that approximates the cryptocurrency market. Using this model, and the research required to develop this model, an investigation of the dynamics of the market will be conducted. The dynamics of individual currencies will first be tracked followed by the interdependency of cryptocurrencies.

Contents

1 Introduction **5**

2 Background **5**

2.1 Technical Background 5

2.1.1 Blockchain 5

2.1.2 Transactions in Cryptocurrency Markets 6

2.2 Related Work 7

2.3 Knowledge Gaps 8

2.4 Significance 8

2.5 Motivation 8

2.6 Aims and Objectives 9

3 Methodology **9**

3.1 Method 9

3.2 Technical Challenges 10

3.3 Requirement Constraints 11

3.4 Justification 11

3.5 Deliverables 11

3.6 Project Management 13

3.6.1 Task Allocation 13

3.6.2 Timeline 13

3.6.3 Budget 13

3.6.4 Risk Management 14

4 Results **14**

4.1 Progress Report 14

5 Discussion **17**

5.1 Findings 17

5.2 Evaluation 17

5.3 Strengths and Weaknesses 17
5.4 Relevance 17
5.5 Future Work 17

6 Conclusion **17**

A Appendix: Source Code **18**

1 Introduction

In October 2008 the paper *Bitcoin: A Peer-to-Peer Electronic Cash System* written by a mysterious individual or group under the name *Satoshi Nakamoto* was released [1]. Over the next ten years bitcoin and other cryptocurrencies have grown into a booming market hitting a total market cap of $300 billion in April 2018 [2]. Many of these currencies rely on the blockchain technology introduced by *Satoshi Nakamoto* which allows for a decentralised ledger of transactions. As a result traders all over the world can safely trade their cryptocurrencies without the need of a central authority to monitor and verify each transaction.

To date the main use of these cryptocurrencies has been for the transfer of wealth. However developers are looking to leverage more of the power that the blockchain technology provides. The Ethereum Project provides functionality for the creation of smart contracts, executing programs on a distributed network and an operating system [3]. Payments for these services are conducted by the trade of the Ether cryptocurrency.

As the functionality of cryptocurrencies grow the need to understand their market characteristics also grows. Cryptocurrencies have the potential to provide the basis for implementing future technology. Thus it is important to learn as much as possible about the dynamics of individual cryptocurrencies as well as their relationship to other cryptocurrencies.

2 Background

2.1 Technical Background

2.1.1 Blockchain

The blockchain allows for a public ledger of every transaction of a cryptocurrency. It was first described in 2008 [1] to replace the role of centralised monetary authorities for electronic payments. As suggested by the name a blockchain is made up of individual blocks of data. Within each block is a header section and a set of transactions that have been verified and completed. The header contains information about the current block and a link to the previous block.

The blockchain is decentralised meaning that copies of it exist all over the network. It is verified based on consensus. The correct blockchain is the most common blockchain in the network. With this structure a single attacker will struggle to propagate their false version of the blockchain through the network as it will be drowned out by the numerous copies of the correct blockchain.

The network uses a process called mining to decide on the next block in the chain. Miners collect transactions that users have requested to be completed and added to the blockchain. Each miner will then attempt to find a specific cryptographic hash of the previous block, a set of new transactions and a special number called a nonce [1]. Effectively the miners use the required inputs to find a random number of a specific format. What makes this process difficult is that there is no way to predict or efficiently work towards producing the desired output.

The process of calculating the hash is fast. The fastest way to create a hash of a certain structure is to brute force the solution, that is to continuously try different values until a correct solution is found. Each miner will attempt to find a nonce value that when combined with their transactions will produce a correct hash. When a miner finds a correct value for their transactions the information is broadcasted across the network. Each node on the network will verify the hash is correct and then add it to the blockchain [1].

The process of mining can be computationally intensive. Powering personal machines to perform these calculations is costly. To reward miners for sharing their computational power, a miner who is successful in calculating the next block for the chain is rewarded with a set amount of new coins as well as the transaction fees from the transactions included in that block. For currencies like Bitcoin, as more of the currency is introduced into the market less is provided as a reward. For example the total number of Bitcoin is capped at 21 million [1]. Eventually once all of the currency is in circulation miners will only be rewarded by the transaction fees. As miners receive the transaction fees from the transactions they include, it is more beneficial for them to include transactions paying a larger fee. This means any trader who wishes to have their transaction processed sooner should pay a larger fee.

