
An Analysis of the Viability and Volatility of Cryptocurrency

Rebecca Kane

Tara O'Kelly

B.Sc.(Hons) in Software Development

APRIL 2018

Final Year Applied Project and Dissertation

Advised by: Dr Ian McLoughlin

Department of Computer Science and Applied Physics
Galway-Mayo Institute of Technology (GMIT)



Contents

1	Introduction	6
1.1	Objectives for the Project	7
1.1.1	Metrics for Success/Failure	9
1.2	Description of Each Chapter	9
1.2.1	Understanding Cryptocurrency	9
1.2.2	Predicting the Prices of Cryptocurrency	10
1.2.3	Currency Analyser Web Application	10
1.2.4	Conclusion	10
2	Understanding Cryptocurrency	11
2.1	The Arrival of the First Digital Currency	11
2.2	The Arrival of Modern Cryptocurrency	12
2.2.1	An Explanation of Modern Cryptocurrency	13
2.2.2	Comparing Traditional Currency and Cryptocurrency	15
2.2.3	A Focus on Bitcoin	15
2.3	Blockchain Technology	17
2.4	The Viability of Cryptocurrency	18
3	Predicting The Prices of Cryptocurrencies	20
3.1	The Volatility of Cryptocurrency	20
3.1.1	Influencing Factors in Cryptocurrency Prices	21
3.2	Transition to Applied	21
4	Currency Analyser Web Application	22
4.1	Methodology	22
4.1.1	Preliminary Research and Project Commencement	22
4.1.2	Issues Encountered Throughout the Development Process	27
4.2	Technologies / Tech Review	29
4.2.1	Python 3 and the Flask Framework	30
4.2.2	Redis	30

4.2.3	MongoDB	30
4.2.4	Vue.js	30
4.2.5	Chart.js	30
4.2.6	TensorFlow	30
4.3	System Design	30
4.4	System Evaluation	30
5	Conclusion	32
5.1	Context/Objectives	32
5.2	Findings	32
6	Appendices	33

About this project

Abstract A brief description of what the project is, in about two-hundred and fifty words.

What it is, analytics part and applied project part, volatility, viability, predicting prices etc.

Authors Will get everyone to write their own?

Acknowledgements

The authors wish to thank their fellow students, who offered advice on many aspects of this project on many occasions.

We would also like to acknowledge the many lecturers we have had the pleasure of knowing throughout our time at Galway Mayo Institute of Technology, many of whom have left a lasting impression on us and will continue to inspire our work long after our time at GMIT has come to an end.

We would like to thank our families and friends for bearing with us in our stressed and worried states, always willing to offer listening ears and emotional support.

Last but certainly not least, we wish to sincerely thank our project supervisor, Dr. Ian McLoughlin, for offering endless advice on every aspect of this project. His always calm and collected nature never failed to reassure us, even when we were at our most stressed. The advice of "get some cake, take a break" will forever encourage us in times of frustration.

Chapter 1

Introduction

Throughout our first three years of Software Development at Galway-Mayo Institute of Technology, we have continuously been encouraged to maintain a comprehensive knowledge of the trends within the technology industry, and to embrace its ever-changing nature.

When initial meetings to discuss possible project ideas began in September 2017, there was a mutual agreement within the team that a concept that would be interesting, distinct from other projects, and most importantly be beneficial and of use in its field, should be pursued. After numerous ideas were considered and after much deliberation, it was decided that a focus on the area of Cryptocurrency and more specifically, analysing changes in the market and attempting to decipher trends in prices, would be appropriate. We felt this was a good decision as we weren't aware of any similar projects from previous years, and most importantly, we all had a keen interest in the topic outside of academia.

A mere five years ago, cryptocurrency was a relatively unheard of phrase to the average individual. In the years since, the likes of Bitcoin and Ethereum have become almost household terms, with many more people investing in various cryptocurrencies and following their repeating rise and decline. While cryptocurrencies were initially a mystery to the average individual, the arrival of user-friendly trading sites has meant they have now become an almost common asset, seen regularly in the news and no doubt discussed over many water coolers.

Although cryptocurrency is no longer seen as an unobtainable investment, meant only for those with an in-depth knowledge of how to keep their digital currency stored safely and properly, there still exists a mystery surrounding when the best time is to buy or sell. This uncertainty, coupled with our own interest in the field, was the inspiration behind this final year project - we wanted to attempt to predict the price of some of the more popular

cryptocurrencies and deliver these predictions to users in a simple manner that could be understood by anyone with even a basic knowledge of the area of cryptocurrency.

In this dissertation, we aim to first give the reader a good understanding of what exactly cryptocurrency is, how it works and the various technologies behind it. We will also examine the volatility of cryptocurrency as an asset, and the influencing factors in the changing of its prices. Following the more theoretical chapters we will move to discussing the applied aspect of this project, in which we will outline and explain the development process and reasoning behind technologies used, among other relevant topics. Finally, we will conclude the dissertation with a summary of the project as a whole, along with any discoveries gained throughout the project.

1.1 Objectives for the Project

As mentioned previously, our main objective for the project was to make the area of cryptocurrency more accessible to an individual with little knowledge of the field.

As our project is divided into a research-based dissertation and an applied project, we will discuss goals in relation to each aspect. Our objectives for this dissertation are

- *Introduce the concept of this project:* We will provide the reader with an introduction to our project, detailing our inspiration and goals.
- *Provide the reader with a rounded understanding of cryptocurrencies:* We aim to explain where cryptocurrency began, and the concept of modern cryptocurrency in simple terms including how to begin trading cryptocurrency and the underlying technologies. We will also explain the overall viability of cryptocurrency as an asset, based on its fundamental components.
- *Explain to the reader how volatile cryptocurrency prices can be:* Having provided the reader with an understanding of cryptocurrency, we will proceed by discussing the prices of cryptocurrency; how they are determined, and what can inadvertently affect them. We will consider the prediction of prices, or rather the inability to predict prices, examining any existing methods which aid in the uncertain forecasting of prices.
- *Describe in detail the applied aspect of this project:* We will examine our approach to the applied project, including methodologies and technologies used, and design and evaluation of the system. We will also

be discussing any issues we had throughout the project and how they were resolved, what we would do differently in future, and what we will be keeping in mind for future group projects.

