

A Game of Coins: The Digitization of Money and the Regulation of Virtual Currencies

Nassiba Idebdou

Supervisor: Professor Patrick Leblond

Graduate School of Public and International Affairs



July 23, 2015

Abstract

This paper seeks to analyze the impact of virtual currencies on the financial system and reviews the risks and opportunities of an emerging payment technology by focusing on a major crypto-currency, Bitcoin. Through an overview of the properties of money, linkages are established between existing traditional monetary and financial frameworks to define the role of virtual currencies in today's financial system. This paper outlines the recent regulatory developments in Canada, the United States and the European Union to mitigate the risks of virtual currencies for the public and the private sectors and to better understand how virtual currency technology can respond to the needs of a growing digital financial system. In a globally connected economy, crypto-currencies should not be only seen as a disruptive to the traditional banking system, but rather as technology used to facilitate the transport and exchange of money between the physical and digital worlds. Virtual currencies are certainly the future of financial innovation, and could prove to be a game-changer in payment technologies in the years to come.

Keywords: Virtual Currencies, Bitcoin, Crypto-currencies, Financial Regulation, Digital Money, Finance 2.0, Digitization of Money, Virtual Currency Schemes, AML, P2P, Virtual Currency Exchange Hubs

Acronyms

AMF	Autorité des Marchés Financiers
AML	Anti-Money Laundering
ATM	Automated Teller Machine
BaFin	Bundesanstalt für Finanzdienstleistungsaufsicht (Germany)
BTC	Unit used to designate Bitcoin (฿)
BSA	Bank Secrecy Act
CHF	Swiss Franc
CRA	Canada Revenue Agency
ECB	European Central Bank
EBA	European Banking Authority
EBA	Euro Banking Association
EUR	Euro
FATF	Financial Action Task Force
FinCEN	U.S. Financial Crime Enforcement Network
FINTRAC	Financial Transactions and Reports Analysis Centre of Canada
GBP	British Pound
IMF	International Monetary Fund
IRS	Internal Revenue Service
KWG	German Banking Act (Kreditwesengesetz)
MBS	Money Business Services
MTA	Money Transmitters Act
P2P	Peer-to-peer network
PCMLTFA	Proceeds of Crime (Money Laundering) and Terrorist Financing Act
PEP	Politically Exposed Person
USD	United States Dollar
VAT	Value-Added Tax
VCS	Virtual Currency Schemes
XBT	Another acronym used for Bitcoin
ZAG	Payment Services Supervision Act (Zahlungsdiensteaufsichtsgesetz)

Table of Contents

Acronyms	3
Introduction	6
Chapter 1: From Coins to Bitcoin, What is Money?	13
1.1 Properties of Money	13
1.1.1 Fiat Money	16
1.1.2 Private Money	17
1.2 Applying the Money Supply Framework to Virtual Currencies	18
1.2.1 Money Supply and Monetary Aggregates	19
1.2.2 Virtual Money as M1 and M2: Using a PayPal Account	20
Table 1: Money Supply – Examples of Monetary Aggregates	21
1.2.3 Two Sides of the Bitcoin: Money or Near Money?	22
1.2.3.1 Bitcoin as Complementary Money	25
Table 2: Monetary Aggregates – Where Could Bitcoin Fit?	28
Chapter 2: A Bit of Change, in Bitcoin?	30
2.1 Literature Review	30
Table 3: VCS Ecosystem	37
2.2 Virtual Currencies	39
2.2.1 Decentralized Virtual Currency Schemes	39
2.2.2 Data and Figures on Virtual Currency Schemes	42
Table 4: Virtual Currencies by Market Capitalization	43
Table 5: Bitcoin Top 10 Trading Platforms by Volume	44
2.3 Trading Up A Coin for Money: Bitcoin	45
2.4 Mastering the Coins: Risks and Advantages of Bitcoin	48
2.4.1 Advantages: A Positive Outlook on Bitcoin Technology	48
2.4.1.1 Anonymity	48
2.4.1.2 A Low-cost Solution	49
2.4.1.3 Usability	50
2.4.1.4 Transportability and Global Reach	51
2.4.2 Bitcoin Risks	52
2.4.2.1 Network Vulnerability	52
2.4.2.2 Hacking, Theft and Fraud	53
2.4.2.3 Volatility and Lack of Funds	55
Chapter 3: Virtual Currencies Regulation, A Must?	57
3.1 The Dark Side of Virtual Currencies	57
3.1.1 Tax Evasion, Profit Shifting and Illegal Activities	58
3.1.1.1 Tax Evasion and Profit Shifting Havens	59
3.1.1.2 Money Laundering and Illegal Activities	60
3.2 Why Regulation Matters	63
3.2.1 FATF: Global Governance and Oversight of Digital Currency	64

3.3 Developments in Regulation	65
3.3.1 Canada	67
3.3.1.1 FINTRAC	69
3.3.1.2 Canada Revenue Agency	69
3.3.1.3 Financial Consumer Agency of Canada	70
3.3.1.4 Québec and the Autorité des Marchés Financiers	70
3.3.2 United States	72
3.3.2.1 FinCEN	75
3.3.2.2 BitLicense and Money Transmitters	77
3.3.2.3 Paying the Government in Bitcoin: Utah, New Hampshire and New York	81
3.3.2.4 Internal Revenue Service	81
3.3.2.5 The U.S. Federal Reserve	82
3.3.2.6 The Security Exchange Commission	83
3.3.3 European Union	85
3.3.3.1 EU Rulings	85
3.3.3.2 Value-Added Tax: The Virtual Currency Tax Puzzle in the EU	91
Chapter 4: Bitcoin, A Game-changing Technology	97
4.1 Globally Connected Economy: Can Virtual Currencies Disrupt the Traditional Banking System?	98
4.1.1 The decline of banking and the pressure of virtual currencies	98
4.1.2 Joining Forces: Banking and Virtual Currency Technology	101
4.2 The Innovative Potential of Bitcoin	103
Conclusion	106
Annex I	109
Figure 1: How the Bitcoin network works	109
Annex II	110
Figure 2: Bitcoin activity vs. other payment networks (2013)	110
Annex III	111
Figure 3: Four Categories of Crypto-technologies	111
Bibliography	112

Introduction

In the 1990s, a spur in payment technology innovation allowed electronic money (or e-money) to first make its appearance in both Europe and North America. The creation of PayPal, in 1998,¹ was only the beginning of a dramatic shift in the payments system landscape. The slower evolution of technologies offered limited options to consumers and developers alike, and, as a result, there was much room to increase functionality and ease of access to more modern internet-based financial technology services. In part, this can be attributed to the demands of a growing globalized market requiring technology with minimal transaction costs, unlike traditional market players (such as Visa, MasterCard and MoneyGram), and having the ability to transfer money almost instantly. The creation of closed-loop currencies – for example, to exchange airline miles and points for goods, such as gift cards as part of a customer rewards program (i.e. frequent flyer points or credit card loyalty points) – can be seen as one of the predecessors of virtual currencies which paved the way to a phenomenon that has grown exponentially in the last 20 years: the digitization of money.² However, in recent years, the inception of a decentralized design of open loop currencies such as Bitcoin – that can be used in various locations and converted into cash – has yielded a system that is borderless, where virtual currency can be traded for *real* money, and which offers an additional layer of privacy and payment flexibility when compared to other systems. Virtual currencies, as it will be discussed in

¹ PayPal is a system that allows consumers or businesses to send, receive and accept money or payments via an encrypted and secure anti-fraud system. See <https://www.paypal-media.com/ca/about>

² Money is no longer a physical object; new payment technologies including PayPal and Interac for example have expanded the use of money to the digital sphere. The transition towards digitized money can be seen through the use of, but are not limited to, plastic credit/debit cards, or through mobile payment technology such as Apple Pay (see <https://www.apple.com/apple-pay/>).

this paper, are blurring the lines between the expansion of virtual currency in the traditional system³ and the digitization of money outside of the Internet. A central theme in this work, crypto-currencies,⁴ and in particular Bitcoin, will be explored in an effort to better understand under which conditions this new technology represents an ambitious alternative to the traditional monetary system. This paper will therefore attempt to answer the following three questions:

- 1) With a continuously evolving global payments system, what does the emergence of virtual currencies mean for the traditional banking system?
- 2) What are the risks and opportunities of virtual currencies for the banking and payments system, consumers, the broader financial system and policymakers?
- 3) How should virtual currencies be regulated and how are they currently governed?

The first chapter of this paper will offer a brief overview of the properties of money and outline the differences between fiat money and private money. In addition, a section of the chapter will attempt to define virtual currencies using the money supply and complementary money frameworks and to establish what value virtual currencies could hold if their value is interpreted using an existing money measurement structure.

³ A system that encompasses entities such as financial institutions, banking institutions, central banks and markets and where the transfer of money (in electronic or physical form), via an instrument or platform, and allowing for transactions, is accepted as a form of payment between investors and borrowers. Other stakeholders interact with the traditional financial system including governments, households, businesses and other entities. See <http://www.bankofcanada.ca/core-functions/financial-system/> and <http://www.imf.org/external/np/exr/facts/banking.htm>

⁴ Crypto-currencies interact with the financial system because they are used as a form of payment for goods and services within the real economy or are exchanged for real currency. As stated by the ECB they are “relevant in several areas of the financial system and are therefore of interest to central banks” (ECB, 2012, p.6).

The second chapter explores the risks and advantages of the virtual currency industry and focuses on the Bitcoin network. The first part looks at the virtual currencies ecosystem and seeks to differentiate the various attributes of the system, namely virtual currency schemes, the virtual currency market, as well as recent innovation in the monetary transaction aspects of digital currencies (e.g. exchange hubs, vaults, wallets). The second part explains the mechanics of Bitcoin and its network, and how the transaction digital infrastructure works within Bitcoin. The last part explores the risks and advantages of Bitcoin, as a mainstream currency and as the first crypto-currency to pose a challenge and provide innovative alternatives to the traditional banking system.

What is more, government regulators and authorities have taken stringent steps to propose a regulatory framework to effectively deal with virtual currencies. Many concerns have been raised in the last four years given the unstable payment system architecture of the virtual currency industry. In this regard, the main areas of concern that will be addressed in this paper are: market stability, consumer protection and law enforcement (CSBS, 2014). Thus far, only Canada, the United States and certain European countries have taken a stand to control and monitor virtual currencies, while most countries in the world do not have the capacity to delineate and adopt measures to protect their payments ecosystem and ensure crypto-currencies are *de facto* not a threat to the financial system's stability. The regulation of activities-based services within the virtual currency industry is another component that regulators and government institutions need to address, including the transmission, exchanges and third-party exchanges, and transmitting services (CSBS, 2014). Specifically, the third chapter first examines the consequences of an integrated decentralized structure, that of virtual

currencies, and applying traditional legislation by interpreting existing laws and regulations to a digital and borderless system. This paper looks specifically at Bitcoin to outline how the usage of crypto-currencies to circumvent the traditional regulatory framework and the risks of illegal activities can consequently lead to an increase in vulnerabilities and threats within and outside the virtual currency industry. The second part of the third chapter presents new developments in law enforcement and regulation of virtual currencies. A growing number of government authorities and regulators have shown interest in adopting legislation to mitigate the risks of virtual currencies and supporting digital currency innovation. This paper analyses the different steps sovereign nations are taking to foster a cooperative environment with the various stakeholders of the traditional system to anticipate and better address the digital currency phenomenon. The idea of a global governance oversight of virtual currencies will also be explored to deal with virtual currencies as governments and global institutions are taking steps to better understand the relationship linking digital currency with real currency in the modern economy.

The fourth and last chapter of this paper explores the reasons why the decline of traditional banking has sequentially increased the needs of consumers and markets alike to transition towards a system through which transactions occur over the Internet. The transportability of fiat money via virtual currency and its convertibility have shifted the modern economy towards a system where these new monetary units are not simply performing traditional functions, such as legal tender, but have dramatically shifted how consumers and markets are starting to value and account for money. The concept of currency, and that of traditional banking, is being challenged by the fact that government

and financial institutions, since the financial crisis of 2008-2009, are no longer the only trusted sources through which money is engineered or transmitted. Virtual currencies offer a new form of virtual money that can viably operate in a global market plagued by the complexity of a traditional banking system in dire need of change. In part, the decline of the traditional banking system came with the emergence of new technologies that do not rely on physical entities and standardized institutions to meet the economic needs of the 21st century. The second and last part of the final chapter looks at the relationship between virtual currency businesses and traditional banks through a case study focusing on Wall Street and U.S. banks.

This analysis is also complemented by focusing on a particular aspect of virtual currency innovation, blockchain technology, which will ensure the long-term sustainability of the innovation in the payments system and a first step to bring financial markets up to speed with digital finance. As such, this paper examines NASDAQ's plan to test blockchain ledgers to compute trading shares transactions and activities to complete deals on the securities exchange markets (Stafford, 2015), and reduce settlement times by relying on a distributed ledger technology that is decentralized rather than relaying transaction information through a traditional clearing payments system. Equally, the last section will briefly review the initiative of governments and regulation authorities to explore the creation of structures to support virtual currency technology.

This paper offers concluding observations with regards to the ramifications of virtual currencies for consumers, businesses, banking and financial institutions, and law enforcement institutions as the traditional banking system, with the advent of virtual

currency technology, is looking to revamp its infrastructure. As a result, in the next years, virtual currencies will have to remain on the radar of governance institutions and policymakers.

As is the case with any thesis paper, there are limitations that should be underlined and consequently, limited the scope of the research conducted. The field of virtual currency and digital finance is in constant evolution, and as such, academic research and literature remains limited on the subject. In that regard, it should also be noted that new evidence is published everyday, and that publications and consultations, as well as adoptions of new legislations are work in progress, as is the case in the three jurisdictions studied for the purpose of this paper.

The study of virtual currencies despite being relatively new is quite exhaustive, and as such, this paper limited the scope of research for the purpose of a thesis at the M.A. level. This research contributes to the literature by offering a review of the history of virtual currencies and the existing literature from the 1990s to 2015, and by thoroughly analyzing the developments in regulation in three jurisdictions that have been forerunners in the development of legislation impacting on virtual currencies; Canada, the United States, and the European Union.

Additionally, given the complexity of analyzing all the work completed so far in every country globally, the case studies for each jurisdiction focused on provinces, states and member states that have completed extensive groundwork on the matter or officially ratified legislation. Moreover, the analysis conducted put the emphasis on the specific

risks and benefits of virtual currencies that stem from the various risks and advantages of dealing with virtual currencies stated by government regulators, financial institutions and Bitcoin-related publications as well as academic literature. Those studied more carefully in this paper capture the way in which virtual currencies affect the payment structure and both the users and administrators of the network.

Lastly, this paper aims to contribute to the analytical review of the implications of virtual currencies beyond their risks and benefits by presenting an argument on the decline of banking and the pressure of virtual currencies. Despite the literature focusing on the decline of the banking system, this paper identifies linkages between the potential of virtual currency technology and the opportunity for the banking system to bridge the regulatory and technological gap between the financial system and new payment technologies and services in the future.

Chapter 1: From Coins to Bitcoin, What is Money?

Over the last few centuries, the definition of money has varied, serving in its oldest form as commodity traded as a form of acceptable payment for other goods and services in a bartering system, and later on evolving to the silver and gold coins system. Indeed, the progression of money over time brings us to scope the definition of money in the modern economy. For the purpose of this paper, this will be done by looking at the functions of money and the definition of private and fiat money as *prima facie* in understanding the linkages and differences between traditional and virtual currency.

1.1 Properties of Money

In today's modern economy, money in the form of currency takes the form of bank notes, coins and deposits at banks and other non-banking financial institutions. The transition from a barter system to a sustainable banking system has facilitated the use of money in any type of economic transaction, whether physical (e.g. physical – at a bank branch or digital – online). Money in this context is discussed by defining its three characteristics and the functions society has attributed to it in part because it does not have a predetermined form or shape. The IMF defines money as “the sum of financial instruments held by money-holding sectors⁵ that are a medium of exchange widely used in an economy, or close substitutes for the medium of exchange that are reliable store of value” (IMF, 2000, pp.59-60).

⁵ Money holders include: nonfinancial corporations, households, OFCs, state and local governments and non-profit institutions serving households (IMF, 2000, p.63).

These functions are important to define as the following chapter explores virtual currencies through these principles. In broader terms, money in its traditional form is an asset that is accepted in lieu of payments for goods or services, or for settling debt (Bank of Canada, 2012).

Store of Value

Money is what enables actors within the financial system to have purchasing power (i.e. make payments for goods or services). In other terms, money facilitates the accumulation of wealth or assets (i.e. savings) as well as the deferment of the payment for goods and services received (i.e. indebtedness) (Bank of Canada, 2012).

Unit of Account

Money allows for a standardized approach to quantify any type of asset, good or service. As a unit of measurement, it gives us the capacity to denominate and compare prices over time. In principle, the value of a payment or an asset can be specified because the same unit of account is used on both sides of a transaction between two actors. In the modern economy, sovereign nations have established their respective currencies and, as such, the unit of account concept is often interchanged with the function of medium of exchange. However, as it is highlighted in this work, the presence of a new competitive currency that is not issued by central governments has “blurred the lines between the specified price of a unit and the medium through which a payment is made for that unit” (White, 1984, p.699).

Medium of Exchange

Money is used as a medium of exchange, *ceteris paribus*, to engage in a transaction to settle debt or acquire (e.g. pay for) an asset/good/service. The confidence of the actors engaging in such a transaction activity is a key element for the exchange mechanism to work (Bank of Canada, 2012). The medium of exchange has been the alternative to a system of interchange known as the barter system, where transactions are facilitated by the transportability and ease of access of currency, or fiat money.⁶ Methods of exchange have evolved to reduce the use of bank notes and precious metals; they include mediums⁷ such as the cheque and clearing system⁸, credit/debit/prepaid cards, foreign banknotes and an international clearing system (Stanley, 1876, p.18). With the advent of virtual currencies, new methods of exchanges have emerged to transfer digital money and avoid the use of a more traditional unit of account such as fiat money or commodity money.

Standard of Deferred Payment

Money also has the function to serve as legal tender⁹ to settle debts incurred. Because it also serves as a unit of account, money is used as a unit to denominate debt. As the intrinsic value of money (its actual value as opposed to its market value or the strength of

⁶ This term is explained in subsection 1.1.1 of this chapter.

⁷ Other mediums of exchange also exist. See additional examples, https://en.bitcoin.it/wiki/Payment_methods

⁸ The clearing and settlement system combines the two steps through which payments are validated. Clearing is the “process of transmitting, reconciling and/or confirming payment orders prior to settlement” and a settlement is “the release of payment obligations between two or more parties by transferring funds between them” (Bank of Canada. See <http://www.bankofcanada.ca/core-functions/financial-system/canadas-major-payments-systems/>).

⁹ Legal tender is a medium of exchange or payment recognized by a legal system to be a valid form of payment or to settle debt. While the definition varies from jurisdiction to jurisdiction, banknotes and coins are the most common form of legal tender in countries across the world. Money as legal tender is normally issued by government institutions such as the central bank and issued under a legislative act (e.g. the Bank of Canada and the *Royal Canadian Mint Act* in Canada).

the issuing country's economy) does not depreciate over time, its function as a standard of deferred payment allows actors engaging in a transaction to establish a contract for future disbursements (Croushore, 2006, pp.51-52). The standard of deferred payment is distinct from the unit of account function, which applies when the unit of a commodity is equivalent to the unit of the same commodity; what is defined as fungibility.¹⁰ It does not however refer to the exchange of one commodity for another commodity that is different than the initial one (Ibid). As such, the standard of deferred payment refers to the accepted way of settling debt; it serves as a benchmark to denominate debt incurred at a present time but that will be paid in the future.

1.1.1 Fiat Money

Fiat money is the most widely trusted medium of exchange and unit of account in today's modern economy. In the 16th century and up until the 1930s, sovereign countries traditionally linked the value of money to a commodity, with gold and silver being the most popular. Given the limited supply of commodities, this link placed a limit on how much money could circulate (McLeay et al., 2014, pp.6-7). Fiat money can be defined as money that is considered legal tender through government legislation, for example paper money or coins, but is not backed by a physical commodity such as gold or a precious metal (Rolnick, Weber, 1997, p.1309). The value of fiat money is derived from supply and demand (and therefore subject to inflation and deflation) and is used as an accepted form of payment but is inconvertible. Fiat money, however, does not only play a key role in the money supply system as a form of legal tender, but also as a currency backed by

¹⁰ See <http://www.investopedia.com/terms/f/fungibility.asp>

the state it belongs to, for example the British pound for the United Kingdom. Contrary to other forms of currency, people intrinsically value banknotes and coins (as one of the main forms of fiat money), and understand that the money they hold, whether it is a Swedish krona, a Canadian dollar or a Chinese renminbi, will, all things being equal, keep the same value over time (McLeay et al., 2014, p.10). Along the same lines, bank deposits held virtually at banking institutions, such as checking and savings accounts, can be seen as the new way through which people receive and make payments. This can be seen as the digitization of fiat money, because it continues to perform the three functions of physical fiat money in the cyberspace. However, it is not the digital banking account for example that would be considered legal tender, but rather the value attached to the account itself. As such, the money in the account is simply recorded electronically on a plastic card or a virtual bank account to facilitate transfers and payments.

