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)

GMIT
INSTITIÚID TEICNEOLAÍOCHTA NA GAILLIMHE-MAIGH EO
GALWAY-MAYO INSTITUTE OF TECHNOLOGY

Contents

About this project

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

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

Authors Will get everyone to write their own?

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. In these short years, we have witnessed the birth, growth and sometimes failure of various technologies, approaches and trends.

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

When we began our journeys on this path in 2014, cryptocurrency was a relatively unheard of phrase to the average individual. In the years since, the likes of Bitcoin and Ethereum have become almost household terms, with many more people investing in various cryptocurrencies and following their repeating rise and decline. While cryptocurrencies were initially a mystery to the average individual, the arrival of user-friendly trading sites has meant they have now become an almost common asset, seen regularly in the news and no doubt discussed over many water coolers.

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

- we wanted to attempt to predict the price of some of the more popular cryptocurrencies and deliver these predictions to users in a simple manner that could be understood by anyone with even a basic knowledge of the area of cryptocurrency.

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

All source code and documentation for this project can be found in the project's GitHub repository.

1.1 Objectives for the Project

Keep in mind the LEARNING OUTCOMES.

- Demonstrate the application of appropriate research methodologies and techniques related to software development.
- Demonstrate an awareness of the present state of the art in a specialist computing area including the ability to evaluate the literature base.
- Integrate disparate technologies and principles to successfully develop and deliver an appropriately integrated solution to a computer-based project.
- Apply research and critical thinking skills to a challenging computer based problem.
- Evaluate, select and apply standard and customised research tools and methodologies of enquiry.
- Design and implement a computing solution that requires preliminary research.
- Critically evaluate the work and research and reflect on the strength, weaknesses and future potential of such work.

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

as a whole was to provide anyone with a very basic knowledge of cryptocurrency with a more in-depth knowledge, and a facility to

- Provide reader with in-depth understanding of cryptos - including different currencies, how to buy and sell, technologies, security, whole process. explain the long term viability of cryptos as an asset to invest in.
- Explain to reader what affects cryptos - explore different influences in prices, attempt to predict prices, explain the volatility of it all.
- Develop a web application to deliver predicted prices to the user, not guaranteed to be right but should clear up when is good or bad to buy. Goal of it is to be used AFTER reading this diss or at least some of it - they'll need to know the general influencing factors and not just blindly trust us.

1.1.1 Metrics for Success/Failure

1.2 Description of Each Chapter

ALL NEEDS TO BE RE-WRITTEN AT LEAST SLIGHTLY.

1.2.1 Understanding Cryptocurrency

In chapter 2, *Understanding Cryptocurrency*, we explain what exactly a cryptocurrency is, and how it differs in various ways from a traditional currency, before briefly examining some of the most popular and well-known cryptocurrencies such as Bitcoin, Ethereum, Litecoin, and more. We also delve into some of the technologies behind cryptocurrency, such as blockchain technology.

1.2.2 Predicting the Prices of Cryptocurrency

Chapter 3 - will need to tidy this explanation up - is where the theoretical analytics and applied elements of this project meet. We discuss the influencing topic for the project, the main driving force behind the project, something like that. Explain the volatility of cryptocurrency, influencing factors on prices such as hype, news, hacks, maybe even the whole ”are the South Koreans awake” thing.

1.2.3 Applied Project Chapter (tbrn)

To be renamed. This is where the applied ”Currency Analyser” aspect of our project is explained. We examine the methodologies and planning used throughout our project, also dealing with any aspects which could have been done/planned/managed/organised 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 untraceable 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. Thank 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]. 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 *Section 2.3*.

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 *Section 2.3*.

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 *Anonimity 2.2.1*, 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 to the public 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.

When the first Bitcoins were released in 2009, the price per coin was estimated to have been a mere \$0.001.

- Beginning of bitcoin - rise of bitcoin -

2.3 Blockchain and Other Underlying Technologies

Security features, bitcoin wallet complicated etc, fluctuations in TCs due to war/government etc vs flucs in CCs down to sheer hype/demand etc.

2.4 The Viability of Cryptocurrency

Overall Viability - all the pros like security, blockchain etc. Section will maybe touch on volatility, but will lead to Ch3 which will mainly discuss the volatiliy.

Chapter 3

Predicting The Prices of Cryptocurrencies

Tie concept of diss with concept of proj.

3.1 The Volatility of Cryptocurrency

3.1.1 Influencing Factors in the Price of Cryptocurrency

Start with explaining what influences traditional currencies, lead into main body of CC influencing factors.

3.2 Segway into applied proj

”Deciding to Analyze the Volatiliy of Cryptos”...?

Chapter 4

Applied Project Chapter

4.1 Context

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

4.2 Methodology

3-5 pages (2-3000 words) Describe the way you went about your project, Was your approach to the problem valid?

- Software development v/s Research methodology. Agile / incremental and iterative approach to development.
- Planning. Did you storyboard? How did you determine the requirements for the project?
- Meetings. Frequency, structure, checks and balances, feedback.
- What about validation and testing? Junit or some other framework.
- If team based, did you use GitHub during the development process.

- Selection criteria for algorithms, languages, platforms and technologies. Was an empirical approach used? How were problems solved? Was any research undertaken first?

4.3 Technologies / Tech Review

About seven to ten pages.

- The “literature review” part of the dissertation. Should be tightly coupled to the context and objective from the introduction. Proves that you researched what you were doing!

- Describe each of the technologies you used at a conceptual level. Standards, Database Model (e.g. MongoDB, CouchDB), XMl, WSDL, JSON, JAXP. Use references (IEEE format, e.g. [1]), Books, Papers, URLs (timestamp) Sources should be authoritative!

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

4.4 System Design

As many pages as needed.

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

Column 1	Column 2
Rows 2.1	Row 2.2

Table 4.1: A table.

4.5 System Evaluation

As many pages as needed.

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

Chapter 5

Conclusion

About three pages.

- Briefly summarise your context and ob-jectives (a few lines).
- Highlight your findings from the evalua-tion section / chapter and any opportuni-ties identified.

5.1 Context/Objectives

5.2 Findings

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).” https://www.wired.com/1994/12/emoney/ Last accessed on 6 Apr 2018.

[3] S. Higgins, “3 pre-bitcoin virtual currencies that bit the dust.” https://www.coindesk.com/3-pre-bitcoin-virtual-currencies-bit-dust/. Last accessed on 5 Apr 2018.

[4] “Cryptocurrency market capitalizations.” https://coinmarketcap.com/ Last accessed on 6 Apr 2018.

[5] “Coinbase.” https://coinbase.com/ Last accessed on 6 Apr 2018.

[6] “Gdax.” https://www.gdax.com/ Last accessed on 6 Apr 2018.

[7] S. Nakamoto, “Bitcoin: A peer-to-peer electronic cash system,” 2008.