The Role Decentralised Non-Regulated Virtual Currencies Play in Facilitating Unlawful Financial Transactions.

CIAN HEALY

ZHE LI

Master of Science Thesis

Stockholm, Sweden 2016
The Role Decentralised Non-Regulated Virtual Currencies Play in Facilitating Unlawful Financial Transactions.

Cian Healy
Zhe Li

Masters of Science Thesis Indek 2016:80
KTH Industrial Engineering and Management
Industrial Management
SE – 100 44 Stockholm
Abstract

As consumer payment services have been developed at a rapid rate in recent years, the introduction to the market of decentralised, non-regulated cryptocurrencies has enabled a significant increase in acts of criminality in the cyber environment. Efforts to combat and curb the continued growth of such illicit activities have included the development, implementation and enforcement of legislation and regulations by governing authorities on a global scale. For the purpose of this thesis, interviews were conducted with several industry experts and governmental officials specializing in the use of virtual currencies for illicit financial transactions, namely fraud, money laundering and tax evasion. While the extent to which decentralised, non-regulated payment services actually contributes to illicit financial transactions remains unclear, it can certainly be said that as the use of new and emerging virtual currencies increases, so too will acts of criminality in the cyber world.

Key Words: Virtual Currency, Cryptocurrency, Bitcoin, Illicit Financial Transactions, Cybercrime.
# Table of Contents

## Contents

1. Introduction ........................................................................................................... 1  
   1.1 Background......................................................................................................... 1  
   1.2 Problem Discussion: ......................................................................................... 2  
   1.3 Purpose: ............................................................................................................ 3  
   1.4 Research Question: ......................................................................................... 3  
   1.5 Delimitations: .................................................................................................. 3  
   1.6 Thesis Outline .................................................................................................. 3  
2. Literature Review .................................................................................................. 4  
   2.1 What is Bitcoin? ............................................................................................... 4  
   2.2 Categorising Acts of Criminality ...................................................................... 5  
      2.2.1 Specific Bitcoin Crimes: ........................................................................... 5  
      2.2.2 Money Laundering: .................................................................................. 5  
      2.2.3 Bitcoin Facilitated Crime ......................................................................... 5  
   2.3 Silk Road ........................................................................................................... 5  
   2.4 Advancements in Innovative Criminal Methods ............................................... 6  
   2.5 Governmental Regulations ............................................................................. 7  
3. Methodology ......................................................................................................... 10  
   3.1 Aim .................................................................................................................. 10  
   3.2 Research Paradigm ........................................................................................... 10  
   3.3 Research Methods ............................................................................................ 10  
   3.4 Interviews ......................................................................................................... 10  
      3.4.1 Direct feedback from respondent............................................................... 10  
      3.4.2 Opportunity to probe and explore............................................................... 11  
      3.4.3 Yields rich data, details and new insights ................................................... 11  
      3.4.4 Topics can be explored in depth ................................................................. 11  
   3.5 Interviewees ..................................................................................................... 11  
   3.6 Literature references ....................................................................................... 12  
   3.7 Development of Research Question .................................................................. 12  
      3.7.1- Principal research questions .................................................................... 12  
      3.7.2- Development of interview questions ..................................................... 13  
      3.7.3- Methods of analysing results .................................................................. 14
List of Figures

Figure 1 Research Process .................................................................................................. 13.
Figure 2 Graph Sample .................................................................................................... 14.
Figure 3 Unlawful Financial Transactions ........................................................................ 15.
Figure 4 Triangular Scheme ............................................................................................. 18.
Figure 5 Regulation ......................................................................................................... 19.
Figure 6 Centralisation ..................................................................................................... 21.
Figure 7 Future of Bitcoin .............................................................................................. 22.
Figure 8 – Future of Bitcoin ........................................................................................... 28.
Definitions

<table>
<thead>
<tr>
<th>Term</th>
<th>Definition</th>
</tr>
</thead>
<tbody>
<tr>
<td>Blockchain</td>
<td>Is a digital ledger that shows all the transactions made by decentralised virtual currencies.</td>
</tr>
<tr>
<td>Bitcoin</td>
<td>Is a decentralised virtual currency that facilitates peer to peer transactions.</td>
</tr>
<tr>
<td>Fiat Currency</td>
<td>Is referred as a currency that is issued by a country's government and is regulated to the entire population.</td>
</tr>
<tr>
<td>Virtual Currency</td>
<td>Is a digital representation of value, not issued by a central bank, credit institution or e-money institution, which, in some circumstances, can be used as an alternative to money.</td>
</tr>
<tr>
<td>Unlawful Financial Transactions</td>
<td>Refers to when money is illegally earned that goes unrecorded in the balance of payment records in a country.</td>
</tr>
</tbody>
</table>

List of Abbreviations

<table>
<thead>
<tr>
<th>Abbreviation</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>AML</td>
<td>Anti-money laundering</td>
</tr>
<tr>
<td>KYC</td>
<td>Know your customer</td>
</tr>
<tr>
<td>VCS</td>
<td>Virtual Currencies</td>
</tr>
<tr>
<td>UFT</td>
<td>Unlawful Financial Transactions</td>
</tr>
</tbody>
</table>
Acknowledgements

First of all, we would like to thank our supervisor Aziza, for all her support during the duration of the thesis. She guided us through the process in a clear and concise manner. Also, we would like to thank KTH Royal Institute of Technology and the department of Industrial Economics and Management for giving us the opportunity to write the thesis. We would like to thank all the interviewee’s who took part in the interviews that we conducted, without their professional advice and expertise the thesis would have lacked information regarding our topic.

We would also like to say thanks to our families and friends for their support during the duration of the thesis.
1. Introduction

1.1 Background

Historically there have been many different forms of payment systems. Bartering is thought years to be the earliest system of exchange and is believed to date back over 100,000 years (Rebello, 2013). Bartering slowly evolved into what we call an early form of ‘commodity money’. This was where universally valuable objects like dyes, salts and animal skins were used as a common medium of exchange (Kramer, 1959).

Skip forward another couple of thousand years and the first manufactured currencies were minted. These official coins began to appear independently in India, China and cities around the Aegean Sea somewhere between 700 and 500 B.C. These set the president and foundation from which the standardized forms of currency we see today emerged (Rebello, 2013). From these standardized forms of currency and centuries of transmutation later, we ended up with what we now have today in the form bank notes, cheques and payment cards.

The first of these payment cards was in the form of a charge card and what was referred to as a Diner Club card. These were introduced in the 1950’s and allowed consumers to purchase goods on credit from a large quantity of stores all the while carrying no physical cash on their persons (Evans and Schmalensee, 1999). Since the inception of these payment cards in the 1950’s, the notion of a cashless society has never been far from discussion. Since then cashless means of payment have become more and more common place and over 50 years later and we find ourselves relying more and more on these digital forms of payment.

VCS and mobile payments have become big players in the way people utilise payment systems in modern day society. VCS such as Bitcoin have seen exponential growth in the past couple of years.

As the decades have passed, the advancements in consumer payment services have developed rapidly. This has led to many acts of criminality materialising as perpetrators have used these new innovations as a means to gain financially for themselves (Home Office, 2013a). Cybercrime can be simply defined as any ‘criminal activity carried out by means of computers or the Internet.’ (Oxforddictionaries.com, 2016) and although cybercrime is often considered a relatively new phenomenon, its origins can be found to date back a few decades (CIO, 2016). The first notable case of cybercrime can be attributed to a man named John Draper. In 1971 he cleverly figured out that he could make long distance phone calls for free by using a toy whistle to trick the phone system into thinking the call had ended (Wozniak and Smith, 2006).
Moreover, we can date back to 1996 where a physician named Douglas Johnson created an online digital currency called e-gold that would be completely backed by actual real gold stored in several locations across the globe (J. Villasenor, 2011). As it grew in popularity, entrepreneur criminal groups viewed this new innovation as an opportunity to launder money. Eventually it drew the attention of the U.S Department of Justice and subsequent action was taken. Skip on 12 years, a new cryptocurrency called bitcoin was developed by a Japanese man named Satoshi Nakamoto. This new decentralised cryptocurrency would enable peers to make transactions amongst themselves in turn eradicating the middlemen e.g. financial institutions. Like e-gold, criminals saw an opportunity with bitcoin to make a personal gain as transactions and accounts are completely anonymous (Peng, 2013).