1.1.2 Private Money

Dowd (2014) describes private money as a form of tender unrestricted by a legal framework and that is accepted as a medium of exchange or payment (p. xiii). Private money only works if accepted by the individuals that engage in transactions activities and accept such monies (i.e. Liberty Dollars)¹¹ as the unit of account in their monetary system. As explained by Dowd (2014), private money is generally unregulated and emerges through market forces that operate outside the control of a centralized government institution (p.85). As it will be presented later on, crypto-currencies like

¹¹ Private currency, available in coins, banknotes, gold and silver certificates and electronic currency produced in the United States by founder Bernard Von NotHaus from 1998 to 2009. See http://www.nytimes.com/2012/10/25/us/liberty-dollar-creator-awaits-his-fate-behind-bars.html?_r=0

Bitcoin are mined and produced by the individuals who have shown interest in the private currency and wish to and thus create a public demand for it (Dowd, 2014, pp. 1-3). The state has, in that sense, hindered the establishment of such currencies but also created favourable conditions for private monetary systems to emerge. In that perspective, this can help contextualize currency technology like Bitcoin and its role in “filling a market niche that the state itself has created” (p.4).

1.2 Applying the Money Supply Framework to Virtual Currencies

The money supply is measured and managed by centralized government institutions, such as the Bank of Canada, the Bank of England or the US Federal Reserve. A spectrum of money aggregates (see below) serves to delineate empirical measures of the supply and to define the various types of money overseen by monetary supply policy. Virtual currencies have not yet been defined using this framework, notably because each currency is a decentralized system managed by its own network. Crypto-currencies can surely be considered a form of broader money, because while they more or less fulfill the functions of near money or state-backed money, they are not regulated by monetary policy framework. It becomes interesting to work within the traditional money supply structure and apply it to crypto-currencies, in particular the one discussed more in-depth in this paper: Bitcoin. The distinction should be underlined once again here, that virtual currency refers to crypto-currencies like Bitcoin and that digitized or virtual money refers to traditional money that performs the three functions of money. As it will be explored, virtual currency does interact with the traditional money supply first, in its digital form (e.g. on virtual currency exchange hubs) and second, in its physical form, when virtual

currency is exchanged and converted to digitized or virtual money (e.g. fiat currency or money deposited to a checking/savings account accessible online), and then withdrawn in the form of banknotes from an ATM.

1.2.1 Money Supply and Monetary Aggregates

Money is controlled by monetary policy regulation. In order to control the money supply, central banks need to measure the supply of money and ideally, limit its fluctuation (i.e. inflation) in order to maintain its store of value function over time. Monetary aggregates are key not only in determining central banking policy but also in providing a snapshot of the “size” of the money supply, in other words the measure of the amount of money circulating in the economy.

The following are standard definitions of the various monetary aggregates used by central banks around the world to measure the money supply:

- i. M0: Also defined as monetary base, it includes currency in circulation, physical bank notes and coins held by the public and by banks as cash reserves.¹²
- ii. M1: Combines both M0 and narrow money that is easily convertible into cash or cash equivalents, such as traveler’s cheques, demand deposits, and other “liquid” deposits, as well as chequing accounts that are held outside the private banking system.¹³

¹² See <http://www.investopedia.com/terms/m/m0.asp>

¹³ Federal Reserve, Appendix B – Glossary Terms: M1 (2005).

- iii. M2: Combines M1 and other assets such as short-term deposits (fixed or timed), MMMFs¹⁴ (< 24 hours) and both money market and savings deposits.¹⁵
- iv. M3: Combines M2 and other long-term deposits varying on the degree of liquidity, MMMFs (> 24 hours), repurchase agreements, other bank deposits of the private non-banking sector.¹⁶
- v. M4: Combines M3 and private sector cash holdings (outside of the banking system), commercial paper, certificate deposits.¹⁷
- vi. M4+: Broader money held in the private and non-private sector that is also convertible and holds a lower liquidity level than M1, M2 and M3, which includes other forms of deposits.¹⁸

1.2.2 Virtual Money as M1 and M2: Using a PayPal Account

In applying the monetary aggregates definition to virtual money deposits, a PayPal Wallet would therefore fall under the M1-M2 category, because the money in the wallet is linked to a banking account (chequing or savings) or to a credit card. This is quite different from virtual currency wallets, which are not typically associated with a user's personal banking account, but rather with the user's private/public key.¹⁹ However, by using the monetary aggregates framework, it should be noted that moving money from a chequing (M1) to a savings account (M2) increases the M1 supply, because there is a

¹⁴ Money Market Mutual Funds.

¹⁵ Federal Reserve, Appendix B – Glossary Terms: M2 (2005).

¹⁶ Federal Reserve, Appendix B – Glossary Terms: M3 (Federal Reserve, 2005).

¹⁷ Bank of England, Explanatory Notes: M4 (Bank of England, 2014).

¹⁸ Federal Reserve, Table 1 (O'Brien, 2007).

¹⁹ How a Bitcoin Wallet works. See <https://blockchain.info/wallet/how-it-works>

movement of funds; in other words money is put in circulation. To put this in context, moving money from a chequing account to a PayPal account does not change the monetary aggregate supply for M2, but if the money is moved from a PayPal account to a chequing account, and then deposited into a savings account, both the M2 balance and M1 balance will be affected. As such, the money available in a PayPal account is equivalent to M1 because it is money that can be spent as easily and is as accessible as banknotes and coins in circulation.

Table 1 represents examples of the different types of traditional money aggregates that form the money supply, and includes PayPal to provide an example of digital money to better understand the conditions under which the monetary aggregate framework could be applied to other monetary technologies.

Table 1: Money Supply – Examples of Monetary Aggregates

Examples	M0	M1	M2	M3	M4
Currency in circulation	x	x	x	x	x
Overnight deposits		x	x	x	x
Deposits with an agreed maturity of up to 2 years			x	x	x
MMMFs (<24 hours)			x	x	x
Repurchase agreements				x	x
MMF shares				x	x
Foreign Currency Deposits					x
Commercial Paper					x
PayPal Wallet (Virtual Money Deposits)		x	x	x	x

1.2.3 Two Sides of the Bitcoin: Money or Near Money?

Where Would Bitcoin Fit?

The quasi-money²⁰ measurement incorporates assets that can hold a store of value function and can be converted into a medium of exchange (O'Brien, 2007, pp.23-29). However, they are not considered *per se* as a globally accepted medium of exchange, which puts them into the quasi-money category. Applying this framework to virtual currencies, we can outline characteristics that apply to near money to evaluate the argument that virtual currencies could be considered as quasi-money in the money supply measurement framework. This can be illustrated by using Bitcoin as an example because it can be converted into fiat currency. Indeed, Bitcoin provides its user with a purchasing power through the amount of BTC units the user holds in his/her Bitcoin wallet,²¹ and in turn, these units can be traded through a trading platform.²²

It is understood in principle that quasi-money holds M2 liquidity levels because it can be used in the payment and purchase of goods and services, or to settle debt, but it does not have the liquidity capacity of banknotes, coins or M0-M1 assets. Quasi-money aims to have relatively lower transactions costs than other assets within the money supply structure, another characteristic linked to virtual currencies. However, even if quasi-money works on the premise that economic agents accept as a form of payment, it cannot serve the medium of exchange function because it is a less liquid asset, even if it can be converted easily into cash. For that reason, virtual currencies cannot only be considered

²⁰ Quasi-Money is synonym of near money. Both are used interchangeably.

²¹ See Chapter 2.

²² Idem.

as a form of quasi-money since they can be used directly for payment purposes and are considered a medium of exchange.

Using the money supply framework once again, we look at the characteristics of M1-M2 in the monetary aggregates to evaluate if Bitcoin can fit within the scope of the money supply. Bitcoin relies primordially on the expectation that it is accepted within and outside the network as a form of value. As a result, users are willing to accept the cryptocurrency because they are assured that another user is also equally confident, that in turn, they can use BTC as a form of payment or to transfer funds to other users. In other words, Bitcoin works as a medium of exchange within and outside the network the same way fiat money is accepted as a form of payment today. While the argument holds that it can be perceived as a medium of exchange because online commerce sites such as Overstock.com and Zynga have accepted Bitcoin as a form of payment without a user having to convert it into fiat money, it is still in the process of becoming a globally-accepted medium of exchange (Lo and Wang, 2014, pp.3-4). The main takeaway, however, is that the majority of the actors within the interrelated global markets are slowly starting to adopt Bitcoin technology or to integrate the currency as a globally accepted form of payment because its users believe in its viability in the long-run. It is in that aspect that Bitcoin fulfills the function of medium of exchange, and could therefore be categorized as a form of M1-M2 in the money supply.

Moreover, Bitcoin's high volatility increases the exchange rate risk to fiat currency, and its fluctuation levels are higher than any other commodity money in the market, which has impacted its capacity to be used as a unit of account (Lo, Wang, 2014, pp.10-11).

Nonetheless, given the market's acceptance of the currency, it has rendered it a more or less suitable form of payment, because the users believe in the long-term stability of Bitcoin's value (Herlin, 2015, p.82-83). Lo and Wang (2014) have attributed the slower acceptance of Bitcoin to the fact that merchants prefer to post prices in standard currencies (like dollars) to limit the impact of Bitcoin's fluctuating value and therefore diminish the conversion exchange rate risks by converting BTCs into currency instantly (p.10). As a result, it is the Bitcoin holder who absorbs any fluctuation of the currency if a sudden devaluation of BTC arises. Based on the definition, Bitcoin could be considered as a form of M1-M2 in the money supply because it is considered a unit of account and it possesses similar characteristics to fiat money (e.g. in the form of banknotes and coins or an online chequing account). The argument here is that Bitcoin holds its unit of account function value because of its acceptance as a form of payment (it can be converted into fiat money easily) and the network's hashing capability – Bitcoin relies on a network of millions of computers that will continue to function and produce BTCs – that will not fail anytime soon (Herlin, 2015, p.82).

Where Bitcoin serves as a store of value, Lo and Wang (2014) make the argument that it can also be used as a vehicle for speculative investment (p.11) and lead to a Bitcoin bubble as it was the case in 2013 where at some point 1 BTC traded as high as USD 1,242.23. Bitcoin can serve as a store of value for as long as the market continues to sustain the value of Bitcoin and to accept it at a market value established by users. Unlike Bitcoin and virtual currencies, M2 assets are not only easily converted into fiat money

²³ Forbes. (2013, October 12). Year of the Bitcoin. See www.forbes.com/sites/kitconews/2013/12/10/2013-year-of-the-bitcoin/

(cash), but they are also backed by money that is legal tender and protected by deposit insurance. On the other hand, store of value of a virtual currency like Bitcoin relies entirely on the supply and demand of those who use it, even if it can be converted into fiat currency. In that regard, Bitcoin cannot be considered as a form of M2 in the money supply.

1.2.3.1 Bitcoin as Complementary Money

Complementary money can be defined as complement to money recognized as legal tender (e.g. fiat money), and can be accepted as a form of payment between individuals within the market as long as it remains a form of accepted payment. Though state-backed money remains the officially accepted form of payment, complementary money is also accepted to complete transactions (Herlin, 2015, p.48).

A perfect example of a complementary money system still in use today is Switzerland's WIR (Wirtschaftsring-Genossenschaft),²⁴ the Swiss Economic Circle's complementary currency system. Created in 1934 in Switzerland, following the stock market crisis of 1929, the WIR Franc is used in a dual-transaction system, now entirely electronic, with the Swiss Franc (1 WIR = 1 CHF).²⁵ The system, which initially served businesses *ad hoc*, has since 2000, offered its credit services to consumers and includes more than 60,000 members (Herlin, 2015, p.49).²⁶ The business credit lines, backed by real assets, are used to transfer complete payments between trade accounts, without the need of

²⁴ See <http://www.wir.ch/de/die-wir-bank/>

²⁵ Herlin, 2015, p. 49.

²⁶ See <http://www.wir.ch/fr/la-banque-wir/>

traditional money (Ibid). Despite the fact that it does not hold parity with any official currency (unlike the WIR), Bitcoin has many similarities with the WIR.

Herlin (2015) proposes five characteristics that can serve to evaluate Bitcoin if it can be considered a complementary currency. The first characteristic is that complementary money was created outside the traditional banking system (Herlin, 2015, p.53-56); equally, Bitcoin is based on a decentralized structure and is managed by the users of the system.

Second, the use of complementary money is not required; consumers and businesses can use a different form of payment, and can exchange complementary money for legal tender money (e.g. currency such as the euro or the dollar) (Ibid); Bitcoin users are not limited by the network and can use BTC to for payments outside the system. They can also exchange virtual currency for fiat currency; unless a transfer is done within the Bitcoin network, users have the freedom of choice to transfer funds or complete payments outside of the network.

Third, the exchange rate of complementary money is pegged against that of an official currency (Ibid); Bitcoin's value is determined by the supply and demand of the market, but its exchange rate is fixed against official currency (e.g. 1 BTC = USD 276.30).²⁷

Fourth, the main function of complementary money is to serve as a medium of exchange rather than a store of value; it aims to facilitate the transfer of funds (Ibid). Bitcoin's main

²⁷ Price Index as at July 21, 2015. See <http://www.coindesk.com/price/>

function is as a medium of exchange, however, it can also serve to as a store of value, despite its sensitivity to market fluctuations.

Lastly, funds in complementary money units are recorded in real-time in a transaction ledger to avoid double-spending and fraud, and consequently, no additional money is created within that same transaction (Ibid). Bitcoin on the other hand, relies on the blockchain approval mechanism to preserve the integrity global public ledger; it is the users who validate the transactions, and unlike the WIR, the validation process can take up to 10 minutes.²⁸

When applying Herlin's framework to Bitcoin, the argument holds that it can certainly be considered as complementary currency. In addition, the decentralized nature of Bitcoin and its ease of access have expanded its the reach beyond that of the WIR. Consequently, the staggering growth of Bitcoin wallet users alone (more than 3.8 million users as of July 2015)²⁹ justifies the application of two different frameworks to attempt a classification of the virtual currency in a traditional system, as it was done with the argument presented above using the money supply/money aggregate framework.

To summarize the analysis through the money supply and complementary money frameworks, Table 2 includes Bitcoin delineate the monetary aggregates parameters under which the crypto-currency could be classified, *ceteris paribus*. If the monetary

²⁸ The mechanics of Bitcoin are explained in more detail in chapter 2.

²⁹ See <https://blockchain.info/charts/my-wallet-n-users>

aggregate framework is applied to Bitcoin, the argument holds that it could be classified as complementary money and as M1.³⁰

Table 2: Monetary Aggregates – Where Could Bitcoin Fit?

Examples	M0	M1	M2 ³¹	M3	M4	CM ³²
Currency in circulation	x	x	x	x	x	
Overnight deposits		x	x	x	x	
Deposits with an agreed maturity of up to 2 years			x	x	x	
MMMFs (<24 hours)			x	x	x	
Repurchase agreements				x	x	
MMF shares				x	x	
Foreign Currency Deposits				x	x	
Commercial Paper				x	x	
PayPal Wallet (Virtual money deposits)		x	x	x	x	
Bitcoin (Crypto-currency)		x				x

Lastly, the emergence of virtual currencies like Bitcoin have certainly shed light on the need to develop a new economic framework to further assess their impact on the overall economy and the money supply. Even if fiat currencies remain predominant in the financial system, virtual currencies have taken away the exclusive status that traditionally defined the monies used today (Herlin, 2015, p.88). The classification of Bitcoin using the monetary aggregate framework and the characteristics of money proposed in this paper provide a hypothetical application of a traditional framework to account for a new form of “money”. This comparison offers the closest parameters to establish a link between money and virtual currencies from an economic perspective, and draws a parallel between the functions of money and that Bitcoin, in fact, derives its ability to

³⁰ Note that this is a hypothetical representation of Bitcoin in the money supply, focusing on its role as a medium of exchange.

³¹ Quasi-Money is included in M2 and encompasses assets that can be converted into cash.

³² Complementary Money.

hold value from the medium of exchange function of money. What this means is that Bitcoin's value comes mainly from its ability to be accepted as a form of payment, as is, to a certain extent, the case with fiat money. That is why the crypto-currency can be compared to M1 in the money supply, but in limited capacity. As a result, classifying Bitcoin as complementary money, places it somewhere between a form of money and quasi-money; it is neither a form of electronic money as legal tender, nor fiat money because it is not state-backed and has yet to be accepted by law as a recognized currency.³³

³³ Some jurisdictions have accepted Bitcoin as legal tender. See chapter 3.

Chapter 2: A Bit of Change, in Bitcoin?

The study of virtual currencies, as a field of study in the realm of international finance and financial governance, has truly emerged in the mid- to late 2000's, and the literature available on the subject is rather new. While the scope of this paper focuses on crypto-currencies, in particular Bitcoin, the review of literature draws attention to the early forms of digital currency that have paved the way for the development of virtual currencies today. Additionally, by first looking at the virtual currency ecosystem, this chapter seeks to draw a portrait of the network, including its actors, and the development of virtual currency technology before focusing on crypto-currencies and Bitcoin. The last section sheds light on the risks and benefits of virtual currencies and provides a clearer picture of the challenge and potential of this technology for the different stakeholders dealing with virtual currencies.

2.1 Literature Review

Decentralized Money

Austrian economist and father of the Austrian School of Economics, Carl Menger, in his discourse *Grundsätze*,³⁴ declared, “[m]an himself is the beginning and the end of every economy” (Menger, 1871, p.viii). His essay was a precursor to the ideology from which the creators of virtual currencies (most notably Satoshi Nakamoto) have established a decentralized structure today. He articulates in “Chapter IX: Influence of the Sovereign Power” that the origin of money is social rather than defined by state institution or by

³⁴ Principles of Economics.

law. He explains that it is the social institution of money that has been refined and improved by state recognition and regulation, just as it was the case with customary laws and statute law, which he exemplifies through the conversion of precious metals by weight to their transformation as coins for a better way to conduct trade (Menger, 1892):

“[t]he competing action of the several commodities serving as currency, and further the circumstance, that concurrent standards induce a manifold insecurity in trade, and render necessary various conversions...[have] led to the legal recognition of certain commodities as money...[and] where more than more than one commodity has been acquiesced in, or admitted, as the legal form of payment, law or some system of appraisement has fixed a definite ratio of value amongst them” (Menger, 1892, p.255).

Karl Menger’s essay was perhaps the first to lay foundation to the idea that the functions of money have been appraised and adopted by state institutions and state laws, but that the very essence of money as a value-based commodity for trade and payment holds value because of the social contract amongst its users and the system actors who have agreed and recognized that it could perform “important functions of state administration” (Menger, 1892, p.255).

Moreover, Friedrich A. Hayek, scholar of the Austrian School of Economics and Nobel Prize winner, offers a critique of alternative currencies in his oeuvre *Denationalisation of Money*. In addressing virtual currencies as an agent of change within the economic system, it is key to assert Hayek’s definition of the market, described as “a complex web of social interactions, institutions and practices” (Raeder, 2013). On the price system, he acknowledges that it is as an evolving medium of communication, which determines the individual’s success of his actions and integrates the actions of groups and individuals into a coherent global order (Hayek, 1976, pp.85-90). In other words, the actions of

individuals provide an order within the market, but it is prices that steer the market's behavior; individuals and groups are incentivized to deploy efforts to reap rewards and command the economic ecosystem. Hayek advocates the integration of private money into the system if it will be most conducive to smooth the functioning of the market process and if it will have a desirable effect on the behavior of the money supply and demand (Hayek, 1976, pp.84-86). Hayek would, under such conditions, welcome the idea behind virtual currencies like Bitcoin to abolish government monopoly and reform the market economy to be inclusive of privately-issued currencies that would circulate regardless of state boundaries. An open competition of currencies, while it would provide groundbreaking changes to the economic market, would not be sustainable if there is no stability in its system.

The challenge for virtual currencies then, would be to compete for a market share on the basis of stability, yet the most popular currency, Bitcoin, is known to be prone to hyperinflation and deflation, its price sensitivity attributed to the social interactions of the market (i.e. the acceptance of the currency as a method of payment), and consequently the demand and supply of BTC in the system. Hayek would certainly agree with a private global currency entering the market, but due to the unstable and unregulated pricing system that many virtual currencies face, and because they still rely on state-backed currencies to provide users with liquidity, it would most likely not be sustainable in the long run (Hayek, 1976, pp.85-90).

Virtual Currencies

E.H. Solomon (1997) was one of the first to study electronic money in its various forms and to offer an analysis on the advantages and disadvantages of digital money. In his book *Virtual Money: Understanding the Power and Risks of Money's High-speed Journey Into Electronic Space*, he provides a solid foundation to explain how every electronic system available in the 1990s works, as well as up-and-coming innovations such as electronic benefit transfers (EBT), electronic wallets and cybermoney. Solomon also provides an in-depth analysis of the risks associated with the evolution of such technologies and their potential impact on national security and the international financial system, but also of the benefits of these technologies, primarily the ability to instantly transfer funds and complete payments across the globe.

A few years later, Edward Castronova (2002) and Hiroshi Yamaguchi (2004) both analysed, in two separate research papers, the virtual economies developed in MMORPG³⁵ gaming worlds where virtual assets were produced and sold using real money in-game in an online trading platform and also traded or sold in real markets with real currency, what they refer to as eBaying.³⁶ Online gaming platforms were the first adopters of virtual markets where digital assets held a certain level of valuableness and where these virtual assets could be defined as early versions of virtual currencies. Indeed, the utilization of these currencies by the players within the platform, as Castronova explains, has the same function as that of money in the real world. Yamaguchi noted,

³⁵ Massively multiplayer online role-playing games.