2.1.2 Transactions in Cryptocurrency Markets

Markets will list the exchange rates for each cryptocurrency they support. These exchange rates will vary from market to market as they reflect the rates used in the transactions conducted through a particular market. When a trader submits a transaction into the market it is compared against existing transactions in the market. If a suitable match is found the transaction is completed up until one of the trader's orders has been completely fulfilled. A suitable match is a transaction that offers an equal or better exchange rate. The exchange rate used for the transaction is that specified by the transaction that has existed for the longest time. These rules are common across many cryptocurrency markets [4]. Most markets accept two types of orders, market and limit orders.

Market orders are opened immediately from their creation and are conducted at the current market price. Due to the rapidly changing nature of the cryptocurrency market the exchange

rate used for these transactions can vary from the time the trader submits the order and the time it is matched. This can result in a trader receiving less then they initially expected. The main benefit of this type of order is that the orders are entered into the market immediately and are often matched quickly.

Limit orders are placed into the market but are only opened once the market price has hit a certain limit price specified by the trader. Often they will include a time limit for when the transaction must be completed by after which the transaction will be cancelled. When the market price is better then the limit price the limit order will become a market order. Limit orders are more reliable as they will always be conducted at the specified exchange rate, or better, but may take longer to complete.

2.2 Related Work

Cocco et al have developed a heterogeneous agent model based on artificial models developed for financial markets [5]. Their model focuses on the performance of Bitcoin compared to a fiat currency. Some of the key features that identified for their model are the completion of transactions with buy and sell orders, initialising traders with a limited amount of financial resources and the random donation of Bitcoin to random traders to represent mining profits. They have chosen to define two types of traders, Random Traders and Chartists. Random Traders make their decision at random and represent traders who are not making a prediction on the future. They also provide a wide range of buy and sell orders for other more strategic traders to invest around. Chartists make transaction decision based on a prediction of the future price of the currency. By tailoring their initialisation and control values they were able to create a model that replicates many of the cryptocurrency market characteristics.

Phillips et al utilise social media data to predict price bubbles in the cryptocurrency market [6]. They determined that the social media platform Reddit [7] is ideal for modelling social media traffic related to a specific currency due to the structure of *subreddits*. Reddit allows communities to discuss and share information in forum like posts. Subreddits are individual pages with the site the contain posts related to a single topic. As a result the individual subreddits for each currency can be tracked and used to represent the media traffic for each currency. Using this data they were able to accurately detect bubbles in the market and form trading strategies that were more effective then the buy and hold strategy over the same period.

Kim et al looked at the relation between price fluctuations and forum activity [8]. They crawled along and tracked the posts and replies on popular forum pages for Bitcoin, Ethereum and Ripple. Each post and reply was classified as either very negative, negative, neutral, positive or very positive. They found that the forum activity was an accurate indicator for

future trends. Using this information they developed a trading model that performs better then that of a random trading pattern.

ElBahrawy et al used mathematical models to determine trends in the cryptocurrency market from April 2013 to May 2017 [9]. They show and exponential growth in the total cryptocurrency market share, decreasing Bitcoin market share and the equalising of the birth and death rates of cryptocurrencies. For the purposes of trading, their model assumes no preference to any cryptocurrency in particular. All cryptocurrencies are treated equally. Their results reflect this with no currency in particular showing to be better then the others. *ElBahrawy et al* also tie significant changes of price to legislation, technical and socio-economic factors.

2.3 Knowledge Gaps

While there has been research conducted into Bitcoin specifically and its market characteristics there has been less research on the interdependence of cryptocurrencies. This project aims to built a model that can allow for a measured analysis between cryptocurrencies. The model will allow for a better understanding of the whole cryptocurrency market not just its most popular currency.