Identity theft, hacking, invasion of privacy and Internet fraud are other perhaps more sinister examples of cybercrimes that have been perpetrated since that date. Currently “Cybercrime is a fast-growing area of crime. More and more criminals are exploiting the speed, convenience and anonymity of the Internet to commit a diverse range of criminal activities that know no borders, either physical or virtual, cause serious harm and pose very real threats to victims worldwide” (Interpol, 2016). As society grew and payment systems evolved, so too have the criminals that prey upon them. History is rife with examples of thievery, fraud and deception. The examples are too plentiful to fathom.

Today in that regard, not much has changed. Criminals will still try to exploit any weaknesses or opportunities that present themselves, be it in the form of a cyber-hack or taking advantage of vulnerability in the payment system infrastructure. Physical cash is becoming more and more of a rarity at the behest of its digital counterpart. We believe and will argue in this paper that the road towards a cashless society will not only inadvertently cause a steep rise in the number of cybercrimes being perpetrated, it will also open up the possibility for cyber criminals anywhere on the globe to target victims across international boundaries and to commit their cyber-crimes with complete anonymity with the aid of VCS.

1.2 Problem Discussion:

Sweden is widely regarded as the country closest to achieving a total cashless society (ComputerWeekly, 2016). Some experts estimate that Sweden could be completely cash free by as early as 2030 (ComputerWeekly, 2016). As people begin to carry less and less physical money on their person, traditional thievery and larceny becomes less incentivised for the common criminal. This paves the way for new technologies to be introduced into the payment sector which can result in fraudulent activity occurring in many cases.
1.3 Purpose:
The purpose of this thesis was to examine whether or not there is a correlation between the uses of VCS for UFT. To do this we first reviewed all of the relevant literature revolving around VCS and its connection to cybercrime. (You can find this in the next section)

The researchers then proceeded to adopt an analytical approach and examined various reports analysing VCS in Europe by governing bodies e.g. European Central Bank. The researchers decided to focus on Sweden for the purpose of this paper due to the countries close links becoming a cashless society and our own familiarity with the country as visiting students.

1.4 Research Question:
This thesis aims to answer the following research question:
- Do virtual currencies significantly facilitate unlawful financial transactions?

1.5 Delimitations:
For the purpose of the thesis, the topic was chosen primarily due to our interest in VCS and the use of VCS for criminal activities. VCS other than bitcoin on the market were not chosen when describing VCS for the use of UFT. This was due to bitcoins popularity amongst the users of VCS. We decided not to focus on the other European countries in this research due to the fact that we are currently studying in Sweden. As the shadow economy is a quite broad, the researchers narrowed the research to three main areas tax evasion, money laundering and fraud.

1.6 Thesis Outline
The following chapter presents the methodology of the thesis, in this section it describes how the research was carried out by means of collecting and gathering data. Following this chapter, the literature review is presented taking into account the various authors scientific and academic articles from either end of the spectrum in relation to research question. The subsequent chapter presents the results and findings that were collected from interviews and other sources. The results are intended to give the reader a clear understanding of whether or not decentralised non-regulated payment services are one of the main drivers in facilitating UFT.
2. Literature Review

As discussed briefly in the introduction the evolution of cybercrime has vastly increased since the digital age was born. As Sweden is swiftly moving towards a cashless society, industry experts estimate this change by as early as 2030 (ComputerWeekly, 2016). This change is seeing a trend of increasing acts of criminality in the virtual environment. In this section, we will explore the various literatures that explain how the advancements in consumer payment innovations are contributing to UFT.

2.1 What is Bitcoin?

Bitcoin is a so-called virtual currency that has been devised for anonymous payments made entirely independently of governments and banks (Segendorf, 2014). Initial reports suggest the founder was Satoshi Nakamoto in 2008 but in recent times an Australian entrepreneur named Craig Wright claims to be the cryptocurrency founder. Bitcoin is a purely peer-to-peer version of virtual cash in which would allow online payments to be sent directly from one party to another (Nakamoto, 2008). The decentralised currency is limited to 21 billion bitcoin (Reid, 2013). The most common ways to purchase bitcoins are through bitcoin exchanges e.g. Coinbase.com (Roose, 2013). Moreover, Bitcoins can then be either mined or received as a payment for goods and services (Ford, 2013).

Bitcoin primarily relies on digital signatures to ensure the correct validation of ownership and a public history of transaction’s in order to eradicate double spending (Nakamoto, 2008). Bitcoin uses a unique cryptographic system to verify transactions between peers by avoiding the usual requirements of a central bank or authority in turn creating a sense of trust in the system between the users (Nakamoto, 2008). Once a transaction is processed so to speak, it is irreversible. As briefly discussed above, one of bitcoin’s main objectives is to eradicate double spending. To ensure this, a distributed timestamp server is used in order to produce computational proof of the sequential order of all transaction’s (Nakamoto, 2008). These transaction records are stored on a database called ‘the blockchain’ whereby all transactions can be viewed by the public. A blockchain is sometimes referred to a distributed ledger (Deloitte, 2016).

The system itself does not record any personal information regarding the transaction, thus giving the user a sense of anonymity. In addition, the block chain is not fully anonymous due to the public nature of the blockchain. While bitcoin can be viewed as an alternative method for consumer payment, it is largely used by criminals for the illegal payment of goods and other criminal activity.
2.2 Categorising Acts of Criminality

Böhme (2015) articulates and defines bitcoin’s UFT into three main categories: specific Bitcoin crimes, money laundering and bitcoin facilitated crime.

2.2.1 Specific Bitcoin Crimes:

These crimes that occur are a direct result of computer based attacks from technological masterminds whose intention is to steal bitcoins and also to manipulate the exchange rate of the virtual currency. Often enough, when these attacks occur there is a lack of knowledge to prevent further attacks from taking place as there is a difficulty in finding who the perpetrator is due to the lack of technological knowhow.

2.2.2 Money Laundering:

Bitcoins can be used for explicit reasons such as money laundering (Böhme, 2015). The movement of funds between accounts can be extremely difficult to trace as funds are routed through mixers as they are hidden from the general public and also law enforcements (Böhme, 2015). That being said, Bitcoin is designed in a way that funds could be possibly traced if required with the exchange platform block chain where transactions are made public. Maybe with the correct skill levels's In analysing the transactional data, the person’s responsible for laundering money could be caught.

2.2.3 Bitcoin Facilitated Crime:

Bitcoin facilitates the payment for illegal goods and services predominantly purchased on a marketplace called the ‘Silk Road’. Criminals who use this illegal site for their personal gain are attracted to it as they perceive it as the perfect scenario as the transaction are irreversible and anonymous. Böhme (2015) explains how VCS attract criminals as they have been banned or not regulated in their country.