³⁶ eBay was used in the 1990s and early 2000s to sell virtual assets owned by a user for real money. This practice was common amongst users of popular online games such World of Warcraft, League of Legends and EverQuest. (MMO Play. <http://mmo-play.com/mmo-blog/mmo-ebay-connection>).

however, that while it is possible to exchange virtual assets for real money, it is the willingness of players to adopt this mechanism and their acceptance of exchange rate risk that ensures viable conditions for the virtual money or asset used in the trading activities online to remain “meaningful” within the trading system.

Additionally, Vili Lehdonvitra (2005) analyses the importance of virtual economies within gaming worlds and the capacity of these worlds to “mimic” real economic activities such as the exchange of goods and services. Lehdonvitra reviews the groundbreaking works of Yamaguchi and Castronova and underlines an interesting question: that is, if such virtual currencies are exchangeable with other currencies and if players continue to allocate resources (i.e. time and assets) to procure these currencies, then these currencies should hold value on a global scale regardless of their issuance within the virtual or real world (Lehdonvitra, 2005, p.4).

However, Luther and Olson (2014) try to underline the application of crypto-currencies as not just a form of money but also of memory. They use Bitcoin as the core crypto-currency to argue that, while it serves the three functions of money, it particularly serves as a public-record keeping device (Luther, and Olson, 2014, p.23). The parallel they draw between money (in this case crypto-currency) and memory is to explain why money circulates and why people tend to use it to keep record, for example of financial transactions. They demonstrate that crypto-currencies, and more so Bitcoin, have the potential to perform the functions of money, especially given the fact that the cost of storage or, as they extensively discuss, the easiness of record-keeping, can facilitate the exchange in the same way as traditional currencies do (Luther and Olson, 2014, p.31).

The monetary literature on virtual currencies has continued to grow with the evolution of the crypto-currency market. The focus has thus far been on the nature of virtual currencies and their functions as a whole, and it is only in the last three years that academics and policymakers have tried to distinguish the generic term “virtual currency” and the specifics of “crypto-currency”. In the financial and payments system, however, it is important to note that the attention has been on crypto-currencies, predominantly on Bitcoin. Given the complexity of the virtual currency market, the following section considers the literature on virtual currency schemes as it pertains to the research outlined in this paper and to the third chapter with regards to policymaking and regulation.

Virtual Currency Schemes

The ECB was the first state institution to publish a report on the technological developments of virtual currency schemes in the monetary system and the impact of virtual currencies on the payments systems. Released in October 2012, the paper carries out an analysis of VCS that are of interest to the financial system and to central banks. The ECB’s work aims to provide clarity on virtual currencies by classifying and defining VCS and assessing the risks and opportunities of virtual currencies via two case studies: Bitcoin and Second Life (ECB, 2012, pp.5-6). The ECB clearly distinguishes between electronic money,³⁷ for which legal foundations remain (e.g. fiat money stored or transferred virtually, for example PayPal), and virtual currency, which is not regulated or followed by an institutionalized oversight mechanism (ECB, 2012, pp. 16-17). Given the

³⁷ The European Union released a directive on electronic money, Electronic Money Directive (2009/110/EC), which can be found here: <http://eur-lex.europa.eu/legal-content/EN/ALL/?uri=CELEX:32009L0110>.

complexity of virtual currency schemes, the ECB's analysis focuses on three types of VCS that have sustainable connections and interactions with "real money and the real economy" (ECB, 2012, p.13):

- a) Closed virtual currency schemes (ECB, 2012, p.13): Starbucks stars (used to redeem free coffees) and "in-game only" currencies, such as Blizzard's World of Warcraft (WoW) Gold, are a good example of closed VCS. In this case, players open an account online and pay a subscription fee to purchase virtual gold and, in turn, use it to purchase virtual goods. Even if under Blizzard's rules, WoW Gold is forbidden to sell or purchase in the real world, it is possible to purchase it on other online platforms (equivalent to a black market for online gaming). In principle, a closed VCS does not have a link to the real economy and cannot be traded outside of the virtual game's market. However, it is sometimes possible to circumvent the constraints of the platform, as was the case with WoW Gold.
- b) Virtual currency schemes with unidirectional flow: this type of currency can be purchased using real money, usually at a fixed exchange rate, but cannot be exchanged back to real currency. This type of currency is also used to buy virtual or real goods or services depending on the type of merchant. An example of this type of VCS includes Amazon Coins,³⁸ created by U.S. retailer Amazon. The coins can be used to purchase digital products from the Amazon Appstore. Amazon Coins are divided into two categories: Purchased Coins, which can be used to receive gifts from

³⁸ 1 Amazon Coin = USD 0.10.

another user or be purchased from Amazon, and Promotional Coins, which Amazon gives as part of promotional giveaways (Amazon, 2014).

- c) Virtual currency schemes with bidirectional flow: this type of virtual currency is interchangeable with real currency, and its exchange rate varies according to the currency it is pegged to. It is a convertible currency used for the purchase of virtual and real goods and services alike. The majority of crypto-currencies, like Bitcoin, fall under this category of VCS.

In February 2015, the ECB published a supplementary report that looks at new developments with regards to VCS technology and their relevance to the financial and payments systems (ECB, 2015, p.4). The publication presents extensive research on the VCS ecosystem and draws a clearer portrait of the limitations and weaknesses of VCS for users and other actors. The ECB provides a description of the relevant actors of the “VCS ecosystem” and presents their own feature as outlined in the following table.

Table 3: VCS Ecosystem³⁹

Actors	Role
Inventors	Creators of virtual currencies, who's identity remains anonymous and who support the development of the VCS (e.g. Satoshi Nakamoto, creator of Bitcoin)
Issuers	Administrator or generator of the VCS. In a decentralized VCS like Bitcoin, there is no single issuer; units are generated by the mining activities performed by the miners who receive units for their mining activities.
Miners	Users (individuals or groups) who validate sets of transactions (block) that are in turn added to the VCS global payment ledger (blockchain). Miners usually receive a reward for their work or require a transaction fee from the users who initiated the transaction to be validated. Miners are central to the decentralized VCS since they ensure the validity of transactions within the system.

³⁹ Definitions summarized from the ECB report (ECB, 2015, pp.7-8).

Actors	Role
Processing Service Providers	Used to facilitate the transfer of units between users; in a decentralized VCS this is often performed by miners.
Users	Refers to the people (i.e. groups, individuals, merchants) that engage in VCS P2P activities (i.e. purchasing, mining or payments of virtual currency).
Wallet Providers	Providers of digitally encrypted wallets that include cryptographic keys, authentication codes and the transaction history of a VCS user. These wallets safeguard the virtual assets of the user on various platforms (i.e. mobile, cloud, PC/Mac devices). Examples of wallet providers include: Blockchain.info and Coinbase. ⁴⁰
Exchanges	Service platform where users can buy/sell virtual currency against main currencies or other virtual currencies (which are only quoted in BTC). VCS exchanges also quote exchange rates and can act as wallet providers. Example of exchange hubs include: CoinMX, Coinbase and Bitstamp. ⁴¹
Trading Platforms	Trading marketplaces where VCS users can trade, buy/sell, and exchange virtual currency amongst them. Trading platforms do not engage in trading activities, unlike exchanges. (See Table 5 for the top 10 trading platforms by volume as at May 25, 2015).
Other Actors	External stakeholders that are not directly involved with the VCS ecosystem, for example software developers, ATM manufacturers and payment facilitators. Additional actors include exchange-traded funds (ETFs) and tumblers, service providers of greater anonymity for VCS users wishing to remain unknown (e.g. Dark Wallet, Tor).

The ECB's analysis also looks at regulatory clarifications outlined by various authorities, including the FATF, notably the impact of VCS on the ECB/Eurosystem, and reviews the definition of virtual currency schemes. Unlike the framework proposed in chapter 1, which applies the structure of money supply and complementary money to define virtual currencies in the economy, the ECB *de facto* does not recognize VCS or virtual currency as concepts that fit within the framework of currency or money as outlined by the economic and legal literature on the financial system (ECB, 2015, p.23). Conversely, the ECB bases its argument on the definition of the functions of money as outlined in the first chapter; it attributes the failure to meet the three functions to the low acceptance of VCS

⁴⁰ Blockchain.info and Coinbase are the globally leading wallet providers for bitcoin wallets. See <http://www.newsbtc.com/2015/03/06/top-online-bitcoin-wallets-2015/>

⁴¹ Bitcoin exchange guide. See <http://bitcoinexchangeguide.com>

by the general public and the high volatility of exchange rates of VCS/real currencies. In that perspective, the ECB offers two definitions to distinguish the terms virtual currency and virtual currency schemes:

- a) Virtual currency: “digital representation of value, not issued by a central bank, credit institution or e-money institution, which, in some circumstances, can be used as an alternative to money”.⁴²
- b) Virtual currency schemes (VCS): “both the aspect of value [i.e. virtual currency] and that of the inherent or in-built mechanisms ensuring that value can be transferred”.⁴³

What is more interesting, however, is the ECB’s argument with regards to law. Its analysis effectively highlights that traditional currencies in the form of coins or banknotes are accepted as legal tender by law, and that e-money or bank money are accepted by choice, as is the case with virtual currencies; they are accepted as a form of contractual obligation only because there is a good will agreement between a buyer and a seller (ECB, 2014, pp.23-24).

2.2 Virtual Currencies

2.2.1 Decentralized Virtual Currency Schemes

The majority of VCS available in the market today are bidirectional; however, they do present technical and functional differences that can be categorized in three main

⁴² ECB, 2015, p.25.

⁴³ Ibid.

categories (ECB, 2015, pp.10-11). The ECB distinguishes decentralized VCS through differences in their validating systems, algorithms, supply of currency and functionality.

The technology used by virtual currency schemes to validate transactions and secure network activity is divided into two categories: proof-of-work (PoW) and proof-of-stake (PoS). The PoW system is a protocol based entirely on the capacity of users or entities to complete computational tasks or hashing;⁴⁴ this system is the one used by Bitcoin and Litecoin, for example (Bitcoin, 2015). Additionally, the PoS system is a protocol based on how much a user can mine depending on how many coins they hold, and unlike the PoW system, it eliminates the possibility of monopoly, double-spending or what is referred to as the “Tragedy of the Commons”⁴⁵ (Graydon, 2014). Rather than mining, the users engage in a process known as forging, meaning that all the active users are able to access the point of the network where the next transaction will be processed and added to the global ledger, the blockchain (ECB, 2015, p. 10).

A hybrid protocol system combining PoS and PoW is also used by certain virtual currencies such as Peercoin (ECB, 2015, p.10). Additionally, a new security protocol was proposed by Bentov et al. (2014), called the proof-of-activity (PoA). It builds on the protocol used by Bitcoin and adds additional security features to reward only the active users maintaining online activities in the network.

⁴⁴ Hashing or hashcash is an application of a proof-of-work algorithm used to convert an input in order to receive an encrypted output. The work to compute or to hash can be verified easily by the receiver, but the reverse, that is, to try and find the input is nearly impossible (Bitcoin Wiki, 2015).

⁴⁵ Tragedy of Commons is a scenario where the entire Bitcoin market fails. This phenomenon could occur when for example, BTC would be produced in lower quantities than the market demand, or that would be consumed in higher quantities than desired. As such, this hypothetical market failure would occur when the block mining reward would drop extensively. See https://en.bitcoin.it/wiki/Tragedy_of_the_Commons

The second element by which the ECB categorizes virtual currencies is the algorithms used. It identifies two main ones: SHA-256 used by Bitcoin and Scrypt (ECB, 2015). The algorithms are mathematical methods used to calculate and process data transactions (i.e. block), which in turn are added to the blockchain to release coins. The third element is the total supply of coins available. While certain VCS have an unlimited coin supply (i.e. Dogecoin) capacity, numerous VCS have a fixed supply available.

The last category is the functionality of VCS systems that are not competing with other virtual currency schemes but rather offer a suite of services that are complementary to the Bitcoin protocol, for example. These decentralized schemes, like Mastercoin or Nextcoin, offer users the ability to complete transactions of other items (i.e. property and securities), which are classified as “smart properties”; that is, assets which can be stored in the blockchain and traded in a P2P marketplace (ECB, 2015, p.11).

So far, the ECB has been the only state institution to propose a comprehensive analysis of the technology advancements made with virtual currency schemes. While other new systems (transaction validation mechanisms and algorithms) are work in progress and continue to be created by the virtual currency community, certain banking institutions are also taking steps to run pilot projects with VCS technology. In June 2015, according to *The Cointelegraph*, Barclays signed an agreement with Swedish startup Safello to test a new form of blockchain technology, proof-of-concept (PoC), to establish an infrastructure capable of managing traditional transaction activities and peer-to-peer interactions (Richards, 2015). In Canada, CIBC announced on June 23, 2014 that it is

also looking at the possibility of using virtual currency technology as the banking system is facing new competitors like Bitcoin (*Chronicle Herald*, 2015).

2.2.2 Data and Figures on Virtual Currency Schemes

While the data on the majority of VCS is quite limited given that there are few websites that offer a comprehensive methodology and statistical framework to compile transaction activities within the financial system, this section scopes out the data and figures on Bitcoin as it is the most traded virtual currency in the world. The information available relies on the platforms that mainly conduct transaction activities in BTC.

According to Coin Market Cap, the total market capitalization, as at May 5, 2015, combining all virtual currencies is valued at USD 3,776,284,971.⁴⁶ There are 549 active currencies, 53 asset currencies and 1751 markets.

Table 4 below shows the top 25 virtual currencies by market capitalization as at May 5, 2015; Bitcoin's total market share is estimated at 87.8%,⁴⁷ and the second virtual currency by market capitalization share is Ripple with 6.7%.

⁴⁶ As at May 5, 2015, data retrieved from: <http://coinmarketcap.com/all/>

⁴⁷ Bitcoin market cap: \$3,318,757,221 and total market: \$3,776,284,971. $(3,318,757,221/3,776,284,971 = 0.877)$.

Table 4: Virtual Currencies by Market Capitalization⁴⁸

#	Name	Market Cap (USD)	Price (USD)	Available Supply ⁴⁹	Total Market Share (%)
1	 Bitcoin	\$3,318,757,221	\$234.92	14,127,000 BTC	87.88
2	 Ripple	\$253,722,762	\$0.01	31,908,551,587 XRP *	6.72
3	 Litecoin	\$54,248,835	\$1.40	38,754,704 LTC	1.44
4	 Dash	\$14,974,977	\$2.80	5,340,672 DASH	0.40
5	 Stellar	\$14,452,871	\$0.00	4,826,988,106 STR *	0.38
6	 Nxt	\$8,974,634	\$0.01	999,997,096 NXT *	0.24
7	 Dogecoin	\$8,833,223	\$0.00	99,280,373,005 DOGE	0.23
8	 Bitshares	\$8,155,866	\$0.00	2,509,520,303 BTS *	0.22
9	 Banxshares	\$7,347,178	\$1.43	5,126,916 BANX *	0.19
10	 Peercoin	\$5,088,701	\$0.23	22,286,410 PPC	0.13
11	 Bytecoin	\$4,348,542	\$0.00	172,326,622,560 BCN	0.12
12	 Namecoin	\$3,627,683	\$0.32	11,469,050 NMC	0.10
13	 Monero	\$3,365,026	\$0.45	7,424,855 XMR	0.09
14	 Ybcoin	\$2,766,861	\$0.92	3,000,000 YBC *	0.07
15	 Counterparty	\$2,491,185	\$0.94	2,641,480 XCP *	0.07
16	 NuShares	\$2,267,364	\$0.00	814,344,811 NSR *	0.06
17	 PayCoin	\$1,798,101	\$0.11	15,736,376 XPY **	0.05
18	 MonaCoin	\$1,397,998	\$0.07	19,346,400 MONA	0.04
19	 ARCHcoin	\$1,306,118	\$0.08	16,339,728 ARCH *	0.03
20	 FuelCoin	\$1,251,112	\$0.01	100,206,032 FC2 **	0.03
21	 NEM	\$1,235,817	\$0.00	8,999,999,999 XEM *	0.03
22	 DNotes	\$1,159,995	\$0.01	98,989,214 NOTE	0.03
23	 BlackCoin	\$1,055,020	\$0.01	74,870,837 BLK *	0.03
24	 Faircoin	\$1,044,292	\$0.02	51,687,898 FAIR *	0.03
25	 BitcoinDark	\$1,031,692	\$0.85	1,216,155 BTCD	0.03

To illustrate the volume of BTC traded, Table 5 looks at the top 10 trading platforms for Bitcoin by volume. For example, at the time of writing, Bitfinex, a Hong Kong-based

⁴⁸ Last updated: May 05, 2015 3:20 PM EST. Data retrieved from: <http://coinmarketcap.com/all/>

⁴⁹ Virtual currency is identified if it not mineable (*) or if it has been significantly premined (**).

company, which normally handles roughly 10% of the total BTC trading volume⁵⁰, halted deposits in late May and suspended trading activities due to a hot wallet⁵¹ hack estimated at 0.06% or roughly 1,500 BTC of the company's total holdings (*CoinDesk*, 2015).

According to *coinmarketcap.com*, the data available on the top 3 virtual currency schemes show that the average 24h trading volume for Bitcoin (USD 17,569,400) remains the highest, followed by Litecoin (USD 3,224,610) and Ripple (USD 855,095), its two main competitors.⁵²

Table 5: Bitcoin Top 10 Trading Platforms by Volume⁵³

#	Source	Pair	Volume (24h) USD	Price USD	Volume (%)
1	OkCoin Intl.	BTC/USD	\$ 2,370,760	\$ 237.60	18.93 %
2	Bitfinex	BTC/USD	\$ 2,179,950	\$ 237.99	17.41 %
3	BitYes	BTC/USD	\$ 1,979,070	\$ 237.91	15.81 %
4	BTC-E	BTC/USD	\$ 1,190,040	\$ 239.42	9.50 %
5	Bitstamp	BTC/USD	\$ 1,080,180	\$ 236.93	8.63 %
6	Coinbase Exchange	BTC/USD	\$ 851,129	\$ 238.20	6.80 %
7	LakeBTC	BTC/USD	\$ 558,895	\$ 239.80	4.46 %
8	Jubi	BTC/CNY	\$ 454,900	\$ 240.97	3.63 %
9	itBit	BTC/USD	\$ 386,156	\$ 236.30	3.08 %
10	Kraken	BTC/EUR	\$ 276,118	\$ 233.24	2.21 %

Despite the presence of other crypto-currencies in the market, Bitcoin remains the most traded VCS in the world, averaging between 60,000 to 70,000 transactions per day

⁵⁰ Bitfinex trading volume from May to June 2015. See

<http://bitcoincharts.com/charts/bitfinexUSD#rg90ztgSzm1g10zm2g25zvzcvzp>

⁵¹ Hot wallet refers to an online Bitcoin wallet (hot storage) while a Cold wallet refers to a Bitcoin wallet stored offline.

⁵² Trading volume in USD. Last updated: Jun 22, 2015 4:00 PM UTC,

<http://coinmarketcap.com/currencies/views/all/#USD>

⁵³ Last updated: May 25, 2015 1:01 PM EST. Data retrieved from

<http://coinmarketcap.com/currencies/volume/24-hour/#USD>

globally (in 2014).⁵⁴ As such, the next section aims to look at Bitcoin and its implications as a virtual currency scheme to assess the risks and opportunities of the crypto-currency on the traditional payments system.

2.3 Trading Up A Coin for Money: Bitcoin

Satoshi Nakamoto's Bitcoin has certainly, since its creation in 2009, been dubbed the gold standard of crypto-currencies. In less than four years, Bitcoin has evolved to become a scarce resource to which users attach value, while the currency itself is backed by virtually no asset (as it is the case with fiat currency).⁵⁵ What is more impressive is that the system itself is built on a peer-to-peer network (or P2P) that is self-sustained and accessible only via the digital sphere, and through which transactions are validated by users rather than a central authority. The success of Bitcoin lies in its capacity to offer extensive privacy protection: it is a cryptographic mechanism developed through a web of complex algorithms that rewards users once blockchains are solved, and has the capacity to provide users with a system that is independent from the traditional controls⁵⁶ present in the financial system. In this digital age, Bitcoin's finite supply, set to cap at 21 million BTC by 2140 (Buntix, 2015), gives it a characteristic attributed to other rare commodities present in the market today, but particularly to gold, which has historically been linked to money.

⁵⁴ <http://blockchain.info/charts/n-transactions>

⁵⁵ The inherent difference is that fiat currency is state-backed because it is the accepted form of legal tender, whereas virtual currencies are entirely decentralized.

⁵⁶ Traditional controls such as, but not limited to, regulatory body oversight of deposit insurance, industry supervision, and inflation or money supply control by central banks.

Bitcoin: How does it Work?

As a major player in the virtual currency industry, Bitcoin's decentralized and bidirectional system does not rely on a centralized authority; the virtual currency relies on a P2P network and proof-of-work (PoW) transaction validation mechanism that ensures the integrity of the system is kept in check. The nodes added to the blockchain at 10-minute intervals,⁵⁷ to mitigate the risks of double-spending or illegal transactions, are entries added to the global digital ledger, and the completed transaction details are monitored by and available to users or "miners" of the system.