2.4 Significance

Cryptocurrencies, like Ethereum, include systems for creating and completing contracts as well as providing the ability to purchase computational power from the distributed network of miners and develop programs using their programming language [3]. Understanding the nature of this volatile marketplace will, in the short term, allow for a better understanding of the trading of cryptocurrencies. In the long term a better understanding of the dynamics between cryptocurrencies will be required if they are to be utilised for other purposes, such as a platform for running programs on a distributed network.

2.5 Motivation

Many people around the world are now able to legally trade in cryptocurrencies. Countries have legislated allowing for the trade of cryptocurrencies like Bitcoin [10]. The Marshall Islands have even issued for a new Cryptocurrency to be used alongside the US Dollar as a legal currency of the nation [11]. With the increase in prevalence of cryptocurrencies there is an increasing need to understand their market characteristics. This project will assist in providing those who wish to invest in the cryptocurrency market an understanding of the

factors they need to consider. Those looking for the future uses of these currencies will benefit from knowledge of their current characteristics and relationships with other currencies.

2.6 Aims and Objectives

The aim of this project is to develop a model that replicates the dynamics of the cryptocurrency market. This model will be used to analyse the:

- cryptocurrency market dynamics
- cryptocurrency market share distribution
- cryptocurrency prices
- cryptocurrency price stability
- effects of the birth and death of new cryptocurrencies
- interdependency of cryptocurrencies

3 Methodology

3.1 Method

To model the cryptocurrency market an agent based model will be developed and used. This type of model was chosen due to the characteristics of the market and its similarities to an agent based model. Within the market are traders who, based on the rules and state of the market, make decisions on how they wish to trade their currencies. Each trader acts as an agent within the environment of the market. They make decisions which in turn change the environment. They then reassess the environment and make their next decision.

The agent based model will be developed in the C++ programming language. A certain number of traders will be initialised with a starting amount of fiat money and cryptocurrencies. The market will be initialised with exchange rates from a given date. At each time step the traders will make a decision on whether they wish to make a transaction and for which currency. They will also decide on their preferred exchange rate and the amount the wish to trade. The market will collect all of these transactions and match the transactions based on the rules of a typical cryptocurrency market.

Cryptocurrency markets generally process transactions by time of arrival. To simulate transactions arriving at different times the list of transactions will be randomised at each time

step. Once a transaction is added to the market it is first checked against existing transactions to see if a match can be found. Transactions are matched when they have an equal or better exchange rate. When a match is found the transactions are completed by using the exchange rate of the oldest transaction, i.e the transaction that arrived at the market first. The total amount exchanged will be the minimum of the two transaction amounts so one transaction will always be completed. If the other transaction requested more of the currency then the first transaction supplied it will be re-added to the queue in its original location requesting the remaining amount.

An example of this would be a when a transaction purchasing 10 Bitcoin is matched with a transaction selling 5 Bitcoin due to there equivalent exchange rates. After completing the transfer of 5 Bitcoin the sell order will be removed and the buy order will be placed back in its original location in the queue requesting the 5 remaining Bitcoin at the same exchange rate.

After running the model over a certain number of days the data each day will be saved analysed in MATLAB [12]. MATLAB is a powerful mathematical based program that allows for the processing and displaying of data. MATLAB programs will be created so, after each test run of the model, the data can be quickly processed, displayed and analysed.

3.2 Technical Challenges

The two largest technical challenges for this project are replicating the behaviour of the market and of the individual traders.

While the role of the market may seem intuitive, to create an accurate model it is important to identify all of the rules and processes. How currency prices are calculated, how traders are matched and how transaction fees are calculated can change from market to market.

For the purposes of our model, fees will be applied to traders who exchange their fiat currency for cryptocurrency. Traders will be able to freely trade between cryptocurrencies. When a trader wishes to exchange their cryptocurrencies back to fiat they will encounter a fee. This resembles the fee structure within the cryptocurrency market.

Initially our model will not run in real-time. In an effort to mimic the cryptocurrency market all submitted transactions will be collected and randomly arranged at each time step. The resulting order will be the order in which the transactions were received. With each iteration the list of transactions will be checked against earlier transactions to see if they can be paired. If a match is found the exchange rate of the oldest transaction will be used, as per the rules for many of the cryptocurrency markets.