With regards to the applied aspect of this project, our objectives for this project are as follows:

- *Create a simple web application which is easy to use and clear to understand:* While the web application is intended to be an extension of our dissertation, we will be developing it with even the most inexperienced of users in mind. In our experience, any websites related to cryptocurrency are often daunting at first sight due to the extensive numbers of graphs, percentages, and unfamiliar terminology - we aim to make our application more encouraging to unfamiliar users.
- *Deliver cryptocurrency prices to the user:* We aim to bring up-to-date prices for the Bitcoin currency to the user in the form of an easily interpreted graph. The user will be able to view the price in comparison to a traditional currency, such as the Euro.
- *Provide an educated guess as to future changes in prices:* We aim to use Machine Learning and Neural Networks to provide the user with an educated estimate as to what a price will change to. We do not aim to predict prices accurately, as this is impossible due to the variety of factors that influence prices, however we will use previous price data to attempt to decipher any trend, and relay that information to the user through our application.
- *Stay in line with the given learning outcomes for this project:* We endeavour to meet all requirements for the research and development process of this project. This includes carrying out extensive research, applying appropriate methodologies and project management techniques, taking advantage of relevant new technologies, and critically evaluating the work including identifying any strengths, weaknesses and future recommendations.
- *Conduct ourselves as a team, in a professional manner akin to what is expected in industry:* We aspire to work together as a team, free from disrespect or inequality. We aim to make sure no one person feels as though they should take over the project, and will work to resolve any issues in a calm and coordinated manner. It is often observed that friendships are compromised when an important project is added to

the equation, but we aim to keep our personal and academic lives as separate as possible for the duration of this project. In the event of a disagreement, we will aim to not let it negatively affect any friendships.

1.1.1 Metrics for Success/Failure

Our metrics for success or failure undoubtedly relate closely to the aforementioned objectives. A definitive list of metrics for success for the project as a whole, including dissertation and web application, is as follows:

- *An easily understood, cohesive dissertation which can be read from beginning to end by anyone unfamiliar with the topic and leave them with a solid understanding of the ideas discussed.* To measure this, we will ask various friends and family who know little about the area of cryptocurrency to read given sections of the dissertation, and ask for their feedback.
- *A simple, effective web application:* Again, to measure this we will ask some friends or family to use the web application for a short time and to give us their opinion of its usability and how informative it was afterwards.
- *Educated guesses of future cryptocurrency prices:* We will measure the accuracy of our predictions against the actual data. We will carry out this examination the week prior to submission.
- *Teamwork:* We will measure the success of our teamwork by reflecting on how we resolved any issues, and how we conducted ourselves in stressful times. As mentioned in our objectives, we aim to not let any disagreements come between the friendships we had when beginning this project - intact friendships at the conclusion of this project will also be a measure for success or failure.

1.2 Description of Each Chapter

In this section, we will briefly outline what each chapter of this dissertation centres around.

1.2.1 Understanding Cryptocurrency

In chapter 2, *Understanding Cryptocurrency*, we first detail where cryptocurrency began, before explaining in simple terms what exactly a cryptocurrency

is, and how it differs in various ways from a traditional currency. We then examine the most popular and well-known cryptocurrency, Bitcoin, before delving into some of the technologies behind cryptocurrency, such as blockchain technology. This chapter centres around the viability of cryptocurrency as a whole.

1.2.2 Predicting the Prices of Cryptocurrency

Chapter 3, *Predicting the Prices of Cryptocurrency* what exactly a cryptocurrency is, and how it differs in various ways from a traditional currency contrasts the previous chapter by detailing how volatile cryptocurrency can be. We will explain what directly and indirectly affects the prices of cryptocurrency, specifically referencing Bitcoin. We then discuss the inability to absolutely predict prices of any cryptocurrency, followed by a more upbeat outlook of making educated estimates of price changes coupled with any existing methods of doing so.

1.2.3 Currency Analyser Web Application

This chapter discusses the applied aspect of this project, building on information discussed in the previous chapters. We examine the methodologies and planning used throughout our project, also dealing with any aspects which could have been planned or managed better. This chapter also explains in detail the technologies used for the applied project, their reasons for being chosen, and any problems that occurred related to the technologies. We then discuss the design of our system including reasoning, followed finally by an overall evaluation of the system.

1.2.4 Conclusion

The concluding chapter of this dissertation will summarise our initial goals and objectives, reflecting on the theoretical and applied aspects of this project, both conceptually and in practice. We will discuss any aspects of the process which could have been done differently, and lastly highlight any findings and any relevant, tangential or even unrelated insights gained during the project life cycle.

Chapter 2

Understanding Cryptocurrency

Since the first signs of digital finance in the 1970s, the financial services industry has relied more and more on new technologies and advancements in existing technologies. With the advent of the internet in the 1990s, becoming popular and more accessible in the 2000s, online banking was soon to become a commonplace financial service. As the internet grew and became faster, we witnessed an increase in both companies and individuals taking advantage of a variety of digital finance software, with respect to buying and selling goods and services and even trading stock.

