Virtual currency and its pseudonymous users: A decentralised system beyond the control of authorities?

Candidate number: 8012.
Submission deadline: 1st of December 2017
Number of words: 17.997.
Table of contents

1 INTRODUCTION.................................................................................................................. 1
  1.1 Topicality and aim of the thesis ..................................................................................... 1
  1.2 Outline ......................................................................................................................... 3

2 MONEY ............................................................................................................................... 4
  2.1 Introduction .................................................................................................................. 4
  2.2 Function of money ....................................................................................................... 4
  2.3 Types of money ........................................................................................................... 5
    2.3.1 Commodity money ................................................................................................. 5
    2.3.2 Commodity-backed money .................................................................................. 5
    2.3.3 Fiat money ............................................................................................................. 5
    2.3.4 Bank deposits ........................................................................................................ 6
    2.3.5 Credit money ......................................................................................................... 6
    2.3.6 Electronic money .................................................................................................... 7
    2.3.7 Virtual currency ..................................................................................................... 7
    2.3.8 Virtual currency issued by central bank ............................................................... 8
  2.4 Payment methods ....................................................................................................... 9
  2.5 Monetary policy and the role of a central bank ......................................................... 9

3 VIRTUAL CURRENCY ........................................................................................................... 13
  3.1 Introduction ................................................................................................................ 13
  3.2 Types of virtual currency ........................................................................................... 13
    3.2.1 Closed virtual currency schemes .......................................................................... 13
    3.2.2 Virtual currency schemes with unidirectional flow ............................................. 14
    3.2.3 Virtual currency schemes with bidirectional flow ............................................. 14
  3.3 History of virtual currency ........................................................................................ 14
  3.4 How to acquire virtual currency ................................................................................ 16
    3.4.1 Mining .................................................................................................................. 16
    3.4.2 Exchange services ................................................................................................. 17
  3.5 Blockchain .................................................................................................................. 19
    3.5.1 Distributed ledger ................................................................................................. 19
    3.5.2 Open or closed networks ....................................................................................... 20
    3.5.3 Encryption ........................................................................................................... 20
    3.5.4 Alternative use of technology ............................................................................. 20
  3.6 System efficiency ....................................................................................................... 21
    3.6.1 Scalability ............................................................................................................. 21
1 Introduction
1.1 Topicality and aim of the thesis

Virtual currency, and especially bitcoin, is all over the news. Some say it is a fad and a bubble. Some say it is revolutionary and will change the world just as much - or perhaps even more - than the introduction of the internet. Part of the attraction seems to be the opportunity to be part of something innovative. Another strong incentive is that, just as under the Dot-com bubble, the increasing market makes it a good opportunity to earn money. At least for those earliest to the party.

The day I start writing this thesis the latest news is that the price of bitcoin is down as much as 19%, this from an all-time high achieved just five days ago. A few days earlier a report from the Danish consultancy firm CPH Revision reached the headlines, predicting that bitcoin will be the world’s most valuable currency within just 12 years. What is certain is that there is a lot of money in virtual currency, and we have seen extreme fluctuations in value.

Nevertheless, so far these fluctuations have been a race for the top. The cost of one bitcoin was USD 0.06 in 2010. The value of one single bitcoin passed the USD 100 mark in 2013, and it passed USD 1,000 at the start of 2017. Today one bitcoin will cost you somewhere around USD 10,000 if you want to buy in.

The extensive media coverage combined with huge increase in price, has undoubtedly resulted in more people investing in virtual currency. According to representatives from the traditional financial market in Norway, the evolution of bitcoin is not only a threat to their own business, but also a threat to the welfare state. In their opinion, virtual currency makes it easier to risk-free avoid taxes, avoid value added tax, and take part in corruption.

---

1 As an example, this moment six out of totally about sixty features on the front page of E24.no, Norway’s largest online newspaper covering economics and business, covers the theme of virtual currency. Website accessed on the 2nd of October 2017.
2 As bitcoin is both a system and a currency, lowercase (bitcoin) will be used throughout the thesis referring to both the currency and the system. Some virtual currencies have different names for the system and the currency, e.g. ether (lowercase) is the currency of the system Ethereum (capitalised).
3 According to JPMorgan CEO Jamie Dimon “Bitcoin is a fraud [...] It’s just not a real thing, eventually it will be closed.” He continued: “It’s worse than tulip bulbs. It won’t end well. Someone is going to get killed.” See Imbert (2017).
4 A more optimistic voice is Stephan Nilsson, founder of Norwegian Bitcoin Foundation, who claims that we are dealing with “one of humanity’s greatest inventions. Larger than the internet.” See Christensen (2017).
5 Kharpal (2017).
7 Coindesk (2017).
8 Staavi & Gjemdal (2017).
An important factor for the growth of virtual currency is that it has been labelled as anonymous. A string of letters and numbers is used to conceal the real world identity of a user of virtual currency. This creates a pseudonymous identity. To conceal identity when trading or storing money is attractive to diverse groups. Liberals and anarchists for political reasons. Technology enthusiasts for idealistic and professional reasons. Criminals when trading illegal items. Investors when trying to avoid tax or to hide secrets from competitors.9

Another key factor is that the decentralised nature of virtual currency makes it difficult to regulate. Authorities cannot impose effective limitations on whom you trade virtual currency with, when you trade, or how much you trade for. With traditional currency a central authority can change the interest rate in an attempt to stabilise inflation and stimulate output and employment.10 Such changes to monetary policies will not necessarily have impact on the value of virtual currencies. No central bank can print more of a virtual currency such as bitcoin.

The topic of this thesis is the regulation of virtual currency, and furthermore what authorities actually have in their toolbox when trying to impose regulations. The decentralised nature of virtual currency challenges the existing economic system in several ways. Authorities could choose to ban trading with virtual currency in its entirety. This will not be investigated any further in this thesis, as few countries have chosen to do so.11 Given that virtual currencies are legal, three perspectives stand out as especially interesting; monetary policy, tax regulations, and anti-money laundering and terror financing.

First, if virtual currency continues to grow at such a fast rate, it will sooner or later impact the central bank’s ability to run an efficient monetary policy. Second, to calculate correct tax the tax authorities are in need of information on the tax subject’s income and wealth, as reported by both owners and third parties. This brings forward the question of who is the third party and what are the owners’ incentive to report correctly. Third, virtual currency has been tied to white-collar crimes, and there are fears that it can be used for terror financing. It is difficult for the police to gain insight when investigating such crimes.

This thesis is written from a broad point of view. The focus is on what virtual currencies have in common. There is nevertheless one single virtual currency that both came first and is significantly bigger than the others; bitcoin. Bitcoin is built on an open source technology called blockchain. It is the benchmark for most – if not all – of the virtual currencies that have fol-

ollowed in its trail. As there are hundreds of virtual currencies, it cannot be ruled out that some of the newcomers have characteristics that differs from bitcoin also in some important areas. I have nevertheless opted to write about virtual currency in general, and not bitcoin in particular.

Virtual currency is of its nature an international subject. Nevertheless, the thesis has a Norwegian perspective. The Norwegian perspective is especially visible in the chapters on tax, given that tax is largely a national issue. Some foreign legislation and examples are used throughout this thesis, mainly from the EU and the US. The chapter on money laundering and terror financing is internationally oriented, as this is an area where cross-border cooperation is vital.

This thesis is updated with news and developments up until 28th of November 2017.

1.2 Outline
Chapter 2 concerns what money actually is, the role of the central bank as a regulator, and the impact the growth of virtual currency might have on monetary policy. Chapter 3 investigates what virtual currency is, how it works, and what the innovative blockchain technology can be used for. Chapter 4 discusses the challenges, and possibilities, that the anonymity of virtual currency raises. Chapters 5 deals with tax liability, and chapter 6 with reporting requirements related to tax. Chapter 7 covers regulation and reporting requirements in relation to money laundring and terror financing. Chapter 8 concludes the thesis.

---

2 Money

2.1 Introduction
Defining what virtual currency is has proven to be difficult. It does not quite fit with any of the existing terms we have for money, currencies, bonds, or other financial instruments. The legal definition of virtual currency was part of the subject in Skattverket v. David Hedqvist, a case for the European Court of Justice in 2015. In the Hedqvist case virtual currency was defined as "a type of unregulated, digital money".13 This must be said to be a rather imprecise definition. Transactions with regular money are exempt for VAT according to Article 135 of the VAT Directive. According to the Hedqvist judgment virtual currency should be treated as the like, at least in relation to VAT.14 If virtual currency is supposed to be treated as money, a starting point will be to look at what money actually is. Compared to traditional money the decentralised nature of virtual currency raises some new issues, especially in regard to regulation.

This chapter will look at the types of money we have had up until now, what kind of traditional money bears the closest resemblance to virtual currency, and how money has traditionally been regulated.

2.2 Function of money
According to economic theory, three main functions must be fulfilled for something to be regarded as money. It must be able to serve as unit of account, as means of payment, and as store of value.15 Money functions as a practical means of assigning value to goods and services and settling trades, while currency gives money visible form.16 How does this fit with virtual currency?

It is possible to read and count an electronic wallet containing virtual currency, the same way as a traditional account in a bank. Virtual currency has a market cap.17 Payments can be made with virtual currency, albeit not necessarily in your local store. The number of businesses that accepts virtual currency is still limited, but a similar problem will occur if you bring anything but a country’s legal tender to the register. US dollars is still money even though you cannot use them when making a payment in most supermarkets in Norway. The fluctuating value of

---

13 Skattverket v. Hedqvist, para 12.
14 VAT is not part of the EEA Agreement, thus the VAT Directive is not applicable in Norway. After a lengthy period of assessment, the Ministry of Finance concluded that the Hedqvist judgment would have effect also on Norwegian VAT regulations. See Lande & Sollie (2017).
17 A list of the current value of many virtual currencies can be found on the webpage coinmarketcap.com.
virtual currency makes it a quite risky store of value, but nonetheless virtual currency obviously serves as a kind of money given these terms.\textsuperscript{18} \textsuperscript{19} The question is what kind of money it is.

\section*{2.3 Types of money}

\subsection*{2.3.1 Commodity money}

It is difficult to point out when the transition from a strictly barter-based economy to a monetary society occurred. Throughout history several objects have filled the function of today’s money. Objects such as gold, shells and beads can serve as examples.\textsuperscript{20} This form of money is called commodity money, i.e. objects that had intrinsic value. These rare objects had to be found, collected, and at times undergo a certain processing. The fact that the objects were rare was part of what gave them value, which again made it difficult for any authority to influence the value of the object.

\subsection*{2.3.2 Commodity-backed money}

Pure commodity money later evolved into commodity-backed (or representative) money.\textsuperscript{21} Paper representing the underlying commodity could be exchanged for a fixed quantity of the underlying commodity, usually gold or silver certificates. The face value was greater than its value as material substance. This had the advantage that it opened for transferral of larger amounts of money.\textsuperscript{22}

\subsection*{2.3.3 Fiat money}

Modern economy is largely based on fiat money. Fiat money has similarities to commodity-backed money, but with an exception that fiat money cannot be redeemed for a commodity.\textsuperscript{23} \textsuperscript{24} What gives fiat money its value is that it is legal tender issued by a central authority. Legal tender means that it is unlawful not to accept the fiat currency as means of payment for all kinds of debt, both public and private.\textsuperscript{25} Each national state administers a money monopoly on their territory, usually allowing for one certain currency as a legal tender.\textsuperscript{26} \textsuperscript{27} For fiat money,

\begin{itemize}
\item \textsuperscript{18} A Financial Action Task Force (FATF) report supports the idea that virtual currency falls under the traditional scope of money. See FATF (2014), p. 4.
\item \textsuperscript{19} Internal Revenue Service (IRS) have concluded that “\textit{virtual currency is a digital representation of value that functions as a medium of exchange, a unit of account, and/or a store of value}”. See IRS (2014), p. 1.
\item \textsuperscript{20} Mehholm (2017), p. 17.
\item \textsuperscript{21} European Central Bank (2012), p. 9.
\item \textsuperscript{22} Ibid.
\item \textsuperscript{23} Ibid.
\item \textsuperscript{24} Fiat in latin means “let it be done”.
\item \textsuperscript{25} Sentralbankloven, § 14.
\item \textsuperscript{26} Christiansen (1987), p. 166.
\end{itemize}
trust in the central authority is key to why people are willing to exchange goods and services for a piece of paper. Trust in fiat currency relies on faith that a government will repay its debts. Fiat money consist of cash, issued as coins or banknotes, and the banks’ deposits in the central bank.28

2.3.4 Bank deposits
Bank (or demand) deposits are claims against financial institutions, stemming for money placed into banking institutions. These claims can be used to buy goods and services. Bank deposit withdrawals can be performed in person, via checks or bank drafts, using ATMs, or through online banking. Bank deposits are not legal tender, but are widely used and usually accepted as payment.29 In today’s society most of us keep the main part of our savings in a bank account, not as notes in our wallets. Furthermore, we access our accounts digitally. Digital money in your bank account is typically regarded as the same currency, and has the same value, as physical money issued as coins or banknotes. This makes bank deposits a digital representation of fiat money.

