

---

# 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

<b>1</b>	<b>Introduction</b>	<b>6</b>
1.1	Project Objectives . . . . .	7
1.1.1	Metrics for Success or Failure . . . . .	9
1.2	Description of Each Chapter . . . . .	9
1.2.1	Understanding Cryptocurrency . . . . .	10
1.2.2	Predicting the Prices of Cryptocurrency . . . . .	10
1.2.3	Currency Analyser Web Application . . . . .	10
1.2.4	Conclusion . . . . .	10
<b>2</b>	<b>Understanding Cryptocurrency</b>	<b>11</b>
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
<b>3</b>	<b>Predicting The Prices of Cryptocurrencies</b>	<b>20</b>
3.1	The Volatility of Cryptocurrency . . . . .	20
3.1.1	Influencing Factors in Cryptocurrency Prices . . . . .	21
3.1.2	The Bitcoin Bubble . . . . .	23
3.2	Deciphering Trends in Prices . . . . .	25
<b>4</b>	<b>Currency Analyser Web Application</b>	<b>26</b>
4.1	Methodology . . . . .	26
4.1.1	Preliminary Research and Project Commencement . . . . .	26
4.1.2	Issues Encountered During the Development Process . . . . .	32
4.2	Underlying Technologies . . . . .	35
4.2.1	Python 3 . . . . .	35
4.2.2	The Flask Microframework . . . . .	35

4.2.3	Redis . . . . .	35
4.2.4	MongoDB . . . . .	36
4.2.5	Vue.js . . . . .	36
4.2.6	TensorFlow . . . . .	37
4.2.7	Heroku . . . . .	38
4.3	System Design . . . . .	38
4.3.1	Web Application . . . . .	38
4.3.2	Machine Learning . . . . .	39
4.4	System Evaluation . . . . .	39
4.4.1	Testing . . . . .	41
4.4.2	Evaluation of Objectives . . . . .	42
4.4.3	Opportunities for Improvement . . . . .	43
4.4.4	Overall Evaluation . . . . .	44
<b>5</b>	<b>Conclusion</b>	<b>45</b>
5.1	Context/Objectives . . . . .	45
5.2	Findings . . . . .	45
<b>6</b>	<b>Appendices</b>	<b>46</b>

# About This Project

## Abstract

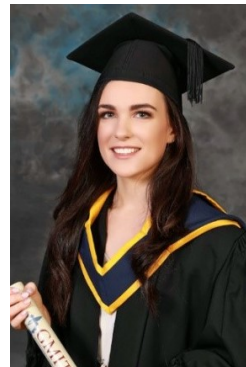
The field of cryptocurrency has enjoyed exponential growth in popularity in recent years. Almost ten years ago, the release of Bitcoin marked the beginning of a new era of innovation in the financial sector. In this dissertation we outline what exactly defines a cryptocurrency, describing fundamental concepts, underlying technologies such as the blockchain, and subsequently the viability of this new digital finance. Building on this knowledge, we examine the infamous volatility of cryptocurrencies, analysing pricing data and the likelihood of these currencies, specifically Bitcoin, being in the midst a financial bubble. We examine the prediction of prices, or rather inability to do so, before introducing the Currency Analyser web application developed as part of this project. Containing up to date prices, this web application is hosted on Heroku for public access and predicts prices of Bitcoin using machine learning. The research, planning methodologies, technologies, and design and evaluation of this application are described in detail in the penultimate chapter of this dissertation, followed by a concluding word on the process as a whole.

## Authors

This project was developed as a 15 credit project by Tara O'Kelly and Rebecca Kane, final year students of Software Development at Galway Mayo Institute of Technology.



*Rebecca Kane*



*Tara O'Kelly*

# 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. This was deemed a good decision as there was no awareness of any similar projects from previous years, and most importantly, all team members 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 personal interest in the field, was the inspiration behind this final year project; price predictions of one of the more popular cryptocurrencies would be calculated

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

This dissertation aims to first give the reader a good understanding of what exactly cryptocurrency is, how it works and the various technologies behind it. The volatility of cryptocurrency as an asset will be analysed, including the influencing factors in the changing of its prices. Following the initial theoretical chapters we will move to discussing the applied aspect of this project, where the development process and reasoning behind technologies used, among other relevant topics, will be outlined and explained. Finally, the dissertation will conclude with a summary of the project as a whole, along with any discoveries gained throughout the project.

## 1.1 Project Objectives

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

As this project is divided into a research-based dissertation and an applied project, goals will be discussed in relation to each aspect. The objectives for this dissertation are as follows:

- *Introduce the concept of this project:* We will provide the reader with an introduction to the project, detailing its inspiration and goals.
- *Provide the reader with a rounded understanding of cryptocurrencies:* We will examine where cryptocurrency began, and the concept of modern cryptocurrency in simple terms including how to begin trading cryptocurrency and the underlying technologies. We will then analyse 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 known indicators which aid in the uncertain forecasting of prices.
- *Describe in detail the applied aspect of this project:* We will examine the approach of the team to the applied project, including methodologies and technologies used, and design and evaluation of the system. Any

issues encountered throughout the development process will also be discussed, including how such issues were resolved and what could be done differently in future.