2.1 The Arrival of the First Digital Currency

One of the first plausible instances of a digital currency, which paved the way for all cryptocurrencies we know today, was DigiCash. In 1983, David Chaum proposed the idea of using "blind signatures" for untraceable digital payments [1]. Similarly to the fears of the public today, Chaum discusses the issue of privacy in banking, also arguing that there would be a need to prevent digital payments from being used inappropriately such as in a criminal manner. Chaum follows by identifying the issue that knowledge of payment details such as payer or recipient details, by anyone other than the payer can often reveal sensitive information about that payer, such as their interests or whereabouts. Furthermore, Chaum also highlights the lack of security and control related to traditional bank notes and cheques. To resolve this issue, Chaum proposed the use of blind signatures, which work by concealing the content of a message through the use of "nested envelopes" (an envelope within an envelope) containing the message being passed back and forth between payer and recipient. More importantly, Chaum describes how this blind signatures system could be used in the implementation of an un-

traceable payments system, outlining an example of how a single transaction would take place -

The payer chooses a value to send to the recipient, and forwards the note to the bank. The bank signs the note, debits the payer's account, and returns the signed note to the payer. At this point the amount has been deducted from the payer's account, and they now have a note which is verified by the bank. The payer makes sure the value of the note is the same as what they initially sent to the bank, terminating the process if not. The payer then provides the note to the recipient, who checks the note. If the note is valid, the recipient forwards the note to the bank. The bank checks the validity of the note, terminating the process if any discrepancies exist. If the note is valid, the bank adds that note to a comprehensive list of cleared notes, terminating if the note is already on the list. Following success in all steps, the bank credits the recipient's account and informs them of acceptance [1].

This method of transferring money indicates that any transactions would be perfectly valid, as any fraudulent transactions would be made obvious at some stage, either through any irregularities in a transaction or by its details already existing in a list of transactions. Chaum went on to implement this system in his electronic cash business venture, DigiCash, formed in 1990 [2]. Built on the idea of freeing digital currency from the control of any government, DigiCash and its underlying technology seemed promising at the time. However despite the viability of DigiCash on paper, the company ultimately failed due to a range of issues such as internal conflict and lack of funding [3]. One could also argue that DigiCash failed partly due to the internet still being relatively young, and therefore demand not yet existing for an online currency.

Times have since changed, and the unprecedented popularity of the internet from the early 21st century on has of course come with added concerns from its users regarding privacy. While DigiCash may have been before its time, the underlying concept of untraceable payments now seemed more desirable, and needed, than ever.

2.2 The Arrival of Modern Cryptocurrency

The beginning of the rise of cryptocurrency can be pinpointed in 2009, when the the first major cryptocurrency was released to the public (*see section*

2.2.3). Much like traditional currency, any cryptocurrency is an asset, designed to be traded in exchange for goods and services. Cryptocurrency is based on cryptography, the study of breaking or creating of codes and ciphers to either encrypt plain text or decrypt cipher text, in order to keep the exchange of digital information safe and secure. Based on [CoinMarketCap](#) figures, one of the most widely used websites for tracking the size and price of various cryptocurrencies, there are currently just over 1500 cryptocurrencies in existence today [4], with some of the most popular being Bitcoin, Ethereum, Litecoin and Ripple. When compared to the relatively small number of the 180 traditional currencies in circulation throughout the world, one might think that cryptocurrencies are more popular than traditional currencies. This is not the case however, mostly due to the fact that anyone can develop and release a cryptocurrency into the virtual world, as explained in 2.3: *Blockchain Technology*.

2.2.1 An Explanation of Modern Cryptocurrency

Each cryptocurrency is its own self-contained system, separate from other cryptocurrencies, much like any traditional currency is its own entity. While the features of each individual currency may differ, such as their value or total available supply, their fundamental concepts are the same and undoubtedly very similar to Chaum's aspirations - an asset, free from the control of one government, party or person, and untraceable back to whomever traded the currency. The main features of most cryptocurrencies include decentralisation, anonymity and ability to be traded online through exchanges.

Decentralised Systems

The simple explanation for a decentralised system is to say it is owned and managed by the public, as opposed to one single centralised entity like a bank or government. While the system varies from currency to currency, most implement this idea through the use of time-stamps or unique serial numbers on each transaction. These unique transactions are recorded in a global ledger, a copy of which is kept on every currency owner's machine. Any anomalies in a transaction will be made obvious when checking the global ledger, avoiding the need for a trusted third party to verify transactions. This feature makes it virtually impossible to forge transactions into any account. The technology behind this global ledger is explained in greater detail in 2.3: *Blockchain Technology*.

Anonymity

As mentioned previously, one of the main flaws with exchange of traditional currencies is the ability to identify sensitive information related to the sender, such as their location or interests. Possibly the most attractive feature of various cryptocurrencies is that they do not store any identifying data related to the user. An owner of a cryptocurrency keeps that currency in a digital "wallet", which is really just an encrypted address. If a person owns multiple currencies, they will have one address for each currency. Similarly, if a user owns a large quantity of one currency, they may want to distribute their currency across multiple addresses, in case one address is lost or has a breach in security. While this address is contained in the global ledger and available for every user to see, it is completely separate from a user's identity and completely the user's responsibility to control. For example, the address [3Pj8fcmuJeEoceD35f7vcgDNk2dtEGgmV9](#) does not reveal any information about its owner, keeping their privacy intact.

Anonymity is extremely important in cryptocurrency in terms of privacy, but also largely in terms of keeping users with vast investments safe from being threatened in their non-virtual lives.

Mining of Cryptocurrency

For most cryptocurrencies, a process called "mining" must take place in order to confirm transactions and add them to the global ledger. This is not something every single user must do, but rather a process that can be done by anyone who wishes to and in exchange for a reward, often in the form of the currency they are mining. Cryptocurrency miners are given a very complex mathematical problem, and when the problem is solved the transaction is added to the ledger. These problems are kept at an extremely high level of difficulty and increase in difficulty to keep up with advancements in processing power, and are therefore mostly done by those with extremely powerful computers. The mining system ensures transactions are valid and adds to the overall security of cryptocurrencies.