2.3.5 Credit money
Credit money is, as opposed to a deposit, the bank lending out money. Money can be lent to both private and legal persons. To access and use credit money works practically the same way as for bank deposits. The functionality is the same, apart from the fact that this is the banks money and not your own. Today most of our money is created by banks issuing credit.30 About 94% of the kroner created in Norway are “printed” by regular banks.31 In actual numbers there are today about NOK 85 billion in circulation issued by the Central Bank, and more than 2 trillion issued by ordinary banks.32 Money created by banks is removed from circulation when someone uses their deposits to repay their loan. Therefore, the total supply of credit money will decrease only when banks’ claims on the rest of the economy decrease.33

To be allowed to give credit, banks are subject to strict licensing and statutory regulation.34 A bank is in need of a license to operate, and according to the Financial Services Act (“finans-
foretaksloven”) banks in Norway must meet with requirements for e.g. capital adequacy, liquidity management, remunerations schemes, and consumer protection. These requirements contribute to limiting bank lending and money creation. As such, trust in both bank deposits and credit money is linked both to trust in the financial institution where you have your account, e.g. your bank, and as for fiat money, trust in the central authority to run a well-functioning monetary policy.

2.3.6 Electronic money
Electronic money is a kind of money that has emerged with the evolution of the internet. EU defines ‘electronic money’ as “electronically, including magnetically, stored monetary value as represented by a claim on the issuer which is issued on receipt of funds for the purpose of making payment transactions”. Only an institution granted authorisation can issue electronic money. Major players such as Facebook and Google have obtained license in the EU to issue electronic money. The purchasing power of electronic money can reside both in a physical device, such as a chip card, or as a software-based product. Electronic money is always pre-paid, and its value is expressed in the same currency as the deposit was made in. Electronic money is not a currency of its own, it is a digital representation of fiat money. An example of electronic money is a pre-paid gift card, which could have been bought either with cash or bank deposits. By contrast, electronic payment apps, such as Vipps, is not electronic money. The app uses information from your bankcard to access your bank account, and is thus bank deposits.

2.3.7 Virtual currency
Virtual currency on the other hand is unregulated, digital money that has no formal ties to fiat money. There is no institution behind virtual currency guaranteeing its value. The value of virtual currency stems purely from a belief in that someone is willing to pay for it. As with fiat money trust is key to the value of virtual currency. Nevertheless, unique to virtual currency is the fact there is no legal entity to trust. Trust must be placed in the market as a whole, not in an institution given a certain responsibility. As virtual currency is not backed by fiat money, but still has some kind of value, virtual currency must be considered as having intrinsic value. Virtual currency is created by ‘mining’, an activity that has a certain

---

35 Regjeringen (2014).
37 Electronic Money Directive, Article 2.2.
38 Ibid, Article 2.1.
40 European Central Bank (2017).
41 Weisenthal (2013).
similarity to looking for shells or gold. As such, it can be said to bear the closest resemblance to commodity money, even though it in practical use mainly resembles bank deposits or electronic money. Virtual currency allows for immediate settlement. Virtual currency does not have to go through a third party, which means that a payment can happen pseudonymously. Virtual currency is either something brand new, or a combination of the types of money mentioned above. The fact that it is difficult to say exactly what virtual currency is, at least using traditional terms, makes its legal status uncertain.

2.3.8 Virtual currency issued by central bank
Recently a few countries have begun researching how to create a national virtual currency. Japan, Estonia, and Kazakhstan are some countries that have publicly said that they have plans to issue fiat-backed national virtual currency, under control of a central bank. If these plans come through the definition of virtual currency will need to be re-written. Backed by a central bank virtual currency will no longer be “unregulated, digital money”. Virtual currency will then also be able to appear as something similar to regulated digital fiat money. By issuing virtual currencies of their own, central banks can take back control of monetary policies. Their control is now challenged by the growth of unregulated virtual currencies. Whether nationalised virtual currency will be a success is an open question. This will mark a breach with the decentralised, unregulated and possibly anonymous nature of virtual currency. These have been important factors for the growth of virtual currency up until now.

The Swedish Central Bank (“Riksbanken”) have issued a report outlining the possibility of an alternative Swedish digital currency, e-krona. The report points to two main reasons as to why this might be necessary. First, the growth in private solutions for digital payments, where infrastructure is dependent on a few commercial entities, might hamper competition in the market and make society vulnerable. E.g. in Norway the company Evry delivers technical solutions for many banks, as well as for authorities and telecom companies. Problems with Evry’s computers have led to technical errors for payment solutions, mobile phones, as well as other digital services. Second, the payment method that currently can replace digital payments in an emergency is cash. Cash is rapidly becoming a marginal payment solution. In Sweden close to 40 percent of payments in the retail business were carried out with cash in 2010, whilst in 2016 it is down to about 15 percent. If people do not have cash in their wallets, and the digital payment solutions go offline, it will be difficult to carry out payments.

---

42 Nicolaiisen (2017).
43 Browne (2017).
The Swedish Central Bank proposes that e-krona can be accessed in two ways. As a register-based currency where customers can make deposits directly to the central bank, functioning much as ordinary bank deposits today, and as a value-based currency stored in an app or a chip-card. This value-based currency is supposed to work off-line, so that small payments can be processed also when infrastructure goes down. Allegedly, it is also technically possible to allow for anonymous payments with e-krona, which may be desirable if e-krona is supposed to replace fully most of the features that cash has today.

2.4 Payment methods
Listing different modern payment methods and pointing out who or what is the guarantor giving money its value, can serve as an illustration of the characteristics of different types of money.

- Fiat money (cash); claim on a central bank. Payments made via banknotes or coins. Allows for immediate settlement.
- Bank deposits; claim on a private bank. Payments via bank card, giro transfer or app on mobile phone. Settlement through third party.
- Credit money; claim on a private bank, which again has a claim on whoever used the credit. Payments via bank card, giro transfer, or app on mobile phone. Settlement through third party.
- E-money; claim on a e-money company. Payments via rechargeable cards or other pre-paid representation of money. Settlement through third party.
- Virtual currency; claim on no-one. Payments via decentralised networks on the internet. Allows, at least in theory, for immediate settlement.
- Virtual currency issued by central bank; claim on central bank. It is uncertain how these payments will function.

2.5 Monetary policy and the role of a central bank
As we can see from the historical overview given above in para 2.3, money is not necessarily issued only by the state. Historically both private institutions and individuals have been able to create money. Today banks are the main issuers of money. The banks are subject to strict regulations. Virtual currencies on the other hand are decentralised and hence difficult to regulate.

A central bank functions as a guarantor to the value of money. The central bank is also the bank of banks, where the banks themselves can borrow money. An important role e.g. during the financial crisis in 2007-2008, when the ordinary banks did not trust each other to borrow money.49 “Money-printing” by the European Central Bank is known as “quantitative easing”, where the bank instead of actually printing money creates additional central bank reserves by purchasing assets in the financial market.50

Central banks can both be state or privately owned. Today the state has ownership of the Norwegian Central Bank, after it initially being private.51 52 In the US the central bank is privately owned.53 Who actually owns the central bank is not important. Authorities can control central banks by regulating them through legislation. The legitimacy of the Norwegian Central Bank is laid down in the Constitution (“Grunnloven”), Article 33 (“Norges Bank er landets sentralbank”). Furthermore, Article 75 states that it devolves upon the Norwegian Parliament (“Stortinget”) to supervise the monetary system of the realm, cf. the Central Bank Act (“sentralbankloven”) § 2.

Today the monetary policy in Norway is that of an inflation target. It is based on the assumption that the best way to achieve long-term growth is through price stability.54 Before the inflation target came into place, the monetary policy was tied to a fixed exchange rate. Norway became part of the Bretton Woods cooperation after World War 2, where US dollars functioned as the anchor currency.55 US dollars were in the seventies replaced by German marks. Norway finally gave up the policy of a fixed currency rate in 1992, and after a period where the monetary policy was in reality based on an inflation rate, this was formalised in 2001.56 The aim is that the annual consumer price inflation is to be kept close to 2.5 per cent over time.57 The central instrument to achieve this is the key policy rate, which is the interest rate on banks’ deposits up to a quota in the Norwegian Central Bank. The key rate influences short-term money market rates. Changes to the key policy rate will thus influence the value of the Norwegian currency NOK. Both the consumer and the market will thus experience a change in interest rate on loans and deposits. This will also take effect on the pricing of goods, especially those either imported or exported.

49 Meholm, p. 33.
51 Norges Bank (2017), "FAQ".
52 Sentralbankloven, § 2 (4).
54 Norges Bank (2017), "Monetary Policy".
56 Ibid, p. 41.
57 Norges Bank (2017), "Monetary Policy".
Throughout history authorities have been tempted to print large amounts of money several times, resulting in hyperinflation. The economy of Zimbabwe and the Weimar Republic are some well-known examples. An advantage virtual currency has is that no central bank can print large amounts of money in a short time, thus eliminating the risk of hyperinflation. On the other hand, a well-executed monetary policy can have positive effects on the economy. Allowing virtual currency to grow into a significant economic factor, will leave an important part of the monetary policy in the hands of the market.

An argument made by virtual currency enthusiasts is that virtual currency can help people to circumvent restrictions imposed by authorities. For example to buy food and other necessities on the black market in Venezuela, or to send remittance to family members in Nigeria during a currency crisis. While solving a problem for those who choose such solutions, virtual currency can also contribute to worsen the crisis for the rest of the economy.

As there are many local exchanges for bitcoins, there are some examples that local politics might actually have an impact on the price of virtual currency. Zimbabwe does not have its own currency, and there is shortage of cash. When the armed forces of Zimbabwe seized the power from Robert Mugabe, bitcoin at the Golix exchange in Zimbabwe jumped to a market value of more than USD 13,000. That is almost twice the rate bitcoin traded for in international markets at that time. As the events in Zimbabwe confirms, virtual currency is most attractive when confidence in institutions falls.

A vital task for banks is to keep the public’s money safe. As banks store large amounts of money, breaking into a bank is attractive to criminals. A bank, and even a central bank, can be hacked. Any centralised system is vulnerable to cyberattacks. In 2016 USD 81 million were stolen from the Central Bank of Bangladesh, wired to an account in the Philippines, and then later disappeared through Philippine casinos. Even though banks take comprehensive security measures, it is easier to hack one bank than to hack all of its customers. Virtual currency has the advantage that money can be stored locally. Nevertheless, users of virtual currency often choose to store their money in exchange services online. It is more convenient, since the

---

59 Lahrichi (2016).
60 Kinsmann (2017).
63 Norges Bank (2017), ”Finansiell infrastruktur”, p. 4.
64 Nicolaisen (2017).
money is more easily accessible. These exchange services can of course be hacked. This happened to Mt. Gox, the main bitcoin exchange from 2010 to 2013, and it had to file for bankruptcy.65 Unlike when a bank files for bankruptcy, the authorities guaranteed for none of the customer’s deposits. The Norwegian Banks’ Guarantee Fund guarantees for a customer’s deposits up to NOK two million per bank.66 In the EU the equivalent guaranteed amount is EUR 100,000.67

67 Deposit Guarantee Schemes Directive, Article 6 (1).
3 Virtual currency

3.1 Introduction

Virtual currency is a term meant to cover many different types of digital money. A term often used is cryptocurrency. Bitcoin is an example of a cryptocurrency. Other terms in use are digital currency, e-money, electronic money, electronic currency, virtual money and so forth. These terms are often used in an equivocal manner, creating confusion as to what different authors actually mean when using them.  