With regards to the applied component of this project, our objectives 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 this dissertation, it will be developed with even the most inexperienced of users in mind. Any quick internet search indicates most popular websites related to cryptocurrency are daunting at first sight due to the extensive numbers of graphs, percentages, and unfamiliar terminology. One of the most important goals for this application is that it be more encouraging to unfamiliar users than existing complicated sites.
- *Deliver cryptocurrency prices to the user:* The web application should 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:* Machine Learning and Neural Networks will be integrated to provide the user with an educated estimate as to what a price will change to. It should be noted that the aim is not to predict prices perfectly, as this is impossible due to the variety of factors that influence prices. However, previous price data will be used to attempt to decipher any trend and subsequently produce a price estimate, which will be relayed to the user through the web application. Natural Language Processing techniques could also be implemented to gather and analyse data on user discussions on relevant topics from sources such as Twitter and news websites, as these discussions have bearing on fluctuations in prices.
- *Work closely with the given learning outcomes for this project:* All requirements for the research and development process of this project will be strived towards by the team. 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 work as a team, in a professional manner akin to what is expected in industry:* It is highly important that each member aspires to



work with other members as a team, free from disrespect or inequality. No one member should feel as though they should take over the project, and any issues should be resolved in a calm and coordinated manner. It is often observed that friendships are compromised when an important project is added to the equation, but the team aims to keep personal and academic lives as separate as possible for the duration of this project. In the event of a disagreement, the team will endeavour to not let it negatively affect any friendships.

### 1.1.1 Metrics for Success or Failure

The metrics for success or failure of this project 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* 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 Bitcoin "Bubble" and 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 centres on the applied aspect of this project, building on information discussed in the previous chapters. We examine the methodologies and planning used throughout the 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. One 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 consider 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 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. In contrast, there is only one direct cause for a change in the price of any cryptocurrency, and that is demand. 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. One could argue that if the price of Bitcoin is affected by the same events as other cryptocurrencies, its prices will change in tandem with those of other cryptocurrencies. However, the size and popularity of Bitcoin lead many to look to its data when considering buying or selling any cryptocurrencies.

For example, consider a sudden increase in negative media content related to Blockchain technology. If the majority agree with the negative content, the majority of the market could decide to sell their investments. Bitcoin, with an estimated market dominance of 40-45% [4], also the majority, would subsequently decline in price. If most of the majority sold their Bitcoin, owners of other cryptocurrencies would be likely to sell due to the majority of the market declining.

By comparing graphed data of the prices of a given cryptocurrency against those of Bitcoin, it becomes clear that Bitcoin activity does in fact have a bearing on other cryptocurrency prices. See *Figure 3.1* below, detailing the prices of Bitcoin and Ethereum over one week.



Figure 3.1: BTC and ETH Prices, Apr 8 - 15 2018 [10]

While one could consider this purely coincidence, with a week arguably not being long enough to decipher any relationships between the two, the same can also be seen for a longer period of three months. Consider *Figure 3.2* below.



Figure 3.2: BTC and ETH Prices, Jan 15 - Apr 15 2018 [10]

In both instances, the prices of both Bitcoin and Ethereum follow roughly the same path. Bitcoin prices can be seen to be much more volatile, rising and falling more severely and in shorter spaces of time than Ethereum prices. For example, one should consider the sharp rise in price of Bitcoin shortly after April 12, 2018 against the slightly more dulled rise of Ethereum. This can also be observed in the rise and fall of the prices from February to March 2018; the price of Bitcoin is seen to be more erratic, detailing many sudden increases and decreases. Ethereum follows the same general path with less sharp changes, implying that Bitcoin does lead to increased buying or selling of Ethereum.

## Hyperbole Across the Media

As introduced above, media content can often play a large role in the changing of currency prices. Of course, it is hard to effectively quantify the effect of social media coverage by simply observing prices on a graph.

In a very recent article, Mai et al found that social media in particular can be a relatively accurate predictor of future Bitcoin prices [15]. Focusing on one of the more popular forums for discussing Bitcoin, [bitcointalk.org](https://bitcointalk.org), Mai et al concentrated on forum posts over three years, from 1 January 2012 to 31 December 2014. Data was also obtained from [Twitter.com](https://twitter.com), in the form of tweets containing the [#Bitcoin](https://twitter.com/Bitcoin) hashtag.

By using natural language processing to determine the number of positive or negative posts, Mai et al carried out tests on the obtained data through the use of vector error correction models to detect any interdependencies between pricing and social media coverage. Based on extensive testing as outlined in [15], Mai et al found that social media activity is in fact at least a partial indicator of future Bitcoin prices.