Trading Cryptocurrency

In order to trade cryptocurrency, one must have an address to store their currency in. There a number of methods and platforms for trading cryptocurrency, but most users start trading cryptocurrency by signing up to trading sites such as [Coinbase](#) [5] or [GDAX](#) [6]. Sites like these offer a user-friendly interface, simplifying the buying and selling of the process as much as possible. Once a user has signed up, verified their identification and added

an associated bank account or card, they can buy and sell a variety of coins at the touch of a button and without worrying about any underlying keys or addresses. These sites also allow the transfer of currency from one account to another provided the destination address is known. These sites also provide up to date prices, often displayed as a graph over a period of time, and users can access their own key or balance at any time. One should keep in mind that these sites are not completely free and that there is a small fee to pay on every transaction, but these sites are an excellent way for beginners to get started in trading cryptocurrencies.

2.2.2 Comparing Traditional Currency and Cryptocurrency

As outlined previously, there are many similarities and differences to be found between traditional currencies and cryptocurrencies.

Firstly, traditional currencies rely on centralised banks and governments to regulate and verify all transactions. This means that one person or group could destroy any proofs of transactions or change any account balances, simply by breaking into or hacking one location. In contrast, cryptocurrencies are decentralised, meaning any potential threat would have to hack in to every user's machine in order to destroy records or accounts. Of course, this would be an issue if there were little or no users but the growing number of owners of cryptocurrency means the likelihood of this is very small.

The decentralised nature of cryptocurrencies and their global ledger also adds to the credibility of each transaction. In contrast to the relative ease of which someone could forge a paper note, the global ledger means cryptocurrency transactions are virtually impossible to forge.

Additionally, any exchange of traditional currency carried out digitally (such as online banking or credit cards) can be easily traced back to the account and person it came from. Use of wallet addresses in cryptocurrency, as explained previously in *2.2.1: Anonymity*, still means the source and destination of the transaction can be seen without exposing sensitive information related to any party.

2.2.3 A Focus on Bitcoin

As mentioned previously, the arrival of modern cryptocurrency can be pinpointed in 2009, when the first major cryptocurrency was released to the public. The concept of this first cryptocurrency, Bitcoin, was introduced in a paper published in 2008 by an author or authors under the supposed

pseudonym of *Satoshi Nakamoto*. In their paper, Nakamoto proposes the idea of a peer-to-peer electronic cash system, based on digital signatures and independent of any financial institution or government [7]. Nakamoto also outlines a solution to verifying transactions, preventing "double-spending" using a proof-of-work method. This would involve time-stamping transactions, adding them to a chain of hash-based proofs, which cannot change one transaction without redoing all previous entries in the proof-of-work. In order to change any entries in the chain, a single CPU would have to redo all entries before any new entries are added, which would require phenomenal computing power. Nakamoto also adds that this means the system is safe from threat as long as "honest" nodes collectively hold more CPU power than any group of attacking nodes.

The Price of Bitcoin

The first 50 coins were mined and released by Nakamoto in 2009, when the price per coin was estimated to have been a mere \$0.001 US dollars. Bitcoin can be traded on various exchanges, as described in *2.2.1: Trading Cryptocurrency*, but what is considered the first real world transaction of Bitcoin occurred in 2010, long before most of these exchanges existed. This transaction of Bitcoin occurred when programmer Laszlo Hanyecz posted on a Bitcoin Forum, offering 10,000 Bitcoin in exchange for someone to order a pizza to his home in Florida [8]. The post still exists today, containing comments from various users at the time as well as more recent comments lightheartedly highlighting the rise in price of Bitcoin.

The currency stayed at very low prices until late 2010, when the price rose to \$0.36 per coin. The price began rising in February 2011 and peaked at \$1.06, reaching "dollar parity", a much sought-after milestone [9]. The price of Bitcoin continued to rise, fuelled by media coverage, and spiked to over \$100 and in 2013. Still rising, prices reached over \$900 at the end of 2013, eventually settling between \$400 - \$800 for most of 2014, 2015, and 2016 [10]. 2017 saw Bitcoin prices soar from just under \$1000 to a staggering \$17,500. One cannot help but be reminded of those two pizzas Hanyecz spent 10,000 Bitcoin on, now worth a staggering \$175 million dollars.

In 2018, the price of Bitcoin fell by roughly 60% and has hovered consistently between \$5000 and \$7000 since. Even so, this is still exceptionally higher than any other cryptocurrency. Ethereum, the second most expensive coin, has averaged in the last month at around \$400-\$700 per coin, a mere 10% of the price of a Bitcoin.

2.3 Blockchain Technology

While there are many different technologies behind various cryptocurrencies, arguably the most well known and important is the concept of blockchain. Blockchain, aforementioned briefly in *2.2.1: An Explanation of Modern Cryptocurrency*, is the global ledger in which all transactions of a cryptocurrency are recorded. Blockchain technology was first proposed by Nakamoto in [7], and thus in this section we will be discussing blockchain technology in relation to Bitcoin.

As outlined by Nakamoto in [7], the blockchain consists of multiple blocks, added to the chain in a chronological order. Each block consists of a number of transactions, which are stored in the block as hashed items. In order for a new block to be added, it must be verified through the mining process. When a miner joins the Bitcoin network and downloads the software for validating and relaying transactions, a copy of the blockchain is also automatically downloaded [11].

Validation of a block, discussed in *2.2.1: Mining of Cryptocurrency*, involves solving a complex computational problem and requires immense processing power. Once a block has been validated, it is added to the chain and the miner is rewarded. Every block, containing information for every transaction, including the first "genesis" block is available to be viewed either on a local copy of the blockchain or on sites such as [Blockchain.info](https://blockchain.info). The Blockchain website in particular provides details for any given block, such as block number, number of transactions within the block, block time-stamp, and block reward. Most importantly, each block also stores the hashed key of the previous and next block in the chain, linking all blocks together.