The term ‘virtual currency’ is used by the Norwegian Tax Administration when referring to current regulations for this area. Even though most virtual currencies are actually cryptocurrencies, in tax terms it makes sense to include as many currencies as possible when outlining a regulatory framework. It is not important for the tax authorities whether the currency is centralised or decentralised, or which level of encryption the currency has. Of importance is what the currency is worth, and what taxpayers win or lose on the investment they have made.

The following chapter will investigate what virtual currency actually is, how it works, and look at alternative usage of the blockchain technology. Mapping what virtual currency is might reveal some characteristics that are problematic from a legislative prospective.

3.2 Types of virtual currency

The European Central Bank divides virtual currency into three main categories; closed virtual currency schemes, virtual currency schemes with unidirectional flow, and virtual currency schemes with bidirectional flow.

3.2.1 Closed virtual currency schemes

Closed virtual currency schemes are at times called “in-game only” schemes, and have little to no link to traditional economy. A typical example is a computer game where items and services can be bought with a currency that only exist within the game. This is a kind of currency that can typically be bought through a subscription fee or acquired through performances. This currency cannot be traded outside the virtual community. However, it is possible to exchange fiat money for in-game money or items on a private basis.

68 ‘Virtual currency’ was not ‘electronic money’ as per the EU definition, but as we will see in para 3.2.2 ‘electronic money’ is a subset of ‘virtual currency’ in the definition made by the European Central Bank.

69 Skatteetaten (2017), "Skattemessige konsekvenser ved bruk av bitcoins".

3.2.2 Virtual currency schemes with unidirectional flow

Virtual currency schemes with unidirectional flow can be purchased using traditional currency at a specific exchange rate, but it cannot be exchanged back to any traditional currency. Such virtual currencies can be used to buy goods and services. This is quite similar to buying a gift card. You can buy what you want for the amount you invest, but only at certain stores.

3.2.3 Virtual currency schemes with bidirectional flow

Virtual currency schemes with bidirectional flow can be purchased using traditional currency. It can be used to buy goods and services, and similarly to any other convertible currency, it can be exchanged. This category is to a large extent unregulated, and well-suited for transferring and hiding money. Bitcoin, litecoin, ether et al are all virtual currencies with bidirectional flow. As such it is also the category of interest to this thesis.

3.3 History of virtual currency

The idea of electronic money is quite old. Almost as old as the idea of the internet itself. It is older than the World Wide Web, which became operational first in 1990/1991 and gained popularity in the mid to late nineties. In 1983 David Chaum published a paper called “Blind Signatures for Untraceable Payments”, written while he was a computer science student at the University of California. In his paper Chaum outlined the theory behind a system where the buyer converts traditional currency into an electronic currency called e-cash; a currency which only exists on the internet. Chaum concluded that he had introduced a new kind of cryptography. It combined auditability and control with increased personal privacy by allowing untraceable payments. Unfortunately for Chaum, the world of e-commerce was not enthusiastic about his ideas. The system he developed has been said to “depend too heavily [...] on existing infrastructures of government and credit card companies”. Chaum depended on financial institutions to implement his electronic currency. When not enough banks accepted the system, it was hard to get customers to use it. His company DigiCash went bankrupt in 1998.

---

72 Hiskey (2010).
73 Chaum (1983).
75 Chaum (1983).
76 Wallace (2011).
77 Pitta (1999).
Others, such as e-gold and liberty dollar, followed suit during the Dot-com bubble. All failed to establish themselves as reliable options to traditional currency. Some reasons given for their failure was that they were shut down due to US regulations, and some put out of business because of criminal activity.

The USA Patriot Act introduced in 2001 proved to be an obstacle for these early digital currencies. The Patriot Act focused on “improving America’s defences against money laundering and possible terror funding.” The Patriot Act expanded the definition of ‘financial institution’ to include not only licensed senders of money, but also underground banking systems. Any person engaging as a business in the transfer of money, both domestically and internationally, was from now on within the scope of the definition. Financial institutions had to comply with all Bank Secrecy Act requirements, which meant record keeping and reporting requirements, including filing suspicious activity reports. Financial institutions also had to offer an Anti-Money Laundering program (AML) and a system called Know Your Customer (KYC), as well as register with The Financial Crimes Enforcement Network (FinCEN). The earliest providers of virtual currency all failed on one or more of these criteria, and by doing so they committed a federal offence according to the Patriot Act.

In 2008, a paper by Satoshi Nakamoto called “Bitcoin: A Peer-to-Peer Electronic Cash System” was published introducing both the open source blockchain technology and the virtual currency known as bitcoin. This happened in the aftermath of the financial crisis. Unlike its precursors, Bitcoin is not a centralised system. By being a decentralised system it is harder to control and ultimately close down. The growth of bitcoin, and the fact that the blockchain technology is open source, has resulted in the emergence of many new currencies trying to develop and improve the original concept. Some examples are Ethereum’s ether and Ripple’s XRP.

---

78 Griffith (2014).
80 Ibid, p. 15.
81 USA Patriot Act, section 359.
82 Mullan (2016), p. 16.
83 Bank Secrecy Act, § 202.
86 Satoshi Nakamoto is a pseudonym, either for a person or a group of persons. Whoever is behind it has not been revealed, but most traces point to members of the Cypherpunk movement. This is a group of privacy oriented liberals interested in cryptography and mathematics. See Meholm (2017) p. 83.
On the 28th of November 2017, the website coinmarketcap.com lists 1327 different virtual currencies, reporting a current total market value of more than USD 300 billion.\textsuperscript{87} 88 The market share of bitcoin is a little more than 65%.\textsuperscript{89} 90 The value and importance of virtual currency in the future is uncertain, but the numbers prove that this has already become a significant economical factor. As more people invest larger amounts of money in virtual currencies, it is increasingly important for legislators to keep up with the technology.

Acknowledging that there had recently been a remarkable increase in the number of new virtual currencies, the Swedish Financial Supervisory Authority ("Finansinspektionen"), issued a warning in November 2017. Virtual currencies are not regulated, and thus not under the supervision of Finansinspektionen or other authorities, leaving the consumer with no formal consumer protection.\textsuperscript{91} According to Finansinspektionen there is a high risk of fraud connected to virtual currencies. The business seems to attract a high number of players not looking for completing projects, but rather collecting money from the public. The most infamous, OneCoin, has repeatedly been called a Ponzi scheme, and e.g. received a fine of EUR 2.5 million issued by the Italian Antitrust and Consumer Protection Authority (AGCM).\textsuperscript{92}

### 3.4 How to acquire virtual currency

To send, receive, and store virtual currency such as bitcoin, one will have to download a free, open-source software.\textsuperscript{93} This software functions as an electronic wallet, and money in the wallet can be stored either locally or at an online wallet service. The wallet has an address; a string of letters and numbers not systematically linked to an individual.\textsuperscript{94} To enhance security one can have more than one wallet, thus storing money in several places.

#### 3.4.1 Mining

There are two ways of acquiring virtual currency. Either by receiving it from someone already in possession of the currency, or through a process called mining. Miners solve mathematical problems, helping to verify transactions and maintain the system. Every 10 minutes, on aver-

\begin{itemize}
  \item \textsuperscript{87} By comparison, there are currently about 1.58 trillion US dollars in notes and coins issued by Federal Reserve in circulation. The amount including money issued as credit is 13.700 trillion. See Federal Reserve (2017).
  \item \textsuperscript{88} The total market value of virtual currencies is about 5 times the market value of Statoil, the largest corporation in Norway. See Oslo Børs (2017).
  \item \textsuperscript{89} Coinmarketcap (2017).
  \item \textsuperscript{90} After splits in the blockchain there are currently several versions of bitcoin; the largest offshoot, called bitcoin cash, has about 9% market share.
  \item \textsuperscript{91} Finansinspektionen (2017).
  \item \textsuperscript{92} Pollock (2017).
  \item \textsuperscript{93} FATF (2014), p. 6.
  \item \textsuperscript{94} Pollen (2017).
\end{itemize}
age, a miner wins a number of bitcoins as a reward. The bitcoin system is programmed so that solving these mathematical puzzles will be gradually more difficult as the system grows.

There is a fixed supply of 21 million bitcoins available for mining, which is supposed to hinder inflation. For ordinary currencies, banks issuing credit is how the main part of new money is created. If virtual currencies adopts the concept of credit, it is likely that inflation will be an issue also for bitcoin.

21 million bitcoins might not sound like much, but one bitcoin contains 100 million satoshi, the smallest unit of bitcoin. That makes 2.1 quadrillion satoshis. It is estimated that all bitcoins will be mined by the year 2140. When the mine has run out of bitcoins, the idea is that transaction fees will take the place of the mining reward system. Note that not all virtual currencies have a built-in mechanism limiting the total amount of money. Ethereum’s ether can be “printed” whenever Ethereum Foundation decides to do so, much like a traditional central bank.

3.4.2 Exchange services
To mine virtual currency requires a lot of computing power, so the easiest way to acquire virtual currency is by purchase. Virtual currency can be bought at certain ATMs or through direct contact between seller and buyer. Nevertheless, it is usually traded with conventional currency at an online exchange. Compared to the real world, these exchanges are the closest thing to a stock exchange or a bank. Exchanges for virtual currency can be either centralised or decentralised.

Decentralised exchanges, peer-to-peer solutions, are particularly difficult to regulate. Still, the case of Pirate Bay showed us that even though it is hard to completely shut down peer-to-peer services, regular access to these websites can be blocked resulting in significantly reduced traffic. A verdict from the Oslo District Court (“Oslo Tingrett”) in 2015 forced mayor ISPs in Norway to block access for its customers to Pirate Bay. Courts in other countries, e.g. the UK, have taken the same stance.

---

95 Lee (2013).
96 Pollen (2017).
100 Warner Bros. et al v. Telenor.
The blocking of Pirate Bay in Norway was imposed pursuant to the Copyright Act ("åndsverkloven"), cf. § 56c. Thus, new legislation is required if virtual currency is to be blocked in the future. Blocking access to websites not willing to collect information on trades with virtual currency, can be carried out without imposing a ban on the virtual currency itself. This as an attempt to force trading with virtual currency into more organised forms. It has to be said that this will be a drastic solution, and a rather unlikely outcome. No official regulatory authority in Norway have so far advocated such a measure. There may also be reason to believe that users of virtual currency are above average tech-savvy, and may find ways to circumvent such blockages.

Centralised exchanges on the other hand often require that the customer register a passport, an address, and a bank account number.102 This as centralised exchanges, depending on regulations where the exchange has its base, can be required to obtain a license, and follow the same AML (Anti-Money Laundering) and KYC (Know Your Customer) regulations as banks.103 In the US, exchanges need to comply with a complicated network of regulatory regimes in all 50 US states, which the industry argues limits start-up growth by increasing the cost of market entrance.104 The office of the US Treasury in charge of currency policy has revealed plans to impose a nationwide program for virtual currency exchanges, similar to the one recently enacted in Japan.105 Not all US states currently require that exchanges obtain licenses, but some do, e.g. New York.106 In Norway, there is currently no license required to operate.

Complying with license requirements can be complicated and expensive, but there also seems to be a gain. Having a license makes the player look serious and legitimate, with sufficient financial backing, which is attractive to customers. Major players in the virtual currency business seem to be attracted to marketplaces where they can deal with a predictable legal framework.

Regulating exchanges is important for legislators. In a decentralised virtual currency, exchanges are the central hub that can gather information on traders of the currency. The problem for legislators and law enforcement is that buying virtual currency through a centralised exchange is only one of several options as to where currency can be bought. As money can be

---

103 Ibid.
104 Del Castillo (2017).
105 Ruther (2017).
106 BitLicense Regulatory Framework, Section 200.3 License (a). “License required. No Person shall, without a license […] engage in any Virtual Currency Business Activity”.
stored both online and offline, it is also limited how much information these exchanges actually have on their customers assets.