Bitcoin relies on a cryptographic hash function known as SHA-256⁵⁸ and offers a certain level of computational efficiency to mathematically generate an input in order to produce an output (a hash) of a fixed value. The current hash rate⁵⁹ is at 370,533,289 GH/s⁶⁰ and the current reward per block is at 25BTC (USD 6,021).⁶¹

The Bitcoin Network

The network relies entirely on the users and stakeholders within and outside the Bitcoin platform – exchange markets, trading platforms, brokers, ATMs and other money transmittal services – that safeguard all the blockchain transaction records added to the global digital ledger. The network's decentralized structure relies on a transaction log

⁵⁷ Bitcoin Wiki. See <https://en.bitcoin.it/wiki/Block>

⁵⁸ A hash algorithm that is used to generate a verifiable set of characters and requires a certain amount of CPU effort (Bitcoin Wiki, 2015).

⁵⁹ The hash rate is the measuring unit of the processing power of the Bitcoin network. <https://bitcoin.org/en/vocabulary/hash-rate>

⁶⁰ Hash rate in Gigahash per second. See <https://blockchain.info/charts/hash-rate>

⁶¹ Bitcoin network data as at June 24, 2015. See <http://www.coindesk.com/data/bitcoin/>

spanning across a network of participating computers that limits any concentration of power. What is more, the irreversibility of transactions and the fact that they are sent through a P2P network protects users and merchants alike. The network identifies users via their cryptographic public key address, a series of random characters (e.g., 3J98t1WpEZ73CNmQviecrnyiWrnqRhWNLy)⁶² that is generated at no cost and usually has single use validity. However, Bitcoin users can choose to have one or multiple addresses or even get an account by using an exchange service like Coinbase or an online wallet service such as Armory (Bitcoin Wiki, 2015).

Two other elements that are important to note within the Bitcoin network are the presence of mixers and the concept of mining pools. Mixers act as a barrier to prevent the tracking of a user's identity or online activity in the system. Transaction records are pooled from a set of transactions in an unpredictable manner for validation to preserve the anonymity of users (Böhme et al., 2015, pp.221-222). While mixers are also used by digital wallet service providers and do have a usage fee, their protocols are not public record and their reliability cannot be proven (Böhme et al., 2015, p.222).

In addition, mining pools have also been a growing trend within the Bitcoin network and have raised concern amongst the Bitcoin network. These pools allow miners to join efforts in mining for BTC and share earnings with others in the pool; the two largest pools as identified by Böhme et al. are AntPool and F2Pool, which account for roughly a third of all Bitcoin mining activities. In 2014, Mining pool GHash.IO came under fire for briefly holding over 50% of Bitcoin's total mining power, threatening the entire

⁶² Bitcoin Wiki. <https://en.bitcoin.it/wiki/Address>

network's hashing power and stability; it has since committed to limiting its hashing power to a maximum of 40%.⁶³

Although the Bitcoin network has proved that it is capable to rectify potential threats without central authority oversight, it is nonetheless important to analyze the risks and opportunities of virtual currencies, and in particular those posed by the leader of the crypto-currency industry, Bitcoin.

2.4 Mastering the Coins: Risks and Advantages of Bitcoin

While the risks of using virtual currencies have cast a shadow over the technological capabilities of the Bitcoin network, given the growth of the virtual currency, it is important to underline the reasons why the technology has many adopters and detractors, and why the financial system has been thus far skeptical to further investigate Bitcoin technology at length.

2.4.1 Advantages: A Positive Outlook on Bitcoin Technology

2.4.1.1 Anonymity

The degree of anonymity provided by virtual currencies is quite unique, and Bitcoin is no exception. Because each transaction and digital wallet has a unique address that is not shared publically, and transactions are irreversible in the Bitcoin network, it is virtually impossible to trace back a transaction to users involved in a specific operation in the system. Should the wallet or transaction be published online by mistake, a new identifier

⁶³ CoinSummit Bitcoin Meeting. <http://www.scribd.com/doc/234153249/CoinSummit-Bitcoin-Meeting>

can be generated in replacement and, as a result, any information relating to a user's wallet becomes very difficult to access. The anonymity feature of Bitcoin is a point of contention because it opens the door to fraudulent activity and transactions cannot be corrected when a mistake occurs (ECB, 2015, p.22). Conversely, in a traditional payments system this risk does not pose a challenge because of the mechanisms put in place by banking and financial institutions to identify the account holder before any access is granted, but it does not eliminate the opportunity for third party institutions to have access to an account holder's financial information (e.g. Equifax).

The anonymity feature of Bitcoin is one of the core principles of virtual currencies, which is why it is argued that crypto-currencies should remain decentralized and monitored by volunteer users rather than a central authority. Lastly, other stakeholders in the network have introduced stealth payment technology, which allows end-users to remain anonymous when sending or receiving satoshis.⁶⁴ The protocols developed by entities like Zerocoin and Dark Wallet, as it will be discussed later in this chapter, change the security model of Bitcoin to further encrypt transactions. This type of technology increases anonymity for users but could affect the blockchain verification process; as such, many users continue to tradeoff some degree of anonymity (e.g. via their Bitcoin key, IP address, etc.) to preserve the integrity of the network.

2.4.1.2 A Low-cost Solution

Since it is Bitcoin users that validate transactions recorded in the global digital ledger (by adding a "block" to the blockchain), the authorization of transactions is shared across the

⁶⁴ Another term used to refer to BTC.

network. Unlike the traditional financial system, there is no intermediary or third-party used to monitor activities within the system; this greatly reduces transaction costs. As mentioned previously, the optional use of mixers or of another service can result in a service fee charge, typically totaling 0.5 of the total value of the transaction.⁶⁵ Users are not forced to pay up when their transaction is validated; a contribution from the initiator of the transaction is voluntary.⁶⁶ For consumers and merchants around the world, this is a benefit that reduces usage costs effectively when comparing to the fees required by international remittance services like Western Union, which can cost more than \$50 (Böhme et al., 2015, p.225), and electronic payments providers Visa or MasterCard, which can charge more than 3% per transaction (Flavelle, 2013). The other high selling point for Bitcoin is that little state legislation was formally developed to oblige users to comply with tax legislation to pay taxes on profits delving from virtual currency activities. So far, Canada and the United States are the only two nations who have issued, respectively via the CRA and the IRS, tax guidance to treat virtual currencies as property rather than currency (CRA, 2013; IRS, 2014). The European Union is in the process of adopting a EU-wide legislation to formally regulate taxation of virtual currencies across member states jurisdictions.

2.4.1.3 Usability

Ownership of a Bitcoin address or digital wallet comes with minimal requirements. As an all-purpose payments system, the technology behind Bitcoin is in theory quite simple to

⁶⁵ BitMixer.IO. See <https://bitmixer.io/fees.html>

⁶⁶ Bitcoin Wiki. See https://en.bitcoin.it/wiki/Transaction_fees

use for payments and exchanges on the network. Usability in this regard does not refer to the mining capabilities, which are more complex mechanisms used by stakeholders well versed in computational activities. Another benefit of Bitcoin is the easiness of checkout for a user or consumer purchasing goods or services online; no additional steps are needed to enter financial information and process a payment using third party encryption remittance systems. Another strong advantage is the speed of the verification and settlement processes for validating transaction,⁶⁷ in the case of Bitcoin of 10 minutes that does not change according to geographical location, unlike traditional payments services (ECB, 2015, p. 18). As such, the clearing of both a transaction and a payment is a globalized process and due to the decentralized nature of Bitcoin, users can quickly validate transactions regardless of their location.

2.4.1.4 Transportability and Global Reach

As an international digital currency, Bitcoin is able to connect buyers and sellers across the globe. Bitcoin thrives on its global reach but also on how easy it is to transport; users only need a device capable of connecting to the Internet. Another strong feature is that Bitcoin, unlike fiat money (divisible into 0.01) or a valued commodity like gold (indivisible), can be divided into 8 decimal places (0.00000001 BTC)⁶⁸ to buy, sell and trade items without the need of having to carry physical money or a payment card. Additionally, Bitcoin can act as a substitute currency to allow users to perform various transactions including the payment of bills. In Canada, for example, consumers can pay

⁶⁷ The approval process of known payment methods (e.g. Visa) is done in real-time, however, the clearing process to validate the transaction can take up from 3 to 10 business days.

⁶⁸ Bitcoin Wiki. <https://en.bitcoin.it/wiki/FAQ>

their bills using Bylls, a bill pay provider, for up to \$5,000 per month.⁶⁹ This service also exists in other countries, notably in Italy, where payment processor Tinkl.it allows users to pay their utility bills to NordOvest Energie, and in the Netherlands, where utility company Bas Nederland began accepting Bitcoin payments in 2014.⁷⁰ Lastly, Hong Kong-based 12charge allows users from over 110 countries (including Canada, the United States and certain European countries) top up on mobile airtime or pay their bills via the online service.⁷¹

Other advantages of Bitcoin proposed in the virtual currency literature can certainly highlight the benefits of using Bitcoin, namely protection against counterfeit banknotes, from the physical loss of assets, from payment blockades,⁷² government-sponsored inflation and from confiscation of assets via a wealth or levy tax as was the case in Spain and Cyprus.⁷³

2.4.2 Bitcoin Risks

2.4.2.1 Network Vulnerability

Like any online network, virtual currency schemes are not exempt to technology failures or attacks by rogue agents from within or outside the system. Bitcoin's network relies on

⁶⁹ See <https://www.bylls.com>

⁷⁰ For the full list of payment service providers, see <http://cointelegraph.com/news/114326/how-people-pay-bills-with-bitcoin-all-around-the-world>

⁷¹ For the full list of countries, see <http://www.prnewswire.com/news-releases/12chargecom-launches-worldwide-mobile-recharge-with-bitcoin-utility-bills-payments-with-cryptocurrency-and-more-300082865.html>

⁷² In 2011, Wiki Leaks faced a financial blockade from the U.S. government, who requested that major payment processors suspend donations to the site after the cable scandal erupted. See <http://www.theguardian.com/commentisfree/cifamerica/2011/oct/27/wikileaks-payments-blockade-dangerous-precedent>

⁷³ CoinDesk. CFPB Warning Ignores Bitcoin's Consumer Protections. See <http://www.coindesk.com/cfpb-warning-ignores-bitcoins-consumer-protections/>

the honesty of users to function. The network's vulnerable point of entry for an attack can only come from a dishonest user capable of creating a false blockchain command; however, such user can only accomplish this kind of illegal activity with computational power greater than the rest of the network (like it was temporarily the case with mining pool GHash.IO). Another network vulnerability could come from a weakness in the encryption system used by Bitcoin, which is similar, in theory, to the one used by financial institutions across the world. Technology failures are more apparent in a decentralized system like Bitcoin due to the structure of the virtual currency scheme; the lack of a central authority to regulate and monitor activities within the system does not make Bitcoin more vulnerable to attacks, but users and stakeholders are left unprotected. The other main network vulnerability is the exposure to Denial of Service (DoS) attacks, where massive strings of data are sent to a node (block) to prevent the approval process of Bitcoin transactions (Grinberg, 2011, p.180). Because DoS attacks are almost impossible to prevent, the Bitcoin community recognizes that the network is vulnerable to attacks, and client protection protocol rules⁷⁴ have been put in place to limit these attacks.⁷⁵

2.4.2.2 Hacking, Theft and Fraud

A recurring theme and area of concern for the users and state regulators is the risk of hacking, theft and fraud within the Bitcoin network. The case of Mt.Gox is an episode that illustrates how a digital attack to steal wallets and coins can have important

⁷⁴ Client protocol rules ensure consistency within the network to protect Bitcoin security guarantees and the main data structure (transactions and blocks). See https://en.bitcoin.it/wiki/Protocol_rules

⁷⁵ See https://en.bitcoin.it/wiki/Weaknesses#Breaking_the_cryptography

consequences on the virtual currency industry as a whole. In 2011, Tokyo-based Bitcoin trading platform Mt.Gox⁷⁶ was hacked due to a security failure in the hashing protocols of the platforms that left accounts exposed. Consequently, users' login information were stolen, resulting in the BTC prices to fall from USD 17.51 to USD 0.01 in a few minutes, resulting in losses nearing USD 8.75 million.⁷⁷ At the time, Mt.Gox did not take measures to rectify and strengthen the security of the client protocol, choosing to suspend activities and reverse transactions to fix the security flaw. As such, in 2013, the company was the target of a distributed denial of service attack (DDoS) triggering a system-wide lag in the trading activities, and a total of 850,000 BTC were stolen, equivalent to USD 460 million.⁷⁸ The reason behind Mt.Gox's failure comes from a series of vulnerabilities, including technological flaws in its software and protocol transaction identifiers. The hack left the exchange service heavily exposed to fraud and theft and demonstrated that the Bitcoin network can be compromised; the BTC exchange rates were directly impacted by the Mt.Gox hack. Mt.Gox ended up filing for bankruptcy in 2014.⁷⁹ In addition, FinCEN tracked it down in 2013 because the business had failed to comply and register its payment provider service, Dwolla, as a money transmitter business.⁸⁰

Moreover, thievery in the Bitcoin network is not uncommon. Another area of concern is the theft and hacking of Bitcoin wallets, as it was the case recently with wallet service providers Coinbase and BitFinex. Since BTC wallets are often stored on hard drives, a virus or DoS attack can easily be hacked by an experience dishonest user. The theft of

⁷⁶ Mt.Gox: Magic The Gathering Online eXchange.

⁷⁷ See <http://www.wired.com/2014/03/bitcoin-exchange/>

⁷⁸ For a complete recount of the Mt.Gox scandal, see <http://www.wired.com/2014/03/bitcoin-exchange/>

⁷⁹ Idem.

⁸⁰ CoinDesk. See <http://www.coindesk.com/why-are-the-feds-seizing-mt-gox-and-dwolla-funds/>

wallets is very difficult to retrace and users need to rely on the network to report the transaction identifiers of the stolen wallets should they reappear in the network, though they are very difficult to retrace. Needless to say that the lack of transparency and the increased anonymity features of Bitcoin pose a real challenge for users and regulators to mitigate the risks of fraud, theft and hacking.

2.4.2.3 Volatility and Lack of Funds

Due to the fixed supply of Bitcoin and the uncertainty surrounding the virtual currency industry, Bitcoin's valuation in the last two years has been subject to high volatility. When looking at the historical price data, the volatility of Bitcoin is flagrant. When BTC was first introduced in 2009, the price of one BTC was below USD 1.⁸¹ In 2013, the price of one BTC reached an exponential rate, trading at USD 1,240.⁸² Today, in 2015, the price of one BTC has dropped to a fifth of that, trading at USD 240.⁸³ As outlined previously, since Bitcoin is decentralized and there is no central bank to regulate inflation or deflation within the system, the currency has also become an instrument of speculation. The wide fluctuations in exchange rates when BTC is valued against other currencies vary tremendously, and the risk is often shifted to users, investors and businesses alike. This drawback is an area of concern that Bitcoin has failed to address so far. This poses a threat to all the stakeholders of the system and is one of the reasons why The potential lack of continuity and lack of liquidity of Bitcoin are two other elements that play against Bitcoin in its capacity to challenge real money. Indeed, the lack of funds

⁸¹ Coin Desk. See <http://www.coindesk.com/price/>

⁸² Ibid.

⁸³ Ibid.

within the system, resulting from discontinuation of services, as it was the case with Mt.Gox, and the reliance on the acceptance of the community (which can cease at any given time) could leave users hanging dry (ECB, 2015, p. 22). In that regard, the market can become insolvent and with no liquid assets to ensure that Bitcoin units continue to hold value. Regulating Bitcoin continues to remain a grey area given the constraints of developing a globalized approach to legislate the virtual currency. The technology underpinning Bitcoin has the potential to produce a shadow market with the capacity to circumvent law enforcement agencies. Consequently, the lack of user protection continues to remain an area of concern mainly because there are no mechanisms in place to protect consumers and businesses from the irreversibility of transactions, fraud, unauthorized transfers and theft.

Chapter 3: Virtual Currencies Regulation, A Must?

The obscure legal status of Bitcoin and other crypto-currencies is one of the major risks faced by the virtual currency. The inconsistency in the development of regulation and supervision of Bitcoin poses a challenge both to users and the financial community. Certain governments have encouraged discussions on the impact of virtual currencies on the financial system (UK, Canada, the United States), while others have decided to ban the use of the currency entirely (i.e., China and Iceland). This leaves Bitcoin users exposed to fraud, theft and other risks that the traditional financial system has mitigated through legislation and government oversight.

For instance, Bitcoin wallets and accounts are not protected by a deposit insurance scheme, as it is the case with banking account deposits (ECB, 2015, p.21). Furthermore, most Bitcoin services are not obligated to comply with minimal capital requirements like traditional banking institutions. In 2015, Hong Kong-based Bitcoin exchange service MyCoin abruptly ceased its operations, “stealing” about USD 387 million from 3,000 clients.⁸⁴ There are, however, a few jurisdictions that are tackling the issue of taxation and regulation of Bitcoin and other crypto-currencies.

3.1 The Dark Side of Virtual Currencies

The decentralized structure of virtual currencies makes it extremely difficult to regulate. Böhme et al. (2015, p.230) highlight important areas of concern that require regulatory oversight: Bitcoin-specific crimes (attacks on the Bitcoin network such as theft and

⁸⁴ CoinDesk. See <http://www.coindesk.com/hong-kong-exchange-mycoin-disappears-387m-reports-claim/>

DDoS/DoS attacks), money laundering (rerouting of funds through mixers to conceal proceeds of crime, illicit financial activities and profit shifting or tax evasion) and Bitcoin facilitated crimes (payment of illegal goods or services or extortion of funds). The concern has delved mostly from the activities related to the Bitcoin network, rather than the other crypto-currencies, and, to that effect, regulatory oversight has tended to target Bitcoin systems.

The risk of collapse and the lack of accountability in the Bitcoin network, as exemplified by the failure and bankruptcy of Mt.Gox, has shown that regulatory action is needed to implement mechanisms to protect consumers against the risks of virtual currencies and to better understand the challenges of imposing constraints and regulating the virtual currency industry.

3.1.1 Tax Evasion, Profit Shifting and Illegal Activities

Counterfeiting and fraud have made virtual currencies notoriously infamous in the eyes of governments across the globe. The ability to mask users' identity and the lack of mechanisms within virtual currency networks to trace a transaction back to users has hindered the capacity of governments and authorities to target tax evaders and profit shifters. Marian (2013) attributes this to the fact that crypto-currencies have similarities with traditional tax havens; they are not taxable and the user's identity remains anonymous. Indeed, virtual currencies allow tax evaders to conceal earnings from any jurisdiction because of the decentralized structure of the system.

3.1.1.1 Tax Evasion and Profit Shifting Havens

Tax-enforcement authorities across the globe have had little success in trying to tax and deter concealed revenues. While G7 members have spearheaded a tax-enforcement regime to battle offshore tax evasion and profit shifting, this remains an emerging global issue that crypto-currencies continue to threaten. As Marian (2013) discusses, virtual currency schemes like Bitcoin are immune to international efforts to counter tax evasion and profit shifting because they are not bound to a jurisdiction like traditional financial institutions. Indeed, Bitcoin funds are held on multiple digital wallets or vaults by the same user and are not dependent on the existence of intermediaries like banks or financial institutions to function (Marian, 2013, p.5). Exchanges (e.g. Coinbase) are not required to transfer BTC funds between two users; the service itself is optional since users have the capacity to move funds using a Bitcoin key. As the author points out, this could mean that crypto-currencies can become the ultimate super tax haven because funds are virtually untraceable.

In Canada and the United States, for example, the earnings accumulated on a Bitcoin wallet by a service provider are taxable. However, such income can be taxable only if the service provider voluntarily reports the revenue given that digital wallet holders are not required to identify themselves when registering for a wallet.⁸⁵ Virtual currency schemes have also evolved to allow for more complex tax evasion and profit shifting through third party platforms like Coinbase's securities exchange Lunar.⁸⁶ Trading securities and

⁸⁵ It should be noted that certain jurisdiction are looking to adopt legislation to make reporting compulsory (e.g. the European Union).

⁸⁶ Bitcoin gets first regulated US exchange. See <http://www.cnbc.com/id/102367943>

commodities using virtual currency schemes provide users with greater opportunities to remain undetected and shift profits exempt from tax. Marian (2013) explains this process by using a Bitcoin investor's interest in capitalizing on the stock of a company through a buying agent that, in turn, would transfer to the investor the Bitcoin value of the amount initially used to pay for the stock in addition to any gaining from dividends.⁸⁷ Since the transaction for the investment is done in BTC, the buying agent does not face any tax liability and is therefore not exposed to any potential economic risk, and the Bitcoin investor is only exposed to the performance of the investment initially made.⁸⁸

3.1.1.2 Money Laundering and Illegal Activities

The deterrence and prevention of money laundering and illicit financing activities has been the core challenge for government regulators across the globe. Despite the implementation of anti-money laundering legislation and an increase in regulatory oversight of virtual currency technology, the two issues continue to impede on government authorities' policymaking to protect consumers and to prevent complete anonymity and virtual currency account ownership. The concern of money laundering has become more present with the creation of "Dark Wallet"⁸⁹ by a group of coders called unSystem looking to keep the Bitcoin network decentralized and its users completely off the grid of government authorities (Shubber, 2014). The application, launched in May 2014, offers a complex level of encryption to its users and is free of charge. One of the designers of Dark Wallet, Cody Wilson, has dubbed the application "a money laundering

⁸⁷ See p.6, <http://ssrn.com/abstract=2305863>

⁸⁸ Ibid.