Block Rewards

When Bitcoin was first released, the reward for validating a block was 50 Bitcoin, as pointed out by J. Donnelly in [12] with reference to Bitcoin's source code [13]. This meant that 50 new coins were released into the market. However, in order to counteract expected increase in demand, a halving function was implemented. There would be 64 "halvings", and a halving would occur every 210,000 blocks. The very first halving event occurred in 2012 and the reward for a block reduced to 25 Bitcoin, followed by a second halving event in 2016, when the reward fell to 12.5 Bitcoin. The next halving event is expected to occur in 2020, and further events will occur after each 210,000 blocks until there have been 64 halvings, at which point the 21 million coin supply of Bitcoin will be reached [12] [13].

Trusting the Blockchain

As previously highlighted in *2.2.1: Decentralised Systems*, the blockchain is a global ledger of sorts, with identical copies of the chain stored on the machines of those who mine the relevant cryptocurrency. The decentralised nature of the blockchain means that no one person or group has control over the blockchain. In [7], Nakamoto explains that any attacking person or group would have to have more CPU power than all of those who were honest within the network in order to change any blocks existing in the chain. Furthermore, due to each block storing the hashed keys of both the previous and next block in the chain, the attacking node or nodes would have to change all previous entries in the chain before a new block was added and the chain updated.

While it should never be considered impossible to manipulate the blockchain, it would be highly difficult to. Perhaps when quantum computers emerge with considerably more processing power than that of today's computers, there could be a significant threat to the blockchain, but the processing capabilities of today's machines are certainly not a threat.

2.4 The Viability of Cryptocurrency

Based on the fundamental ideas discussed in this chapter, cryptocurrencies would appear to be a very promising alternative to traditional currency when trading in exchange for goods and services. While traditional and digital currencies have their similarities, it is ultimately the innovative concepts brought to light by various cryptocurrencies which make them a promising alternative to traditional currencies.

Due to its global and decentralised nature, cryptocurrency can be used by anyone, anywhere, provided they have access to a digital device and a digital address from which to send and receive currency. When Bitcoin was first released in 2009, the global economy was in the depths of a severe recession and trust in financial institutions and governments was at an all time low. A certain unease still exists around how much trust should be placed in large financial bodies, but that trust is not needed in cryptocurrency. Technologies such as the blockchain ensure that no one person or group has control over the ledger, and not even a large group working together to corrupt the chain could be fast or powerful enough to succeed. Therefore the records remain intact, and can be trusted to be completely truthful.

The security of cryptocurrency is undoubtedly an attractive feature to any potential investor, however the anonymity that comes with trading in cryptocurrency is something to be valued also. With recent privacy scandals

such as the Facebook-Cambridge Analytica debacle [14], concern around public privacy is at its highest. While financial institutions are undoubtedly more secure than any social network, it would not be impossible for any person or group to compromise this security and obtain the records of account holders, containing addresses, transaction destinations, account balance and other sensitive identifying information. The features of cryptocurrency discussed in 2.2.1: *Anonymity* would reassure any user that their sensitive data is safe. By using a single hashed address of seemingly random numbers and letters for both sending and receiving a given amount, cryptocurrencies do not require any information similar to what financial institutions require. This system which requires absolutely no trust in any third party, is indeed a much more attractive approach than that of financial institutions and governments.

To conclude, in this chapter we have explained the fundamentals of what exactly cryptocurrency is, followed by an analysis of how cryptocurrencies work and their underlying technologies. Based mainly on its security features but also on its rising popularity, we can consider at least the largest cryptocurrencies such as Bitcoin and Ethererum to be a viable asset in terms of value and trading. While it is difficult to predict how the future of cryptocurrency will pan out or how the technology will endure in the long term, the solid foundations on which the concept is built suggest it will endure for some time.

Of course, this chapter has centred on the benefits associated with cryptocurrency. In the following chapter, we will discuss some of its shortcomings and flaws, with a focus on how volatile the cryptocurrency markets can be.

Chapter 3

Predicting The Prices of Cryptocurrencies

Contrary to the title of this chapter, the price of cryptocurrencies, or any currency for that matter, cannot absolutely be predicted. We can however make an educated guess based on a variety of factors as to whether the price will rise or fall, or how severe a change in price will be. In this chapter, we will discuss the various influencing factors in prices of cryptocurrency, followed by an examination of some existing methods of attempting to decipher a trend in cryptocurrency prices.

3.1 The Volatility of Cryptocurrency

As outlined in *2.2.3: A Focus on Bitcoin*, the prices of cryptocurrency can be extremely unstable. For example, data taken from CoinDesk [10] on April 12 2018, shows that in the space of one hour (11:00-12:00 GMT) the price of Bitcoin spiked from just under \$7000 to just under \$8000. There are countless of occurrences of this happening throughout the lifetime of Bitcoin. Another example of this volatility is when the currency reached its highest price on December 16 2017 of over \$19,300, before plummeting to \$13,800 a mere five days later - a drop of almost 30%. It is the sheer instability of cryptocurrency prices and the rate at which they change that determines there will never be a dependable method of predicting prices.

However, one can take into account a variety of things when considering buying or selling cryptocurrency to determine if the time is right. It is important to clarify that the price is solely governed by demand, but there are indeed a great number of factors which may indirectly influence the price of cryptocurrency.

3.1.1 Influencing Factors in Cryptocurrency Prices

Traditional currencies are influenced by many things, such as warfare, political instability, and national debt. While demand is the only thing that directly affects cryptocurrencies, many things influence the current level of demand.

Price of Bitcoin

Due to its popularity, the price of Bitcoin often affects the price of other cryptocurrencies.