3.5 Blockchain

3.5.1 Distributed ledger

A ledger is the principal book or computer file for recording and totalling economic transactions. Ledgers serve as systems of record for a business’ economic activities and assets. These ledgers are often run through a centralised and trusted third-party, such as a financial institution, clearinghouse or other mediators. When transferring money your payment is at some point in the hands of a third party; the bank. You have no insight into when or how the transfer occurs. Transferral of money is dependent on the customers trust in the banking system. A payment from one bank to another will go through the central bank, and cross-border transactions will involve more third party actors. The lack of transparency, as well as the possibility of fraud and corruption, may lead to disputes. Resolving disputes and reversing transactions, can be costly and time-consuming. Blockchain offers a solution to these problems.

A distributed ledger is a type of database, which is being shared, replicated, and synchronised among the members of a network. In this distributed ledger participants in a network can record transactions, such as the exchange of assets or data. The participants in the network govern and agree by consensus on the updates to the records in the ledger. There is no third-party involved. By communicating peer-to-peer businesses can, in theory, save time and costs while reducing risks.

In a blockchain a transparent transaction history is created in a distributed ledger. Unlike a conventional database, each of the parties, or “nodes”, participating in the blockchain network maintain a copy of the distributed ledger. For bitcoin there are currently almost 12000 nodes, each maintaining a copy of the ledger. Changes to the ledger will automatically

---

107 Brakeville & Perepa (2016).
108 Ibid.
109 A 2012 survey showed that only 15% of Americans had “a great deal” or “quite a lot” of confidence in the US banking system. See Robison (2012).
110 Brakeville & Perepa (2016).
111 Ibid.
113 Bitnodes (2017).
114 United States has 3542 nodes, about 30% of the network, and is by far the largest player. By comparison, Norway has 66 nodes.
be rejected if not supported by at least 51% of the other nodes.\textsuperscript{115} Once a transaction is registered in the distributed ledger, it is locked in place and cannot be changed. An advantage is that such a distributed ledger is difficult to hack, since a hacker would need to alter multiple nodes in the exact same way at the exact same time.\textsuperscript{116}

3.5.2 Open or closed networks
Networks can be either open or closed. An open network is a community free for anyone to join, potentially allowing anonymous or pseudonymous participants. Bitcoin is an open network. A closed network on the other hand is a ledger where all of the entities are known, and where joining the network requires permission. If virtual currencies are going to follow the same KYC (Know Your Customer) regulations as the banks, this will be significantly easier to accomplish in a closed network.

3.5.3 Encryption
Members of a network communicate using encryption technology, via both public and private ‘keys’. A ‘public key’ is the users’ address on the blockchain, and information (e.g. amount of bitcoin) is sent across the network recorded as belonging to that address. While the ‘private key’ function as a password giving the owner access to their digital asset.\textsuperscript{117} The history of asset exchanges taking place between members in the network, is permanently recorded in a sequential chain of cryptographic hash-linked blocks.\textsuperscript{118} Confirmed and validated transactions are linked and chained from the beginning of the chain to the most current block, hence the name blockchain.

3.5.4 Alternative use of technology
The blockchain technology was originally created to serve as the open source backbone of the bitcoin currency, but the same technology can potentially be used in a multitude of ways. Blockchain can be used as a tool for anything dependent on registration and record keeping. An example of the use of blockchain technology is BP, Shell, Statoil and other energy companies’ plans of creating a digital platform for trading energy commodities.\textsuperscript{119} Blockchain technology can provide the companies with accurate timestamps to each part of the trade, eliminating confusion over ownership of cargo. According to a press release, Statoil claims that adopting blockchain technology in energy trading can make it a quicker, cheaper and

\textsuperscript{115} Meholm, p. 106.
\textsuperscript{117} BlockGeeks (2017).
\textsuperscript{118} Brakeville & Perepa (2016).
\textsuperscript{119} Varghese & Serapio Jr. (2017).
more secure process. The blockchains biggest advantage is that it removes the risk of a single point of failure. This is not only of interest for finance and businesses, but also for authorities. Blockchain can for example be used to register votes in an election, making it practically impossible for anyone to vote more than one time. Estonia have been a particularly early adopter of the blockchain technology. The country has since 2012 e.g. used it for registries for national health and judicial records. A national ID card, with a cryptographically secure digital identity, is also backed by blockchain technology.

A blockchain-related buzzword is ‘smart contracts’. Smart contracts is computer code stored within the blockchain network, designed to execute certain functions triggered by information in the blockchain shared ledger. Smart contracts allow for automated transactions or modifications. An example is selling a stock when the price reaches a predefined value at a stock exchange, executed in a more transparent and effective way. Transactions involving both tangible and intangible assets can be handled by smart contracts.

Different usage of the blockchain technology ought to trigger different types of regulatory legislation. To date a few US states have proposed regulation that distinguish between virtual currency and blockchain. An example of such regulation is a proposed amendment to Washington’s Uniform Money Services Act. In this proposal it is clarified that businesses using distributed ledger technology for other purposes than virtual currency, will not require licensing in Washington State. While in Delaware, corporations have been allowed to maintain shareholder lists, along with other corporate records, using the technology. Such legislation is indicative of increasing acceptance that blockchain technology can increase efficiency, as well as better the protection of data.

3.6 System efficiency
3.6.1 Scalability
A new system or technology must offer some improvements compared to the one that people are already using. It must be inexpensive, reasonably safe, as well as convenient to use in regards to speed, capacity, and availability. In short, a new system must be more efficient than the old one.

120 Statoil (2017).
121 Meola (2017).
Virtual currencies have met a technical problem as they are growing; most (if not all) virtual currencies have proven to have a problem with scale. As a network grows bigger in number of users and frequency of transactions, it is increasingly difficult to preserve the virtue of privacy, security, and low transaction costs.127

For the bitcoin system to be secure, new transactions must be approved by other users of the network, forming the blockchain. These transactions are stored in blocks. As the number of blocks in the blockchain grow bigger, it is increasingly harder to maintain the system. The size of bitcoin’s blockchain is currently about 180 gigabytes of data, and it has almost doubled in size the last year.128 129 To verify a block a participant will need a copy of the entire ledger, thus the system requires a large storage capacity. Especially in the future, if the bitcoin currency is going to continue its growth. Ethereum’s ledger is already said to be about the same size as the bitcoin ledger, and for Ethereum this has happened over a significantly shorter period of time.130

A number of solutions have been proposed, among them allowing for larger blocks, unlimited blocks, or off-chain payments.131 The problem is that these solutions, especially off-chain payments, challenges the security of the blockchain. The fact that the ledger is shared and transparent is exactly what was supposed to make the trusted third party obsolete. Both bitcoin and Ethereum use a work intensive method of verifying transactions called proof-of-work. For Ethereum there are plans to switch to a verifying method called proof-of-stake.132 Proof-of-stake is less work intensive, but also seemingly less secure. Lower level of security might make it possible to perform double-spending, i.e. using the exact same money in several transactions.133 Solving the double-spending problem is vital for people to trust a virtual currency.

Disagreements on how to deal with the problem of scaling, has resulted in bitcoin’s blockchain splitting in multiple paths.134 Network members will then have to choose which chain

127 Hayes (2017).
129 Different sources provide very different numbers for the size of the blockchain. According to Meholm (2017), p. 99, the size is as much as 30 terabytes.
130 Suberg (2017).
131 Lerner (2017).
133 ‘Double-spending’ is an error in a digital cash scheme in which the same single digital token is spent more than once.
134 Chen & Lam (2017).
they believe in. Splits in the blockchain are known as a fork. The last split resulted in two versions of bitcoin; the original bitcoin and the newcomer bitcoin cash.\textsuperscript{135} Bitcoin cash is currently the third most valuable virtual currency, behind bitcoin and ether.\textsuperscript{136} Bitcoin was expected to split again in November 2017, with hopes of a new version enabling larger blocks and increased efficiency.\textsuperscript{137} This did not happen, and the result was the bitcoin market price dropping 29\%.\textsuperscript{138}

Nevertheless, the main problem is not the number of gigabytes in the blockchain. Rather it is the fact that in order to control the monetary base, mining is made more difficult than it could be.\textsuperscript{139} The first miner to solve a problem gets a number of bitcoins as a reward. To hinder inflation these problems get gradually harder, as more computational power is constantly being added to the network. If the mine depletes too soon, there will be no point in mining. Much hardware, engineering and power is used in order to solve mathematical problems that are artificially made extremely complex. It is a paradox that the complexity of mining is both choking the system, as well as keeping the system running. There is apparently no quick fix to this problem.

### 3.6.2 Transaction capacity

It is apparently relatively easy to set up a system that can handle quite few transactions, but a system aiming to replace our current banking system must be able to tackle thousands of transactions per second. This has, past and present, at some point proven to be a problem for virtual currencies. For bitcoin only so many transactions can be added, as many as fit in a block. A more traditional payment alternative like Visa is able to handle up to 56,000 transactions per second.\textsuperscript{140} To compare, the capacity of the bitcoin network is currently at seven transactions per second.\textsuperscript{141} An alternative like Ethereum is also said to be lacking a solution for increased transaction capacity.\textsuperscript{142} For virtual currencies to grow into a serious contender for Visa et al, this issue must be resolved. A lot of claims have been made recently that this issue \textit{will} be resolved, but whether it does so remains uncertain.\textsuperscript{143} One solution is to create a

\begin{footnotesize}
\begin{enumerate}
\item[Ibid.]
\item Coinmarketcap.com (2017).
\item Framstad (2017).
\item Ibid.
\item Houy (2014), p. 2.
\item Visa (2015).
\item Ibid.
\item Marshall (2017).
\end{enumerate}
\end{footnotesize}
system that is less decentralised. Ripple is a virtual currency built more like a traditional bank, and they claim that they can handle up to 1000 transactions per second.144

3.6.3 Transaction speed
The speed of transactions made with virtual currencies might vary, as the speed depends on capacity of the network. I.e. how many other payments are currently waiting for confirmation. It also depends on how much you are willing to pay in transaction fee. Miners confirming transactions will prioritise those who are willing to pay the most. This implies that a payment with virtual currency can take a while if you are not willing to pay for it. On the other hand, a payment made with a virtual currency can also be carried out quickly. By centralising the verification process, it is possible to achieve a significant increase in transaction speed. Ripple is said to settle an international payment in three seconds on average.145

Transaction speed in the banking world is more predictable, even though there are differences between large and small transactions. Domestic transfers of smaller amounts of money from one Norwegian bank to another takes place five times a day.146147 For a payment to an account abroad, the recipient must expect about 3-5 days before the money is available.148 Purchases made with bankcards, e.g. BankAxept or Visa, are seemingly completed instantly at the store, but also these take time to clear. In addition to the traditional bank system services like e.g. MoneyGram, Hawala, Transferwise, and so forth are also available, and widely used in countries where the banking infrastructure is less developed.149

3.6.4 Transaction costs
A bank transfer between two Norwegian accounts is usually free for the customer, but it still has a cost.150 The cost the bank has for processing an ordinary payment in Norway is on average estimated to one dollar (eight NOKs).151 Nevertheless, the price varies between different solutions, which each are operating with a fixed price. According to a report from the Norwegian Central Bank the price of a payment made with BankAxept is NOK 2,93, whilst payments made with international cards such as Visa and MasterCard cost NOK 12,60.152

144 Roberts (2017).
145 Ibid.
146 Finans Norge (2016).
147 These numbers are for regular payments. In the banking system, large amounts of money can be transferred instantly, if the sender/receiver is willing to pay for it.
149 Ibid.
150 DNB (2017).
increased use of bankcards and electronic payment systems (e.g. Vipps), increases the transac-
tion costs of banks.\textsuperscript{153} Banks are eager to reduce this cost, particularly as new EU legislation
imposed from 2018 will increase competition in the market for payments.\textsuperscript{154} A report by Ac-
centure claims that by adopting the blockchain technology banks can vastly improve the effi-
ciency of clearing and settlement, potentially reducing their costs with up to 70\%\textsuperscript{155}

While domestic transfers are relatively cheap or free for the public, this is not the case for
transferring money abroad. In 2016, a sum of USD 429 billion were officially transferred to
developing countries, mainly transferred by migrants sending money to family in their home
country.\textsuperscript{156} The global average cost of sending remittances in 2016 was 7.45\% of the trans-
ferred amount. People sending money abroad will be interested in new and cheaper services.
Here virtual currencies might offer a good alternative.