Concluding their findings, Mai et al also highlight the issue of silent majority, vocal minority; in that most social media users simply observe content as opposed to actively discussing the content. While this of course will skew results, the authors found this issue to be less common in the specified forum

as opposed to Twitter. The group therefore concluded based on tests that any sentiments expressed on a forum have a bigger bearing on Bitcoin prices than those expressed on Twitter.

### **3.1.2 The Bitcoin Bubble**

A bubble, defined as *"a state of booming economic activity that often ends in a sudden collapse"* [16], is a term commonly used in conversations across a variety of finance-related conversations. Often referring to a very lucrative or advantageous period of time, these occurrences rarely last long, often "popping" suddenly as a physical bubble would.

#### **Historic Similarities**

The world has seen many bubbles end badly in the last 20 years, most notably "The Great Recession" which began in late 2007 [17]. Prior to this downturn, the economy of the developed world had enjoyed great success financially, with financial institutions fuelling this by offering increased levels of loans and mortgages.

While there are ongoing arguments as to whether Bitcoin is a bubble or not, and what the severity of a possible crash will be in the event that it is, it is hard to definitively agree with one argument or another. Any bubble in regards to Bitcoin would be brought on much differently to that of The Great Recession, and would likely run its course and recover differently to how the world economy recovered from The Great Recession. There are substantially more influences in the activity of the world economy than there are for any cryptocurrency activity, the prices of which are governed solely by demand.

One example of a historic bubble which has been likened to the popularity seen by Bitcoin is that of the "tulip mania" bubble experienced by the Netherlands in the 1600s. While the tulip mania bubble was not as disastrous or as widespread as is commonly believed, it did leave many merchants in debt. Similarly, if Bitcoin were to collapse tomorrow, only those who had invested would be affected and not the national or international economy. Unlike tulips however, Bitcoin does have core uses outside of simply existing; it can be used as a transferable asset, as well as a store of value [18].

#### **The Future of Bitcoin**

Of course, with such a volatile asset as Bitcoin, it is hard to say if any major collapse will ever occur, or if prices would ever recover from such a collapse. Any possible collapse of Bitcoin could occur for a number of reasons, such as

the advent of quantum computers capable of compromising the blockchain, or a simple sudden loss of faith in the resource.

The initial years of Bitcoin saw a relatively stable increase in prices, slowly climbing to just under \$1000 by the end of 2016 [10]. It is clear this growth in price was fuelled by a gradual, natural growth of Bitcoin's popularity, easily seen by exploring the popularity of the term in Google searches over time [19]. For most of its life, Bitcoin had been a relatively unknown term, or at least certainly not understood by the majority. In 2017 however, the term began to gather momentum as prices surpassed the \$1000 mark, with prices rising exponentially for the duration of 2017. At Bitcoin's peak of \$19,661.63 on 17 December 2017 [10], prices had risen by a staggering 1870% in one single year. While there is no concrete calculation that can be done to determine what actually qualifies as a bubble, the sharp, almost irrational growth of prices would be difficult to refer to as anything other than a bubble. In keeping with the characteristics of every boom and bust cycle, Bitcoin suddenly plummeted to \$13,857.14 on 22 December 2017. In the months since, prices have continued to rise and fall toward an overall gradual decline, which could be interpreted as simply a correction of the ridiculous prices to prices that reflect more accurately the cryptocurrency's worth, as opposed to an actual crash.

As very recently summarised well by Derousseau in [20], factors such as increased interest by governments, the arrival of Bitcoin futures, and the growing number of alternative cryptocurrencies could all be leading factors in price declines. Bitcoin has now been banned by governments in a number of countries, which of course negatively affects the market as those countries' residents sell of their currency. Bitcoin futures, allowing investors to simply bet on whether Bitcoin prices will rise or fall, means that those interested in cryptocurrency no longer need to own that currency in order to profit from it, possibly leading to a decline in the market in future. Lastly, as more cryptocurrencies are added to the market, the market space for existing currencies reduces. While popularity of the bigger currencies may remain steady, the addition of newer varieties is likely to steal some of the spotlight from Bitcoin as people invest early with the hopes of these new currencies eventually reaching Bitcoin prices.

To conclude, the volatility of Bitcoin prices and cryptocurrency prices in general determines that one will likely never be able to accurately predict the price changes of these currencies. While Bitcoin itself may have gone through a bubble-like phase in 2017 and early 2018, its stabilisation is unlike that of a national economy after a financial crash. Perhaps Bitcoin will continue on a path similar to that of the last year, rising and falling but remaining in the order of thousands of dollars per coin. Perhaps interest and ultimately faith



in Bitcoin will dwindle, resulting in the outright collapse of the currency. Nonetheless, it would be absolutely absurd to claim one or the other will definitely occur - we are simply going to have to observe these events as they happen.

## **3.2 Deciphering Trends in Prices**

It is with this knowledge in mind that we progress to the applied aspect of this project. As examined above, there is no method to accurately predict the prices of any cryptocurrency. However, there are certainly trends in prices, which can be examined and attempted to be forecast using a variety of new technologies.