Start with explaining what influences traditional currencies, lead into main body of CC influencing factors. Security features, bitcoin wallet complicated etc, fluctuations in TCs due to war/government etc vs flucs in CCs down to sheer hype/demand etc.

3.2 Transition to Applied

Tie concept of diss with concept of proj. "Deciding to Analyze the Volatiliy of Cryptos"...?

Chapter 4

Currency Analyser Web Application

Building on the information discussed in the previous chapter, we will now examine the applied element of our Final Year Project. In this chapter, we will examine our web application by reflecting on our approach to this project, and whether there are any aspects which we would do differently in hindsight. We explain the technologies behind the web application, as well as our decisions behind using them and any problems encountered. We then describe the overall design of our finished system, concluding with an evaluation of the system.

4.1 Methodology

In this chapter, the way in which the project was planned, organised, managed and decisions made throughout its life cycle will be discussed. Initial research and decisions regarding the team's approach to this project will be examined, before detailing any differences in the way in which this project ultimately panned out.

4.1.1 Preliminary Research and Project Commencement

The team had their first meeting in late September, shortly after specifications for the project and dissertation had been given. It was agreed that getting started as soon as possible was best, and an agreement was reached to decide on an idea and carry out some research before starting any of the applied aspects of the project.

While the team had a number of basic possible concepts which would be suitable for the scope of a final year project, taking on a data analytics project in the form of analysing cryptocurrency was considered to be the most interesting. The team had also agreed that machine learning should be incorporated into the project if possible, and saw pursuing this idea as an opportunity to include some innovative machine learning technologies in an interesting and relevant way. It was decided that a web application containing graphs of currency prices and a future price prediction feature would be ideal for this purpose and to demonstrate all theoretical aspects of this project, which would be discussed in the dissertation.

Following this decision, the first meeting with the team's supervisor was organised, in which all ideas were discussed. It was agreed that a cryptocurrency data analytics project would be a suitable and interesting project, and the team were given advice as to what technologies should be considered for use. Taking this advice on board, the team began more detailed research.

Research Methodology

As all team members had some previous experience with cryptocurrency, it was agreed that major preliminary research into the concept was not a requirement. The team did some light reading of the latest news items relating to cryptocurrency and moved on to researching a list of technologies, examining which would be best to include in the applied project.

Database of Prices: Based on the team's collective experiences from the previous academic year, it was first agreed that *Python 3* would be ideal for obtaining data. The team carried out some quick searching online and found there to be numerous free cryptocurrency APIs (*Application Programming Interfaces*) available, all of which stored vast amounts of records for prices of cryptocurrency against a variety of traditional currencies for increments of time, usually every minute. The team concluded this was often enough for a web application which does not deal with trading and therefore does not need to be accurate. Due to previous experience again, the team felt MongoDB would be a favourable option for storing this data. After refreshing collective knowledge of MongoDB documentation [15], the team agreed on using a MongoDB database to save data into from an API via a Python 3 script.

Web Application Back-End: Having decided the details of the project's database system, the team began discussing the back-end of the application. Once again, previous experiences encouraged the use of Python 3 and the Flask Framework. All team members had enjoyed using this combination for previous web application projects, and felt it would simply make sense to do

so again.

Web Application Front-End: Based on the advice of the team’s supervisor, research on *Vue.js* [16] and *D3.js* [17] was carried out. It appeared this combination would work well for creating a web application with simple yet intuitive design, as well as creating striking visual representations of our data.

Machine Learning: With regards to attempting to decipher trends in prices, the team’s supervisor recommended the use of TensorFlow [18]. Having been using this machine learning framework in class for some time at this point, the team were familiar with the framework and had been using the technology with Python 3. It was agreed that this combination should be used, as it would fit in well with the overall project architecture.

Agile Development

Having learnt about the various approaches to software development in previous academic years, the team felt the *Agile Methodology* [19] was the best to follow. In [20], Highsmith et al highlighted the attractiveness of the agile approach, stating that working code and a team who work together effectively are the two main concepts stressed in agile methods [20] - working code proves to both developers and clients exactly what has been done, and an effective team can achieve cost savings as well as flexibility. Regular interaction between team members and the closeness of a team are also fundamental to agile methods, further pointed out by Highsmith in [20]. The team agreed this was the ideal methodology to follow, as regular communication and a stable, consistent timeline of work were strongly desired.

Agile approaches often include the division of work into short periods of time called sprints, often a two to six weeks in length. At the beginning of each sprint, a goal for the end of the sprint is defined, such as a particular component of the project to be working, or some element to have been tested extensively. It was agreed that the inclusion of sprints in this project’s life cycle would further help the team to keep on top of the project workload, providing a definitive timeline of progress.

Version Control

Having used free online version control software GitHub for a number of years, the team decided it would be ideal for keeping track of source code throughout this project. One particularly useful feature of GitHub is branches, allowing users to push to a given repository without necessarily affecting the original master branch. The team intended to have a branch for each mem-

ber's work, a branch for developing (where individual work would be tied together), a branch for testing, a branch for machine learning, and a branch for dissertation work. Workload was divided between the team members as follows:

- Tara O'Kelly: Front-End Development, including visualising currency data on a graph.
- Johnny Glynn: Back-End Development, including obtaining and saving currency data.
- Rebecca Kane: Dissertation, including relevant research.

It was decided that it would be best if the team worked collectively on any machine learning elements after the work specified above was complete, and thus didn't initially allocate it to any one member.

It was acknowledged that GitHub's *Issues* feature would come in very useful for keeping track of any problems. The team planned to use this to organise both technical code-related issues and issues related to the dissertation, such as information being required from one member or another on a particular subject or technology.

GitHub's *Projects* resource would also add to the overall organisation of the project. *Projects* are very similar to to-do lists and can be used in conjunction with *Issues*, allowing to-do items to be assigned to certain members. GitHub allows the creation of multiple *Projects*, meaning one could be created for each major component of this project, such as Dissertation or Machine Learning.