2.3 Silk Road

The internet is increasingly viewed as one the key drivers of the contemporary drug markets by the promotion of drug shopping in web based outlets (Bingham, 2013). Research has shown that through the advancements in technology the birth of online drug market places have become increasingly innovative and dynamic (Griffiths, 2010)

When the anonymous online marketplace called ‘Silk Road’ came to fruition it was described as a new phenomenon. According to Schumer (2011), ‘Silk Road, is a certifiable one stop shop for illegal drugs that represents the most brazen attempt to peddle drugs online that we have ever seen. It’s more brazen than anything else by lightyears”. The colloquial methods of online sales of drugs prior to the existence of this new revolutionary platform were bulletins on forums online with payment including PayPal (Kim, 2014). Researchers who have analysed spending behaviours of people that use Silk Road as drug users who purchase illegal drugs for their own
personal consumption (Christin, 2013). When bitcoin came into existence, the decentralised currency was the means of payment when purchasing off Silk Road. It is said that the time between Silk Road started in 2011 to closure in 2013; it did $1.2 billion worth of business (Jeffries, 2013).

2.4 Advancements in Innovative Criminal Methods

As internet technologies are growing at a rapid rate, so have the ways and methods in which groups of entrepreneurial criminals use them for unlawful activities. Anderson (2012) believes that fraudulent activity is more likely to occur as more transactions go online and that the protection of the consumer will diminish as new payment systems are replacing the traditional framework. With the introduction of new and innovative methods in the virtual eco system, and the ease of which a person’s anonymity is disguised has helped change the criminal underworld, offering new ways to move large quantities of money with ease (Pearce, 2012). Anderson (2012) explains how it is wrong to reject the advancements in innovation even if it leads to an increase in fraudulent activity in the cyber world. As a result of this rapid increase in the innovation of consumer payment services, many governments are searching for ways to adapt to the changing market in order to implement regulatory frameworks to this new digital era of non-traditional payment methods (Tropina, 2014). This new shift in implementing regulatory frameworks is a direct result due to the increasing levels of fraudulent activity that currently exists in order to protect consumers (Tropina, 2014). UFT such as money laundering have been in existence for decades. Taking this into consideration, a new term used to describe money laundering on the internet called ‘Cyberlaundering’ has been created (Weaver, 2005).

The ease of which unlawful transactions are being transferred in virtual environments by money launderers when the colloquial means of transferring money fails, is becoming an ever growing problem for government officials trying to prevent these transactions from occurring (AUSTRAC, 2012). The risks of virtual environments such as bitcoin has been largely debated amongst professionals with some believing that these cryptocurrencies are in need to be regulated with legitimate legislation similar to ones in the real world (Pearce, 2012). However, on the other hand others strongly feel that VCS do not have the capacity to which withstand such large quantities of money laundering as discussed in the financial action task force report (FATF, 2015).

In AUSTRAC (2012) report on VCS, it was stated by the Australian government officials that because as the adoption rate of using such a currency is quite small and is limited in purchasing goods and services from business, it therefore limits the movement of UFT from occurring. In addition, AUSTRAC (2012) believes that these cyber criminals may be forced into using such VCS for small scale unlawful activities.
It can be argued that bitcoin is a disruptive innovation in its kind and can be seen as a benefit to society. The virtual currency poses a real threat to the more common methods of payment such as debit cards and cash. Taking into account the positives aspects of the virtual currency, Sullivan (2008) highlights the issue on how these new virtual environments are fruitful and desirable towards criminals due to the lack of efficient monitoring of unlawful transactions, sparse due diligence, poor customer identification records and the insufficient methods of detecting fraudulent activity. It is suggested that the main reason for these inefficiencies is due to the fact that these VCS are not regulated which in turn paves the way for criminals allowing monumental amounts of money to be transferred between accounts and in turn providing a tax haven for them (Sullivan, 2008). Leinonen (2008) shares the same view along with the Anderson (2012) & Sullivan (2008), being that future e-crimes will be committed directly as a result of stolen funds from e-payment systems. These entrepreneurial criminal groups are quickly adapting to these new technologies and learning how to best hack these systems in order to profit for them.

2.5 Governmental Regulations

The evolution of decentralised non regulated payment services such as bitcoin has led to the virtual currency entity wanting to make central banks obsolete by ultimately replacing their primary role as money issuing through a decentralized alternative.

That being said, according to the European Central’s Bank (ECB) report on virtual currency’s, the analysts that reside in the ECB have stated that from an economic perspective, the VCS are deemed not as functional as normal centralised currencies and fail to meet the required three distinctive functions of money in relation to economic literature: i) medium of exchange (Money main function is a medium in order to facilitate transaction and in turn avoiding the inconvenient of a barter system); ii) store of value (Money must be able to hold its value of a certain period of time); and iii) unit of account (Money as a function must enable the correct measure of goods and services being sold) (ECB, 2015). Moreover, the ECB argue that even though bitcoin is by far the most popular virtual currency, it fails to meet the adequate level of vital functions as money. Therefore, it is stated that bitcoin has a limited function as a medium of exchange because it has a low acceptance rate amongst the population of countries (ECB, 2015).

Furthermore, while the more traditional payment methods have been regulated with a view to preventing money laundering, online payment services or peer to peer payment services still today remain heavily unregulated (FATF, 2015).

Currently in the EU, VCS are not regulated but as it is a relatively new phenomenon which is growing swiftly, it is too early to change or tailor the legislation in case one day it is made a legal tender. One major factor to take into consideration when challenging bitcoin’s potential to be a legal tender in the future is the requirement of
In addition, cryptocurrencies like bitcoin are being perceived by many legal entities as cyber tax havens for fraud and tax evasion, due to the anonymity and challenging task of locating IP addresses. Technologies such as the Tor network, which is a system specifically used to prevent any leaks of anonymity facilitated by surveillance software (Nicol, 2016). Taking this into account, as cryptocurrencies are viewed as tax havens, there is still a high degree of uncertainty with governmental bodies on how to efficiently enforce laws and regulations in order to prevent acts of fraudulent activity when there is no ‘point of sale’ like in the physical world (Europe, 2012). Traditionally, the more common payment methods implement checks on their consumer transactions in order to see if there is any sign of suspicious activity occurring with some organisations preforming “Know your customer” (KYC) techniques but the more non-traditional payment service provider’s fail to do so (Tropina, 2014). The main focus of implementing of KYC techniques is that it sets out appropriate measures for customers when identifying themselves and gaining a deeper understanding of the customers spending habits and their expected financial activities (Liu, 2012). This is vital in order to determine the money laundering financial risk of that customer.

Furthermore, one major issue with the bitcoin platform is that there is such a multitude of traffic occurring each day it is almost an impossible task to track all major movements for possible instances of tax evasion and until this is enforced it will continue to happen but this ultimately goes against the decentralized and open source nature of bitcoin (Marian, 2013). It is quite visible to see that there has been virtually no transparency between managing the risks of tax evasion with bitcoin’s decentralised which has not been solved to an adequate manner (Kapoor, 2016). To ensure tax evasion is monitored to a correct level with decentralised non-regulated payment services, a system would have to be implemented whereby every transaction is monitored closely and realistically this is impractical. It would require an extreme amount of resources (Marian, 2013).

Marian (2013) describes how cryptocurrencies have the required characteristics of tax havens. In addition, two crucial aspects of these cryptocurrencies to take into consideration are that their operations are not dependant on central financial institutions and that they are explicitly anonymous (Marian, 2013). Recently, governments have been zoning in on catching offshore accounts with most recently the highlighting of the panama papers and these cryptocurrencies have the ability to defeat the governmental bodies. Experts in the field of decentralised payments have researched and analysed transaction habits of bitcoin users which has resulted in them finding that large quantities of bitcoins are distributed between several different small accounts (Shamir, 2012). In addition, these cunning tactics are normally used by tax evaders and money launderers in order to hide their assets and resources.
A small number of researchers working in the field believe that they are numerous money laundering schemes when it comes to the decentralised non-regulated virtual currency banks and also they highlight the fact that these have the potential to become money laundering centres (AUSTRAC, 2012).