Traders of cryptocurrencies make decisions in many different ways based on different sources

of information. They each invest different amounts and have different goals. It is important for an accurate model that the traders make decisions similar to those of the real world. The reasons behind a trader making a transaction could range from the market prices to exposure from cryptocurrency media or based upon their own individual thoughts and feelings. Identifying logical ways of representing these processes is crucial to developing an accurate model.

One approach will be to include Google Trends data on cryptocurrency related searches into our model. This will replicate the amount of media exposure on the traders.

To ensure traders used in our model accurately represent those in a real market the traders will be initiated with a proportionate amount of cryptocurrency. This will ensure that there is an appropriate amount of low and high stakes traders so that the performance of each can be tracked.

3.3 Requirement Constraints

As this project is research focused there are very few requirement constraints. There is flexibility in both the scope of the project and the methodology. The main constraint of this project is time. There are several deliverables that must be provided by the specified deadlines.

3.4 Justification

One key decision for this project was to use an agent based model. This model was chosen for two main reasons, the first being that this type of model is quite similar in structure to the cryptocurrency market. The second reason is that an agent based model can be built with a modular approach. This will allow for individual components to be upgraded while maintaining the rest of the project. This will be beneficial during the development for this project as well as any future work that may be conducted using this model.

3.5 Deliverables

Proposal Seminar

The first deliverable is the proposal seminar. The seminar will be presented to a group of peers. At this seminar a brief background on the topic, an outline of the scope of the project and its propose approach will be presented.

Draft Thesis

The draft thesis marks the mid point of the project. The purpose of the draft thesis is to demonstrate progress on the project. At this point much of the work that will be included in the final thesis could be included. The draft thesis will include a literature review, an outline of the methodology and preliminary results.

Project Video Summary

Upon completion of the project it has been requested that a short video review of the project be created and uploaded to the video hosting site YouTube. The video will provide for a brief introduction into the project and the results.

School of Electrical and Electronic Engineering Honours Wiki Page Entry

There is a Wiki page for all honours projects completed under the school of Electrical and Electronic Engineering. At the completion of the project the Wiki page will be populated with a synopsis of this project.

Supervisor's Projects Wiki Entry

Similar to the School's Honours Wiki page, one of the supervisors has requested that a Wiki page be completed for this project on his site. However this page will be structured as more of a repository of the information collected and created during the project development.

Project Poster

At the end of the project, a poster will be created for display at the Adelaide University's Ingenuity Event. At this event the project will be presented to university staff, industry representatives, other University Students and the general public. The poster will serve as a means to briefly convey the scope and results of the project.

Software Model

The software model used for this project will be packaged and delivered for the purposes of following and reproducing the results from this project as well as for future groups to expand and improve the model.

Final Thesis

The final thesis designates the end of the project in terms of development. A complete description of related work, methodology and results will be included. A full evaluation of the project and the results will also be included.

3.6 Project Management

3.6.1 Task Allocation

The project has been divided into two main sections. The focus of my work has been to investigate the details of the cryptocurrency market and to start implementing our model. The focus of my partner's work has been to source and collect real world data related to the cryptocurrency market and begin creating tools for the analysis of its characteristics.

3.6.2 Timeline

The project timeline in figure 1 shows the key project tasks in orange and the internal project milestones in blue. All start dates refer to when work on the task must start by, work can begin beforehand. All project tasks must be completed by their deadline. Milestone deadlines are soft deadlines. Should a task not be completed by its deadline a review will be conducted to assess its progress and to review the cause of its delay. Significant delay in the completion of the task would either suggest a failure in progress or an underestimation of the workload for this task. If required, adjustments will be made to the project timeline based on the reasons of any delays.