Virtual currency on the other hand, does not have a fixed transaction fee. Whenever you trans-
fer bitcoin, you can choose how much you want to offer as transaction fee. A low offer will
result in a slow transaction, as it will not be prioritised by miners. While offering a high fee
will result in several miners competing for verification, resulting in a quicker transaction. A
minimum bitcoin miner fee is said to be about 360 satoshis, substantially lower than a bank
transfer abroad, but this price is fluctuating.\textsuperscript{157} \textsuperscript{158} There is also uncertainty as to what will
happen with transaction fees as mining new bitcoins will gradually be more difficult and re-
quire more computing power.

3.6.5 Energy consumption
Even though the customers do not receive a large bill for bitcoin transactions today, it still has
a significant cost for society. There are large costs for electricity and computer hardware, to-
day covered mainly by the miners. The bitcoin network must find a more efficient technical
solution as the mining rate decreases, or else the transaction fees will have to increase signifi-
cantly.

\textsuperscript{153} Olsen (2017).
\textsuperscript{154} Hellström (2017).
\textsuperscript{155} Accenture (2017), p. 5.
\textsuperscript{156} World Bank (2017), p. V.
\textsuperscript{157} BitPay (2017).
\textsuperscript{158} Again, different sources give very different numbers. According to Smart (2016), fees exceeding as low as 50
satoshis will result in VIP service, removing transaction delays of any kind.
The large amount of data that is processed to keep a blockchain running, is a problem both in regard to cost and to the environment.\textsuperscript{159} Bitcoin is currently occupying as much as 0.12\% of the world’s energy consumption, and Ethereum 0.05\%.\textsuperscript{160} According to calculations by Digiconomist this corresponds to the power consumption of Nigeria and Ghana, respectively. A single bitcoin transaction currently consumes 236.00 KWh, the same as the daily consumption of 7.99 US households.\textsuperscript{161} To compare, Visa consumes just a fraction of the electricity to process a number of payments that is far bigger than the number of bitcoin transactions.\textsuperscript{162}

3.7 Future of virtual currencies

The general trend for ordinary currencies in recent years have been fewer currencies, e.g. currency unions such as EU’s euro cooperation. Fewer currencies makes it easier to trade internationally, whilst adding another currency to a trade adds risk and uncertainty. The currency rate might change, and it will be more difficult to compare prices. The main argument for retaining a variety of currencies, is that different monetary policy might be needed in different countries. This is difficult to accomplish within a market with one currency acting as legal tender.

A future with thousands of virtual currencies does not seem sustainable. Only a few of these will survive as an alternative to today’s fiat money. Seller and buyer must have a limited set of payment solutions and currencies to deal with in order to interact effectively. There are currently many providers trying to get a piece of the market, but only the virtual currencies with the best and most innovative solutions will prevail in the end.

The largest virtual currencies today are bitcoin, Ethereum’s ether, and Ripple’s XRP.\textsuperscript{163} Bitcoin is by far the largest. It is the most talked about virtual currency, and it is being used as an example when people are trying to explain how virtual currency works. The result is that bitcoin, as a self-reinforcing effect, appears as both a safer option and as more understandable than the others. The main problem for bitcoin is that it is highly ineffective, and with the technical solution of today, it will become even more ineffective as the system grows. Bitcoin is built in way where it becomes safer and more robust as more people are using it, but it also gets slower and slower. This problem must find a solution if bitcoin is to continue its growth.

\textsuperscript{159} Malmo (2017).
\textsuperscript{160} Digiconomist (2017).
\textsuperscript{161} Ibid.
\textsuperscript{162} Swartz (2012).
\textsuperscript{163} The third largest currency, bitcoin cash, is excluded here, as the system is so similar to regular bitcoin.
Ethereum appears to have inherited much of the same problem with efficiency as bitcoin, as it is built on the same blockchain technology. The currency has also been a target for hackers and theft, arguably more so than bitcoin.\textsuperscript{164} Ethereum's advantage is that it is built for smart contracts, thus the system can be used for more than just being a virtual currency. Large companies like Microsoft, IBM, and Intel, base their blockchain technology on Ethereum.\textsuperscript{165} Ethereum’s functionality as a currency looks more uncertain.\textsuperscript{166} A system where nearly every company issues their own tokens, working as a currency within the currency, appears somewhat confusing and not very user-friendly.

The third major virtual currency is Ripple. Ripple is not so much a currency as it is a system for money transferal, without the need for a central counterpart.\textsuperscript{167} Ripple appears as the banks’ favorite, and more than 75 banks are now using Ripple to transfer money.\textsuperscript{168} Instead of holding local currency in accounts around the world, banks can use Ripple to consolidate their liquidity for global payments. A bank customer sending money to an account in another country might not even know that the bank actually used Ripple’s currency XRP when transferring the amount. The downside of Ripple is that it seems less transparent, more like a traditional bank. For customers who are drawn to the anonymity aspect of virtual currency, Ripple might seem less tempting. This as Ripple has built in AML (Anti-Money Laundering) and KYC (Know Your Customer) features.\textsuperscript{169} Ripple is an example of how blockchain technology seem to make the banking system more efficient. A more efficient banking system will result in cheaper international transfer services for customers.

Not everything that pretends to be a virtual currency is actually a virtual currency. The system OneCoin is a rather small player in the world of virtual currencies, but still deserves a special mention. This so-called currency has more than 6000 customers in Norway, and about 56.000 customers in Sweden.\textsuperscript{170} OneCoin has been called “virtually worthless”, and banks have been refusing to transfer money on behalf of customers who wants to buy it.\textsuperscript{171} The Norwegian National Authority for Investigation and Prosecution of Economic and Environmental Crime (“Økokrim”) has labeled it as a Ponzi scheme.\textsuperscript{172} Ponzi schemes are illegal according to the Lottery Act (“lotteriloven”), § 16. OneCoin claims that it is a cryptocurrency, and that it is

\textsuperscript{164} Popper (2017).
\textsuperscript{165} Ibid.
\textsuperscript{166} Mehholm (2017), p. 128.
\textsuperscript{167} Ibid, p. 126.
\textsuperscript{168} Roberts (2017).
\textsuperscript{169} FinCEN (2015), para 12.
\textsuperscript{170} Dahl (2017).
\textsuperscript{171} Penman (2016)
\textsuperscript{172} NTAES (2017), p. 13.
based on blockchain technology. Yet there is no available ledger, neither to the public nor to the members. Another problem is that the currency is not listed with any of the independent exchanges for virtual currencies, e.g. coinmarketcap.com. Furthermore, it is not possible to buy anything for the currency. That implies that you can buy currency from OneCoin, but you cannot currently sell it. As such, it does not even qualify as money according to the traditional definition of money, see para 2.2. In the meantime, the company is telling its customers that the value of the currency continues to rise. According to representatives from OneCoin their currency will finally be available for the market in 2018. The year 2018 will certainly be an exciting one for OneCoin owners, eager to get some money back on their investment. Whether they get anything at all is an open question.

\[173\] Vanderbuilt (2016).

\[174\] Nuyten (2017).
4 Anonymity versus pseudonymity

4.1 Introduction

An underlying principle for effective tax administration is that it is possible to track and report transactions. Cash is by its nature generally untraceable to a particular person or transaction. There are claims that also virtual currency is untraceable, and therefore hinders state regulations and fosters criminal activities.\textsuperscript{175} OECD have pointed out that as the use of cash is decreasing, virtual currencies may be the future of criminal payments.\textsuperscript{176} New technology can enable taxpayers with more sophisticated methods for tax evasion, but also provide tax administrations with new opportunities and tools to enhance compliance.\textsuperscript{177} This chapter will give an overview of the technology arms race between anonymisers and de-anonymisers.

4.2 Technology

Trade with virtual currency is pseudonymous. A pseudonym is a state of disguised identity. Transactions in the bitcoin blockchain are public, whilst the identity of the account owner is apparently unknown. A transaction is not linked to an individual person, but to an account address, which is a string of letters and numbers. Traders are therefore not anonymous, but use the account address as a pseudonym. The major challenge related to virtual currency is how to gather information on the users behind these transactions, this according to a Norwegian report on threats posed by new methods of payment.\textsuperscript{178}

Each transaction in the blockchain is recorded in a distributed ledger. These distributed ledgers can be either open (public) or closed (private), see para 3.5.2.

4.2.1 Anonymity in open networks

In an open distributed ledger account addresses are published online, but they are not directly linked to an individual. Nevertheless, it does not imply that you are completely anonymous while trading with virtual currencies. Studies show that it is possible to track a person and identify an account owner by using publicly available information in the distributed ledger. Uncovering identities in pseudonymous networks is possible by combining information from multiple sources. A study by researchers at Dublin University College showed that with the appropriate tools it is possible to observe the activity of users in detail.\textsuperscript{179} A study at Princeton University came to a somewhat similar result; third party web trackers using cookies can de-

\textsuperscript{175} Bohannon (2016).
\textsuperscript{177} Ibid, “Technology Tools to Tackle Tax Evasion and Tax Fraud”, p. 6.
\textsuperscript{178} NTAES (2017), p. 15.
\textsuperscript{179} Reid & Harrigan (2013), pp. 201-202.
anonymise users of virtual currencies.\textsuperscript{180} Online merchants leaking cookie information to third parties for e.g. advertising purposes, can directly reveal identity, as well as reveal exact transaction information. The Princeton paper points out that their method of gathering cookie data, can be used to build a forensic tool for law enforcement usage. Open distributed ledgers increase transparency, but might actually decrease privacy for its users.

4.2.2 Anonymity in closed networks

In a closed distributed ledger information is not published online for everyone to see. Only specific parties are selected to verify given transactions in the blockchain, thus being able to observe data.\textsuperscript{181} This method increases privacy making it more difficult to identify the owner of a given account address. On the other hand, as closed distributed ledgers are less transparent, they are also more prone for fraud and corruption. It is also worth noting that closed ledgers require that the users identify themselves before taking part in the network. Thus, there is a centralised register keeping track of the identity of the users of the blockchain. Centralised registers may be hacked, or whoever is in control of the ledger can be forced to hand over information to authorities.

Thus, the choice between an open or a closed ledger, is in a way a choice between whether you primarily want to hide your identity or hide your transactions. You cannot have both.

4.2.3 Tools to enhance anonymity

There are technological ways for an individual to increase their privacy, in addition to the technology behind the virtual currency itself. For instance, a person can create a new account for each trade and by that making it harder to see a pattern for identification. Furthermore, a person can use VPN-services, such as TOR, disguising their IP-addresses, which can be used for identification. Another tool is a «mixer». A mixer changes the transaction chain in a blockchain, and by that making it hard to figure out the sender and receiver of a transaction.\textsuperscript{182} A problem with the mixer solution is that the user must hand over control to the mixer service, trusting the service to return the users virtual currency after performing the laundry.\textsuperscript{183} The Princeton study by Goldfeder points to browser extensions that can block cookies as a measure that can protect identity.\textsuperscript{184} There are also other technologies to enhance personal privacy, and new methods and tools are invented as the older ones turns out to be less effective.

\footnotesize
\textsuperscript{180} Goldfeder, Kalodner, Reisman et al (2017), p. 15.
\textsuperscript{181} Suda, Tejblum & Francisco (2017), p. 98.
\textsuperscript{182} FATF (2014), p. 6.
\textsuperscript{183} Ludwin (2015).
Some virtual currencies have extended privacy baked into the protocol, and promise untraceable transactions.\textsuperscript{185} One such system is Monero. Nevertheless, anonymity weaknesses have been revealed for Monero too. A recent study at the National University of Singapore managed to trace as much as 88% of inputs to the Monero blockchain.\textsuperscript{186}

Compared to traditional currency there is an assumption that virtual currency is more anonymous and secure. Given that there is a public distributed ledger, it can be argued that user privacy is actually less secure. With traditionally currency, a third party, e.g. a bank, holds all user information, both regarding transactions and personal information. This information is not publicly available. In an open distributed ledger, all transaction information is transparent and publicly available under pseudonyms.

If a pseudonym in open distributed ledger is at first revealed, it can open a forensic trail than can suddenly make an entire financial history public information.\textsuperscript{187} In an immutable ledger this can compromise entire networks, as it will be possible to see who, or at least which addresses, the revealed identity has traded with.\textsuperscript{188} Given that pseudonymous users can be de-anonymised, one can argue that there is always a risk of the identity being exposed. If a person is observed buying something with bitcoin at a store, and the time and amount is known, then it will be possible to find that exact transaction in the public ledger. This could reveal the person’s identity as well as wallet address. With a match of identity and wallet, it will be possible to track other purchases made by that person.