Building on the information discussed in this and previous chapters, we will now examine the applied element of this project; a web application for displaying Bitcoin prices against the Euro and predicting future values of Bitcoin.

It should be noted that while the web application was designed to be as easily understood as possible, it is still encouraged that the user has at least partly read and understood the preceding chapters of this dissertation.

# Chapter 4

## Currency Analyser Web Application

In this chapter, we will examine all components of this project, theoretical and applied, by reflecting on the approach to the process from its inception to its concluding days. The research and development methodologies used throughout this project will be explained, including any aspects the team would have done differently in hindsight. The technologies behind the web application are explained, as well as any team decisions behind using them and any problems encountered during their integration into the project. The overall design of the finished system is then analysed, 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. After refreshing collective knowledge of MongoDB documentation [21], 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* [22] and *D3.js* [23] 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.

**Web Application Hosting:** During preliminary research, the team considered both Microsoft Azure [24] and Heroku [25] for deployment of the final application. Having deliberated over the technologies for some time, the team considered using Microsoft Azure due to previous experience and its vast quantity of features, all of which could be confidently relied on. However, it was noted that this was not a definite decision at the time, and the team were still open to the possibility of using Heroku if it were more suitable when the time came to deploy the application.

**Containerisation:** Having heard about the benefits of containerisation, the team researched Docker [26], a leading platform in containerisation. Containerisation, put simply, is the packaging of applications *with* all relevant libraries and dependencies. This feature eliminates issues when trialling applications on different machines which may arise due to conflicts in installed software and the software the application was initially built with. While this was not a crucial element to the project, it would be convenient to implement should any related problems arise.

**Machine Learning:** With regards to attempting to decipher trends in prices, the team’s supervisor recommended the use of TensorFlow [27]. 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.

## Initial Expected Architecture

Based on the research described above, the architecture depicted in *Figure 4.1* was decided upon. Of course, no aspect of this architecture was a concrete decision as the team felt it necessary to allow for discovery of new, possibly more suitable technologies.

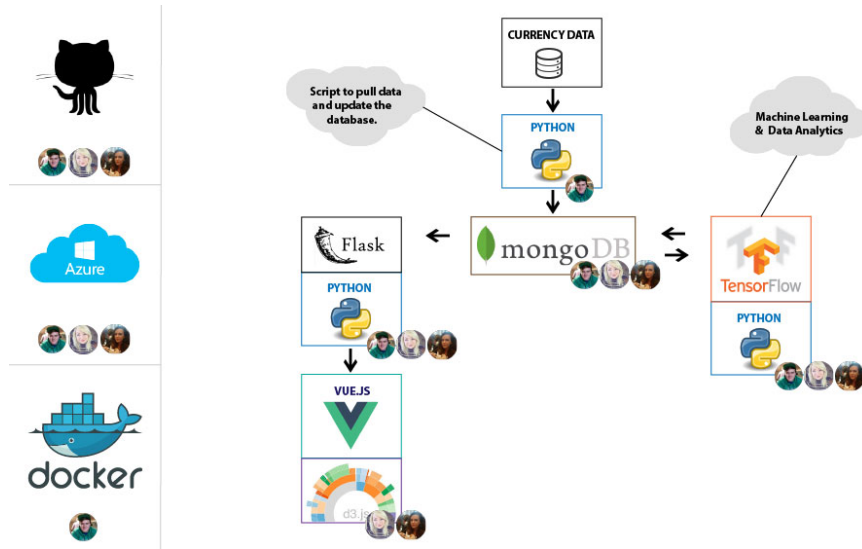


Figure 4.1: Planned Architecture, *October 2017*

## Agile Development

Having learnt about the various approaches to software development in previous academic years, the team felt the *Agile Methodology*[28] was the best to follow. In [29], 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 [29] - 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 [29]. 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 member'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 During 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, plan for subsequent work 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*" [28]. 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 integration problems closer to the deadline, 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 since the previous semester. 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 [30], 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 [30] 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 Underlying Technologies

### 4.2.1 Python 3

Python is a high-level, easy to read programming language, ideal for programmers with any level of skill. Python has become one of the most widely used programming languages, certainly due mostly to its simple yet powerful design. Unlike languages such as *Java* and *C*, Python syntax is relatively uncomplicated and thus not as daunting as more traditional languages. This theme carries across into Python documentation [31], which remains simple and arguably easier to understand than, for example, Java documentation.

For the purposes of this project, the Anaconda distribution [32] of Python 3 was used, as it is aimed at data science and machine learning applications. Anaconda's virtual environment manager, Anaconda Navigator, is included with the open source distribution and makes installation and updating of packages a much simpler process. There are a large number of external libraries available in the Anaconda distribution of Python 3, including some powerful data science packages like Scikit-learn, TensorFlow, and SciPy. It was for these reasons, as well as past experience with Python 3, that the team chose to work with this particular distribution.