⁸⁹ See <https://www.darkwallet.is>

software”, because it allows for a quasi-untraceable flow of funds via virtual currency platforms (Shubber, 2014). The innovation of Dark Wallet is quite unique because it integrates laundering by default into every payment and transactions users make. The “CoinJoin” feature⁹⁰ of the wallet automatically mixes multiple payments across the network to shuffle transactions, rendering it impossible to find out where the money has gone (Shubber, 2014). As a result, after only 8 transactions, the coins in the transactions can end up in more than 256 locations (Shubber, 2014).

Dark Wallet’s stealth addresses, the application’s other laundering feature, allows users to generate a “stealth address” and a “secret key”, a surrogate address created by a user to completely hide payment made to the user’s real Bitcoin address. As Dark Wallet’s founders look to further develop additional privacy tools, they will also aim to combine the Stealth addresses and CoinJoin features to fully integrate them with the anonymity software Tor⁹¹ to protect both a user’s IP address and Bitcoin wallet information.⁹² This will enable users to completely evade regulatory oversight and allow the Bitcoin network to remain a fertile ground for money laundering.

Another challenge for regulators is the emergence of websites in the “dark web” as it was the case with Silk Road, which hosted a clandestine online service of illegal activities on Tor where payments were only accepted in Bitcoin. Silk Road displayed a myriad of illegal services and goods including the flow of illicit funding and the payments of illicit activities (Böhme et al., 2015, p.231). The founder of the website, Ross Ulbricht, was

⁹⁰ For a detailed explanation of the CoinJoin feature, see <http://www.wired.com/2014/04/dark-wallet/>

⁹¹ Tor (The Onion Router) is an anonymity network. See <https://www.torproject.org/about/overview>

⁹² See <http://www.wired.com/2014/04/dark-wallet/>

indicted on multiple charges and more than 144,000 BTCs were seized by the FBI when the website was taken down in a large-scale operation in 2013 (Ibid). Equally, in 2014, according to Tom Brewster from *The Guardian*, law enforcement authorities from 17 countries, as part of “Operation Onymous”, proceeded to shut down more than 413 “dark websites” based on the Tor network, including Silk Road 2.0 (Silk Road’s revamped version following the shut down of Ulbricht’s website), and seized among other things, more than USD 1 million worth of BTC (Brewster, 2015). Law enforcement agencies, as was the case with “Operation Onymous”, were able to exploit flaws in the website structures, and deter criminal activity due to social engineering (as undercover administrators) and to human security errors that compromised the users arrested, rather than due to the direct use of virtual currencies (Brewster, 2015). Fighting money laundering, tax evasion and the financing of crime activities has certainly become a rigorous task requiring the international collaboration of law enforcement agencies. As the virtual currency technology evolves, the development of “dark web” platforms using Bitcoin protocol and other anonymity features such as those introduced by Dark Wallet for example, continue to demonstrate that the decentralized nature of virtual currencies remains a challenge for both the believers of the technology and policymakers alike.

As Böhme et al. (2015) argue, it is difficult to impose regulatory constraints in an industry with multiple intermediaries and stakeholders, more so when the Bitcoin network closely interacts with the traditional financial system, because the users of the network are spread across the world and the privacy protections embedded within the system itself. As such, users will avoid the use of intermediaries to circumvent regulatory scrutiny and consequently hide illegal revenues from financial institutions (Böhme et al.,

2015, p.231). The authors also noted that if Bitcoin services face an important regulatory burden, these services might decide to set shop elsewhere and users might resort to anonymity service provides like Dark Wallet or Zerocash for additional security measures (p.232).

3.2 Why Regulation Matters

Virtual currencies offer an alternative to consumers to take control of their personal information as they engage in different transactions to pay for goods and services or receive funds in the cyberspace. Users have access to a technology that provides them with a virtually hack-proof online system without having to share their information with an intermediary to safeguard transaction and consumer data. Bitcoin's decentralized system is vested in offering a libertarian alternative to traditional payment systems, one with a decentralized structure that self-regulates via a global digital ledger to keep the Bitcoin network in check.

Virtual currencies have garnered a fair amount of skepticism from government regulators and the technology's detractors since Bitcoin's value against the greenback soared to unprecedented exchange rates back in 2013. Unlike Bitcoin's advocates proposed, the grass was not greener where the virtual currency flourished, and the collapse of Mt. Gox was the first of many symptoms of the risks posed by the Bitcoin network. The hacking attacks, leaving both users and administrators of Bitcoin vulnerable to theft, fraud and other digital crimes was a resonating bell for financial regulators across the globe. Governments also saw the potential of virtual currencies to become fertile ground for money laundering, terrorism financing and other illegal activities, as it was the case with

Silk Road. As it will be discussed, many states pledged to implement regulatory measures for the fight against money laundering, tax evasion and terrorism financing, and the spotlight shifted to virtual currencies, a prime vehicle to flow illicit funds across jurisdictions.

3.2.1 FATF: Global Governance and Oversight of Digital Currency

In June 2015, the FATF issued “Guidance for a risk-based approach to virtual currencies”⁹³ and urged for a closer monitoring of digital currencies to counter money laundering and terrorism financing. As the global leader for AML and counter-terrorist financing (CTF), the FATF serves as a global governance institution to support national authorities in understanding and developing regulatory laws to address the money laundering and terrorism financing risks of virtual currencies. The guidance published by the FATF proposes a series of recommendations designed to ensure international collaboration between government authorities to identify the risks and challenges posed by the anonymity features of virtual currencies and the new technology developed to further remove the ability of a law enforcement agency to identify rogue users of the Bitcoin network. A regulatory oversight is important because of the proliferation of “underground” technology designed to circumvent legislation (e.g. Dark Wallet) and maintain the Bitcoin network entirely deregulated. By building the capacity of countries to counter proceeds of illicit activities and bringing together an international network of law enforcement agencies via a global governance institution like the FATF, meaningful cooperation can certainly ensure that the risks associated with virtual currencies are

⁹³ See <http://www.fatf-gafi.org/media/fatf/documents/reports/Guidance-RBA-Virtual-Currencies.pdf>

mitigated but also that a regulatory strategy is implemented to allow for the growth and the development of virtual currency technology for the benefit of the consumers and businesses, and the globally interconnected system.

The virtual currency network is quite complex and involves several entities spread across the world to transfer funds or execute cross-border payments. The segmentation of services and as a result the system enables users and developers to create new technology and continuously improve the structure partly because the system is decentralized. The objective of virtual currency regulation should not be to constrain technology innovation, but to foster a secure environment and to avoid abuse of a system meant to ensure fair participation and treatment within the network. Bitcoin and other crypto-currencies are not immune to vulnerabilities nor are able to protect the system from risks associated with illicit activities, and that is where law enforcement agencies can provide a regulatory framework to foster an innovative environment for the development of virtual currency technology while also ensuring that the integrity of the financial system is not at stake. Certainly, governments can leverage their expertise to work with the virtual currency industry in addressing the risks associated with virtual currencies and to develop a legislative framework that is inclusive of new technologies, and more specifically of alternative payments systems.

3.3 Developments in Regulation

The regulatory aspect of virtual currencies is quite unique, because they replicate the functions of money while also competing with official currency. Virtual currencies like Bitcoin are not restricted by a geographical area and are available to users with an

Internet access across the globe. This certainly poses a challenge to policymakers and regulators in passing legislation and establishing a regulatory framework, first, to define the role of virtual currencies in the financial system and, second, to apply traditional court rulings and statutes to VCS.

So far, users have looked to use Bitcoin or other crypto-currencies as a form of payment in lieu of legal tender currency. According to Grinberg (2011, p.188), it can be concluded that given the fact that users see it as a competitor to other forms of payment, whether digital or physical, many states have taken steps to interpret the statute of virtual currencies as a form of currency with regards to the legislation for the tax or legal treatment of virtual currencies.

In this regard, a close reading to scope, for the purpose of this paper, the recently published proposed guidance and legislations in Canada, the United States and the European Union was completed to draw a portrait of the proposed and adopted regulatory measures to assess the benefits and risks of virtual currencies and to provide an extensible framework as the financial system looks to adopt digital currency technology.

As it will be shown in the following section, the challenge remains in regulating a global crypto-currency. Indeed, regulatory oversight tends to vary greatly depending on the jurisdiction; some countries have completely banned the use of virtual currencies like Bitcoin while others have taken a rather libertarian approach to allow for the development and inclusion of virtual currencies in the payments and financial system.

3.3.1 Canada

In 2014, with the Royal Assent of Bill C-31, “*An Act to Implement Certain Provisions of the Budget Tabled in Parliament on February 11, 2014 and Other Measures*”, to amend the *Proceeds of Crime (Money Laundering) and Terrorist Financing Act*, S.C. 2000, c. 17 (“PCMLTFA”), Canada was the first country to implement a legislative piece to regulate new financial transactions technologies and to adopt a nationwide digital currency law. Pursuant to the amended PCMLTFA, the legislation provides Canadian government authorities and agencies with a legal framework to have strong oversight over digital currencies as they relate to anti-money laundering law. Bill C-31 extends the application of the PCMLTFA to individuals and entities “dealing in virtual currencies”⁹⁴ and enhances client identification, verification, record keeping and registration requirements under the *Act* as money services businesses (MSB). The legislation has also redefined the money service business to include entities dealing in virtual currencies inside and outside of Canada, as follows:

244.7 (4) If subsection 256(2) comes into force, then on the later of January 1, 2015 and the day on which that subsection comes into force,

(a) the definition “money services business” in section 244.1 of the *Act*, as enacted by subsection (1), is replaced by the following:

“money services business” means an entity

(a) that has a place of business in Canada and that is engaged in the business of providing at least one of the following services:

(iv) dealing in virtual currencies, as defined by regulation[.]

⁹⁴ Bill C-31, Division 19, Part VI. See http://www.parl.gc.ca/content/hoc/Bills/412/Government/C-31/C-31_3/C-31_3.PDF

(b) that does not have a place of business in Canada, that is engaged in the business of providing at least one of the following services that is directed at entities in Canada, and that provides those services to their customers in Canada:

(iv) dealing in virtual currencies, as defined by regulation[.]⁹⁵

While MSBs operating inside and outside Canada who offer services to entities and clients in Canada are subject to Bill C-31, this does not extend to MSBs in Canada that provide digital currency services to individuals and businesses outside of the jurisdiction. Bill C-31 certainly bolsters policies and regulation to counter money laundering, terrorist financing and illegal activities from unregistered MSBs, and provides both CRA and FINTRAC with a comprehensive legislation to deter and monitor suspicious financial transaction by way of virtual currencies. However, Bill C-31 remains vague in detailing in what manner virtual currencies will be treated (i.e. what types of transactions will be subject to the law), only that the legislation will solely apply to Digital Currency MSBs. That being said, banking institutions are proscribed from opening or maintaining an account for unregistered MSBs.

Moreover, Bill C-31 changes the reporting requirements with regards to PEP, and expands the definition of PEPs to include foreign, domestic persons and the head of an international organization.⁹⁶ This is an important element of the bill because it will serve identify PEPs that are involved in transactions of \$100,000 or more and the source of funds. This is an important component of the compliance work done, as the challenge remains to monitor money laundering activities across multiple jurisdictions.

⁹⁵ Bill C-31, Part XV.1, Art. 244.1.

⁹⁶ Division 19, see Art. 258. See http://www.parl.gc.ca/content/hoc/Bills/412/Government/C-31/C-31_3/C-31_3.PDF

3.3.1.1 FINTRAC

FINTRAC is a key player in the regulatory oversight of Digital Currency MSBs, because any entity dealing in virtual currencies is required to register with the agency and remain in compliance with the reporting requirements set out by the PCMLTFA. FINTRAC's Guideline 6C: Money Business Services⁹⁷ refers specifically to all the record keeping and client identification requirements as they relate to MSBs. FINTRAC's compliance examination determines if, for example, an MSB has implemented a compliance regime to prevent and deter money laundering and the financing of terrorist activities, including the reporting of suspicious transactions, regardless of the dollar amount. In addition, obligations to report include when an MSB receives an amount of cash of \$10,000 (or its equivalent in foreign currency) from a client in a single transaction.⁹⁸ The guidelines and compliance regimes serve to provide clarity on the regulatory obligation set by the amended PCMLTFA and to ensure digital currency MSBs, as they integrate the traditional financial system, continue to engage with FINTRAC in harnessing the risks emerging from the virtual currency industry and the threats that arise from money laundering and terrorist financing in Canada and around the world.

3.3.1.2 Canada Revenue Agency

The CRA issued guidance on the tax treatment of digital currency used to pay for goods and services in barter transactions (Interpretation Bulletin IT-490, Barter Transactions),⁹⁹

⁹⁷ See <http://www.fintrac-canafe.gc.ca/publications/guide/guide-eng.asp>

⁹⁸ See 3.2 Large cash transaction records. <http://www.fintrac-canafe.gc.ca/publications/guide/guide6/6C-eng.asp>

⁹⁹ See <http://www.cra-arc.gc.ca/E/pub/tp/it490/README.html>

and when digital currency is used as a commodity resulting in losses or gains, that is taxable capital or income (Interpretation Bulletin IT-479R, Transactions in Securities).¹⁰⁰ As such, individuals and entities are not exempt from tax obligations under the *Income Tax Act*, but are treated as a commodity subject to the barter rules of the legislation. In other words, the purchase of goods and services and the resulting gain or loss should be recorded in tax returns, and GST/HST applies at fair market value when a virtual currency is used in a purchase or payment transaction.

3.3.1.3 Financial Consumer Agency of Canada

The FCAC has issued a brief overview on virtual currencies, outlining in particular the risks for Canadians using virtual currency. It notes that virtual currencies (i.e. wallets, vaults, funds stored on a hardware device or online) are not covered by Canada's Deposit Insurance Corporation deposit insurance nor are they by the provincial governments, and as a result, legal recourse is limited given the unprotected financial risk exposure consumers face when engaging in virtual currency transaction activities.¹⁰¹

3.3.1.4 Québec and the Autorité des Marchés Financiers

The *Money-Services Businesses Act*, S.C. 2010 which came into force on April 1, 2012 requires that entities and individuals offering services stipulated in the *Act* (c. 40, Sch. I, s. 4.), such as currency exchange, funds transfer and the operation of ATMs are under obligation by law to obtain a license from the AMF. Pursuant to the *Act*, MSBs that are

¹⁰⁰ See <http://www.cra-arc.gc.ca/E/pub/tp/it479r/README.html>

¹⁰¹ See <http://www.fcac-acfc.gc.ca/Eng/forConsumers/topics/paymentOptions/Pages/Virtualc-Monnaies.aspx>

both based in Quebec and those that are not established under the laws of the province or who do not have a physical space (i.e. headquarters or offices) but offer their services in Quebec or to individuals and entities in Quebec over the Internet are also required to remain in compliance with the legislation.

The *Act* was a stepping-stone in the Quebec Government's direction to counter money laundering and tax evasion in the province and to support other authorities and forces at the provincial and federal level in deterring illegal financial activities. The *Money-Services Businesses Act*, like the PCMLTFA and FINTRAC, provides the AMF with the legal framework to monitor and oversee the MSB license application process and is enforced separately from, albeit in addition to, the PCMLTFA.

Compliance obligations remain different between federal and provincial jurisdictions; the *Money-Services Businesses Act* does not have provisions pertaining to Digital Currency MSBs like the PCMLTFA. However, the *Act* covers MSBs dealing in digital currencies under the categories of MSBs requiring licensing, for example digital currency trading platforms that carry out fund transfers would be categorized under a fund transfer MSB. The regulatory expectations in Quebec continue to parallel the approach taken by the federal government and extend to scope in virtual currencies by including them in the money services business.

The Quebec and federal government are the only two jurisdictions in Canada that have adopted legislation to push for a greater regulatory oversight of Digital Currency MSBs. Paul Redman, Principal Economist for the Ontario Securities Commission (OSC), during

a Standing Senate Committee on Banking, Trade and Commerce meeting on March 12, 2015 explained that the OSC has released general guidance in their Investor News Bulletin on the potential risks associated with virtual currencies, and the release was consistent with what was published by the AMF, the U.S. Securities Exchange Commission and the North American Securities Administrators Association.¹⁰² Redman noted that the OSC continues to monitor the developments in regulation as they apply to virtual currency but he did not mention any future plans to implement legislation at the provincial level because the OSC does not have jurisdiction over digital currencies and the Commission's engagement on the matter has remained limited. As such, the OSC would only take action if there were violations of the *Ontario Securities Act* and the PCMLTFA provides the necessary regulatory oversight until the Ontario government needs to move forward with a bill proposition.

3.3.2 United States

The *Bank Secrecy Act* (BSA) – referred to as the *Currency and Foreign Transactions Reporting Act* of 1970 – is also known as the anti-money laundering law BSA/AML and is the main U.S. legislation regulating financial transactions and requiring financial institutions to report and record transactions and suspicious activities resulting from money laundering, tax evasion, or other illicit activities including terrorist financing.¹⁰³ Several AML legislations were also ratified to amend the BSA to reflect the application of the legislation by the Secretary of Treasury and FinCEN, including the *Title III of the*

¹⁰² Meeting minutes, Standing Senate Committee on Banking, Trade and Commerce. See <http://www.parl.gc.ca/content/sen/committee/412/BANC/51978-E.HTM>

¹⁰³ Bank Secrecy Act. See http://www.fincen.gov/statutes_regs/bsa/

USA PATRIOT Act (referred to as the International Money Laundering Abatement and Financial Anti-Terrorism Act of 2001),¹⁰⁴ the *Intelligence Reform & Terrorism Prevention Act* of 2004,¹⁰⁵ the United States Code Title 31 U.S.C. 5330 - Registration Of Money Transmitting Businesses (31 USC 5311-5330),¹⁰⁶ and Title 31 Chapter X - Financial Crimes Enforcement Network (formerly known as 31 CFR 103).¹⁰⁷ The latest revisions of BSA/AML legislation came with FinCEN's issuance in March 2013 of proposed Guidance entitled "Application of FinCEN's Regulations to Persons Administering, Exchanging, or Using Virtual Currencies" (FIN-2013-G001)¹⁰⁸ to clarify how the application of the regulations implemented by FinCEN, as stipulated in the BSA, apply to users, administrators and exchangers of convertible virtual currency (Sidley Austin LLP, 2013). In the Guidance, users of virtual currency are exempt from MSB registration, record keeping and reporting requirements, whereas administrators or exchangers of virtual currency (money transmitters) are identified as MSBs and therefore

¹⁰⁴ Title III of the *Patriot Act* is the most comprehensive anti-money laundering ratified legislation since the BSA and the Money Laundering Control Act of 1986. Its enactment serves to "prevent, detect and prosecute entities (namely MSBs) and individuals engaging in money laundering and terrorist financing activities". See http://www.fincen.gov/statutes_regs/files/311--LR-NoticeofFinding-Final.pdf

¹⁰⁵ The Act, enforced by the Secretary of Treasury, requires prescribed financial institutions to report international electronic transmittal of funds. See http://www.fincen.gov/news_room/aml_history.html

¹⁰⁶ 31 USC 5311-5330 requires MSBs to register their businesses with the Secretary of Treasury and defines the money services business as money transmitting business or service, which includes "money transfer system or any network of people who engage as a business in facilitating the transfer of money domestically or internationally outside of the conventional financial institutions system" (art. 2(d)(1)(A)). See http://www.gpo.gov/fdsys/pkg/USCODE-2011-title31/html/USCODE-2011-title31-subtitleIV-chap53-subchapII-sec5330.htm#5330_1

¹⁰⁷ As at July 11, 2011 ruling 76 FR 43585 ratifies § 1022.380 to clarify which entities are subject to the definitions of MSBs under the BSA and 31 CFR Chapter X (Parts 1010, 1021 and 1022). The legislative changes delineate that foreign MSBs engaging in activities within the United States are subject to BSA obligations and includes evolving technologies (i.e. virtual currencies as part of the MSB definition). See <http://www.gpo.gov/fdsys/pkg/FR-2011-07-21/pdf/2011-18309.pdf>

¹⁰⁸ See http://www.fincen.gov/statutes_regs/guidance/pdf/FIN-2013-G001.pdf

required to comply with the BSA.¹⁰⁹ The guideline also distinguishes “real” and “virtual” currency and focuses principally on convertible virtual currency “a type of virtual currency that has either an equivalent value in real currency, or acts as a substitute for real currency” (FinCEN, 2013, FIN-2013-G001).