### 4.3 Virtual currency as replacement for cash

Some characteristics cash has is that it offers the possibility of anonymous payment. There is no need for a third party or technology, the settlement is swift and final, it is available to everyone, there is no credit-risk, and it serves as a mandatory payment method. Some of the same characteristics can be used describing virtual currency. Exceptions are that it relies on technology to function, it is not necessarily 100% anonymous, and it does not serve as mandatory payment method in any country. Electronic transactions will also invariably create data, and can thus never be completely untraceable.\textsuperscript{189} On the other hand, virtual currency has the great advantage that it is much easier to transport and store than cash.

\begin{itemize}
  \item \textsuperscript{185} Ibid.
  \item \textsuperscript{186} Kumar, Fischer, Tople et al (2017), p. 17.
  \item \textsuperscript{187} Bohannon (2016).
  \item \textsuperscript{188} Ludwin (2015).
  \item \textsuperscript{189} Nuth (2007), p. 73.
\end{itemize}
Police attorney Richard Beck Pedersen said in an interview with Norwegian paper E24 that “the blockchain technology makes all transactions public, so combined with our investigative material and our methods we have good opportunities to catch criminals who make use of cryptocurrency”. He went on saying: “Personally, I would rather see physical cash disappear than bitcoin”. The Norwegian National Criminal Investigation Service (“Kripos”) have so far made three seizures of virtual currency, and claims that the international trend is that criminals are now moving away from virtual currency and back to traditional cash.

### 4.4 Silk Road as case law example

A criminal caught with a bag of money can be connected to the bag of money. A user of virtual currency caught engaging in illegal activity, can be connected to a whole history of transactions, as all transactions are stored in an immutable ledger. A well-known case where an identity has been revealed in connection to virtual currency, is United States v. Ross Ulbricht. Ulbricht ran the Silk Road website, and was convicted for inter alia money laundering, computer hacking, and conspiracy to traffic narcotics. Silk Road operated using TOR, and all purchases on Silk Road occurred using bitcoin, in an attempt to secure the anonymity of everyone involved. Nevertheless, law enforcement agents were able to track IP-addresses and match Ulbricht’s regular online activity with the pseudonym operating Silk Road. In connection to the investigation, the Government seized 144.336 bitcoins connected to activity found on Ulbricht’s laptop computer. The United States Marshals Service sold the seized bitcoins for more than USD 48 million in 2017.

Ulbricht appealed the judgement in 2016, after being sentenced to imprisonment for life. Ulbricht complained that his rights had been violated, as the surveillance by law enforcement agents of his online activity was in violation with the Fourth Amendment. The Fourth Amendment states that people shall be “secure in their persons, houses, [...] against unreasonable searches and seizures”. The appeal court decided in 2017 that the surveillance of Ulbricht, and extraction of data from his Google and Facebook accounts, did not violate the Fourth Amendment.

---

190 This author’s translation.
191 Hopland (2017).
192 Ibid.
194 United States v. Ulbricht (2017), 858 F.3d 84.
195 Department of Justice (2017).
196 US Const. amend. IV (1791).
197 United States v. Ulbricht (2017), 858 F.3d 105.
4.5 The General Data Protection Regulation (GDPR)

In May 2018, EU’s General Data Protection Regulation (GDPR) is coming into effect. One of the new principles in the regulation is the right to erasure, or more commonly named ‘the right to be forgotten’. This implies the individual’s right to control personal information, as well as erasure of data upon request. ‘Personal data’ means any information relating to an identified or identifiable natural person. The right to be forgotten is applicable for data that has e.g. been collected illegally, or which there is no longer need for.

The right to erasure might be in conflict with the blockchain technology. A blockchain can in principle not be altered since alteration will affect the blockchains credibility. If a blockchain contains information that will be regarded as personal information under the GDPR, the blockchain will not comply by the regulation and be subject for suspensions. A standard transaction with virtual currency in an open distributed ledger is traded pseudonymously. The question is whether trading virtual currency pseudonymously is regarded as identifiable under the GDPR. As shown in para 4.2.1, it is possible to de-anonymise pseudonymous users. Transactions recorded in a closed distributed ledger is connected to a real world identity, see para 4.2.2. Particularly transactions in closed ledgers may conflict with the right to erasure.

Authorities gather a lot of information about the inhabitants in a country, and authorities must comply with the GDPR. Among the data controlled by authorities, is information gathered for tax purposes about the economy of the inhabitants. This will also be applicable for tax data on virtual currency. These data will rarely be covered by the right to be forgotten, since they are neither irrelevant or gathered illegally.

The GDPR lists certain categories of sensitive information in Article 9. This is data that is particularly worthy of protection. Registering such data is prohibited, unless permission is explicitly mentioned in Article 9 (2). Tax data can be classified as confidential ordinary personal data, but they are not included in the list of particularly sensitive information in Article 9. Tax data is worth being protective of, but they are not regarded as offensive to one’s integrity.

---

198 A regulation is a legal act of the European Union that does not require national governments to pass any enabling legislation, as opposed to a directive that needs to be transposed into national law. A regulation is thus directly binding and applicable.

199 GDPR, Article 17.

200 Ibid, Article 4 (1).

201 Ibid, Article 17.

202 Ibid.

5 Tax liability

5.1 Introduction
Whenever virtual currency changes hands, there are tax impacts. Virtual currencies are often stored and traded across borders. The fact that this is also a new technology, adds to the uncertainty of both where the user is tax liable, and what information the taxpayer is supposed to forward to the tax authorities. Official numbers on how much money Norwegians have invested in virtual currencies does not exist. One of the main exchanges, Bitcoins Norway, claim in an ad that they have brokered bitcoins for more than NOK 500 million.\(^{204}\)

This chapter will investigate who has to pay tax according to Norwegian legislation, and what taxes you have to pay when trading virtual currency.

5.2 Taxpayer
As the main rule, any physical person living in Norway is liable to pay tax in Norway, cf. the Tax Act (“skatteloven” - sktl.) § 2-1 (1). Whether you are defined as living in Norway in tax terms depends on the length of your stay. If your stay in Norway exceeds 183 days during a period of 12 months, or 270 days in total during a period of 36 months, you are regarded as a tax resident, cf. sktl. § 2-1 (2). A person defined as a tax resident will be liable to tax in Norway on all global capital and income, cf. sktl. § 2-1 (9).

It is possible to be globally tax liable to more than one country at the same time. In order to avoid double taxation on the same income and capital, Norway has entered into tax treaties with many other countries.\(^ {205}\) The purpose of these tax treaties is to clarify which country is entitled to tax a certain income and capital.

A person not defined as a tax resident in Norway can also be liable to pay tax in Norway, as far as the person has income or capital here, cf. sktl. § 2-3. This will not impose a global tax liability, but rather a limited tax liability, i.e. limited to the income or capital the person has in Norway.

In an internet setting, such as when trading with virtual currency, it can be rather complicated to figure out which country capital is actually stored in, or from where income originates. This as a person can physically operate from one country, use a service in a second country, have the digital files stored in yet another country, and so on. Nevertheless, this issue will not be investigated any further in this thesis. Although it is both relevant and interesting, it will be a

\(^{204}\) Bitcoins Norway (2017), “Meglet bitcoins for over 0,5 milliarder”.

\(^{205}\) Regjeringen (2016), “Skatteavtaler”.

34
far too extensive matter to cover. Said issue is also not unique for virtual currency, but very often relevant for all sorts of digital commerce.

Tax liability for companies domiciled in Norway is regulated in sktl. § 2-2 (1). A company with domicile in Norway has global tax liability, cf. sktl. § 2-2 (6).

Any physical or legal person trading virtual currency, and who has global tax liability to Norway, is according to Norwegian tax law obliged to report about his or her capital and income.206 A person with limited tax liability on the other hand, will have to report only about income and capital with a Norwegian source.

5.3 **Tax object**

There are two possible tax objects when trading with virtual currency; wealth tax and tax on gains and losses. Up until 2017, virtual currency were subject to VAT in Norway. After the Hedqvist judgment, trades with virtual currency are exempt of VAT.207

5.3.1 **Wealth tax**

As a main rule, any asset with economical value is counted as part of your wealth, cf. sktl. § 4-1 (1). According to the Norwegian Tax Administration virtual currency must be seen as an asset with economical value.208 For a tax resident, this value shall count as part of your wealth in the Norwegian tax report, regardless of which country the virtual currency is actually stored in.209 How much virtual currency is worth depends on the market value. What people are willing to pay for virtual currency at any given time can be checked at a digital asset exchange, for example gdax.com.210

The value of virtual currency tends to fluctuate. It is the value on January 1st of the taxable year that goes into your tax return when reporting capital, cf. sktl. § 4-1 (1). The value of virtual currency must be calculated into Norwegian kroner. The Tax Authorities refers to The Central Bank of Norway (“Norges Bank”) for currency conversion. For currencies not listed with Norges Bank, the bank refers to oanda.com.211 Oanda.com lists e.g. bitcoin the same way

---

206 Skatteforvaltningsloven, § 8-2 (1) letter a, cf. § 8-1.
207 Regjeringen (2017).
208 Skatteetaten (2017), “Skattemessige konsekvenser ved bruk av bitcoins”.
209 Ibid.
210 Determining the fair value of a virtual currency can be challenging as there are a number of exchanges, and the value might differ slightly. Nevertheless, the same goes for traditional currencies, so this is probably not much of a practical problem.
211 Skatteetaten (2012).
they do with any other regular currency issued by a nation. As such, calculating the value of virtual currency and filing it in your tax report is not necessarily more complicated than calculating the value of for example dollars or euros. In your tax report the value of virtual currency belongs in post 4.5.4 “Other taxable capital”.212

The practical effect of filling in wealth in your tax report, is to calculate whether you will have to pay wealth tax or not. Your taxable assets, for example real estate, bank deposits, cars, stocks, and virtual currency, are added together. The sum you get from this calculation, with a deduction for any debt, is your net wealth. For 2017, the entry point for wealth tax is set at 1.480.000 NOK.213 Any net wealth above the entry point determines the amount of wealth tax that is payable to your municipality and the state. For 2017, rates are 0.7% to the municipality, and 0.15% to the state.214

5.3.2 Gains and losses
According to the Norwegian Tax Act § 5-1 (2) there is tax liability on capital gains earned from the realisation of property assets. Similarly, losses from realisation are deductible, cf. sktl. § 6-2 (1). This implies that gains from the fact that the value of virtual currency was lower when purchased than when it was sold is taxable income. Losses due to the fact that virtual currency was purchased at a higher price than it was sold is a deductible cost.215

Note that the term ‘realisation’ covers not only a regular sale of virtual currency, but also spending of virtual currency. Every time virtual currency changes hands, a realisation has happened. Spending virtual currency is in tax terms two transactions in one; you are disposing the virtual currency and spending the equivalent amount in NOK. A practical example is if you have bought virtual currency for NOK 50.000 in 2014, and then in 2017 when the price had increased significantly, you used the virtual currency to buy a car for NOK 550.000. The profit of 500.000 will be a taxable gain, even though you never had NOK 500.000 in your account.

Exchanging currency is to be considered a realisation. To be able to buy virtual currency one often have to purchase the currency with dollars. There can be many exchanges taking place before an investment in virtual currency in the end is traded back to NOK. To keep track of all these realisations can be difficult. A possible solution to make this easier could be to adopt a system similar to the share savings account regime introduced in 2016 (valid from the tax year

212 Skatteetaten (2017), “Skattemessige konsekvenser ved bruk av bitcoins”.
2017), where gains and losses are taxed first when they are taken out of the account, cf. sktl. § 10-21 (3) and (4).