### 4.2.2 The Flask Microframework

The Flask microframework [33] is designed for building simple web applications with a Python back-end. By using the Anaconda distribution, Flask can be installed simply through Anaconda Navigator, and all Flask applications can be run on any computer and accessed via opening a browser at <http://127.0.0.1:5000/>. The back-end of a Flask application looks very similar to a standard Python file, with added `@app.route()` decorators to handle what happens at specific URLs. For example, `@app.route("/")` defines the home page of any web application, which in most cases simply loads the specified html file when the URL is called in the front-end. In short, the Flask microframework allows users to create web applications with a Python back-end quickly and easily.

### 4.2.3 Redis

While MongoDB had initially been intended for use as the store for currency data, research into Redis was carried out based on advice from the team supervisor. Redis, meaning *REmote DIctionary Server*, is an open source in-memory data store which supports many different data types [34]. The

use of in-memory storage as opposed to disk storage offers a number of advantages, mainly making retrieval of data in Redis extremely fast, capable of performing roughly 110,000 **SET** operations or 81,000 **GET** operations per second [35]. While Redis can be used for multiple purposes, such as caching or message queues, its main purpose in this application was the storage of short-lived currency data.

### Forex-Python

The Redis store of currency data within this project is updated using a Python script, which obtains the data using the [forex-python](#) library. This library contains prices for most traditional currencies, as well as prices for Bitcoin obtained through CoinDesk's [Bitcoin Price API](#).

## 4.2.4 MongoDB

MongoDB is an open-source document-based database [21]. As mentioned in the above section, MongoDB was initially considered for the storage of currency data, subsequently replaced with Redis. However, the machine learning data and predicted prices of Bitcoin also needed to be stored somewhere. While Redis is suitable for short-lived currency data, it would not be suitable for storing any data related to the machine learning element of this project. It was decided by the team that due to previous knowledge of MongoDB, it would make sense to use it in this respect.

Within a separate Python script, data is obtained from the [forex-python](#) library and saved into a MongoDB document. As the machine learning model does not need to be retrained regularly, this is done at a much lesser frequency than that of the Redis script.

## 4.2.5 Vue.js

Vue.js is a JavaScript framework for building user interfaces, designed to be capable of integration into a project at any stage. Despite the team having no experience with Vue.js, the technology was adopted following advice from the team's supervisor and some intensive research and tutorial-based learning. While Vue.js was initially difficult to adapt to, the wide variety of tutorials and documentation available online greatly helped. The team did briefly consider changing to an alternative framework, but determined it was best to continue with Vue.js due to the time invested in learning. Ultimately, Vue.js proved to be a powerful tool; one the team would be comfortable working with again in the future.

## Chart.js

The team had initially intended to use D3.js to handle the representation of currency data through graphs, and spent a short period of time attempting to develop the application with this technology. After some difficulty with integration of D3.js in the initial weeks of development, the team had discussed the technology with fellow students who had also found D3.js difficult to incorporate into projects. Based on recommendations by fellow students, the team researched a similar technology called Chart.js.

Chart.js [36] allows developers to display data in a number of differently formatted graphs, all of which are capable of animation and customisation. Using the simple HTML5 `<canvas>` tag, Chart.js was much easier to adapt to than D3.js. Following brief research and some online tutorials, the team opted for the simplicity of Chart.js. Considering the graphs in this project did not need to do anything extraordinary, Chart.js was perfectly suited to this application.

### 4.2.6 TensorFlow

TensorFlow is an open source framework, designed to allow high performance numerical computation for machine learning purposes [27]. The software can be used with a number of languages such as C and C++, with the most popular and well-documented language being Python.

TensorFlow is based upon data flow graphs. Simply put, data flow graphs detail an input, some operations often on multiple levels, and an output. With regards to TensorFlow, each node in a graph represents a mathematical equation to be performed on the given edges which contain data (often multidimensional data arrays, described as tensors) which flow between them.

TensorFlow can be used in many applications, such as type prediction, value prediction, and image recognition; this application of TensorFlow within this project concerns value prediction. Data is loaded in, manipulated into the correct format to work with a specific model, and fed to that model. The model is first trained using historical data, in this case previous prices of Bitcoin, until it computes the correlation between actual and predicted values. Once trained, the model can be given unseen data to be tested. TensorFlow was deemed the most suitable technology for the machine learning aspect of this project, due to the team's previous experience of the technology and its extensive documentation and tutorials available online.

### 4.2.7 Heroku

Having initially expected to use Microsoft Azure for application deployment, when it came time to begin thinking about deploying the application it became obvious that this technology was excessive for this instance. As mentioned previously, Microsoft Azure offers an extensive range of services, and thus can be quite complex to use even for the most basic of applications. The team had also considered Heroku in the beginning and having since gained more experience of the technology through other projects, decided it was the best option for this project.

Heroku is an open source cloud application platform, providing extensive documentation for many facets of the deployment process and life cycle [37]. Heroku is arguably much easier to use than Microsoft Azure, allowing a developer to create and deploy an application from scratch in a very small amount of time. Heroku also allows applications to be deployed using Git, a tool the team were very familiar with due to extensive previous experience of GitHub. It was for the ease of deployment and comprehensive, easy to follow documentation that the team ultimately decided to use Heroku when deploying this application.