Tropina (2014) describes how to tackle the increasing problem of money laundering in the virtual environment is by creating awareness amongst the involved stakeholders trying to combat the problem. The private sector must become involved and conjure up possible techniques that can be successfully implemented to prevent further unlawful transactions from being allowed to take place. Leinonen (2008) stance on key stakeholder involvement is similar to Tropina (2014) view as he highlights how the problems that we are facing such as the transferring of illegal funds electronically are growing four fold. It is necessary for good traceability to be put in place in order to uncover potential criminal payments. In the areas of data protection and payment criminality, it is important to deal with the increasing electrification and globalisation of payments. As the internet is such an open area, e-crimes will continue to increase and it is vital that there is international cooperation between the main stakeholders. In such a fast moving market, regulations have to be clear and concise with central banks promoting consumer protection especially with the emergence of VCS in recent times, privacy protection and a high level risk assessment to avoid any fatalities to consumer personal funds.

In conclusion, having researched and analysed the various literatures addressed in this section of this thesis, it is evident to see that many authors have expressed their different views on non-cash payments and the security measures that surround this ever growing topic of discussion. For the purpose of this thesis which is focused on mainly the effects of cybercrime as Sweden is moving swiftly towards a cashless society, it is essential that measures are put into place in order to prevent fraudulent activity in this area.
3. Methodology

3.1 Aim

The methodology section aims to give the reader a description on how the thesis was developed. In order to obtain primary data, we adopted the method of conducting interviews. In regards to the different opinions and positions of our interviewees will be discussed later.

3.2 Research Paradigm

A research paradigm is a philosophical framework that guides the researchers how scientific research should be conducted. For the purpose of this thesis, the research paradigm that was used was an interpretivist approach which “rests on the assumption that social reality is in our minds and is subjective and multiple” (Collis & Hussey, 2009). Interpretivists adopt a range of methods whilst conducting research that ‘seek to describe, translate and otherwise come to terms with the meaning, not the frequency of certain more or less naturally occurring phenomena in the social world’ (Van Maanen, 1983).

3.3 Research Methods

There are a lot of methods for collecting primary data, including interviews, observation and questionnaires. Each method has its respective advantages and disadvantages. In order to achieve accurate and credible data from the respective interviews; we adopted a qualitative approach by conducting interviews and researching literature references to support our viewpoint in this thesis. Qualitative research is primarily exploratory research. The strength of qualitative research is its ability to provide complex textual descriptions of people experience on a given research issue (Mack, 2005). Qualitative research is also used to discover tendency in thought and opinions, and go deeper into the question (Mack, 2005).

3.4 Interviews

There are mainly four reasons that could explain why we chose the interview method to collect primary data (Kvale, 1996).

3.4.1 Direct feedback from respondent

Since there was a short time scale for our thesis, we devised a shortlist of potential companies in which interviews could be conducted in order to gain a deeper understanding of the topic and ultimately in doing so to answer our research question. In addition, we contacted companies that exchange bitcoin’s on the market and also we contacted various governmental bodies. Initially, emails were sent to the every company and governmental body on our list. Furthermore, often enough it was quite difficult to receive a response from the sent email. We then started making phone calls and also using professors from KTH as a networking tool in order to get in contact with people.
3.4.2 Opportunity to probe and explore
While the interviews were being conducted, we could get a more complete, better explained set of responses from interviewee’s by verbal or nonverbal expressions (Opdenakker, 2006).

3.4.3 Yields rich data, details and new insights
While the interviews were being conducted, it was essential that the interviewees could supply us with relevant information and knowledge in their field. The interviews are always conducted under a harmonious atmosphere, which may stimulate respondents enabling more primary data to be acquired.

3.4.4 Topics can be explored in depth
Prior to the interviews, we utilised our knowledge to brainstorm interview questions and then designed the final version of interview questions. Through this method, it was easier to focus on our objective and goal, in which further and deeper unintended ideas or themes raised by the respondents that relates to the thesis.

3.5 Interviewees
In order to achieve credible data, it was essential to choose the right interviewees. For our interview process, Sweden was chosen as our case study. Some interviewees were chosen based on initial contact via email and then we were referred to other interviewees as a result of our interviews e.g. snowball sampling (Collis & Hussey, 2009). Niklas Arvidsson, a researcher at KTH put us in contact with some of our interviewees. Some interviews were conducted via Skype due to the long distance. Prior to the interviews, we did not know any of the interviewees that we conducted interviews with.

During the interviews, several questions were asked but as the interviews progressed, the line of questioning pivoted as each interview sprung up new and relevant information. All interviewees were offered anonymity and the interviews were also recorded with the interviewees consent.

As some of our interviews were conducted with two persons, this may be deemed ineffective as the results could have been effected (Collis & Hussey, 2009). As the topic is a relatively new phenomenon, the answers that were received from some interviewees may have been given in a way that would not cause any harm to the organization that they reside. Taking this into account, no such scenario occurred and all interviewees were very clear and concise in their answering.
The sample of our interviewee’s professions includes:

- COO & Marketing Manager of a bitcoin exchange company.
- Financial Adviser at the Riksbank
- Experts in fraud & cybercrime at the Polisen
- PHD researcher in the field of cryptology and digital currencies.
- Public prosecutor of the Swedish Economic Crime Authority (SECA)

In addition, the main aim was to interview professionals and practitioners that have different backgrounds in order to gain a clear and unbiased set of data.

The list of interviews can be found in Appendix.

3.6 Literature references

The literature review refers to the reviewing of all secondary data sources that are relevant to a particular study (Collis & Hussey, 2009). Since the research question is a relatively sensitive topic. The first-hand data is quite limited and lacks credibility in certain cases. Literature references can be indirect methods to access our conclusion. We sought to investigate articles written by authors to see if there were any similarities in conjunction to what our interviewees said. To do this, the KTH online library resource and also google scholar’s search engine were utilised.

3.7 Development of Research Question

3.7.1- Principal research questions

At the beginning of the thesis, our research question was quite broad and wide. We then proceeded to specialise in the area of virtual currency transactions, especially bitcoin seeing as it’s the most popular VCS. Lastly, our research was focused in Sweden due to country becoming a pioneer towards a cashless society, and this trend will become more and more apparent in the future.

The principal research question that this thesis seeks to answer is:

*Do virtual currencies significantly facilitate unlawful financial transactions?*

In order to answer this question, it is broken down into a number of questions in the interview process, each of which will guide the data collection process. After collecting data and analyzing the results from the interviews, we summarized the interview conclusions and combined a large amount of literature references, enabling us to draw a conclusion.
3.7.2- Development of interview questions

When developing our interview questions, several questions were brainstormed and designed the final core questions for the interview. The interview results have strong connections with thesis and research question, which lead to our interviewees giving relevant answers. Below are some question samples

**Question 1 - Do you think virtual currencies like Bitcoin will be centralised in the future?**
VCS are disruptive innovations in the financial field, potentially having a profound impact on our society in the near future. Since VCS is a relatively new innovative idea for the majority of people, there are not many people familiar with virtual currencies at present. As more and more people are getting familiar and starting to use virtual currencies, the government or financial institutions may get involved in taking some actions to influencing virtual currencies, which may affect companies who are doing business by virtual currencies.

**Question 2 - Do you think the digital currencies are contributing to the UFT?**
This question directly relates to our core research question. We interviewed different people with various backgrounds by same question. Since our interviewees have different standpoints, we could understand each result better with their positions.