Testing

It was agreed by the team that in keeping with the metrics discussed in 1.1.1, testing should be user driven for the most part. Based on the metrics outlined in the aforementioned section, the team decided on the following tests related to each metric:

- *Metric One - Easily understood, cohesive dissertation*: In order to test whether the team had succeeded in providing a clear and comprehensive examination of cryptocurrency in this dissertation, the team agreed it was best to ask those who had little or no understanding of cryptocurrency to read Chapters 2: *Understanding Cryptocurrency* and 3: *Predicting the Prices of Cryptocurrency*. It was decided that those who read the chapters would be asked to rate how well they understood the

content on a scale of 1 to 5, with 1 being no understanding and 5 being perfectly understood. The team agreed a test sample size of five people would suffice.

- *Metric Two - Simple Web Application:* Again, it was decided that in order to test the simplicity of the web application, it would be best to ask those who had little or no knowledge of cryptocurrency. Similar to the above, five users would be asked to use the web application for a brief period of time and provide feedback on their opinions of its usability, using the same scale as above.
- *Metric Three - Future Cryptocurrency Price Estimates:* In order to test the accuracy of the web application's predictions, it was agreed that the predictions should be tested over a period of one week, or seven predictions. Due to TensorFlow's training and testing facilities, this test could be carried out in one sitting. The TensorFlow model would be trained, and subsequently shown seven unseen prices, and asked to predict the new price. For example, the model can be shown a price from 11 December 2017 and asked to predict the price for the following day, which can then be compared against the actual data from 12 December 2017.
- *Metric Four - Teamwork:* Of course, teamwork is not something which can be measured in a definitive way. It was determined that in order to measure the success of this, the team would simply reflect at the conclusion of this project on how issues were resolved, and if relationships were affected by any disagreements.

Supervisor Meetings

During the first meeting with the team's supervisor, it was discussed what the frequency of supervisory meetings should be. The collective feeling was that a weekly meeting would be too often, as some weeks would naturally allow for more or less work to be done than others. It was determined that it was best not to have meetings if a substantial amount of work had not been done, and it was concluded that meetings would be best if only had when warranted, ideally every few weeks.

4.1.2 Issues Encountered Throughout the Development Process

While the team initially had great intentions and did begin work on this project as soon as requirements were available, numerous issues ultimately surfaced.

Interfering Factors

Of course, at certain stress points throughout the academic year, work on this project was postponed due to upcoming exams or deadlines related to the team's other projects. As the first semester of this year involved more modules and therefore more work than the second semester, the collective decision was made by the team to put other projects first from late November 2018 through to early January 2019, when the second semester began. However, significant progress was made by the team between September and the end of November and this decision was believed to not have seriously jeopardised the progress of this project. A supervisory meeting was arranged in late November to discuss the work achieved thus far, and again in early January to discuss the direction of the project from that point. After regular contact with the team's supervisor, work proceeded again from mid January onwards.

Communication Issues

While communication was not an issue in the first semester of this year, it quickly became a problem as one team member unfortunately became ill in late January 2019, and remained so for the rest of the duration of the project. Contrary to what Agile development encourages, the team began to rely on messages, emails and occasional phone calls in order to keep in contact with the absent member. This ultimately led to a strain on development, as it grew more and more difficult to express ideas and opinions through messages and calls. As the Agile Manifesto states, "*The most efficient and effective method of conveying information to and within a development team is face-to-face conversation*" [19]. The team fully supports this statement, as there was no comparison between discussing components of the project through practical examples in person, and trying to do the same simply over the phone. There were also a number of occasions where a meeting was agreed for a certain day and time, only to result in two members being present due to lack of communication.

These communication issues ultimately delayed development, as other

team members had to wait on the absent member to publish work on GitHub or reply to messages, as opposed simply seeing each member's work in person, or talking face to face and having an immediate reply.

Lack of Working Code

As mentioned in the previous section, one team member had become ill and was absent from late January onwards. The two remaining team members continued to work on research based elements for some time, as they required work from the ill member in order to progress properly with their own work. While we acknowledge that some work could have been done by the remaining members by assuming the work of the absent member had been done in a certain manner, any progress made by the remaining members would ultimately have had to have been altered to suit the absent member's work. This method likely would have resulted in more unnecessary work for the remaining members, and thus it was decided that we would wait for the absent member to publish their code on GitHub.

While the absent member reassured remaining members that work was being done, there had been a lack of published code on their behalf for a period of two months. Nearing the end of the project, the remaining members continued to request that they see working code on the basis of being unable to spend any more time not moving forward in development.

Resolution of Problems

On the basis of the issues discussed above, two members of the team brought their concerns to the project supervisor to look for advice. The options of continuing along the same track with all members contributing to the one project, or a division of the group to work on two separate projects were presented to the team. A discussion was held between all three team members, and it was mutually agreed on 9 April 2018 that the option to work as two separate teams from then on was best for all members. Keeping in mind the teamwork objectives outlined in *1.1: Objectives* and *1.1.1: Metrics for Success or Failure*, the team agreed to not let any of these issues affect their friendships, and have succeeded in doing so thus far.

Development Following Group Partition

As there was little time left after the decision to separate into two groups, development in the last week of the project became somewhat erratic, following aspects of Extreme Programming development methodologies. The team could not afford to put large quantities of time into planning, and thus

decided to only use a few hours to plan for what needed to be completed in the week ahead.