Ripple Labs Inc. and XRP II, LLC

The BSA enforcement by FinCEN underscores the importance of the Guidance issued by the agency and the U.S. Department of Treasury’s proactive response in tackling money laundering and ensuring MSBs adopt adequate measures to comply with obligations stipulated in the BSA. Indeed, the U.S. Attorney’s Office for the Northern District of California (“USAO”) and FinCEN prosecuted San Francisco-based virtual currency exchanger Ripple Labs Inc. and its subsidiary XRP II, LLC in May 2015 for violations of the BSA,¹¹⁰ a first major pursuit against a virtual currency exchanger (DOJ, 2015). The settlement agreement, totalling USD 700,000 in monetary penalty (of which USD 450,000 included forfeiture and full cooperation of Ripple Labs) was established because Ripple Labs operated money services business XRP, one of the largest currency by capitalization and a direct competitor to Bitcoin, without prior registration with FinCEN and failed to implement an anti-money laundering program, as it is required under the BSA (DOJ, 2015). Ripple Labs also did not comply with KYC (“Know-Your-Consumer”) requirements in 2013 in a USD 250,000 sale transaction with a consumer who refused to provide information (DOJ, 2015). Additionally, its subsidiary XRP failed

¹⁰⁹ MSB Rule. 31 CFR § 1010.100(ff)(1-7). See <http://www.gpo.gov/fdsys/pkg/FR-2011-07-21/pdf/2011-18309.pdf>

¹¹⁰ Statement of Facts and Violations. See http://www.fincen.gov/news_room/nr/pdf/Ripple_Facts.pdf

to file a suspicious activity report (SAR) with FinCEN when the MSB declined a USD 32,000 transaction with a consumer due to the uncertain provenance of funds (DOJ, 2015).

3.3.2.1 *FinCEN*

Administrative Rulings

On January 2014, FinCEN penned two administrative rulings to further clarify the application and enforcement of the dispositions regarding MSBs in the BSA. The first ruling, entitled “Application of FinCEN’s Regulations to Virtual Currency Mining Operations” (FIN-2014-R001), stipulates for example the provisions amended under the BSA to modify the definition of money transmitter to include individuals that “provide money transmission services or that is engaged in the transfer of funds” (FIN-2014-R001).¹¹¹ Moreover, the ruling also focuses on Bitcoin mining and the use of virtual currency mined for a user’s own usage. It specifies that any user mining Bitcoin for personal usage be not considered an MSB because mining activities do not involve “the “acceptance” nor “transmission” of a convertible virtual currency (as defined in the guidance FIN-2013-G001) and are not the transmission of funds within the meaning of the Rule (76 FR 43585)” (FIN-2014-R001). As such, users engaging in mining operations are not subject to FinCEN’s regulation, reporting and recordkeeping requirements for MSBs, pursuant to the BSA.

¹¹¹ See http://www.fincen.gov/news_room/rp/rulings/pdf/FIN-2014-R001.pdf

The second ruling, entitled “Application of FinCEN’s Regulations to Virtual Currency Software Development and Certain Investment Activity” (FIN-2014-R002), outlines the conditions under which a business investing in virtual currency and the production and distribution of software to facilitate the company’s purchase of virtual currency for its own investment may or may not result in the company being categorized as a money transmitter under the BSA (FIN-2014-R002).¹¹² The ruling specifies that under the Rule (76 FR 43585), the definition of money transmitter does not include the production and distribution of software, as it does not represent a transmission or acceptance of value, even if the software is used to purchase virtual currency, and therefore, the company would not be subject to money transmitter regulation under the BSA (FIN-2014-R002).

However, as per the guidance FIN-2013-G001 issued by FinCEN, a user of virtual currency is a person who obtains virtual currency to purchase goods and services for their personal use, and as such, that user is not considered an MSB under FinCEN’s regulation. Furthermore, the BSA labels the mining process under a broader definition, that is obtaining virtual currencies (also referred to as earning, mining, creating, manufacturing, auto-generating, purchasing and harvesting),¹¹³ Consequently, the legal characterization remains broad and the BSA focuses on the manner through which a user sends virtual currency (accepting and transmitting) to determine if an individual or a business fall under the money transmitter category. Based on the provisions of the BSA, FinCEN’s ruling determined that if a company is not engaged in the business of exchanging convertible virtual currency for legal tender or on behalf of other individuals, and that the

¹¹² See http://www.fincen.gov/news_room/rp/rulings/pdf/FIN-2014-R002.pdf

¹¹³ FIN-2014-R002.

company only uses currency as an investment for its own account, then it is not a money transmitter or an MSB, but it acts as a user and the pertaining regulations to users of convertible virtual currency will apply (FIN-2014-R002).

3.3.2.2 *BitLicense*¹¹⁴ and Money Transmitters

New York

The New York State Department of Financial Services (NYDFS) was the first U.S. state to issue a tailored regulatory approach to Bitcoin and virtual currency. The BitLicense regulation adopted in June 2015 and titled “TITLE 23. Department Of Financial Services Chapter I. Regulations Of The Superintendent Of Financial Services Part 200. Virtual Currencies”,¹¹⁵ outlines the dispositions of a regulatory framework formally requiring both virtual currency businesses and individuals to apply for a BitLicense (non-refundable fee of USD 5,000) by August 8, 2015.¹¹⁶ The dispositions of the NYDFS’s regulation outline requirements similar to the provisions of the BSA, including record keeping, reporting and anti-money laundering requirements as well as definitions of virtual currency and fiat currency and the persons to which the legislation applies to. The text does not provide dispositions for sanction measures if an entity or an individual is not in compliance with the law.

¹¹⁴ It should be noted that 48 states currently regulate money transmitters, and many are considering application to virtual currencies (FATF, 2015, p.21).

¹¹⁵ See <http://www.dfs.ny.gov/legal/regulations/adoption/dfsp200t.pdf>

¹¹⁶ New York State Register. The 45-day grace period began on June 24, 2015. New York State Register June 24, 2015/Volume XXXVII, Issue 25, pp.7-9. See <http://docs.dos.ny.gov/info/register/2015/june24/pdf/rulemaking.pdf>

What is more, the NYDFS granted its first charter to a New York virtual currency company on May 7, 2015, itBit Trust Company, LLC.¹¹⁷ The commercial BTC exchange obtained the banking license under the New York Banking Law after the NYDFS conducted an in-depth review of the exchange and will continue to closely monitor itBit Trust Company, LLC's operations as they move to apply for a BitLicense.¹¹⁸ The NYDFS continues to review other applications for a banking license, in light of much needed regulatory oversight of virtual currency exchanges, the Department will move with further BitLicensing to ensure regulatory requirements are applied and as the state of New York works with the virtual currency industry to provide regulatory oversight.

California

The state of California is also seeking to increase regulatory oversight over money transmitting businesses. Similar to the NYDFS's BitLicense, California's Bill AB-1326, introduced to the Assembly on February 27, 2015 as the "Virtual Currency" bill, looks to address the regulation of virtual currency businesses and to require MSBs and money transmitters to register with the state's Commissioner of Business Oversight.¹¹⁹ The bill draws on comparable requirements, notably the USD 5,000 application fee and compliance with existing federal legislation. This increased regulatory oversight comes at a time when the Golden State faces multiple challenges to increase consumer protection and to mitigate the risks of crypto-currencies. As a groundbreaking move in the support of technology innovation, the Governor of California ratified bill AB-129, entitled

¹¹⁷ See <http://www.dfs.ny.gov/about/press/pr1505071.htm>

¹¹⁸ Ibid.

¹¹⁹ See http://leginfo.legislature.ca.gov/faces/billTextClient.xhtml?bill_id=201520160AB1326

“Lawful Money”, which states that alternative currency such as digital currency will be accepted as legal tender in the state of California.¹²⁰ Bill AB-129 repeals the “existing law, which bans the issuance or circulation of anything but lawful money of the United States”¹²¹ and allows for the acceptance of alternative currencies as legal tender in transactions within the state. However, the law does not obligate consumers and businesses to accept virtual currencies in transactions.

North Carolina

The proposed Bill H289, the “*Money Transmitters Act*” (MTA), was introduced in March 2015 in the state of North Carolina to regulate money transmission and to implement mandatory licensing for virtual currency businesses.¹²² Bill H289, which passed the House reading in May 2015, is similar to how Bitcoin is treated in other states like New York and California where the approach is to recognize Bitcoin businesses as money transmitters. However, North Carolina’s minimum net requirement is set at USD 250,000 and businesses are required to post a security bond of USD 150,000,¹²³ which is much stricter than the application for a BitLicense in comparison to New York or California.¹²⁴

At the federal level, Bitcoin is defined as property, but North Carolina’s approach pushes towards a ratification of the *Money Transmitters Act* at the federal level to encompass

¹²⁰ Assembly Floor Analysis (06/19/14). See http://leginfo.legislature.ca.gov/faces/billAnalysisClient.xhtml?bill_id=201320140AB129

¹²¹ Ibid.

¹²² Bill H289. See <http://ncleg.net/Sessions/2015/Bills/House/PDF/H289v1.pdf>

¹²³ Bill H289, opt. cit. § 53-208.46(a), § 53-208.47(a),(b).

¹²⁴ A BitLicense application in New York and California is set at USD 5,000.

virtual currencies, as is the case with the proposed NC Bill H289¹²⁵. The MTA reduces the regulatory burden on MSBs and money transmitters dealing with virtual currencies because its regulatory framework for money transmission could enable businesses to obtain one license to operate in multiple states as stipulated in § 53-208.43(a) and (b) of Bill H289.¹²⁶ This is different from New York's BitLicense for example, which requires compliance with federal laws, but obliges businesses from other states, already holding a "BitLicense", to apply for one to specifically operate in the state of New York.

Since NC's MTA bases its AML framework on the guidance issued by FinCEN and the BSA at the federal level, businesses are required to comply with anti-money laundering and registration requirements as postulated in the federal legislation. Conversely, while the licensure requirements imposed by California's Bill AB-1326 are also similar to the federal MTA and to NC's Bill H289 in principle, but as per the language governing the definition of virtual currency business, entities providing exchange services would not be required to seek licensure (AB-1326, §26000(c)). Equally, agents of virtual currency businesses are not required to comply with state legislation, as the provisions were removed from the proposed bill (AB-1326, §26008.2). The licensure requirements have not yet been formally adopted by the state legislature in the states of North Carolina¹²⁷ and California,¹²⁸ but the proposed process sets the tone as other state regulators try to

¹²⁵ Ibid.

¹²⁶ See <http://ncleg.net/Sessions/2015/Bills/House/PDF/H289v1.pdf>

¹²⁷ As of June 23, 2015, the sponsored bill has passed second House reading and first Senate reading and was to be studied during the next Committee on Commerce meeting. See

<http://ncleg.net/gascripts/BillLookUp/BillLookUp.pl?Session=2015&BillID=H289&submitButton=Go>

¹²⁸ As of July 21, 2015, the sponsored bill has passed Assembly reading, and is at first Senate reading. The bill was referred to Senate Committee on Banking and Financial Institutions. See https://leginfo.legislature.ca.gov/faces/billStatusClient.xhtml?bill_id=201520160AB1326

determine if licensing and virtual currency regulation, in addition to federal regulation, is appropriate to govern users, administrators and agents engaging in virtual currency activity.

3.3.2.3 Paying the Government in Bitcoin: Utah, New Hampshire and New York

Three states, Utah (Bill HCR-6),¹²⁹ New Hampshire (Bill HB552)¹³⁰ and New York (Bill LS 2535),¹³¹ have introduced proposed bills to accept virtual currency for the payments of state services. The New York bill sponsored by City Councilman Mark Levine aims to enable New Yorkers to pay for their parking fines in BTCs.¹³² All three states are considering the important benefits of accepting Bitcoin as a form of legal tender for tax payments and other government services. Of course, long-term objective is to bridge the gap between emerging virtual currency technologies and the regulatory framework implemented at the state level.

3.3.2.4 Internal Revenue Service

The IRS issued virtual currency guidance in March 2014 regarding the tax treatment of virtual currency as property under U.S. federal tax law. Notice 2014-21 provides general guidelines for the application of property transactions rules for virtual currencies. The IRS refers to FinCEN's guidance on convertible currencies (FIN-2013-G001) and defines the treatment of virtual currency reporting requirements as similar to those for property. The application of the tax regulation resembles those implemented by the CRA in

¹²⁹ See <http://le.utah.gov/~2015/bills/static/hcr006.html>

¹³⁰ See <https://legiscan.com/NH/text/HB552/2015>

¹³¹ See <http://www.coindesk.com/new-york-city-bill-bitcoin-fines-fees/>

¹³² Ibid.

Canada, where taxpayers must report any income received from dealing with virtual currencies and that the dollar amount is determined at fair market value. The IRS notice will apply to previous years and any Bitcoin payments exceeding \$600 in U.S. dollar value, once converted at fair market value, is be subject to IRS tax reporting, requiring persons and businesses trading in virtual money to pay tax and provide supporting documentation to the revenue agency.¹³³

3.3.2.5 The U.S. Federal Reserve

So far, no other U.S. financial governance authorities have not issued rulings supporting the framework established by the IRS; the U.S. Federal Reserve has only published a Bitcoin Strategy paper outlining opportunities to improve the payments system, which include virtual currencies.¹³⁴ The Federal Reserve recognizes that a Digital Value Transfer Vehicle (DVTV)¹³⁵ like Bitcoin can “facilitate the transfer of value between two individuals” (Badev and Chen, 2014, p.1). The Federal Reserve’s interest to modernize the payment’s system would impact five primary areas encompassing more than 29 billion payments, which represents 12% of payments in the U.S. annually (Federal Reserve, 2015, p.39).

The report also outlines various strategies where Bitcoin could fit the Federal Reserve’s approach, including the implementation of a safer, standardized and faster payments system (Federal Reserve, 2015, p.3). This could certainly prove to be a challenge to the

¹³³ See <http://www.irs.gov/pub/irs-drop/n-14-21.pdf>

¹³⁴ See <https://fedpaymentsimprovement.org/wp-content/uploads/strategies-improving-us-payment-system.pdf>

¹³⁵ Decentralized digital stores of value that can be exchanged (Federal Reserve, 2015, p.39).

technology developed, should the Federal Reserve move with the option to design and develop its own digital transfer vehicle system (Federal Reserve, 2015, p.39-41).

3.3.2.6 The Security Exchange Commission

Lastly, the US Securities and Exchange Commission (SEC) adopted rules to facilitate crowdfunding for startup companies. Virtual currency companies will benefit from Tier-based offerings of securities as per the SEC's Regulation A+: "Tier 1 – up to USD 20 million in a 12-month period, with not more than \$6 million in offers by selling security-holders that are affiliates of the issuer, and Tier 2 – up to USD 50 million in a 12-month period, with not more than \$15 million in offers by selling security-holders that are affiliates of the issuer" (SEC, 2015). Under the previous rule "Regulation A" for example, a Tier 2 offering was limited to USD 5 million for any 12-month period, with no more than USD 1.5 million of securities offered by security-holders of the company.¹³⁶ What this means is that the tier requirements will pave the way for small businesses dealing in virtual currencies to raise and have access to capital by completing an initial public offering (IPO) for up to USD 50 million without having to be a reporting or publically listed company and by following the streamlined SEC review and compliance process which, with the adoption of Regulation A+, eased the reporting burden on small businesses (SEC, 2015). The revamped amendments to the regulation is attractive for smaller businesses looking to raise capital, and will provide blockchain technology companies within the virtual currency industry with a low-cost avenue to sell

¹³⁶ RIN 3235-AL39: Proposed rule amendments for small and additional issues exemptions under section 3(b) of the Securities Act, p.9. See <http://www.sec.gov/rules/proposed/2013/33-9497.pdf>

securities to potential investors over the Internet without the administrative burden they have to usually face with SEC registration (SEC, 2015).

Despite the complexity of state and federal legislative structure in the United States, its government institutions and law enforcement agencies at the state level are spearheading legislation propositions to adopt virtual currencies or its technology to some degree. While the MTA at the federal level offers a broader legal framework to regulate money-transmitting businesses, the regulation at the state-level focuses on the development and adoption of licensing requirements for businesses engaging in virtual currency activity, as is the case with the states of California, North Carolina and New York.

However, state regulators are moving in a different direction than the guidance proposed at the federal level in shaping U.S. virtual currency regulation. While regulatory bodies at the federal level have published guidance and ratified already existing legislation, state institutions, on the other hand have moved to specifically regulate virtual currencies in such way to promote legislation that is more friendly to virtual currency technology, like in the state of California where virtual currencies (amongst them Bitcoin) were granted legal money status.¹³⁷ Many states, as mentioned previously, have led the way to promote wider virtual currency adoption. So far it seems that the other states are looking to build the right framework to support virtual currency oversight without limiting the development of the virtual currency. What this could mean is that even if states are drafting virtual currency specific legislation or ratifying existing laws to create virtual

¹³⁷ Bill AB-129, Lawful Money. See http://leginfo.legislature.ca.gov/faces/billNavClient.xhtml?bill_id=201320140AB129#content_anchor

currency technology-friendly legislation, two areas of concern, consumer protection and anti-money laundering, will remain at the core of the debate, and that could prove to be a challenge for the virtual currency industry.

3.3.3 European Union

3.3.3.1 EU Rulings

The European Central Bank (ECB) published two reports on virtual currency schemes, “Virtual Currency Schemes” in October 2012¹³⁸ and subsequently in February 2015 “Virtual Currency Schemes – a further analysis”¹³⁹ discussed in chapter 2 of this paper. The reports are the only studies conducted by the EU on the matter and, so far, no legislation has passed to regulate virtual currencies or those dealing in virtual currency activities. The ECB’s reports concluded that virtual currency schemes fall out of the scope of the Payment Services Directive 2007/64/EC¹⁴⁰ because the payments institutions required to comply with the regulation are not authorized to issue money (Library of Congress, 2014).

However, Directive 2000/46/EC on the taking up, pursuit of and prudential supervision of the business of electronic money institutions¹⁴¹ could apply to virtual currencies, money transmitters and MSBs. Articles 3(a) and 3(b) of the Directive define electronic money institution as “an undertaking or any other legal person, other than a credit institution

¹³⁸ See <https://www.ecb.europa.eu/pub/pdf/other/virtualcurrencyschemes201210en.pdf>

¹³⁹ See <https://www.ecb.europa.eu/pub/pdf/other/virtualcurrencyschemesen.pdf>

¹⁴⁰ See <http://eur-lex.europa.eu/LexUriServ/LexUriServ.do?uri=OJ:L:2007:319:0001:0036:EN:PDF>

¹⁴¹ See <http://eur-lex.europa.eu/LexUriServ/LexUriServ.do?uri=CELEX:32000L0046:EN:HTML>

which issues means of payment in the form of electronic money”¹⁴² and electronic money as having “monetary value as represented by a claim on the issuer which is (1) stored on an electronic device, (2) issued on receipt of funds of an amount not less in value than the monetary value issued and (3) accepted as means of payment by undertakings other than the issuer”.¹⁴³ Equally, the definition of electronic money as per the Electronic Money Directive 2009/110/EC, as outlined by the ECB’s report, only applies to virtual currencies on two aspects: that it is a form of electronic storage and that there is acceptance as a means of payment by a legal or natural person other than the issuer (Library of Congress, 2014).

The European Banking Authority (EBA) issued a warning for consumers engaging in virtual currency activities given the fact that the EU Commission has not yet formally proposed legislation to regulate virtual currencies across the EU. The EBA cautions against the risks of virtual currencies, noting that consumers are at risk of losing money, and these funds are not protected by legislation. What is more, given the instable value of crypto-currencies like Bitcoin, consumers are not covered by deposit insurance and are at risk should a virtual currency business cease its operations.¹⁴⁴ The EBA notes that while there is no legislation in place to regulate platforms, exchanges and virtual currency transaction activities, consumers should keep in mind that the use of such might have tax implications even if used outside of the EU.¹⁴⁵

¹⁴² Directive 2000/46/EC, art. 3(a).

¹⁴³ Directive 2000/46/EC, art. 3(b).

¹⁴⁴ See <http://www.eba.europa.eu/-/eba-warns-consumers-on-virtual-currencies>

¹⁴⁵ Ibid.

In an attempt to strengthen regulatory oversight of virtual currency activities linked to money laundering and terrorist financing, the European Union Commission adopted new rules in May 2015, as part of the key actions on the European Security Agenda,¹⁴⁶ to fight money laundering and terrorism financing. The anti-money laundering rules mark a new turn in the EU's commitment to the international community in tackling the illicit flow of funds to crime networks and activities.

The regulatory framework stems from recommendations set forth by the FATF in 2012 to implement AML policies and regulations and to combat terrorism financing. The package issued in June 2015 included the proposal by the EU of a Directive “on the prevention of the use of the financial system for the purpose of money laundering and terrorist financing”¹⁴⁷ which will require EU banking institutions of all member states to report on customer accounts and transactions receiving or sending more than EUR 1,000 (or the equivalent in virtual currencies).¹⁴⁸ As per Article 2(4) of the proposed Directive, EU banks will also be required to establish AML processes to closely monitor and flag any single transactions as well as multiple transfers below EUR 1,000.¹⁴⁹ By implementing stricter AML rules to hinder illicit financial activities and terrorism financing opportunities, the Commission aims to safeguard the integrity of the financial system and to ensure consistency between the EU and the international approaches to address emerging threats and technologies.

¹⁴⁶ See IP/15/4865, http://europa.eu/rapid/press-release_IP-15-5001_en.htm

¹⁴⁷ See <http://eur-lex.europa.eu/legal-content/EN/TXT/HTML/?uri=CELEX:52013PC0045&from=EN>

¹⁴⁸ Ibid.