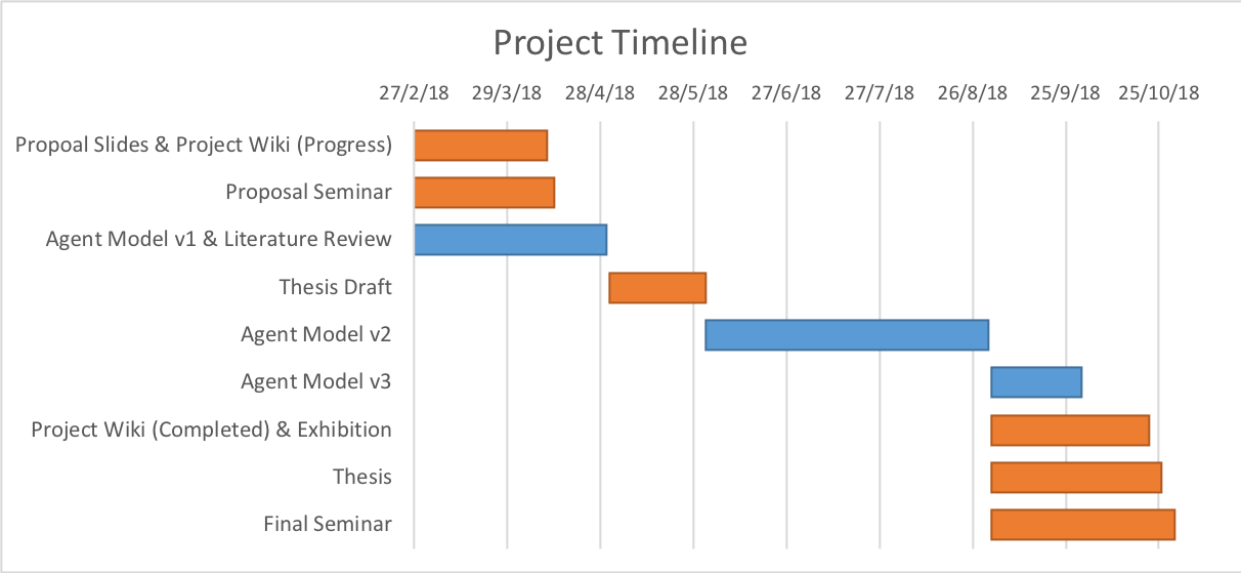

Figure 1: Gantt chart for this project. Orange tasks have fixed deadlines. Blue tasks have variable deadlines.

3.6.3 Budget

Much of the data and resources required to complete this project are either freely available from online resources or freely available via the University's licences. As a result there are

no expected expenses for this project.

3.6.4 Risk Management

The main risk associated with this project would be the loss of the model source code. This component of the project would be the hardest to recover. To mitigate this risk Github, a free online version control application, will be used to store all source code related to this project.

4 Results

4.1 Progress Report

Work on the model has begun with the creation of the market, currency, trader and transaction classes. These classes have been created as the following.

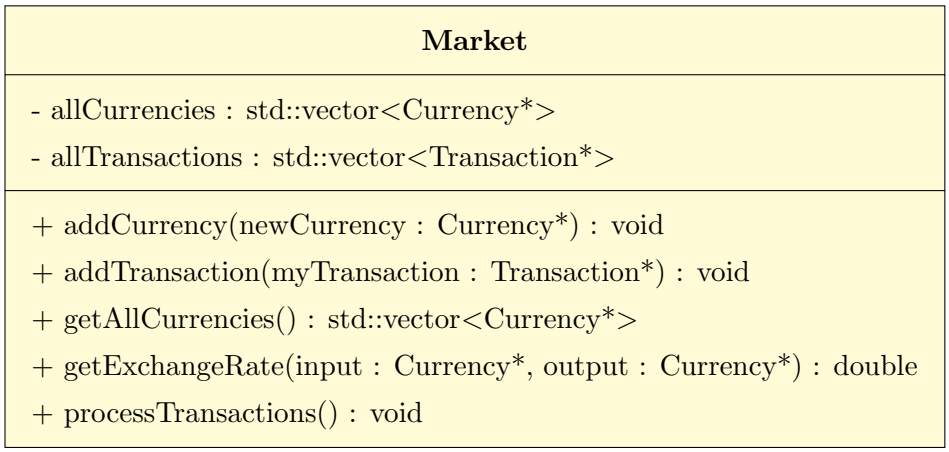

Figure 2: UML Diagram for Market Class

Various trader classes will be derived from the base Trader class. Each type of trader will have a different implementation of the *calculateTransaction* function.