Such a system would not come without problems, as this would necessarily be a centralised system and thus a breach with the idea of decentralisation which can said to be part of the core of most virtual currencies. It will also imply that authorities endorse virtual currency, making it more attractive to invest in these currencies. For a number of reasons authorities might not want to do that. Authorities in many countries, including Norway, seem to have taken the position that it is best to wait and see how this evolves, rather than imposing premature regulations. Nevertheless, the current system is that each trade is a realisation, and gains and losses must be calculated separately for each trade.
6 Reporting requirements related to tax

6.1 Introduction

Basis data is the information the Tax Administration uses to pre-complete the tax return, and it is a cornerstone of the agency’s business. Basis data stems largely from reports from third parties, such as employers and financial institutions. The Tax Administration considers that the information received today from these players is of a high quality, and provides a good basis for the pre-complete tax return. Correct third party reporting helps to ensure correct tax assessment with the least possible use of resources. The duty of disclosure imposed on taxpayers and third parties must thus be adapted in such a way that it contributes to acceptance and compliance with tax regulations. This without the taxpayers feeling monitored, while tax authorities must be able to detect and prosecute tax crimes.

This chapter will investigate reporting duties for individuals and third parties, penalties for not reporting correctly, and control mechanisms. An underlying theme is the problem caused by the lack of a third party to report data in relation to virtual currencies.

6.2 The tax object’s duty to report

The tax object’s obligation to report is set in the Tax Administration Act (“skatteforvaltningsloven”) § 8-2 (1) letter a, cf. § 8-1. According to § 8-1 it is the person’s duty to provide correct and complete information, and to notify the Tax Administration in case of any errors. I.e. if you have traded virtual currency, and the tax report does not already include correct information about capital or income stemming from these trades, it is your duty to correct the tax return.

The Tax Administration Act is a consequence of Norway’s agreement with the United States on the automatic exchange of information and implementation of the Foreign Account Tax Compliance Act (FATCA). Updated legislation was also required to implement OECD’s new international standard for the automatic exchange of financial account information in the tax area, known as the Common Reporting Standard (CRS).

Norwegian taxpayers will have to fill in a tax report every year, a report which is based mainly on information sent in by a third party. The tax report is pre-complete with basis data from banks, insurance companies, employers, NAV, and others. Over 70% of taxpayers make no

---

217 Ibid.
218 Skatteetaten (2017), ”Skatteforvaltningshåndboken”, § 7-3.
changes to their tax report, which signals that most people consider the pre-complete information trustworthy and correct.\textsuperscript{219}

Follow-up and control of items without basis data is particularly demanding. It is difficult for the taxpayer to keep track of current regulations and fill in information correct, and mistakes happen more often when information is not pre-complete.\textsuperscript{220} These errors can be both to the taxpayer’s advantage or disadvantage. Although for virtual currency, there is reason to believe that the problem will mainly be lack of information about wealth and gains. Either because the taxpayer is used to information being correctly pre-completed, and thus thinks virtual currency does not belong there, or because they are under the assumption that the controlling agencies will not find out anyway.

NTAES (National Centre of Cross-Agency Analysis and Intelligence) concluded in a recent report, that it is “very likely” that use of virtual currency will be a major challenge when fighting economical crime in the future.\textsuperscript{221} 222 Back in 2012, and to some extent in 2014, the agency concluded differently; that the introduction of virtual currency did not pose a large threat to the Tax Authorities. Mainly because of lack of user acceptance, low trading volume, and relatively low exchange rate.\textsuperscript{223}

There are many different virtual currencies, most of which are technologically created a little differently, making it hard for the police and other agencies to keep up knowledge wise. Even if they acquire knowledge of the currencies, it is hard to gather information about the users behind the transactions.\textsuperscript{224}

A Danish survey from 2011 involving 40,000 individual taxpayers, concluded that the tax evasion rate was close to zero for income subject to third party reporting. On the other hand, it was substantial for self-reported income.\textsuperscript{225} There seem to be no reason to think that the result of such a survey in Norway would be any different.

In order to ensure correct tax, also from virtual currency, it would be preferable to have information from third parties as well as from the tax object itself.

\textsuperscript{219} Dalen (2016), p. 8.
\textsuperscript{220} Ibid, p. 10.
\textsuperscript{221} NTAES (2017), p. 15.
\textsuperscript{222} “Very likely” in this setting means that NTAES considers it to be a certainty of more than 90%. NTAES, p. 18.
\textsuperscript{223} Heggstad (2014).
\textsuperscript{224} NTAES (2017), p. 15.
6.3 The third party's duty to report

§ 7-3 of the Tax Administration Act regulates which financial institutions that are obliged to provide information about financial matters and insurance, and what information they should provide. Among such institutions are banks, insurance companies, mortgage companies, e-money companies, and so forth.

Information about your holdings in Norwegian kroner mainly comes from your bank. A bank has information about the amount you have on your account, as well as how much interest you have received. By comparison, the Tax Administration cannot contact a bank, or a similar institution, to get an overview of someone’s assets in virtual currency. Virtual currency is stored in an electronic wallet. Such wallets are often not held at centralised institutions, the storage thus bearing more similarities to cash storage than a bank account.

Because of the decentralised nature of virtual currency, it is difficult to track down a legal entity obliged by law to report to the Tax Administration. Of the financial institutions listed in § 7-3, an e-money provider has the most obvious similarities with a virtual currency such as bitcoin. E-money companies are obliged to report, but e-money companies must e.g. be organised as a centralised issuer, cf. the Financial Undertakings Act (“finansforetaksloven”) § 2-4. Bitcoin has no centralised issuer of money, and is therefore not within the scope of the definition.

Bitcoin is neither a bank, a mortgage company, or any of the other financial institutions listed in the Tax Administration Act § 7-3. There is simply no organisation from where the Tax Administration can demand a report. As of today, no third party reports are known to be sent to the Norwegian Tax Administration with information about the taxpayer’s involvement in virtual currency.226

Trading with virtual currency is usually done through a digital currency exchange. These exchanges are legal entities that can be required to report, but they are not considered to be covered by today’s legislation.227 If the currency exchanges were to report, the information that could be obtained from them would have some limitations. They do not necessarily store money for their customers, but acts merely as a link between the seller and buyer. They usually charge a fee for this service. The currency exchanges could store information about the

---

227 Ibid.
trades they are involved in, and report about these. This would still give an incomplete insight
to the information that tax objects are obliged to report in their tax report.

It will be easy for traders in virtual currency to use several currency exchanges, also some
based in other countries. Although, the same can be said about bank accounts. It is quite easy
to set up an account in another country, but safety and availability are important features
when people are choosing where to store their money. Most traders will probably use a currency exchange based in their own country. There is little reason to believe that a large number of virtual currency owners will opt for exchanges based abroad mainly for tax evasion reasons, especially if that option seem more insecure and is more difficult to use.

The two main exchanges for virtual currency in Norway, Bitmynt and Bitcoins Norway, have made the following statements on their websites, on what data they provide to the Tax Ad-

ministration and other officials:

“I store as little information about you as possible that can be used for identification, and I continuously delete data I do not need. [...] I do not report data to anyone.”228

“The services that we offer is for the time being not regulated by any specific legislation in Norway. It is your own duty, to report to the tax authorities any information that is relevant for calculation of correct tax and payment of fees.”229 230

Exchanges do not provide third party reports, and they are currently not obliged to do so ei-
ther. The result is that users of virtual currency must try to gather correct information them-
selves. This may prove difficult. Especially as taxpayers are used to tax reports pre-completed by professional parties.

Growth in virtual currencies could imply that the Tax Administration in the future will receive a less complete picture of income and assets. This could reduce the quality of the pre-
complete tax return, increase the possibility of errors, and have consequences for the tax base.231 Differences in reporting obligations for players operating similar businesses can con-
tribute to differences in competitive conditions, and such inequality may weaken the public’s trust in the tax system.

228 Bitmynt (2017).
230 This author’s translations.
6.4 Penalties for violation of the duty to provide correct information

Penalties for breach of the Norwegian tax regulations are listed in chapter 14 of the Tax Administration Act. A taxpayers failure to provide information can result in enforcement fines and additional tax, cf. §§ 14-1 and 14-3. Enforcement fine is a day-to-day compulsion when information is not provided within the deadline, cf. § 14-1 (1). According to (2) the total enforcement fine cannot exceed one million NOK. An additional tax of 20% can be imposed if the taxpayer have had a tax benefit of the incorrect information, cf. § 14-5 (1). For particularly gross violation of the duty to provide correct information, the additional tax may rise even 20 to 40%, cf. § 14-6 (3).

The tax authorities may impose a violation charge on third parties, who do not fulfill their disclosure requirements according to chapter 7, cf. § 14-7. According to § 14-12, a third party required to provide information that gives false or incomplete information to the tax authorities, or fails to provide mandatory information, risk a fine or imprisonment for up to two years.

As of today, these are hypothetical penalties for exchanges of virtual currency, as they are not obliged to report.

6.5 Currency register

Physical or electronic transfers of money in and out of Norway shall be registered in the currency register (“valutaregisteret”). Banks, financial institutions and payment institutions with a license from the Financial Supervisory Authority of Norway (“Finanstilsynet”) must report to the registry, cf. § 4. The register functions as a tool for authorities to control e.g. base data. The purpose is to prevent and combat crime, and to contribute to the proper taxation of taxes, cf. the Foreign Exchange Register Act (“valutaregisterloven”) § 1. Information in the registry is available to e.g. the police and the Tax Administration, cf. § 6. Exchanges of virtual currency are not listed as required to report to the registry. Thus, no information on movements of virtual currency in and out of Norway is registered.

6.6 International cooperation

Reports from third parties have for years been something which stems mainly from national sources, whilst international data have been something that taxpayers must gather and fill in themselves. This is about to change. Head of the Norwegian Tax Administration, Hans Christian Holte, recently made the following statement: “It is important that tax authorities have an international perspective. We need to share knowledge between countries, start using new
methods, collaborate more, share more information, and make use of big data and analysis to get a better overview.”

In the autumn of 2017, OECD introduces the Common Reporting Standard (CRS) as a means of sharing tax data across borders. The CRS calls on jurisdictions to obtain information from their financial institutions, and automatically exchange that information with other jurisdictions on an annual basis. This implies that the Norwegian Tax Administration will receive data on assets Norwegian taxpayers may have abroad, as well as data on payments connected to these assets. Initially, these data will be used as a control mechanism, and not as part of the pre-complete tax return. As of November 2017, 96 jurisdictions have signed the agreement. This includes major players such as Japan, Russia, United Kingdom, and Germany, but also jurisdictions that have been more reluctant to exchange tax data, such as Switzerland, Luxembourg, Bermuda, and the Cayman Islands. As 2017 is the first year that CRS is in effect, the quality of the reported data is yet uncertain. International reporting will not help if the reporting body does not have relevant data of a certain quality related to the taxpayer and the tax object.

The problem in relation to virtual currencies is that CRS information will usually not contain data on virtual currency assets. Few exchanges are reporting to tax authorities, and if they do, there is a fair chance that they do not have a complete picture of their customer’s assets. As CRS is supposed to leave fewer options as to where it is possible to hide money from taxation, CRS might make it even more tempting to hide money using virtual currencies.

---

233 This author’s translation.
236 OECD (2017), “Signatories of the CRS”.
237 Exchange of data with the US is already in place through FATCA.
7 Reporting requirements related to Anti-Money Laundering (AML) and Countering the Financing of Terrorism (CFT)

7.1 Introduction

The purpose of money laundering is to hide the origin of profit from criminal activity. Money that has been successfully laundered can be integrated into the regular economy, appearing as legitimate. Terror financing is contributing to a terrorist act, or involvement in the maintenance of a terrorist organisation. Crimes related to money laundering and terror financing are perceived as so serious and harmful to society, that it justifies a more comprehensive reporting and surveillance regime. In the world of virtual currency, exchange services control the main body of data.

This chapter will investigate whether legislation is in place to go after these exchanges for AML/CFT purposes.

7.2 Norway

In Norway, a number of financial institutions are listed as required to comply with certain reporting requirements, cf. the Money Laundering Act (“hvitvaskingsloven”) § 4. The list is exhaustive, and exchanges of virtual currency are not included. The law requires the institutions listed under § 4 to register the identity of their customers, cf. § 8. An institution is required to report if it suspects that a transaction is connected to proceeds of criminal offence, or terrorist activity, and further assessment has not disproved the suspicion, cf. §18, cf. § 17. Such a transaction shall be reported to the Norwegian National Authority for Investigation and Prosecution of Economic and Environmental Crime (“Økokrim”), cf. § 18.