The full list of interview questions can be found in the appendix section.
3.7.3- Methods of analysing results

After the first-hand data was obtained from our interviewees, charts were created based on the data that was scribed from the interviews that were conducted. This process was done in order to help further analyse the data and give the reader a clear understanding of the data.

As seen above in Figure 2. The X-axis represents the interviewees and the Y-axis indicates the score. The score is judged from 1 to 5 and we define 1 is not likely and 5 is likely. From the graph, it is easier to analyse the opinion from each of our interviewee's and gain a better understanding of their views.

3.8 Ethics and Sustainability

There are many social ethical and sustainability issues that arose while the research was conducted. Our thesis is about the use of virtual currencies for the payment of UFT and in turn, these unlawful payments are enabling criminals to gain financially due to the vulnerability and clever use of such systems. Moreover, due to these unlawful payments in the shadow economy, it hinders Sweden’s economy as the entire unrecorded economic activity leads to negative growth for the economy and in turn reduces the sustainability in the near future. On the other hand, the social morale code of ethics is damaged due to these entrepreneurial groups of criminals engaging in criminal activities. The interviewees who were interviewed are working hard to combat these criminals from engaging in these crimes in the future in order for Sweden’s society and economy to have a sustainable future.
4. Findings

After an in-depth analysis of the various literatures that is associated with UFT from VCS coming from different ends of the spectrum, it was integral to present the findings and results that we have acquired. While a cashless society has its benefits, the literature suggests that there is an overriding feeling of pessimism within the field of cybercrime. Our main focus in this section is to critically analyse all the findings and results that we have gathered and researched from the multiple interviews we conducted and other sources to further prove that cybercrime is and will continue to have a damaging effect on Sweden’s economy as the country is striving towards becoming a cashless society. The results that were obtained are broken down into themes mainly emerging as a direct result from the interviews that were conducted. Throughout this section, the reader will be exposed to quotes and graphs based on the interviewee’s answers, in doing so gaining a deeper, clearer understanding of the topic. In the graphs, the x-axis represents the interviewees and the y-axis indicates the score. The score is judged from 1 to 5 and we define 1 is not likely and 5 is likely. It is easier to analyse the opinion from each of our interviewee’s and gain a better understanding of their views.

4.1 Unlawful Financial Transactions

Whilst conducting interviews, the main objective was to answer our research question that we developed. During the interviews, it was evident to see that each person had a different view and opinion on the questions that were place in front of them. In addition, this gave the results & findings are far greater in depth analysis from professionals working in the field related to our thesis.

“Do you think the virtual currencies are one of the key drivers in contributing to Illicit Financial Transactions?”

![Virtual currencies contributing to unlawful financial transactions](image-url)
As this interview question is related to our research question, it was interesting to get the views of experts and professionals working in the different fields. Whilst it is unclear to what extent VCS are contributing to UFT, there was a consensus from one of the interviewees that even though VCS transactions like bitcoin are anonymous, so is the physical cash notes that we use in everyday life.

“Not really, of course at the beginning people take advantage of a new technology and exploit it, real cash and gold is still the biggest drivers in contributing to the black economy UFT in my view”

According to J. Herlin-Ljunglof, CMO of BTCX bitcoin exchange, the way in which cash is transferred between people can be seen as anonymous as a note could have been used to buy illegal drugs or other unlawful activities and there is no way of knowing which person had the note and for what reason. A similar view was posed by J. Landstrom, a cybercrime expert at the Polisen who stated that “the more traditional payment methods are the most common options for illicit payments but we have seen bitcoin enter the arena in recent years”.

As previously stated in detail in the earlier sections, bitcoin’s platform enables the person’s identity to be anonymous when a transfer is made but that transfer can be viewed on the blockchain. If there is enough suspicion there are acts of fraudulent activity occurring amongst peers using bitcoin then the transaction can analysed to a certain extent and over time can find the culprit described in detail by K. Agelfors, Chief Operating Officer at BTCX.

“If a person does something to a high level of criminality using bitcoin they will find you like if you use an anonymous email – in the block chain, as long as they know the end part of the transaction, they can track it back, it takes time “.

As VCS are relatively new to the consumer payment market, it is difficult to say that they are one of the key drivers in contributing to unlawful financial activities but there have been a lot of cases where quite a large amount of bitcoins have been found on laptops seized due to acts of fraudulent activities as expressed by B. Segendorf, Riksbank.

Taking this into consideration, identifying the main actors when it comes to virtual currencies is important. One of our interviewees, J. Tibbling of the Swedish economic crime authority (SECA) outlined the three actors he believes are the key users of VCS. These actors are anarchists who use VCS due to the fact they want to abolish the way banks operate in society, investors and criminals. He continued to add that “we are talking to investors in relation to their investments with VCS and our question that we ask is the anonymity feature of VCS like bitcoin the reason for this to be a success”. Ultimately, his stance on the matter was that “You do not need
anonymity to accomplish this and the anonymity has really created the criminal market”.

4.1.1 Tax Evasion

One form of using bitcoin for UFT as previously discussed in the literature comes in the form of tax evasion. When asked was there a direct correlation between using a virtual currency like bitcoin for the simple purpose of evading tax, there were some interesting responses. It was stated that as bitcoin is easy to hide due to its anonymous feature, tax evasion does exist but to what extent is an answer that cannot be truly answered due to the lack of clarity of transactions in the blockchain. Early adopters, who spotted the gap in the market to invest in bitcoin’s when it started, have seen exponential growth in their bitcoin’s.

An interesting fact was shared on how people who initially invested have gained in wealth will not notify the authorities on how much profit they have made. If the time comes that they wish to withdraw their bitcoin’s to a fiat currency then the tax authorities will notice the withdrawal of funds and will take subsequent action. Taking this scenario into account, the point was made that as people who wish to withdraw these highly stocked bitcoin’s, will go down the route of using offshore accounts in order to avoid paying tax. It was stated that there are many people whose job is to make this transformation of virtual currency into a regulated fiat currency run smoothly and efficiently as possible in order to avoid the risk of getting caught.

4.1.2 Fraud

There are several clear disadvantages with VCS, and acts fraud is one of the most specialised areas for criminals. Since VCS have no third party interruptions and are anonymous, they are easily used by the people who seek to use it for acts of criminality. The allocation of responsibility between the payer and payee may be unclear if there any mishaps with the payment process.

From conducting the interviews, it was found that there are some incidents involving acts of fraud since the birth of VCS. We will introduce a scam method as described by J. Jogenfors called the ‘triangular scheme’, which resulted in a lot of people getting scammed. Below is a diagram describing a fraud process called the triangular scheme.
Firstly, the perpetrator contacts a bitcoin seller and states that he/she wants to purchase bitcoins.

Secondly, the perpetrator will advertise a product to be sold enticing a harmless victim to purchase the item. The perpetrator proceeds using fake personal credentials and ultimately cheats the victim selling this fake product e.g. the perpetrator pretends to sell a new iPhone and victim transfers the money to the bank account.

Lastly, after the victim transfers money into what he/she perceives to be perpetrators bank account, it is transferred into the bitcoin seller’s bank account. Through this, the perpetrator receives the bitcoin transaction as the bitcoin seller has been paid.

In this process, the perpetrator actions are extremely difficult to catch by law enforcements as it is difficult to link the Bitcoin to individuals in practice given its anonymity feature.