¹⁴⁹ See <http://cointelegraph.com/news/114659/eu-banks-forced-to-report-bitcoin-linked-accounts-transacting-over-1000>

A Europe-wide approach to harmonize virtual currency legislation has been a challenge given the implications of member states, which also need to adopt a cohesive legislative framework across all jurisdictions. The regulatory situation in the EU is scattered, and beyond the studies and recommendations of the ECB, the Commission and the EBA, EU states have taken different steps to regulate, restrict or accept virtual currency technology. According to the report titled “Regulation of Bitcoin in Selected Jurisdictions”¹⁵⁰ issued in January 2014 by the Library of Congress, 16 EU member states (of the EU-28) out of the 47 jurisdictions reviewed, reported on central banks and government authorities releasing statements, discussions, directives, guidance, rulings or proposals of legislation on virtual currencies transactions, virtual currency as legal tender, the impact of virtual currencies on national currency and security, risks of fraud, money laundering and terrorism financing as well as tax law (Library of Congress, 2014).

It should be noted that the countries surveyed focused on Bitcoin-related activities and the Bitcoin network in general. Given the extensive research conducted by multiple jurisdictions and the different stages of regulation and discussions across the EU, this paper highlights the regulation and applicable proposals of two selected jurisdictions that have taken considerable steps on the matter: the United Kingdom and Germany. Other jurisdictions in Europe have also investigated the implication of virtual currencies (especially Bitcoin) with regards to tax law and other legislation to counter money laundering activities but have not issued advanced guidance on the matter.

¹⁵⁰ See <http://www.loc.gov/law/help/bitcoin-survey/regulation-of-bitcoin.pdf>

United Kingdom

On November 3, 2014 the UK government launched a 3-month public consultation on digital currencies to examine the risks and benefits and to determine if further government action is required to mitigate potential threats. Among the stakeholders consulted were members of various financial sectors, academics, virtual currency users and developers and other government departments.¹⁵¹ The UK's HM Treasury published the follow-up report to the call for information on March 18, 2015 summarizing a total of 120 responses outlining the benefits of digital currencies as a method of payment as well as the risks, such as those linking virtual currencies to crime and illicit activities (HM Treasury, 2015). Amongst the proposed next steps introduced by the UK government at Budget 2015 were the application of AML regulation to virtual currency exchanges in the UK and a consultation in the new Parliament for a regulatory framework to monitor and apply AML legislation to the virtual currency industry (HM Treasury, 2015).

Additionally, the government will launch a GBP 10 million new research initiative joining the efforts of the Research Councils, Alan Turing Institute, Digital Catapult and the virtual currency industry to address the challenges of digital currency technology.¹⁵² The HM Treasury will also work with the Financial Conduct Authority, and the Prudential Regulatory Authority to develop a regulatory framework to address the needs and risks of virtual currency technology.¹⁵³ Finally, the government will seek guidance from the British Standards Institution to create consumer protection standards for digital

¹⁵¹ See <https://www.gov.uk/government/consultations/digital-currencies-call-for-information/digital-currencies-call-for-information>

¹⁵² Ibid.

¹⁵³ See <http://www.coindesk.com/breaking-uk-treasury-issues-landmark-digital-currencies-report/>

currencies and virtual currency industry best practices.¹⁵⁴ The UK government with these policy and changes do not aim to keep a regulatory grasp on users, merchants and administrators of virtual currencies, but to consider regulations in a context of a much larger global market for virtual currency services. Albeit the regulatory constraints, virtual currency users and businesses in the UK have the potential to work in a unique environment with a clear set of rules and pledging for the government for research to better understand the technology and the virtual currency environment.

Germany

Germany's BaFin, the Federal Financial Supervisory Authority, published a series of supervisory assessments regarding Bitcoin and virtual currencies and providing an overview of the risks to consumers using a "non-government substitute currency" (BaFin, 2014). The BaFin established that, pursuant to section 1 (11) sentence 1 of the *German Banking Act* (KWG),¹⁵⁵ BTCs are legally binding financial instruments as a form of unit of account but are not considered to be legal tender (BaFin, 2014). As such, the BaFin concluded that BTCs are therefore considered to be private money, because the properties of virtual currencies are similar to those of units of value in barter transactions. Additionally, under section 54 of the *Act*, commercial use of BTC could be subject to regulation under the KWG, but licensing is not required for the way in which BTCs are acquired (mining) or accepted as form of payment (BaFin, 2014).

¹⁵⁴ Ibid.

¹⁵⁵ See

http://www.bundesbank.de/Redaktion/EN/Downloads/Tasks/Banking_supervision/Acts_Regulations_Guidelines/banking_act.pdf?__blob=publicationFile

Equally, under the provisions the *Payment Services Supervision Act (ZAG)*,¹⁵⁶ BTCs are not considered electronic money (BaFin, 2014). In the near future, Germany has not excluded the possibility to implement a mandatory licensing for users and administrators of the virtual currency.

3.3.3.2 Value-Added Tax: The Virtual Currency Tax Puzzle in the EU

Since January 1, 2015, the new regulatory changes adopted via the Council Implementing Regulation (EU) No 1042/2013¹⁵⁷ and amending Implementing Regulation (EU) No 282/2011¹⁵⁸ introduced new changes to the VAT tax laws regarding the place of supply of services and new measure to the VAT tax. As a result of these regulatory changes, ratified to prevent tax evasion and money laundering, companies within and outside EU member states are required to record the country of residence (location) of their consumers, therefore reducing profit-shifting opportunities for business entities and consumers alike.

The Directorate General for Taxation and Customs Union (DG TAXUD) published explanatory notes on the EU VAT changes outlining the legally binding provisions, including the types of transactions covered by the regulatory changes and the nine options under which a company can provide the location of the consumer – companies are required to collect two different pieces of evidence as proof.¹⁵⁹ According to the

¹⁵⁶ See

http://www.bafin.de/SharedDocs/Downloads/EN/Aufsichtsrecht/dl_zag_en.pdf?__blob=publicationFile

¹⁵⁷ See <http://eur-lex.europa.eu/LexUriServ/LexUriServ.do?uri=OJ:L:2013:284:0001:0009:EN:PDF>

¹⁵⁸ See <http://eur-lex.europa.eu/LexUriServ/LexUriServ.do?uri=OJ:L:2011:077:0001:0022:EN:PDF>

¹⁵⁹ Ibid, p.61/92. Example of evidence includes: billing address, IP address, bank details, SIM card country code, location of fixed land line and other commercially relevant information.

explanatory notes, the definition of digital services and goods is very broad and its interpretation seems to include in virtual currencies “the supply of digitised products generally, including software and changes to or upgrades of software”.¹⁶⁰

Given the lack of an EU-wide agreement and of member states on the classification of virtual currencies for tax purposes (e.g. Finland and Germany have exempted virtual currencies from VAT, unlike the UK), taxation for virtual currencies remains a point of contention as members states look to integrate this type of revenue into domestic tax framework. Normally, the VAT is based on the taxation rate of the nation of consumption rather than where the supplier is located. With the new legislative changes, users of virtual currencies are facing double taxation that could result in important tax increases. As it stands, virtual currencies users and administrators will find it difficult to comply with the location requirements of the new rulings, because of the degree of anonymity Bitcoin and other crypto-currencies offer.

As EU member states look to implement the VAT rulings, central legislators in Sweden have submitted a request to the European Court of Justice (ECJ) in 2014 for a preliminary ruling to determine if VAT should be applicable to virtual currency transactions for goods and services.¹⁶¹ The adoption of the ruling on the Swedish inquiry could oblige users to reconsider the implication of using virtual currencies (such as the disclosure of location and double taxation) and merchants to comply with data collection on consumers and face increased VAT levels when accepting virtual currencies as a form of payment.

¹⁶⁰ Ibid, p.85/92.

¹⁶¹ See <http://curia.europa.eu/juris/document/document.jsf?docid=154888&doclang=EN>

However, since the preliminary application,¹⁶² on July 16, 2015, the Advocate General of the ECJ, Juliane Kokott, published a legal opinion stating that as per article 135, paragraph 1(e) of the VAT Directive 2006/112/CE,¹⁶³ Bitcoin-related transactions (i.e. purchases and sales) should be exempted from VAT.¹⁶⁴

United Kingdom

On the tax regulation front, HM Revenue and Customs, the UK's tax authorities, released on March 3, 2014 a brief titled "Revenue and Customs Brief 9 (2014): Bitcoin and other cryptocurrencies"¹⁶⁵ announcing policy changes to the tax treatment of Bitcoin and other crypto-currency activities as they relate to the VAT, Corporation Tax (CT), Income Tax (IT) and Capital Gains Tax (CGT).¹⁶⁶ As such, any income received from Bitcoin mining activities will be exempt from VAT, as well as income received by miners for other activities including services given for the verification of transactions and other transactions as defined under the EU VAT Directive (2006/112/EC).¹⁶⁷ Similarly, Bitcoin exchanged for real currencies such as the Sterling (GBP) will be exempt from VAT.

¹⁶² Case C-264/14. See

<http://curia.europa.eu/juris/document/document.jsf?text=&docid=154888&pageIndex=0&doclang=en&mode=lst&dir=&occ=first&part=1&cid=270415>

¹⁶³ See <http://eur-lex.europa.eu/legal-content/EN-FR/TXT/?uri=CELEX:32006L0112&from=EN>

¹⁶⁴ Text available in French only as at July 20, 2015. See

<http://curia.europa.eu/juris/document/document.jsf?text=&docid=165919&pageIndex=0&doclang=FR&mode=lst&dir=&occ=first&part=1&cid=358404>

¹⁶⁵ See <https://www.gov.uk/government/publications/revenue-and-customs-brief-9-2014-bitcoin-and-other-cryptocurrencies/revenue-and-customs-brief-9-2014-bitcoin-and-other-cryptocurrencies>

¹⁶⁶ Ibid.

¹⁶⁷ Article 135(1)(d): "transactions, including negotiation, concerning deposit and current accounts, payments, transfers, debts, cheques and other negotiable instruments, but excluding debt collection". See <http://eur-lex.europa.eu/legal-content/EN/TXT/HTML/?uri=CELEX:32006L0112&from=EN>

As per the brief, the only instance where VAT will be applied is for transactions of exchanging BTC for goods or services; VAT will be due in GBP equivalency at the initial point of transaction. However, the CT and IT tax will respectively apply for transactions resulting in gains or losses from currency movements, and for profits and losses in accounts belonging to non-incorporated businesses dealing with Bitcoin transactions. Instances where chargeable gains are considered, CT and CGT rules will apply on losses or gains incurred if they are accrued by an individual or a company. HM Revenue and Customs noted that tax treatments outlined by the brief pertain to the taxation of crypto-currencies could be reviewed in light of potential regulatory changes resulting from changes to the EU VAT Directive.

Germany

Germany's Finance Ministry, the Bundesministerium der Finanzen (BMF), took a different approach than the one adopted by its British counterpart. According to a document issued by the BMF on May 14, 2014 in response to a parliamentary question from member Dr. Tim Ostermann, the Ministry suggested that the sale of goods and services should be subject to German tax law and pursuant to Article 4(8)(b)(c)(d)(f)(g) of the UStG (German VAT law),¹⁶⁸ Bitcoin and other crypto-currencies would have the same tax treatment as foreign currencies. The BMF also concluded that under Article 135.1(d) of the EU Directive 2006/112/EC,¹⁶⁹ virtual currencies would be exempt from VAT, given the fact that a payment is not considered a service under the provisions of the

¹⁶⁸ BMF, DOK: 2014/0393906. See <http://www.bundesverband-bitcoin.de/wp-content/uploads/2014/05/140512-Antwort-PStS-Meister.pdf>

¹⁶⁹ Ibid.

EU Directive. The BMF's decision contrasts with the United Kingdom's move to exempt the commercial sale of BTC from VAT obligations, and includes the taxation on a sale of goods and services as well as the exchange of BTCs to foreign currency which businesses convert following a sale transaction.

Unlike the UK's Treasury, the BMF's tax ruling treats Bitcoin as a commodity rather than private money with regards to tax liability for consumers and businesses. What is at stake, however, is the legal structure other members of the EU will follow (for example Spain has adopted VAT exemption, but Sweden has not) as Germany and the United Kingdom remain divided on the tax treatment of virtual currencies and as mentioned previously, as the VAT landscape in the EU continues to take shape. Nevertheless, many key players within the EU have taken different steps to regulate virtual currencies, as is the case with Germany and the United Kingdom.

The supranational institution that is the EU has shown that consensus is quite difficult to achieve, and that it will take some time before all member states are on the same page. So far, as seen with Germany and the UK, the only areas of agreement are the warnings issued against the risks of using virtual currencies, in particular the risks of money laundering, and the needs to further assess virtual currencies to protect consumers and to implement mechanisms to mitigate the risks of virtual currency activity. It is by joining efforts and working in collaboration that EU member states will be able to take advantage and explore the long-term benefits of virtual currency technology for the EU public and private sector alike.

Lastly, the three jurisdictions assessed, that is Canada, the United States and the EU, have all concentrated efforts to increase the understanding of virtual currencies, and have proactively discussed, developed and ratified legislation and guidance in this area. All three jurisdictions have, at the federal and state/member state level, to a degree, drafted institutional frameworks to legislate virtual currencies. However, the *laissez-faire* approach of most provincial jurisdictions (to the exception of Quebec) has perhaps hindered Canada's capacity to issue virtual currency specific legislation (even if it was the first country to adopt a nationwide law on virtual currencies), as it was done in the United States and the EU.

Despite the complexity of the legislative structure in two of the most important jurisdictions in the world, the EU and the United States were able to breakthrough and formalize a process in adopting virtual currency technology while also defining its regulatory parameters. What can be concluded is that all three jurisdictions have developed promising avenues for the future of virtual currencies, such as the BitLicense in New York and California, the definition of MSBs in Bill C-31 in Canada and the VAT Directive in the EU. In the future, the next step will be to work together in homogenizing the status of virtual currencies across jurisdictions within the existing regulatory frameworks and to support a global approach to better regulate the virtual currency industry.

Chapter 4: Bitcoin, A Game-changing Technology

The characteristics that define virtual currencies (i.e. security, low transaction costs, blockchain technology) have garnered the attention of a big player in the financial system, the banking sector. The advent of new technologies has shaken an industry rooted in a traditional structure. The banking system has fended off new payment technologies since the creation of PayPal, creating less effective technologies,¹⁷⁰ but has found a challenge in adapting and understanding virtual currencies. As a new technology, virtual currencies have shown that they can not only function within a decentralized system, but also show promising opportunities to open up the market and revamp the financial system, as we know it. Whether it is blockchain technology or smart digital assets (e.g. asset registries), the virtual currency industry is embracing its role as both a disruptor and an agent of change in the financial system, and the banking sector has started to pay attention. This chapter focuses on the two roles of virtual currencies as a disruptor to the traditional banking system, and that of an agent of change to facilitate the adoption of new technologies. The argument presented demonstrates that virtual currencies were initially introduced as challengers to the banking system, however, the potential of virtual currency technology serves as an accelerator of change within a system that has been slow to respond to the demands of consumers and businesses. As a result, unconventional payment technologies were able to capitalize on the development of payment and banking services outside of the traditional system.

¹⁷⁰ For example, in 2013, French banks worked together to develop a payment system equivalent to PayPal, more than 15 years after the leading payment system came into the market. See <http://techcrunch.com/2013/09/17/with-paylib-french-banks-work-together-to-compete-with-paypal/>

4.1 Globally Connected Economy: Can Virtual Currencies Disrupt the Traditional Banking System?

4.1.1 The decline of banking and the pressure of virtual currencies

The third theme of this paper is the erosion of power of the traditional banking system,¹⁷¹ in particular that of banking institutions, due the pressures of new technologies challenging the centralized nature of the banking industry. Indeed, virtual currencies are changing the nature of the business operations of banks and the market structure of the banking industry with respect to changes in regulation, information exchange, transportability of money, trading delivery and technology, and the competitive nature of the global banking system (Llewellyn 1996, p.142-143).

The declining role of banks in the financial system has allowed the emergence of non-financial and non-banking institutions to position themselves in the financial system and erode the market share of banking institutions. As such, this structural change has enabled virtual currencies to become supplier of certain “banking” services that were usually limited to the banking sector. Llewellyn outlines two characteristics that make banking firms essential to the traditional banking system: they possess certain monopoly powers such as their role in asset transformation and they have a clear comparative advantage attributed to certain technicalities (such as liquidity of assets and inside information that is not available to the general public), which give them a dominant status in the market (Llewellyn 1996, p.145). However, both these advantages have been

¹⁷¹ For the purpose of this paper, the traditional banking system includes banking institutions, but excludes national central banks.

undermined by financial innovation and deregulation, two areas where virtual currencies have been able to undercut the competition.

As a result, in the words of Llewellyn (1996), the lack of strict disclosure laws and the decline of entry barriers have hindered the capacity of banks to maintain monopoly status vis-à-vis new technologies. Adding to that, the lower costs of using virtual currencies have provided consumers with a wider access to alternative methods of payments accessible virtually anywhere and at any time. Consumers have access to more opportunities as more choices are offered to them via Bitcoin or other crypto-currencies, for example. Llewellyn also underlines an interesting point; that banks have traditionally had a monitoring role within the traditional financial system, a fee-based activity that has now shifted under the umbrella of rating agencies. This problem is inexistent with virtual currencies because the system itself is decentralized and, as such, users of the network undertake the monitoring process without having to rely on any intermediary.

Where banks still hold the upper hand on virtual currencies is on the question of deposit insurance; virtual currencies do not have contingency measures to completely protect the funds of a user of the system, if funds are stolen, they are very difficult and almost impossible to recover (e.g. Mt. Gox). In various ways, our traditional financial system still profoundly relies on a centralized and well-defined structure (central banks, banking institutions, markets, etc.), and the demand for banks will continue to increase. Llewellyn (1996, p.152) outlines three circumstances where virtual currency businesses and industry cannot compete with the banking structure: first, consumer preferences for a product or service may change at any time; second, the demand for a certain service or firm shifts as

new players integrate the market and third, consumer preferences change as alternative ways to satisfy a demand become available. A driving force of the banking sector is that while the industry might be in decline, it does not mean that the firms within it are as well. The business of banking is in constant evolution and continues to be influenced by national and international institutions to renew itself (IMF, 2009, p.3-5). Virtual currencies can become disruptors of the traditional banking system as they have the potential to render information accessible to the public. Their decentralized approach is not as impacted by what Llewellyn refers to as “excess structure”,¹⁷² because the entire network is in the cyberspace and it does not require a physical location to function.

Another feature that can be referred to is the process of deconstruction, also discussed by Llewellyn, which allows new entities to enter a market since they do not have to be part of the whole process. Indeed, the banking system transitioned from a very rigid framework, where banks offered multiple services at once (e.g. insurance, securitization, deposits, etc.), to a system where services are decomposed to be offered by different firms at once resulting in the market becoming both diversified and competitive. Unlike banks, the virtual currency industry has the capacity to efficiently provide payment and exchange services on a stand-alone basis.

That being said, the banking system should look at virtual currency technology as an agent of change rather than of disruption. The decline of banking is a consequence of a system that is very slow to progress and where change comes sporadically and often

¹⁷² In multiple jurisdictions, the number of branches is excessive with an implicit unnecessary duplication of banking infrastructure: fixed costs and delivery facilities (Llewellyn, 1996, p.161).

times is not unanimously adopted. Virtual currency technology can have a direct impact on how financial services will be delivered to consumers, because it reduces the dependence of having physical locations across the network, which is part of the core structure of the banking system (Llewellyn, 1996, p.168).

4.1.2 Joining Forces: Banking and Virtual Currency Technology

Indeed, alternative technologies have already transformed how people keep track of their finances, mobile banking being a prime example, but virtual currencies offer a new way of securing transactions and personal information online, a potential game changer for the banking system. The adoption of virtual currency technology by banks (i.e. blockchain technology), which is analyzed in the section below, could bring more efficiency, security and speed to the system. The potential of settling transactions in minutes rather than days without the risks of fraud (i.e. manipulation of transactions) is unprecedented, and major banking institutions like UBS, Barclays and Goldman Sachs, are buying into it (Kelly, 2015). But how can the banking sector benefit from the innovative potential of virtual currency technology? The Euro Banking Association published a report in May 2015 exploring the application of electronic and alternative payments (e.g. virtual currencies) to the banking sector. The EBA draws attention to the practical implications of crypto-currencies into four categories: currencies, asset registries, application stacks and asset-centric technologies.¹⁷³ In addition to the exchange service, the EBA proposes the use of virtual currencies for real-time payments, documentary trade and asset servicing (EBA, 2015, p.4) and analyzes their relevance to the banking and payments

¹⁷³ See Annex III.

system. As such, the EBA concluded that virtual currencies do not “pass the test” to be acknowledged as fiat currencies despite their capacity to hold the same characteristics as fiat money (EBA, 2015, p.7). Instead, virtual currencies should be regarded as digital assets and payment service providers (PSPs) rather than as legal tender (Ibid). This can also be attributed to the different interpretation of crypto-currencies across jurisdictions, as outlined in chapter 3. On the other hand, the EBA recognizes the potential of crypto-currencies as asset registries for assets other than BTCs, including but not limited to, stocks and vehicles, to record ownership of an asset using the global public ledger technology (Ibid). Another example where banks could benefit from crypto-currencies as asset registries is in the development of blockchain technology to record transaction data for an initial public offering.

Moreover, another innovative aspect for the banking sector is the development of application stacks; that is using crypto-currencies to execute and complete payments through decentralized networks, a sort of “cloud service”¹⁷⁴ for the banking sector (EBA, 2015, p.9).