Extreme Programming: Based on the fundamentals of the Extreme Programming methodology, outlined by Wells in [21], this methodology is successful partly due to its encouragement of developers adapting to change, sometimes late in the development life cycle. The loss of one team member could be considered difficult to adapt to so late in this project's life cycle, but the team decided to follow the principles of Extreme Programming closely in order to overcome this. The team decided to self-organise around the problem to solve it as quickly as possible [21] and began reallocating tasks based on their importance. Once tasks had been outlined the team kept Wells' summary of a successful Extreme Programming project in mind - *communication, simplicity, feedback, respect, and courage*. Over the final week of the project, the team kept in near constant contact with each other, also regularly discussing various facets of the project with their fellow students. Of course, at such a late stage the design of any further implementations must be as simple and clean as possible, a concept the team strived towards. Rather than test numerous implementations and methods, the team decided it best to research possible solutions to any problems, before implementing them. Ultimately, this saved much time, as a chosen solution was subsequently well understood and highly likely to work as expected. Finally, in keeping with initial objectives for this project, the team aspired to continuously be respectful in this time of high stress, while being courageous and trusting in their own decisions.

To conclude, the final week of this project was of course very demanding and stressful. One may have expected any work produced in this time frame to be cluttered, thrown together with haste in an attempt to meet deadlines. Fortunately, the quality of work by the team actually improved due to the crucial planning necessary in order to produce a large amount of work in such a short period of time.

4.2 Technologies / Tech Review

About seven to ten pages.

- The “literature review” part of the dissertation. Should be tightly coupled to the context and objective from the introduction. Proves that you researched what you were doing!
- Describe each of the technologies you used at a conceptual level. Standards, Database Model (e.g. MongoDB, CouchDB), XML, WSDL,

JSON, JAXP. Use references (IEEE format, e.g. [1]), Books, Papers, URLs (timestamp) Sources should be authoritative!

- A technology review that includes a lot of de facto or de jure standards supports the methodology! Each chapter buttresses some other aspect of the dissertation.

4.2.1 Python 3 and the Flask Framework

4.2.2 Redis

4.2.3 MongoDB

4.2.4 Vue.js

4.2.5 Chart.js

4.2.6 TensorFlow

4.3 System Design

As many pages as needed.

- Architecture, UML etc. An overview of the different components of the system. Diagrams etc... Screen shots etc.

Column 1	Column 2
Rows 2.1	Row 2.2

Table 4.1: A table.

4.4 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 5

Conclusion

About three pages.

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

5.1 Context/Objectives

5.2 Findings

Chapter 6

Appendices

Source Code on Github: <https://github.com/rebeccabernie/CurrencyAnalyser>

Heroku Web Application Link:

Bibliography

- [1] D. Chaum, “Blind signatures for untraceable payments,” in *Advances in Cryptology*, pp. 199–203, Springer, Boston, MA, 1983.
- [2] S. Levy, “E-money (that’s what i want).” Last accessed on 6 Apr 2018. URL: <https://www.wired.com/1994/12/emoney/>.
- [3] S. Higgins, “3 pre-bitcoin virtual currencies that bit the dust.” Last accessed on 5 Apr 2018. URL: <https://www.coindesk.com/3-pre-bitcoin-virtual-currencies-bit-dust/>.
- [4] CoinMarketCap, “Cryptocurrency market capitalizations.” Last accessed on 6 Apr 2018. URL: <https://coinmarketcap.com/>.
- [5] Coinbase, “Buy and sell digital currency.” Last accessed on 6 Apr 2018. URL: <https://coinbase.com/>.
- [6] “Gdax: The most trusted digital asset exchange.” Last accessed on 6 Apr 2018. URL: <https://www.gdax.com/>.
- [7] S. Nakamoto, “Bitcoin: A peer-to-peer electronic cash system,” 2008.
- [8] L. Hanyecz, “Bitcoin forum post: Pizza for bitcoins?,” May 2010. Last accessed 9 Apr 2018. URL: <https://bitcointalk.org/index.php?topic=137.0>.
- [9] B. Wallace, “The rise and fall of bitcoin,” 2011. Last accessed 7 Apr 2018. URL: https://www.wired.com/2011/11/mf_bitcoin/.
- [10] “Coindesk: Bitcoin usd price.” Last accessed on 7 Apr 2018. URL: <https://www.coindesk.com/price/>.
- [11] M. Swan, “Blockchain 1.0: Currency,” in *Blockchain: Blueprint for a New Economy*, pp. vii–xvi and 1–7, O’Reilly Media Inc., 2015.

- [12] J. Donnelly, “What is the ‘halving’? a primer to bitcoin’s big mining change,” 2016. Last accessed on 8 Apr 2018. URL: <https://www.coindesk.com/making-sense-bitcoins-halving/>.
- [13] Various, “Bitcoin core source code.” Last accessed on 8 Apr 2018. URL: <https://github.com/bitcoin/bitcoin>.
- [14] O. Bowcott and A. Hern, “Facebook and cambridge analytica face class action lawsuit,” Apr 2018. Last accessed on 8 Apr 2018. URL: <https://www.theguardian.com/news/2018/apr/10/cambridge-analytica-and-facebook-face-class-action-lawsuit>.
- [15] MongoDB. Documentation. Last accessed 9 Apr 2018. URL: <https://docs.mongodb.com/>.
- [16] Vue.js. Last accessed 9 Apr 2018. URL: <https://vuejs.org/v2/guide/>.
- [17] D3.js. Last accessed 9 Apr 2018. URL :<https://d3js.org/>.
- [18] TensorFlow. Last accessed 9 Apr 2018. URL <https://www.tensorflow.org/>.
- [19] K. Beck, “Principles behind the agile manifesto.” Last accessed 9 Apr 2018. URL: <http://agilemanifesto.org/principles.html>.
- [20] J. Highsmith and A. Cockburn, “Agile software development: The business of innovation,” *Computer*, vol. 34, pp. 120–122, 2001.
- [21] D. Wells, “Extreme programming: A gentle introduction,” 2009. Last accessed on 10 Apr 2018. URL: <http://www.extremeprogramming.org/>.