From conducting the interviews, we know that bitcoin transactions are not completely anonymous. It is possible to identify the transaction through the history and records on the blockchain. However, it is very difficult to link the wallet to individual users, which means that the transaction is in practice anonymous. This quality can make bitcoin attractive for use in criminal transactions and money laundering (Segendorf, 2014)

4.2 Implementation of Regulations

In any scenario, when a new technology enters the market it is suspect to regulation by governmental bodies. During the interview process, it was essential to gain a deeper understanding on the opinions of the interviewees in relation to governmental regulations in terms of combating UFT in the virtual environment. It was stated during one of the interviews that bitcoin is relatively new when it comes to regulation and is in the infant stage.
“It’s too new for now in relation what to do with regulation but regulation will certainly happen in the near future”

A scenario was depicted by J. Herlin-Ljunglof of BTCX bitcoin Exchange; he suggested that even though bitcoin’s anonymity is essential for many illegal activities, it cannot be discarded in terms of all the other aspects of payment methods available to people that is illegal already. He begins to explain how if a person uses bitcoin for acts of fraudulent activities that Bitcoin is legal and is the same as using other forms of payment e.g. cash.

“No matter what asset a person’s uses to commit a crime in the form of payment, oh you did it with bitcoin, well it is legal”

Another interesting difference that J. Jogenfors, a PHD researcher in Linkoping University outlined how regulation for VCS is fast approaching as we are starting to see an increase in unlawful payments in the narcotic’s area and also in acts of fraud.

“I think we are certainly starting to see an increase in illicit payments with VCS in terms of fraud from what I have been talking to people in the law enforcement here in Linkoping”

In the near future, it will be necessary for “the implementation of better governmental regulations” when it comes to combating the problem of using VCS for UFT as expressed by J. Jogenfors. He illustrated how Swedish law enforcements are working hard on getting back on track with bitcoin in investigating its use for unlawful activities as they have been lacking in knowledge and the technological knowhow on how to deal with the problem. Furthermore, a similar argument was proposed by the European central bank in their virtual currency report. In this report, it states that
“users are exposed to losses resulting from fraud organised by such actors”. By using a virtual currency for the payment of goods and services, consumers are not subject to the same level of protection as they would be if they used a normal regulated fiat currency and are not entitled to any refund rights for transfers in a traditional payment account, as stated in the EU law. Moreover, the report highlights a scenario that occurred with the default of the exchange Mt. Gox in February 2014 resulting in 19’000 bitcoins stolen from wallets of its users with a value of €342’000 million (ECB, 2015). Nonetheless, there are no governmental regulations put in place in order to combat these scenarios from happening again in the near future as previously stated by the interviewees.

In addition, B. Segendorf of the Sveirge Riksbank expressed how there is a need for governmental intervention when it comes to regulating VCS due to the many grey areas surrounding it.

“The only reasonable approach is think is to try bringing these non-traditional payment methods within the standardised legal framework so that you will have a level playing field between the various different types of payment services”

Similar too many of the other interviewees, J. Tibbling of the SECA stance on regulation stems back to the point on “regulations may as well not be in existence unless you have control of who is behind the virtual wallet”. A person who purchases bitcoins with a fiat currency is subject to anti-money laundering regulation which was entered into force in 2009 by the Swedish government and will in turn be investigated. Furthermore, he continued to explain how the tax authorities in Sweden were curious if certain bitcoin exchange companies actually paid taxes or reported everything honestly at the end of the tax year. Through this, the tax authority wanted to acquire the identities of the user’s wallet but this type of information cannot be obtained as it is disclosed.

Furthermore, the implementation of regulation in the area of VCS is likely to grow due to various anti-money laundering schemes. As discussed by J. Landstrom, he explained that it is quite difficult to retain a good degree of cash flow with non-traditional payment methods especially with cryptocurrencies. “You need a big backing of fiat money, transferring virtual currency into fiat currency and that’s a major bottleneck”. It was suggested that it’s a lot more of a complexed task to launder large sums of money using VCS; it is a lot easier to get away with smaller amounts. In addition, whilst we haven’t seen many scenarios of this happening today, “in the future I’m sure we will see cases” as expressed by J. Landstrom.
4.2.1 Centralisation of Virtual Currencies

Centralized VCS are defined as one that has a “centralized repository”, which is similar to a central bank or a “central administrator”

Compared to centralised VCS, a decentralized currency was defined by the US Department of Treasury as a “currency that has no central repository and no single administrator, and that persons may obtain by their own computing or manufacturing effort.” A centralised has an institution or authority that could record and control the currency system. On the other hand, the decentralised virtual currency is based by the computer algorithm and mathematic. There is no central authority regulation in the decentralised currency.

During our research, bitcoin was chosen as a case study due to its popularity. From figure 5, it is clear to see that the opinion of whether or not bitcoin will be centralised in the near future is quite divided between the various interviewees. Although our interviewees gave different answers about bitcoin whether or not it will be centralized in the future, they have their opinions and concerns respectively.

![Figure 6 Centralisation](image)

B. Segendorf of the Riksbank, expressed his view on how he thinks VCS will be centralised in the future, if people are willing to put more money into VCS then it is necessary to know who is responsible for the blockchain and ultimately where the money is being kept.

“You want that to be under supervision perhaps even if it is run by a bank and is classified as some kind of account”

He continues to add that the area of centralisation becomes more and more valuable for companies and households and “it must become something of a financial sector”. 
If a company accepts VCS as a form of payment then it must be linked with a bank account and then if you get a lot of trouble with anti-money laundering requirements it won’t really work.

“Somehow virtual currencies must be issued and ultimately handled by supervision entities”

BTCX outlined that as the EU are analysing VCS deeper and deeper, organizations, nations, countries, may not centralize Bitcoin, however, they could centralize their own digital currency, for example Swedish banks could centralize their own digital currency any time any place. The findings from our interviews also suggests that VCS will live on decentralized for the most part, but there will be more regulations are published in the future. They will study and watch on VCS transactions carefully said by Bra.

4.3 Adoption Rate of Bitcoin

One area we intended on exploring whilst conducting the interviews was the future of bitcoin in Sweden in order to give the reader a clear, concise and vivid picture on the current state of play of the virtual currency. Bitcoin is a rapidly growing currency here in Sweden. As it is a relatively new Phenomomen, the rate of adoption amongst the people of Sweden has vastly increased over the past couple of years. As described by K. Agelfors, COO, of BTCX Bitcoin exchange, the future of bitcoin in Sweden is “bright, really bright”, the company itself is expanding rapidly as they have seen an increase in their customer base since they started 4 years ago. It was also highlighted that initially, authorities and banks fought them but now a days the relationship has blossomed into a cooperative one.

As we see more and more companies and vendors in Sweden accepting bitcoin as a form of payment, this will in turn lead to an air of legitimacy that surrounds the virtual currency as it is still viewed as a relatively new Phenomomen. As the virtual currency
is slowly getting accepted, the fact that has to be taken into consideration is that in a
country like Sweden that has a very efficient banking infrastructural system; there
may be no need for an alternative in the day to day life for payment methods for the
population as described by J. Jogenfors, a PHD candidate in Linkoping University. It
was also suggested that bitcoin may have a real future with a high adoption rate in
countries that do not have the privilege of such an efficient banking system like
Sweden. In addition, a study performed by the European central bank which
analysed the amount of daily virtual currency payments compared with non-cash
payments. The studies result showed 69'000 VCS payments compared to 274
million non-cash payments within the EU (ECB, 2015). As the number of VCS
payments are increasing it directly coincides with the interviewee’s opinion on how
VCS are gaining in popularity.

On the other hand, another interesting difference that one of our interviewee’s spoke
on the future about of bitcoin was a pessimistic view primarily due to the fact that it is
not regulated and it is not brought into the same sphere as other the other payment
services. As expressed by B. Segendorf, if this implementation of regulation fails to
materialise then in his view “VCS occupy small niche markets”. He depicted such a
scenario of bitcoin meeting the needs of a niche market e.g. sending a payment to a
person in Africa. He continued on to explain how it is very difficult for innovative
companies that want to sell their services based on bitcoin to open a bank account
because of “anti-money laundering regulation”.