A single market is created. Currencies are added to the market as being open for trade. Each trader is successfully initialised with a starting amount of the currency. At each time step each trader selects a currency to buy and a currency to sell. These transactions are successfully created and added to the market. Currently the market fails to correctly identify matching transactions. Once this is achieved the decision making process of the traders can be improved to incorporate factors that affect cryptocurrency traders.

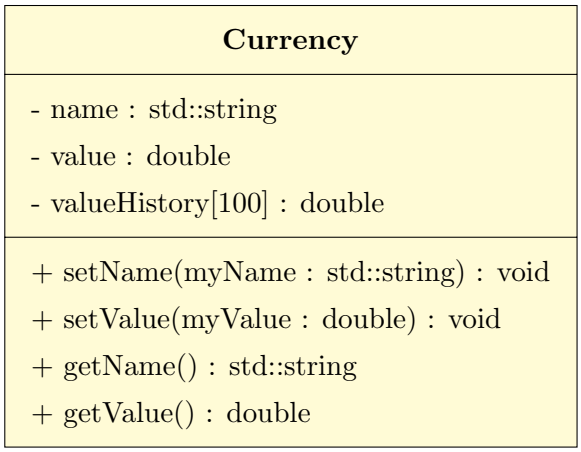

Figure 3: UML Diagram for Currency Class

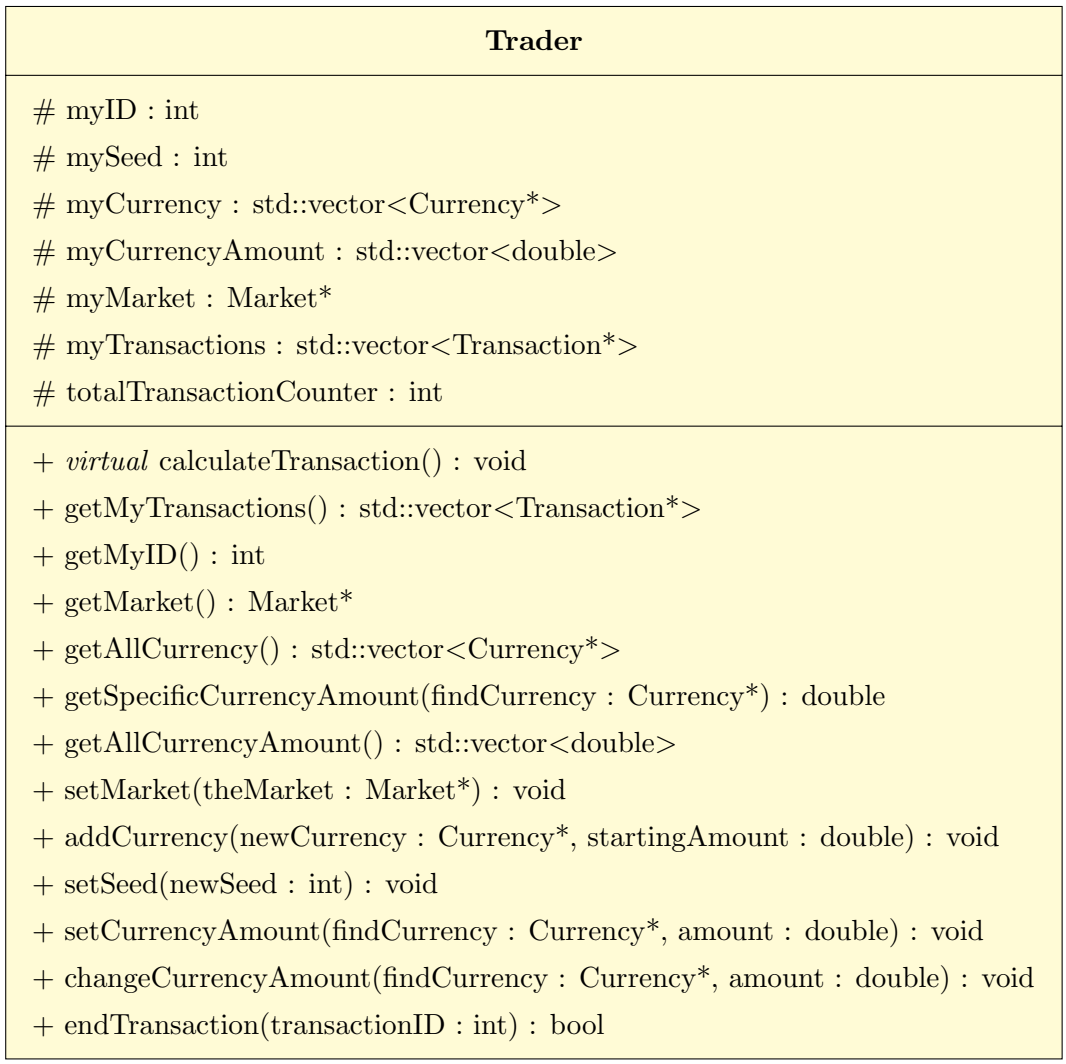

Figure 4: UML Diagram for Trader Class

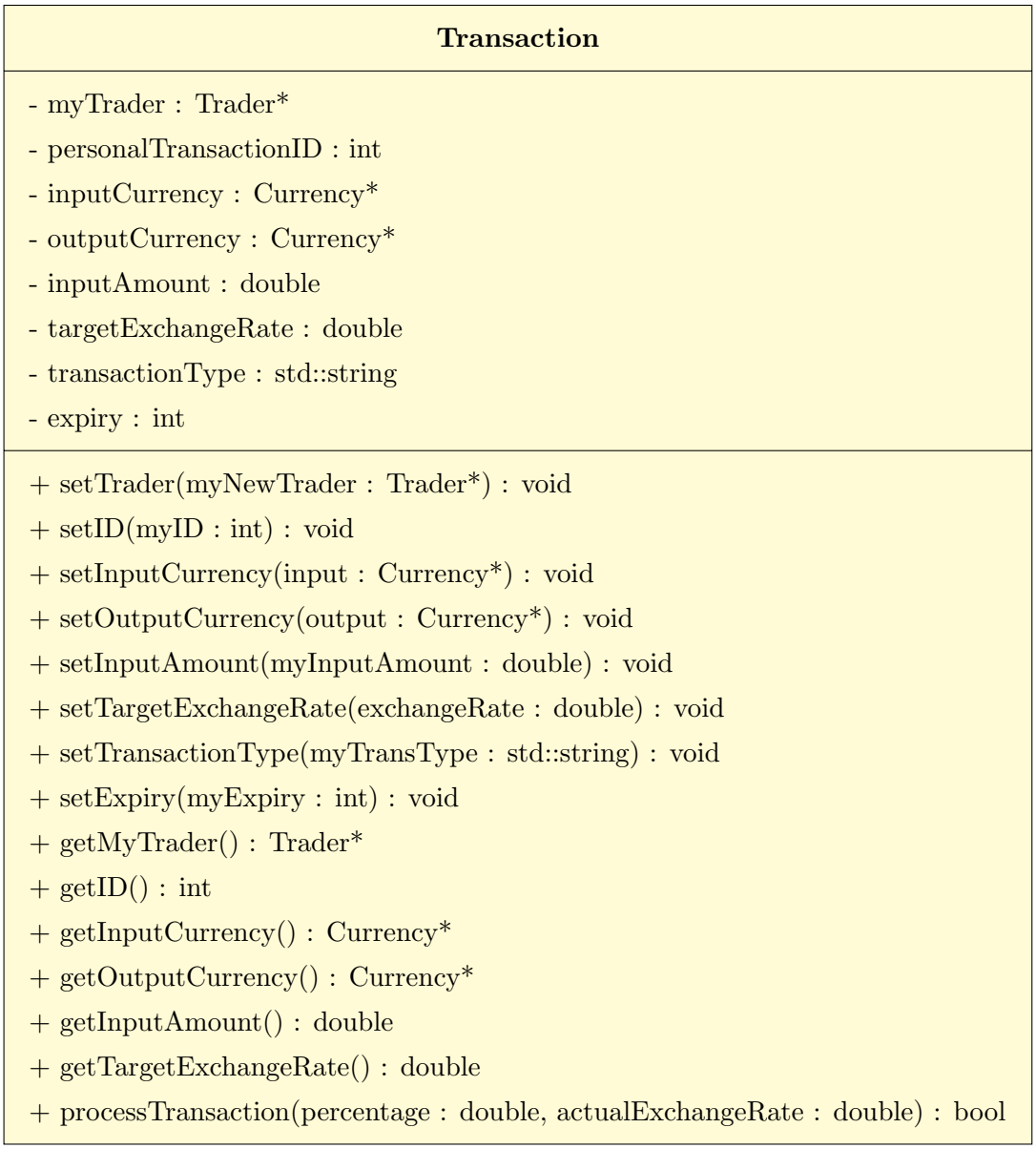

Figure 5: UML Diagram for Transaction Class

5 Discussion

5.1 Findings

5.2 Evaluation

5.3 Strengths and Weaknesses

5.4 Relevance

5.5 Future Work

6 Conclusion

With the growth of the cryptocurrency market it is important to develop an understanding of the factors that effect the price of cryptocurrencies. As means to better understand how certain factors relate to any individual currency, as well as across multiple