## 4.3 System Design

Throughout the development life cycle there were a number of changes regarding technologies and overall design of the web application. Having initially intended to follow the architecture detailed in (*Figure 4.1*), a number of problems and events ultimately led to some changes.

The restructuring of this application was not major but did greatly benefit the project, seeing the addition of new technologies and removal of those that were deemed unnecessary.

### 4.3.1 Web Application

#### Currency Data

Initially intended to be stored in a MongoDB document, currency data is now stored a Redis database.

( EXPLAIN SCRIPTS ) ( EXPLAIN FILES )

### 4.3.2 Machine Learning

Use LSTM(Long Short Term Memory) an efficient, gradient-based Model introduced by Hochreiter and Schmidhuber in 1997

<http://www.bioinf.jku.at/publications/older/2604.pdf>.

Recurrent Neural Networks attempt to address memory issues in traditional neural networks by adding loops within them, allowing information to persist ( <http://colah.github.io/posts/2015-08-Understanding-LSTMs/> ). A resonable analogy, is to envision recurrent neural network as numerous copies of the same network, each passing a message to a parent. This chain-like nature resembles the behaviour of sequences and lists, making them naturally suited to the architecture of a neural network. Unfortunately, RNNs are burdened with the problem of hadling long-term dependencies. As the neural network grows, gaps between past relevant data grows, and the RNN model becomes unable to learn to connect the information.

In theory, RNNs are absolutely capable of handling this issue. In fact, some are. Long Short Term Memory is an extension of or type of RNN that is capable. LSTM is very efficient on a large variety of problems, including timeline data

<https://dashee87.github.io/deep%20learning/python/predicting-cryptocurrency-p>

and are now widely used. LSTMs have another loop learning what data to forget and what data to remember. LSTM models still have this chain like structure, but with four different layers communicating in a certain way.

[ EXPLAIN FILES, PROBLEMS ETC ]

### Final Architecture

In conclusion, the final architecture indeed differs somewhat from that which was originally planned. A diagram of the complete final architecture for the system is detailed below.

## 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.

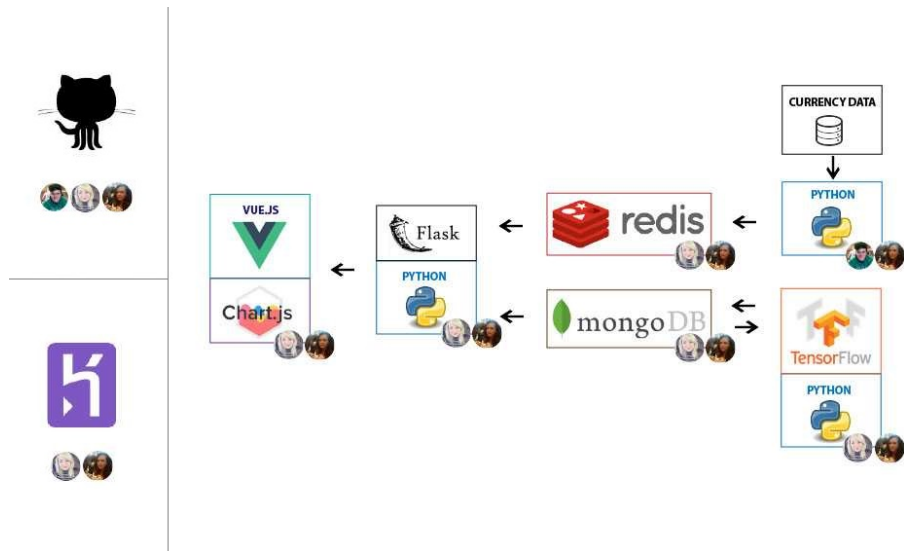


Figure 4.2: Final Architecture, *April 2018*

- Highlight any limitations or opportunities in your approach or technologies used.
- Highlight any limitations or opportunities in your approach or technologies used. Identifying limitations is not a sign of weakness. It is proof of insight.

Reflecting on the objectives discussed in *1.1: Project Objectives*, the following is a condensed initial list of objectives for both the dissertation and applied aspects this project:

***Dissertation Objectives:***

1. Introduce the concept of the project.
2. Provide the reader with a rounded understanding of cryptocurrencies.
3. Explain to the reader how volatile cryptocurrency prices can be.
4. Describe in detail the applied aspect of this project.

***Applied Project Objectives:***

1. Create a simple web application which is easy to use and clear to understand.
2. Deliver cryptocurrency prices to the user.



3. Provide an educated guess as to future changes in prices.
4. Work closely with the given learning outcomes for this project.
5. Conduct work as a team, in a professional manner akin to what is expected in industry.

#### 4.4.1 Testing

Based on the objectives outlined above, the following tests were carried out to gain an insight as to the success and robustness of this application.