5. Discussion

The main focus of this thesis was to analyse if there was a direct correlation between the use VCS for engaging in UFT and if so to what extent. Having conducted several interviews with the objective of answering our research question, there was an overriding split opinion on the topic with each interview conjuring up new and relevant information. Whilst there was a divided opinion on some aspects of our interview questions, it was clear to see from our interviewee’s answers that the use of virtual currencies for UFT is growing. This section aims to explore the answers that we have obtained from our interviews and to see if it agrees with our research question and the literature.

As previously stated, our research question that we have aimed to answer is:

“Do virtual currencies significantly facilitate unlawful financial transactions?”

The results that were obtained fluctuated with our interviewees as they conjured up some interesting views on the matter. As suggested by a few our interviewee’s, the more traditional payment methods like cash and gold are still the most predominant ways of encouraging UFT for money laundering etc. To what extent decentralised VCS are contributing to UFT is unclear due to the anonymity of bitcoin but it was clear to see from our interviewee’s results that there was an overriding feeling that VCS are becoming more and more popular with adoption rates increasing amongst the population. That being said, this result differs from the ECB’s report which was previously stated in the literature review whereby it was suggested that VCS like bitcoin have a low acceptance rate.

The use of VCS for unlawful activities will likely to grow in the future with groups of entrepreneurial cyber criminal’s likely gain from these activities. The different opinions by our interviewee’s on whether or not they perceive virtual currencies are one of the key drivers in contributing to UFT can be seen in the previous section in figure 1.

UFT can come in many different forms. For the purpose of this thesis, we decided to take a deeper look into individuals using virtual currencies for the sole purpose of fraud, money laundering and tax evasion. The results that we obtained from our interviewee’s when asked, varied maybe due to the fact that they had different professional backgrounds and motives. One significant pattern that can be seen through the results was that tax evasion doesn’t seem to be one of the key drivers in contributing to UFT; this can be identified with our interview with the Polisen and BTCX Bitcoin Exchange. This is a direct contradiction in terms of what the literature poses as Marian (2013) highlights the point that such cryptocurrencies like bitcoin have the required characteristics to be a tax haven as they are not dependant on financial institutions and taking into account the anonymity feature of the cryptocurrency. Furthermore, as there is a sense that tax evasion doesn’t occur to the extreme extent as compared to more traditional methods due to the fact that
some perceive that VCS do not have the same capacity to withstand such large quantities of money laundering as discussed in the financial action task force report (FATF, 2015).

In addition, despite this it can be suggested that in the future more and more people who wish to evade paying tax will use virtual currencies as they have the required characteristics to be a tax haven. Also, it has to be taken into consideration that money laundering and tax evasion schemes with traditional payment methods have been in existence a lot longer than the infant virtual payment methods and it is a relatively new way of conducting these types of unlawful activities for criminal. There is a consensus amongst the interviewee’s that unlawful payments in conjunction with virtual currencies will continue to grow in the near future.

The whole area surrounding VCS and whether or not decentralisation is the correct procedure to take in the future by implementing new regulations from governmental bodies in order to combat the problem of UFT is somewhat of a pessimistic view as discussed by some of the interviewee’s. There was an overriding feeling amongst the majority of the interviewee’s that VCS like bitcoin will not be centralised due to the fact that taking the nature of the VCS platform, they are built and designed in order to be decentralised so it would take an extraordinary amount of hardware to centralise the system.

As these VCS are based primarily on their anonymity feature, it has to be taken into consideration by centralising such a system could almost take away the novelty of what it originally was built for. On the other hand, if centralisation was implemented a legal entity could be possibly be created that could ultimately be responsible for the governance of the VCS allowing it to be regulated and in turn enabling the VCS to be fully integrated with the other regulated financial services currently available on the market (ECB, 2015). In addition, the main role this legal entity would play would be to ensure a high level of integrity is maintained for the newly converted centralised system. Furthermore, the newly appointed legal entity would in turn be obliged to comply with the regulation and ensure the correct level of supervision in order to reduce the risks associated with VCS. Initially, appointing a legal entity to oversee the governance may portray a sense of animosity as VCS are a decentralised system that does not require any central bank. Be that as it may, the creation of this legal entity does not imply that VCS have to be centralised. It can remain decentralised and can be processed through a transaction ledger e.g. blockchain. This coincides with what Tropina (2014) outlined when it was stated that the private sector must become involved and conjure up possible techniques that can be successfully implemented to prevent further UFT.

As previously discussed in the literature review, Anderson (2012) stated how it is wrong to reject the advancements in innovation if even it leads to an increase in fraudulent activity in the cyber world. In addition, by introducing more effective governmental regulations it could potentially lead to a more efficient and well
monitored financial system. This coincides with the results that were obtained during the interviews that we conducted. As described by Jan Tibbling, “we are not like China, you can’t just abolish these virtual currencies if needs be”. Taking this into account, a distinct pattern that emerged from our interviewee’s was there was an overriding opinion that banks are looking into developing their own digital currency in the near future as a direct response due to the ever increasing popularity and competition of bitcoin. Most recently, Bank of England have launched plans to develop and implement their own virtual currency called RSCoin and will also function on the blockchain (Varshney, 2016). As we see more and more financial institutions trying to implement and replicate the blockchain technology, it has to be pointed out that as these new potential cryptocurrencies are centralised that there is still a sense of hesitation as to the increased level of corruption that many believe would be connected to a private system (Varshney, 2016). As we see this shift towards banks devising their own digital currency, it leads us to think that the only reasonable approach is to try bring these non-traditional methods within the standardised legal framework so that there will be a level playing field amongst the various different types of payment systems that currently exist.

5.1 An Increase in Fraudulent Activity

As there is not a multitude of evidence to show that bitcoin facilitates UFT, there are clear tendencies that scam and fraudulent activities with the aid of bitcoin are increasing in these years and near future. The feedback we received from of our interviewees highlights there a clear consensus that it will occur.

In this section, an analysis is devised into the two main types of acts of fraud and these are classified into the investor perspective and user perspective.

5.1.1 Ponzi Scheme

Latest technology always entices new investors to enter the newly developed market due to the promise of large revenue payback. Bitcoin is a pioneer innovation in financial field that has attracted many investors. As a result, an investment scam called the ‘Ponzi Scheme’ is be used by investors. Ponzi scheme is an investment scam that involves the payment of factitious returns to existing investors from funds that are ultimately contributed by new investors (SEC, 2015). In many Ponzi schemes, the criminals who engage in such a scam main focus is attracting new large sums of money to make promised payments to the early adopters of the scheme as well as financially gaining from these invest funds for personal use (SEC, 2015). In recent times, VCS have become one of the key methods of implementing such a scheme due to the anonymity feature that VCS like bitcoin has. This attracts fraudsters as there are less regulatory measures implemented than normal fiat currencies as previously discussed.
5.1.2 Bitcoin Transaction Scam

There are many examples that describe this scenario e.g. phishing scams, exchange scams etc. Emails and advertisements are crucial tools for informing people that victims have been awarded bitcoins. When users access the link and log into their own bitcoin wallets or bank wallets, this enables the fraudsters to record the person’s credentials and controls the account. Moreover, there are some fraudulent bitcoin exchanges that attract victims to exchange bitcoins by offering a more competitive rate. When victims complete the payment, the fraudulent bitcoin exchanges do not transfer any bitcoin that was purchased. Further, as we have mentioned previous in the findings, the ‘triangular scheme’ is also a typical method in the scams.