currencies, development on an agent based model has begun. The model will utilise data from the real world to inform traders the factors that will affect their decision making process.

A Appendix: Source Code

The source code for this project can be found via the following GitHub link (University of Adelaide login required):
`https://github.cs.adelaide.edu.au/a1670595/CryptocurrencyModel`

References

[1] S. Nakamoto, “Bitcoin: A Peer-to-Peer Electronic Cash system.” Oct. 2008

[2] P. Ivancic, CryptoSlate (2018, Apr. 12) “Cryptocurrency Market Cap Surpasses $300 Billion On Strong Bitcoin Rally”[Online] Available: https://cryptoslate.com/cryptocurrency-market-cap-surpasses-300-billion-on-strong-bitcoin-rally/

[3] ”Ethereum Project”, Ethereum.org, 2018. [Online]. Available: https://www.ethereum.org/. [Accessed: 01- Jun- 2018].

[4] ”Order matching and price determination”, GDAX, 2018. [Online]. Available: https://support.gdax.com/customer/en/portal/articles/2429575-order-matching-and-price-determination. [Accessed: 01- Jun- 2018].

[5] L. Cocco, G. Concas, M. Marchesi, “Using an artificial financial market for studying a cryptocurrency market.” Oct. 2015

[6] R. C. Phillips and D. Gorse, “Predicting Cryptocurrency Price Bubbles Using Social Media Data and Epidemic Modelling” Nov. 2017

[7] ”Reddit: the front page of the internet”, Reddit.com, 2018. [Online]. Available: https://www.reddit.com/. [Accessed: 01- Jun- 2018].

[8] Y. B. Kim, J. G. Kim, W. Kim, J. H. Im, T. H. Kim, S. J. Kang, C. H. Kim, “Predicting Fluctuations in Cryptocurrency Transactions Based on User Comments and Replies.” PLoS ONE 11(8): e0161197. doi:10.1371/journal.pone.0161197, Aug. 2016

[9] A. ElBahrawy, L. Alessandretti, A. Kandler, R. Pastor-Satorras, A. Baronchelli, “Evolutionary dynamics of the cryptocurrency market” Oct. 2017 *R. Soc. open sci.*

[10] U. W. Chohan, “Assessing the Differences in Bitcoin and Other Cryptocurrency Legality across National Jurisdictions” Sep. 2017

[11] A. Hamacher, Blockchain News (2018, Feb. 28) “Marshall Islands Issues Own Cryptocurrency”[Online] Available: http://www.the-blockchain.com/2018/02/28/marshall-islands-issues-cryptocurrency/

[12] ”MATLAB - MathWorks”, Au.mathworks.com, 2018. [Online]. Available: https://au.mathworks.com/products/matlab.html. [Accessed: 01- Jun- 2018].