##### Usability Testing

Undoubtedly, a large portion of this project as whole surrounds explaining to the reader the fundamentals of cryptocurrency. The goals which cannot be quantified were considered to be all *Dissertation Objectives*, and *Objective 1* in the *Applied Project Objectives* list. In order to measure the success of these goals, it was decided that the best way to do so was to ask others with varying levels of knowledge to read one or many chapters and briefly use the web application, and to gather feedback from them.

We created a survey through Google Forms, and sent its [link](#) to those who had kindly offered to read this dissertation. All information other than the number of chapters read was on a scale of one to five.

The form asked participants five questions; their initial level of knowledge of cryptocurrency, which dissertation chapters they had read, how easy they felt terminology was to understand, how much the reading had improved their knowledge of cryptocurrencies, and how easy they felt the corresponding web application was to use. Identity remained anonymous, as it was deemed not required for the purpose of the survey. The link was only sent to those who had agreed to participate, and thus the form's results would not be skewed by anyone who had not participated.

A summary of the results is detailed in *Figure 4.3* below.

Based on these results, we can conclude that while those with expert levels of initial knowledge did not learn much more, those with moderate or beginner levels of knowledge did increase that level of knowledge. For example, the second last entry details someone with initial knowledge of 2 and following their reading of all three theoretical chapters, had felt their knowledge of the area had improved substantially.

<i>Previous Knowledge</i>	<i>Chapters Read</i>	<i>Terminology Used</i>	<i>Improvement of Knowledge</i>	<i>Use of Web Application</i>
2	1, 2	4	4	4
5	1, 2, 3	5	2	5
4	All	3	4	5
1	1, 2	3	5	4
2	1, 2, 3	2	5	4
3	1, 2, 3	4	4	5

Figure 4.3: Survey Results *April 2018*

#### 4.4.2 Evaluation of Objectives

Following the objectives discussed above, the remaining objectives of the applied project were evaluated in the following ways:

**Objective 2 - Deliver cryptocurrency prices to the user:** Cryptocurrency prices were delivered to the user in the form of Bitcoin price in Euros, plotted on a graph contained in the web application home page. The data is obtained using the `forex-python` library, which is queried every thirty seconds for the latest Bitcoin price. The graph is updated to include this new value, with graph polling of data occurring every three seconds. This ensures that the prices are as up to date as can be.

**Objective 3 - Provide an educated guess as to future changes in prices:** Through the use of machine learning, estimating the following day's closing price of Bitcoin has been achieved and implemented within the application. Due to the limitations of the system's prediction model, the estimate of close price is only applicable on a day to day basis and cannot be used for long term predictions, thus the system is retrained once per day on updated currency data. The predictions are delivered to the user via a graph, displaying previous predictions versus actual close prices. Unfortunately, natural language processing techniques were not implemented in this project, offering opportunity for future development.

**Objective 4 - Work closely with the given learning outcomes for this project:** The expected learning outcomes for this project included applying appropriate research and development methodologies, demonstrating awareness of innovative technologies and incorporating them into the project where relevant, and the ability to critically evaluate the work and any potential for future work. As outlined in *4.1.1: Preliminary Research and Project Commencement*, the team conducted extensive research into a variety of dif-

ferent technologies and methodologies before beginning the project. While most of the project relies on faithful technologies such as Python, an effort was made to integrate newer technologies such as TensorFlow for Machine Learning, where it was deemed important to take advantage of the newest innovations in the field. Finally, the project has

***Objective 5 - Conduct work as a team, in a professional manner akin to what is expected in industry:*** As discussed in 4.1.2: *Issues Encountered During the Development Process*, there were a number of problems faced by the team throughout this project's life cycle. All disagreements were discussed in a calm manner, giving each team member an equal platform on which to discuss their concerns. The team believe to have conducted themselves in a professional manner throughout the project, evident in the endurance of their friendships through any disagreements.

#### 4.4.3 Opportunities for Improvement

Highlight any limitations or opportunities in your approach or technologies used. Identifying limitations is not a sign of weakness. It is proof of insight.

While the project achieved its initial objectives in some capacity or another, the point at which any project is complete and unable to be improved upon is difficult to pinpoint.

The preliminary planning of this project inevitably meant most of the technologies chosen were chosen for the right reasons, and if not were quickly replaced by more appropriate technologies. While the team is content with the technologies implemented in the final solution, there is of course opportunity for improvement with regard to extra features in the web application.

***Natural Language Processing:*** As mentioned in the initial 1.1: *Objectives*, natural language processing can and has previously been used [15] to determine fluctuations in prices of cryptocurrency. This project could greatly benefit from such technology, through implementing a component which would search given sites for negative or positive discussions on cryptocurrencies. This information could be used to predict an incoming change of price, or simply display the changing popularity of given cryptocurrencies from day to day.

***Long Term Predictions:*** In addition to natural language processing, a neural network model for long-term prediction could also be implemented. Unfortunately the current application only estimates short-term values effectively, and the addition of a long-term estimate using both machine learning and natural language processing would make this application more attractive to those considering long-term investment in cryptocurrency.