Avoiding bitcoin scams is essential and creating awareness is vital to preventing further mishaps. The three most dominate ways to prevent such scams from happening are creating transparency, implementing regulation and also changing to the correct mind. Most victims are scammed due to their speculative mind-set. The mind-set of these individuals is profit driven and they fail to see the risk that is embroiled with engaging in such an activity. Moreover, checking to see that the bitcoin company has been auditioned publicly is essential that cannot be taken lightly. It is vital to check the company’s credentials and never leak private information via emails as they are useful measures for avoiding being scammed. Lastly, the financial institutions and authorities also have important roles to play. With the development of VCS, people are more and more familiar with it and VCS will be widely used in many fields. More and more regulations should be implemented in the near future to prevent further incidents from occurring. Regulations are not always bad but by implementing regulations the VCS have the potential to develop into a fruitful and successful platform.
5.2 The Future of Bitcoin in Sweden

From the graph shown above, the opinion of each organization represents various views respectively. BTCX Bitcoin Exchange believes the future of bitcoin is bright, on the contrary, Riksbank and SECA are not as optimistic. Our other interviewees have a neutral opinion. In our opinion, we believe future of bitcoin in Sweden is one that is unclear but currently it’s gaining in popularity in recent years.

Through our analysis and findings, VCS transactions are increasing in comparison with the traditional payment methods. However, the road to be accepted by public has the potential to grow as Sweden is on the path to becoming on the first cashless society. As mentioned above, there are some shortcomings existing currently, such as scams, no buyer protection, bitcoin capacity (in comparison to card payment) and so on. Furthermore, for the safeguard of using bitcoin for consumers in the future, it is vital for the cooperation between law enforcement agencies all over the world but we have to work together with the financial industry to find a way that so this extremely valuable invention could fulfil its real potential because currently it is more or less hijacked by criminals which means that it will not fulfil its real possible potential. Discussions with serious financial actors is integral for the process as regulation can do something but it is necessary to cooperate with the involved to actors to find a viable solution.
6. Conclusion

In conclusion, from our results and findings it is suggested that virtual currencies do not significantly facilitate unlawful financial transactions, while the more traditional payment methods e.g. cash and gold are still the more preferred ways of engaging in UFT. The adoption rates of VCS are increasing and in turn could potentially result in a vast increase in acts of criminality in the cyber environment in the near future. The benefits of virtual currencies are plentiful and consumer adoption rates are seemingly ever increasing. With this big shift from tangible money to a digitalised payment infrastructure, there are inherent dangers that haven’t shared the same exposure as their positive counterparts.

The main focus of this thesis was not to state the obvious and suggest that as digital payments through VCS become more common, cybercrime is sure to follow. This is a reasonable assumption to make and one we have given validity to in this paper.

While crime in general has steadily declined over the past decade in Sweden, cybercrime has more than doubled. And while a certain influx of cybercrime is to be expected as Sweden stays on progress to become the world’s first cashless society.

Cybercrime is unlike traditional crime in the sense that the perpetrator can be sitting at his desk or by a beach in the Bahamas drinking a cocktail. Police are no longer combating criminals on the street. They could be fighting an enemy 1000 miles away and not even know it. As cashless infrastructures and payment systems continue to increase in popularity, so will sophisticated cybercrime. The cashless society appears to be upon us in Sweden whether we like it or not.

Some merchants don’t even accept cash anymore. The individual is forced to put their trust in technology that appears safe today but tomorrow may not be. Larger effort needs to be taken by governing bodies to combat the serious likelihood of a sharp increase in the use of VCS for UFT. Failure to do so would be reckless and grievous.

6.1 Limitations: Due to the limited time constraints, lack of prior knowledge and minimal network in this field, the data we have relied on for this thesis has been first hand interviews and secondary data. The data that was collected was by interviews which coincided with official government reports, research articles and journals and compiled it through our qualitative research methods before cataloguing our results in the findings section. With a wider scope in time and resources, it would be interesting to conduct interviews with a lot more governmental officials across the globe and compare the results that were obtained from this thesis.

Seeing as our research question was based around the concept of decentralised payments incorporated with the shadow economy which is defined as all the
unregistered economic activities that contribute to the officially calculated gross national product UFT can come in many different forms (Schneider, 2012). Furthermore, a lot of data and indeed methods were kept confidential. As with any paper written on crime it is difficult to find interviewees currently embroiled in the field willing to discuss it openly on their previous convictions. As a result we relied on data from our interviewee’s and past public cases for some of our analysis.
7. Potential Areas for Further Research

One possible area for further research is looking at this research question in the context of developing countries. Africa, India and Brazil have all declared interest to in taking strides towards implementing a cashless society. It would be an interesting topic of research to establish whether our findings are consistent or effected when tested in different countries (Especially developing countries). One could discover if possessing different payment infrastructures and alternative security practices would contribute to cybercrime in a more radical sense and compare it against that of a country like Sweden who has already taken massive strides to becoming cashless.

Other areas of possible research include looking into how best governments can collude and collaborate together in an effective manner to diminish the growing threat of Cybercrime with VCS. Crime is no longer being bound by national borders. It has expanded via the advances in technology to be an international issue and must be tackled accordingly. The advancement in innovative consumer payment services brings a grey area in law along with it. Much of the current legislation in countries currently was not created to be adequately being able to deal with cybercrime. The necessity to amend national laws and legislation due to a cashless economy is another fascinating area for possible future research.
References:


Akinola, Olalekan S. "Cashless Society, Problems and Prospects, Data Mining Research Potentials."


ECB, 2015. Virtual currency schemes - a further analysis,


Kim, V., 2014. Dutch National Pleads Guilty to Running Online Marketplace for Drugs, s.l.: Los Angeles Times


Kvale, S, 1996. An Introduction to qualitative research interviewing


Oxforddictionaries.com. (2016). cybercrime - definition of cybercrime in English from the Oxford dictionary. [online] Available at:


Tropina, T., 2014. *Fighting money laundering in the age of online banking, VCS and internet gambling*. pp. Pg1-16


### Appendices

#### Appendix A: List of Interviews

<table>
<thead>
<tr>
<th>Name(s)</th>
<th>Title(s)</th>
<th>Organisation</th>
</tr>
</thead>
<tbody>
<tr>
<td>Joakim Herlin (1) &amp; Kristofer Agelfors (2)</td>
<td>CMO (1) COO (2)</td>
<td>BTCX Bitcoin Exchange</td>
</tr>
<tr>
<td>Jonathan Jogenfors</td>
<td>PHD Candidate</td>
<td>Linkoping University</td>
</tr>
<tr>
<td>Lars Korsell</td>
<td>Researcher</td>
<td>Crime Prevention Council (Bra)</td>
</tr>
<tr>
<td>Bjorn Segendorf</td>
<td>Financial Adviser</td>
<td>The Riksbank</td>
</tr>
<tr>
<td>Jan Tibbling</td>
<td>Public Prosecutor</td>
<td>The Swedish Economic Crime Authority (SECA)</td>
</tr>
<tr>
<td>Jan Olsson (1) &amp; Johan Landstrom (2)</td>
<td>Fraud Investigator (1) Cybercrime Expert (2)</td>
<td>Polisen</td>
</tr>
</tbody>
</table>
Appendix B: General Interview Guide

1. Do you think virtual currencies will be centralized in the future?
2. Do you think the virtual currencies like bitcoin are one of the key drivers in the contributing to illicit financial activities?
3. What role do you see institutions like authorities and banks in Sweden play in relation to non-traditional payment methods?
4. What role do you see regulations play for non-traditional payment methods in relation to financial crime?
5. In your opinion, what measures should be put in place in order to combat the problem of illicit financial activities using virtual currencies?
6. Do you think virtual currencies are used as a disguise in order to avoid paying taxes?
7. What’s your opinion about the future of bitcoin in Sweden?