7.3 EU

The Norwegian Money Laundering Act is an implementation of the EU Directive on Anti-Money Laundering. The current Directive does not explicitly mention virtual currencies. The European Banking Authority (EBA) has recommended that EU legislators consider declaring exchanges of virtual currencies, to become ‘obliged entities’ under the Directive. Such change in legislation will make these exchanges subject to AML and CFT requirements. In a current proposal for changes to the 4th Anti-Money Laundering Directive, it is suggested that exchange services between virtual currencies and traditional money, so-called wallet-providers, will have to report as set forth in the Directive. Nevertheless, a problem is that

---

238 Finanstilsynet (2016).
239 Straffeloven, § 135.
240 Kaiser (2016), 211.
these exchanges do not always have detailed data on their customers, see para 3.4.2. It is thus uncertain how this will be carried out practically, and whether it will have the desired effect.243

7.4 Other countries
In 2017, China, Japan, and Australia have regulated virtual currency, requiring exchanges in these countries to comply with regulatory requirements.244 Exchanges in Australia will be brought under the remit of the Australian Transactions and Reporting Analysis Centre (AUSTRAC). AUSTRAC aims to prevent, detect, and disrupt money laundering, terrorism financing, and other threats to the Australian economy.245

In the US the only significant regulation of virtual currency on a federal level, is related to anti-money laundering.246 In March 2013 a compliance guidance was issued by the Department of Treasury’s Financial Crimes Enforcement Network (FinCEN). Exchangers and administrators of virtual currency are required to register and implement AML programs.

On a state level, several states have passed laws or regulations focusing on virtual currencies, requiring exchangers to be licensed. One example is New York. In New York consumers do not need a license to trade with virtual currencies, but anyone involved as a business must register and obtain a BitLicense.247

Financial Action Task Force (FATF) have issued a report outlining potential risks posed by virtual currencies for the AML/CFT area.248 FATF is an independent inter-governmental body whom Recommendations are recognized as the global AML and CFT standard.249 Virtual currencies can be designed with a high degree of anonymity, where sender and recipient are not adequately identified.250 Historical record of transactions are not necessarily associated with a real world identity, but rather an IP-address. In addition, virtual currencies commonly rely on complex infrastructures that involve several entities, often spread across several countries, to transfer funds or execute payments. This segmentation of services means that responsibility for AML/CFT compliance and supervision/enforcement may be unclear. Customer

244 Graham (2017).
245 AUSTRAC (2017).
247 New York State Department of Financial Services (2017).
248 FATF (2014).
249 Ibid.
250 Ibid, pp. 9-10.
and transaction records might be held by different entities, often in different jurisdictions, making it more difficult for law enforcement and regulators to access them. Components of a virtual currency system might be located in jurisdictions that do not have adequate AML/CFT controls.

A major problem for law enforcement is that they cannot target one central location or entity for investigative or asset seizure purposes. Authorities are left with the possibility of targeting individual exchangers for client information that the exchanger may collect.\textsuperscript{251}

### 7.5 Enforcing AML and CFT regulations

Payment systems such as Visa, Mastercard, Paypal et al shut down payments to WikiLeaks in 2010.\textsuperscript{252} Neither the companies nor US authorities have confirmed that this was a result of decisions made by authorities, but the companies have stated that they were afraid of breaking US legislation if funds were transferred to anyone running an illegal business. Politicians such as Senate Minority Leader at that time, Mitch McConnell, have branded WikiLeaks founder Julian Assange a terrorist.\textsuperscript{253} Congressman Peter King said WikiLeaks should be designated “Foreign Terrorist Organisation”, which would result in funds to be frozen and support made a federal crime.\textsuperscript{254} When enforcing AML and CFT regulations it is a problem to determine exactly who is a terrorist organisation. One man’s terrorist is another man’s freedom fighter. WikiLeaks have received much of its donations in bitcoin since then, and according to Assange the rising value has resulted in a 50,000\% return for WikiLeaks.\textsuperscript{255}

In 2017, FinCEN took enforcement action against the virtual currency exchange BTC-e. A civil money penalty of USD 110 million was assessed, for willfully violating US anti-money laundering laws.\textsuperscript{256} According to FinCEN, BTC-e did not obtain the required information from their customers, and instead of acting to prevent money launderers, they embraced the pervasive criminal activity conducted at the exchange. BTC-e was accused of processing 300,000 of the bitcoins stolen from Mt. Gox, as well as at least USD 3 million of facilitated transactions tied to ransomware attacks such as “Cryptoclocker” and “Locky”.\textsuperscript{257}

\textsuperscript{251} Ibid, p. 10.
\textsuperscript{252} Greenberg (2010).
\textsuperscript{253} Ibid.
\textsuperscript{254} McCullagh (2010).
\textsuperscript{255} Assange (2017).
\textsuperscript{256} FinCEN (2017).
\textsuperscript{257} BitLegal (2017).
BTC-e is not based in the US, but conducted transactions that included funds sent from customers in the US to recipients who were also located within the US. Regardless of geographic location, the company was required to comply with US AML laws. Jamal El-Hindi, Acting Director for FinCEN, stated that FinCEN “will work with foreign counterparts across the globe to appropriately oversee virtual currency exchangers and administrators who attempt to subvert US law and avoid complying with US AML safeguards”.

The BTC-e case is an indication that US authorities are prepared to go after currency exchangers regardless of which jurisdiction they are based in. This implies that to hide large amounts of money in virtual currency that are stemming from criminal activity, or assets that can be linked to terrorist organisations, is a rather risky business. On the other hand, the number of cases where state authorities have taken enforcement action against owners, exchangers, or others involved in virtual currency is currently low. These cases also have a tendency to involve large sums of money.
8 Conclusion

While virtual currencies themselves might be able to exist outside regulatory structures, they will usually have to touch the real world if assets are to be realised. The bridges between a virtual currency and the real world are subject to existing regulation. Exchanges and payment services can be instructed to register as money transfer services, with the consequence that they will have to comply with regulations for registration and reporting.

Studies have shown that users of virtual currencies can be de-anonymised. As of today, the number of actual examples are few, but it is possible to reveal the real world identity behind transactions in virtual currency. However, it requires sufficient resources to be set aside for active investigation. Cases which involves large sums of money, and relates to AML or CFT violations, may be perceived as so serious and harmful to society that such action is justified.

State regulations based on passive information gathering, such as taxation, is a problem yet to be solved. Tax is dependent on an effective system of third party information to function in a cost effective way. It is difficult to see how a decentralised system, with no third party, can ever provide reliable information in regard to tax.

To regulate virtual currency is a difficult balancing act between providing innovators with regulatory clarity and certainty, and avoiding restrictive regulations that can stifle innovation. The Norwegian and Swedish attempts to impose VAT on virtual currency is one example of mismanaged regulation. Nevertheless, increased legislative action seem likely. The large sums involved implies that virtual currency cannot be ignored by legislators.

The problem is the lack of full-bodied solutions. What seem to be on the way is that exchanges are required to register and acquire a license, as well as impose systems for AML and KYC. If this is the future of virtual currencies, it will mark a breach with much of the pseudonymity and decentralisation that virtual currencies have enjoyed so far. In this way, the system will quickly resemble today’s banks. Hopefully the blockchain technology will at least provide banks, old or new, with a cheaper and more efficient system for registering, storing and processing data.
Table of reference

Norwegian Legislation, Regulations, and Judgments

1814 Lov av 17. mai 1814 Kongeriket Norges Grunnlov (Grunnloven)

1961 Lov om opphavsrett til åndsverk mv. (åndsverkloven)


1999 Lov av 26. mars 1999 om skatt av formue og inntekt (skatteloven – sktl.)

1999 Lov av 25. juni 1999 om finansavtaler og finansoppdrag (finansavtaleloven)

2004 Lov av 28. mai 2004 om register over opplysninger om valutaveksling og overføring av betalingsmidler inn og ut av Norge (valutaregisterloven)

2005 Lov av 20. mai 2005 om straff (straffeloven)

2009 Lov av 03. juni 2009 om tiltak mot hvitvasking og terrorfinansiering mv. (hvitvaskingsloven – hvvl.)

2015 Lov av 10. april 2015 om finansforetak og finanskonsern (finansforetaksloven)

2017 Lov av 27. mai 2016 om skatteforvaltning (skatteforvaltningsloven)


International Conventions, Directives, and Judgments

Case C-264/14 Skattverket v. David Hedqvist, 22 October 2015


Regulation 2016/679/EU on the protection of natural persons with regard to the processing of personal data and on the free movement of such data, and repealing Directive 95/46/EC (General Data Protection Regulation - GDPR)

**Foreign (National) Legislation and Judgments**


Act to amend the Federal Deposit Insurance Act to require insured banks to maintain certain records, to require that certain transactions in U.S. currency be reported to the Department of the Treasury, and for other purposes 1970 (Bank Secrecy Act) URL: [https://www.gpo.gov/fdsys/pkg/STATUTE-84/pdf/STATUTE-84-Pg1114-2.pdf](https://www.gpo.gov/fdsys/pkg/STATUTE-84/pdf/STATUTE-84-Pg1114-2.pdf) [Retrieved: 4th of October 2017]


Books and Articles


Reports and Guidelines from Public Institutions and International Bodies


Henriksen, Torhild, Geir Teigland, Nonna Kuznechikov Risnes, and Inger Marie Lindberg, “Digitalisert økonomi – gamle problemer i ny innpakning”, in Analysenytt, No 2, Skatteetaten


Newspaper Articles


Dahl, Carl Alfred, “Lotteritilsynet vil delta på møte om den omstridte nettvalutaen onecoin”, *Aftenposten*, 24th of February 2017. URL:


Imbert, Fred, “JPMorgan CEO Jamie Dimon says bitcoin is a ‘fraud’ that will eventually blow up”, CNBC, 12th of September 2017. URL: https://www.cnbc.com/2017/09/12/jpmorgan-ceo-
jamie-dimon-raises-flag-on-trading-revenue-sees-20-percent-fall-for-the-third-quarter.html
[Retrieved: 2\textsuperscript{nd} of October 2017]

Kharpal, Arjun “Bitcoin correction sees nearly $4 billion wiped off value of the cryptocurrency as price falls 19\%”, CNBC, 29\textsuperscript{th} of May 2017. URL: http://www.cnbc.com/2017/05/29/bitcoin-correction-price-value.html [Retrieved: 29\textsuperscript{th} of May 2017]


Lee, Timothy, “12 questions about Bitcoin you were too embarrassed to ask”, Washington Post, 19\textsuperscript{th} of November 2013. URL: https://www.washingtonpost.com/news/the-switch/wp/2013/11/19/12-questions-you-were-too-embarrassed-to-ask-about-bitcoin/?utm_term=.53fe1fa67900 [Retrieved: 10\textsuperscript{th} of November 2017]

Lerner, Sergio, “Is there a better Scaling Solution than SegWit?”, CryptoNews, 17\textsuperscript{th} of March 2017. URL: https://www.cryptonews.net/a-better-scaling-solution-than-segwit/ [Retrieved: 2\textsuperscript{nd} of November 2017]

Ludwin, Adam, “How Anonymous is Bitcoin?”, Coincenter, 20\textsuperscript{th} of January 2015. URL: https://coincenter.org/entry/how-anonymous-is-bitcoin [Retrieved: 23\textsuperscript{rd} of November 2017]

Lunde, Anders, “En molotovcocktail til bankene”, Morgenbladet, 12\textsuperscript{th} May 2017. URL: https://morgenbladet.no/aktuelt/2017/05/en-molotovcocktail-til-bankene [Retrieved: 8\textsuperscript{th} of November 2017]

Madeira, Antonio, “Bitcoin is Still Illegal in These 6 Countries”, Bitcoinst, 18\textsuperscript{th} of May 2017. URL: http://bitcoinist.com/bitcoin-still-illegal-six-countries/ [Retrieved: 11\textsuperscript{th} of November 2017]

Malmo, Christopher, “A Single Bitcoin Transaction Takes Thousands of Times More Energy Than a Credit Card Swipe”, Vice, 7\textsuperscript{th} of March 2017. URL:


**Web Sources**


Olsen, Kai A., “Norge blir kontantfritt”, NHO Reiseliv, 2017. URL: https://www.nhoreiseliv.no/contentassets/e20bc1fbc8454fa9bbbf59a0a8050066/norge-blir-kontantfritt.pdf [Retrieved: 7<sup>th</sup> of November 2017]