**Docker:** As outlined in *4.1.1: Research Methodology*, Docker was initially considered for its containerisation capabilities. The technology was not crucial and due to time constraints was not implemented to facilitate more crucial work being completed. However, the use of Docker in the system would add an extra layer of robustness, allowing for easy local deployment should the Heroku deployment ever be unavailable.

#### 4.4.4 Overall Evaluation

To conclude, this application and dissertation have achieved the main objectives described in *1.1: Objectives* in full or some capacity. Based on usability tests, any given is likely to benefit from either the web application or the dissertation, or both. The project is built on solid and enduring technologies such as Python, with newer, innovative technologies such as TensorFlow incorporated to add an extra layer of interest and allure to the project. Despite numerous problems and associated delays, the project has achieved initial goals and objectives in an appropriate manner, leaving room for further additional development.

# 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: <https://currencyanalyser.herokuapp.com/>

Screencast: <https://github.com/rebeccabernie/CurrencyAnalyser/blob/master/Screencast.mp4>

# 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/](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] F. Mai, Z. Shan, Q. Bai, X. Wang, R. Chiang, “How does social media impact bitcoin value? a test of the silent majority hypothesis,” *Journal of Management Information Systems*, vol. 35, no. 1, pp. 19–52, 2018.
- [16] Merriam-Webster Incorporated, “Bubble; noun.” Last accessed on 11 Apr 2018. URL: <https://www.merriam-webster.com/dictionary/bubble>.
- [17] Investopedia LLC., “The great recession.” Last accessed on 11 Apr 2018. URL: <https://www.investopedia.com/terms/g/great-recession.asp>.
- [18] M. Mihaly, “Comparing bitcoin to tulips is absurd. stop it.,” 2017. Last accessed on 11 Apr 2018. URL: <https://medium.com/@themihaly/comparing-bitcoin-to-tulips-is-absurd-stop-it-9c8b489727fc>.
- [19] G. Trends, “‘bitcoin’ search term popularity.” Last accessed on 11 Apr 2018. URL: <https://trends.google.com/trends/explore?date=all&q=bitcoin>.
- [20] R. Derousseau, “Why the air is coming out of the bitcoin bubble,” *Money*, vol. 47, no. 2, pp. 31–33, 2018.
- [21] MongoDB Inc., “Mongodb documentation.” Last accessed 9 Apr 2018. URL: <https://docs.mongodb.com/>.
- [22] E. You, “Vue.js: The progressive javascript framework.” Last accessed 9 Apr 2018. URL: <https://vuejs.org/v2/guide/>.
- [23] M. Bostock, “D3.js: Data-driven documents.” Last accessed 9 Apr 2018. URL :<https://d3js.org/>.



- [24] Microsoft Corporation, “Microsoft azure: Cloud computing platform and services.” Last accessed on 29 March 2018. URL: <https://azure.microsoft.com/en-us/>.
- [25] Salesforce.com, “Heroku: Cloud application platform.” Last accessed on 8 Apr 2018. URL: <https://www.heroku.com/>.
- [26] D. Inc., “Docker documentation.” Last accessed on 29 Mar 2018. URL: <https://docs.docker.com/>.
- [27] Google Brain Team, “Tensorflow: An open source machine learning framework for everyone.” Last accessed 9 Apr 2018. URL <https://www.tensorflow.org/>.
- [28] K. Beck et al, “Principles behind the agile manifesto.” Last accessed 9 Apr 2018. URL: <http://agilemanifesto.org/principles.html>.
- [29] J. Highsmith and A. Cockburn, “Agile software development: The business of innovation,” *Computer*, vol. 34, pp. 120–122, 2001.
- [30] D. Wells, “Extreme programming: A gentle introduction,” 2009. Last accessed on 10 Apr 2018. URL: <http://www.extremeprogramming.org/>.
- [31] Python Software Foundation, “Python 3.6.5 documentation.” Last accessed on 10 Apr 2018. URL: <https://docs.python.org/3/>.
- [32] Anaconda Inc., “The most popular python data science platform.” Last accessed on 10 Apr 2018. URL: <https://www.anaconda.com/what-is-anaconda/>.
- [33] A. Ronacher, “Flask (a python microframework).” Last accessed on 10 Apr 2018. URL: <http://flask.pocoo.org/>.
- [34] S. Sanfilippo et al, “Redis.” Last accessed on 10 Apr 2018. URL: <https://redis.io/>.
- [35] Tutorialspoint, “Redis - overview.” Last accessed on 10 Apr 2018. URL: [https://www.tutorialspoint.com/redis/redis\\_overview.htm](https://www.tutorialspoint.com/redis/redis_overview.htm).
- [36] E. Timberg et al, “Chart.js: Simple yet flexible javascript charting for designers and developers.” Last accessed on 10 Apr 2018. URL: <https://www.chartjs.org/>.
- [37] Salesforce.com, “Heroku deployment documentation.” Last accessed 9 Apr 2018. URL: <https://devcenter.heroku.com/categories/deployment>.