As noted by the EBA, the application stack function is still at its early development stages, and consequently, they focus on the asset-centric functions for crypto-currencies (i.e. exchange, real-time payments, documentary trade and asset servicing). These functions hold promise to leverage virtual currency technology and benefit the banking sector because they can: offer lower conversion and cost advantages (when used to

¹⁷⁴ This application is referred to as DApps (Distributed Applications) and DAO (Distributed Autonomous Organisations). It is a form of open source application with encryption capabilities; Bitcoin for example, is a form of DApp. (EBA, 2015, p.9 and p.23).

convert fiat currency, e.g. Forex) as an exchange service and to clear real-time payments, and reduce auditing and governance expenditures when used for documentary trade (e.g. use of a letter of credit in international trade) and asset servicing (e.g. liquidation of an investor's position) (EBA, 2015, p.12-18).

The application of crypto-currency technology at different levels can certainly benefit the banking sector, as outlined by the EBA. The advantages of a decentralized application system can serve to improve the banking sector and to encourage the banking sector in developing a collaborative partnership with the currency industry. As a result, the banking and payments system, by integrating crypto-currency technology through the four areas identified, can continue to ensure the financial system remains secure and efficient.

4.2 The Innovative Potential of Bitcoin

As explained in this paper, virtual currencies offer innovative opportunities that deliver efficient and easy-to-use payment technology. For example, Australians are able to send BTC funds directly to their banking accounts using service provider Living Room of Satoshi, thus extending the reach of the virtual currency outside of the Bitcoin network, which was unprecedented.¹⁷⁵ Bitcoin in particular combines four technologies that showcase its potential to facilitate the movement of funds, increase user security and provide opportunities for the financial system in its role as a decentralized P2P network, a

¹⁷⁵ This allows for the transferability of funds between the traditional and the virtual currency system. See <http://cointelegraph.com/news/114566/australians-can-now-send-bitcoin-directly-to-their-bank-accounts-or-anyone-elses>

currency-issuing system, a transaction-verification system (global digital ledger) and as a public ledger relying on blockchain and sidechain technology (Senate, 2014, p.10).

First, in a decentralized P2P network like Bitcoin, BTCs can be transferred between users, businesses and exchanges without the interference of an intermediary. Second, because Bitcoin is a currency-issuing system, if the currency in a jurisdiction cease to exist, as was the case with Zimbabwe's fiat currency in June 2015,¹⁷⁶ the value of BTCs can still be held or exchanged without the use of banknotes or coins. In addition to these innovative capacities, where Bitcoin's global digital ledger and blockchain technology offer can be used in a number of applications that can translate in opportunities for the financial system. Indeed, the global digital ledger is one of the few decentralized and encryption transaction-verification systems to prevent cyber-attacks and counterfeiting attempts (Senate, 2014, p.12). In that aspect, virtual currencies can play an important role in shaping the payments system due to its privacy protection and record keeping.

Where the traditional system can unlock the real potential of Bitcoin is in its blockchain and sidechain technology.¹⁷⁷ The objective of sidechain technology is to have a blockchain built to support a country's national currency and without the need of banknotes and coins (Back, Corallo, Dashjr, Friedenbach, Maxwell et al., 2014). While it seems like an ambitious project, banking institutions have started paying attention. In its response to the call for information on digital money issued by HM Treasury, Citigroup cites that the

¹⁷⁶ Zimbabwe is the first country to see its currency expire. See <http://cointelegraph.com/news/114553/one-paper-currency-is-officially-extinct>

¹⁷⁷ Sidechain technology is new blockchain technology backed by Bitcoin contract, the same way the U.S. dollar is pegged against gold.

potential use of virtual currencies can be realized through the issuance of a state legal digital tender, a currency that would replace the current physical tender and other electronic payment technologies (Citigroup, 2014). They explain that not only can a new form of digital tender reduce the cost of “moving and handling money” but also that blockchain technology can secure transactions involving digital assets (Citigroup, 2014).

The technology behind Bitcoin’s digital ledger has also garnered the attention of Wall Street. The New York’s stock exchange NASDAQ is testing blockchain technology application to oversee stock trades on its Private Market, designed for private companies to manage shares before an IPO.¹⁷⁸ In this case, blockchain technology serves to simplify private trading in a secure system where the pre-IPO company can track transactions activities for stock trades and stock ownership in real time.¹⁷⁹ Ultimately, the banking system must balance the open nature of virtual currency technology and the need for privacy and transaction monitoring. The relationship between virtual currency technology and the financial system is quite complex, but the influence of the banking system can only increase the potential of Bitcoin and other crypto-currencies to create efficient and unconventional ways to deliver financial services and to move virtual currencies away from the role of disruptors towards that of innovators and solution providers of a traditional financial system embracing the digitalization of its system, one transaction at a time.

¹⁷⁸ See <http://www.wired.com/2015/05/nasdaq-bringing-bitcoin-closer-stock-market/>

¹⁷⁹ Ibid.

Conclusion

Certainly, the decentralization of virtual currency enables consumers to transfer funds, send payments and connect with other consumers for financial opportunities outside the traditional financial and payment system structure normally requiring the use of a banking institution. The main crypto-currency analyzed in this paper, Bitcoin, has the potential to remain a major player in advancing virtual currencies, more so as it seeks to become a mainstream currency. Bitcoin can hold the three functions of money to a certain degree, making it a viable alternative to real currency. As a form of complementary money, it combines the characteristics of both money and quasi-money, but only time will tell if it becomes a mainstream form of legal money accepted globally.

Though what Bitcoin really means for the payments and banking system is the emergence of a new technology that can adapt to the demands of a traditional system in much need of change. Through blockchain technology, the protection of information, or even its global digital ledger, the footprint of Bitcoin as a pioneer of crypto-currencies continues to grow. As the Canadian Senate concluded, for virtual currencies to continue to remain fertile ground for advancements in payment and transaction technology “[it] requires a light regulatory touch – almost a hands off approach, in other words, not necessarily regulation, but regulation as necessary” (Senate, 2015).

Needless to say that the cautious attitude exhibited by policymakers, governments, law enforcement authorities, consumers and the global financial system towards virtual currencies can be understandable. As the growth of the virtual currency system is likely

to unrelentingly continue for the years to come, it will become more challenging for regulators, users and the virtual currency network to find a middle ground between a centralized structure and a decentralized system, and that is because virtual currencies look to facilitate the flow of funds outside of the conventional financial system and to remain unregulated. Virtual currency funds flow in private systems and bypass the regulatory burden faced by financial and banking institutions within the system, relying on the network itself to comply with regulations set forth by law enforcement agencies.

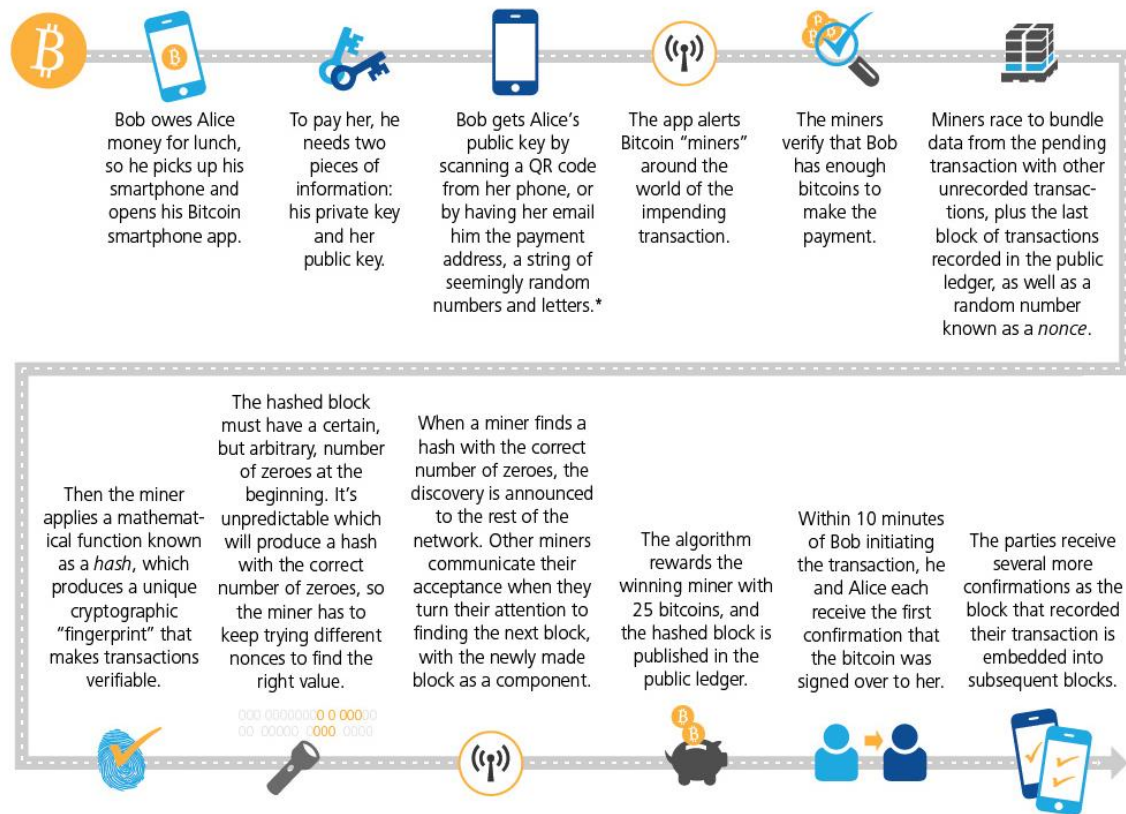
As it was discussed in this paper, the actions taken by government authorities globally have shown that regulation has already started to reach the virtual currency industry, and that even if virtual currencies were, by design, meant to circumvent the laws, the very users of the technology are supportive of regulation that does not hinder innovation but keeps the integrity of the system in check. At present time, it is no surprise that the role of government is coming into focus as various jurisdictions, especially in North America and Europe, have already adopted virtual currency legislation or have begun a process of regulatory rulemaking to better assess and understand virtual currency technology. The regulatory challenge faced by the three countries analyzed in this paper (i.e. Canada, the United States, the EU) is that multiple jurisdictions within are working on the same issues using different approaches. Consequently, this process can prove to be lengthy and difficult to follow, and that is where a comprehensive regulatory framework, similar to the one developed by the EU on the VAT Directive, can provide a stronger governance mechanism to regulate virtual currency technology. So far, it seems that it is the United States that has emerged as the frontrunner in embracing virtual currency technology, with California being the first state to recognize virtual currency as legal money. One thing is

certain; the key takeaway is that as public interest for virtual currencies continue to grow in major economies, an increased global cooperation can provide a global governance structure to help deter money laundering and illicit activities, and to shape the future of payment technology innovation.

The analysis conducted in this paper can help address another interesting question, that is the issuance by government virtual currency-based technology in the form of legal tender and to digitize other components of the financial system as proposed by Citigroup. Surely, virtual currencies can both be a gateway for technological advancement and promote a comprehensive approach of governance to address market demand, banking sector concerns and consumer protection. Virtual currency systems have the capacity to transform relationship of consumers with money, and to bring new opportunities to the financial sector. As it was analyzed in this paper, this could change the governance structure of the traditional banking system vis-à-vis payment technologies, especially as the banking sector continues to explore blockchain technology. Undoubtedly, the digitization of money requires a certain level of compliance and regulation. Any future for Bitcoin and other crypto-currencies will require a strong partnership with governments and the financial system to preserve the right to self-regulation of virtual currency systems, to foster new technology developments and to protect consumers from the potential risks of virtual currencies. The success of Bitcoin and other crypto-currencies can be attributed to a collective desire to challenge institutions, structured legislative frameworks, the state and governments; but the viability of virtual currencies and its technology will be the fruit of a collaborative effort as we step into a digitized economy in the years to come.

Annex I

Figure 1: How the Bitcoin network works



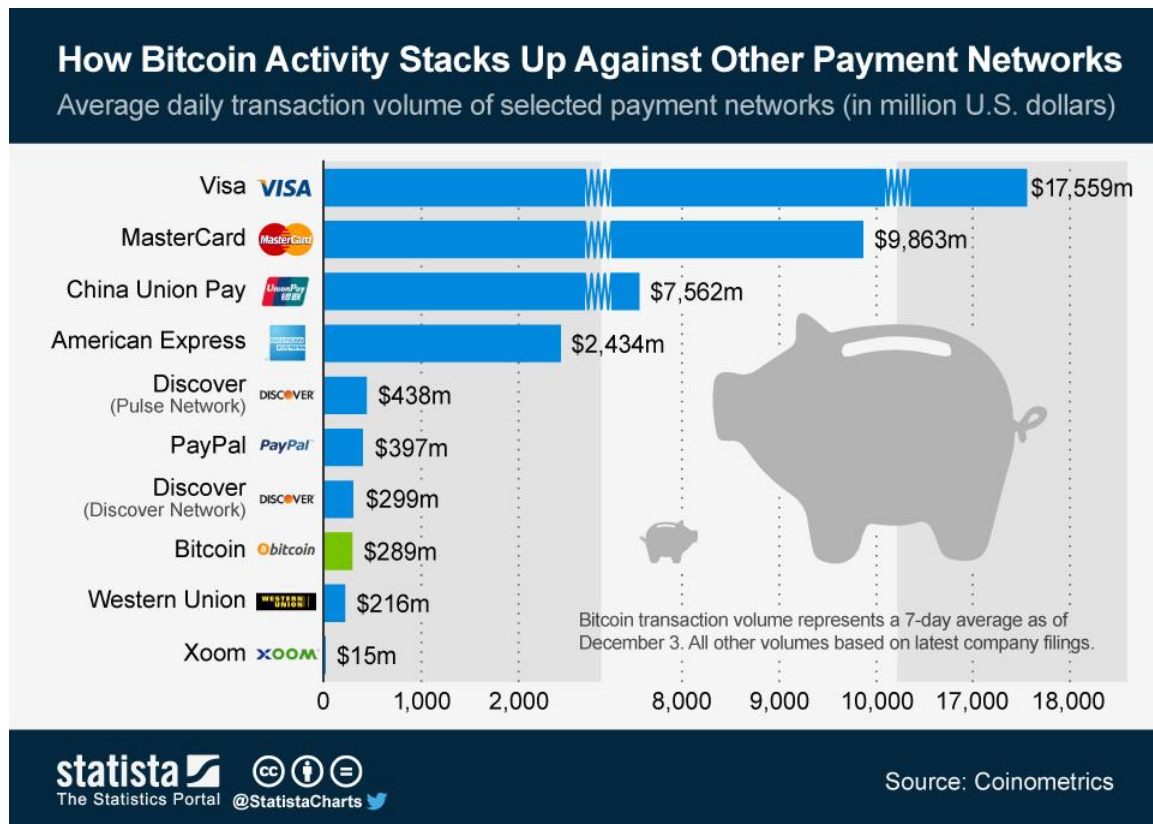
* Anyone who has a public key can send money to a Bitcoin address, but only a signature generated by the private key can release money from it.

Source: American Banker, <http://cdn.americanbanker.com/media/ui/how-bit-works-big.jpg>.

Graphic: Deloitte University Press | DUPress.com

Annex II

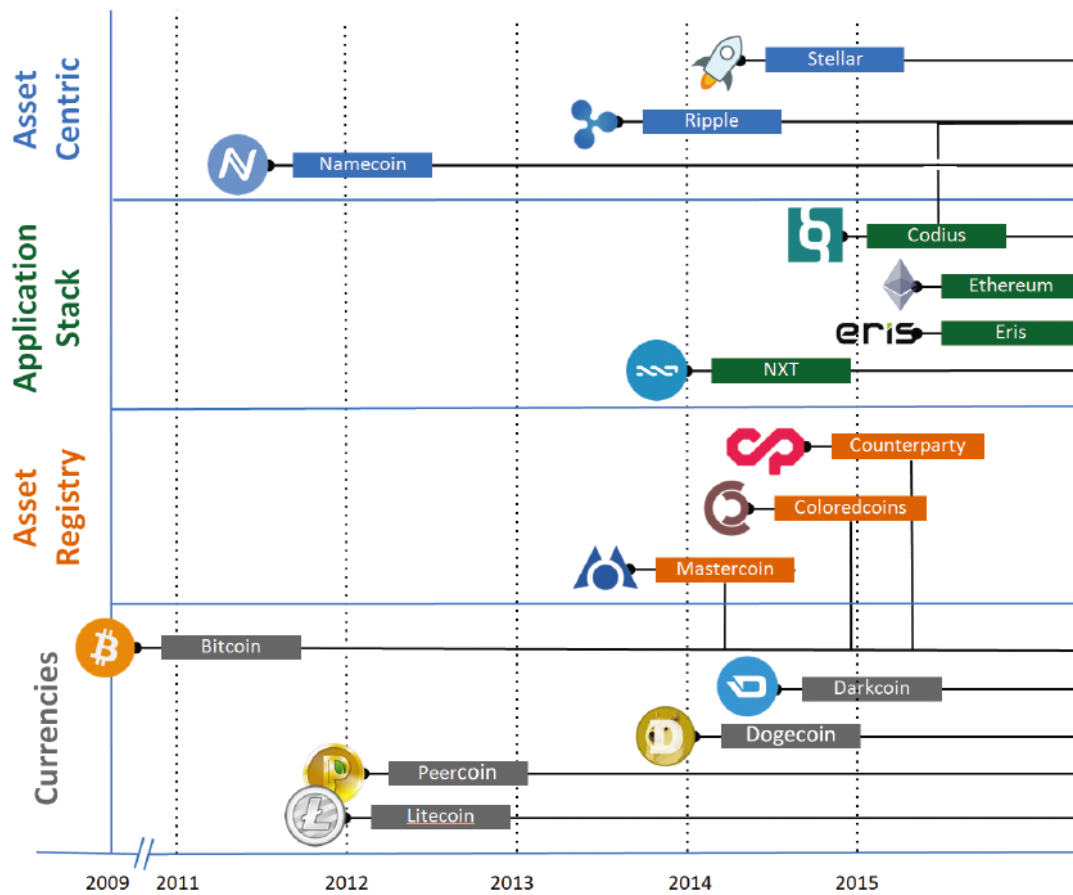
Figure 2: Bitcoin activity vs. other payment networks (2013)



Source: <http://www.statista.com/chart/1681/daily-transaction-volume-of-payment-networks/>

Annex III

Figure 3: Four Categories of Crypto-technologies



Source: EBA, 2015, p.5.

Bibliography

- Amazon. (2014, November 17). *Amazon Coins terms and conditions*. Retrieved from <http://www.amazon.com/gp/help/customer/display.html?nodeId=201434520>
- Back, A., Corallo, M., Dashjr, L., Friedenbach, M., Maxwell, A. M., et al. (2014). *Enabling blockchain innovations with pegged sidechains*. Retrieved from <https://blockstream.com/sidechains.pdf>
- Badev, A., Chen, M. (2014). Bitcoin: Technical background and data analysis. *Finance and Economics Discussion Series Divisions of Research & Statistics and Monetary Affairs, Federal Reserve Board*. Retrieved from <http://www.federalreserve.gov/econresdata/feds/2014/files/2014104pap.pdf>
- BaFin (2014). Bitcoins: Supervisory assessment and risks to users. *BaFin Expert Articles*. Retrieved from http://www.bafin.de/SharedDocs/Veroeffentlichungen/EN/Fachartikel/2014/fa_bj_1401_bitcoins_en.html
- Bank of Canada. (2012). What is money?. *Bank of Canada*. Retrieved from http://www.bankofcanada.ca/wp-content/uploads/2010/11/what_is_money.pdf
- Bank of England. (2014). Explanatory Notes - M4. *Bank of England*. Retrieved from <http://www.bankofengland.co.uk/statistics/Pages/iadb/notesiadb/M4.aspx>
- Bentov, I., Lee, C., Mizrahi, A., Rosenfeld, M. (2014). Proof of Activity: Extending Bitcoin's Proof of Work via Proof of Stake. *Cryptology ePrint Archive*. Retrieved from <https://eprint.iacr.org/2014/452.pdf>
- Bitcoin Wiki. (2015). *Proof of work*. Retrieved from https://en.bitcoin.it/wiki/Proof_of_work
- Bitcoin Wiki. (2015). *Hash*. Retrieved from <https://en.bitcoin.it/wiki/Hash>
- Bitcoin Wiki. (2015). *Address*. Retrieved from <https://en.bitcoin.it/wiki/Address>
- Böhme, R., Christin, N., Edelman, B., and Moore, T. (2015). Bitcoin: Economics, technology, and governance. *Journal of Economic Perspectives*, 29(2): 213-38. DOI: 10.1257/jep.29.2.213
- Brewster, T.F. (2014, November 7). Silk Road 2.0 targeted in 'Operation Onymous' dark-web takedown. *The Guardian*. Retrieved from <http://www.theguardian.com/technology/2014/nov/07/silk-road-20-operation-onymous-dark-web-drugs-takedown>

- Buntix, J.P. (2015, March 20). What is Bitcoin? – Finite coin supply. *Digital Money Times*. Retrieved from <http://digitalmoneytimes.com/novicebeginners/what-is-bitcoin-finite-coin-supply/>
- Canada Revenue Agency (CRA). (2013). *What you should know about digital currency*. Retrieved from <http://www.cra-arc.gc.ca/nwsrm/fctshts/2013/m11/fs131105-eng.html>
- Castronova, E. (2002). On virtual economies. *CESifo Working Paper Series No. 752*. Retrieved from <http://ssrn.com/abstract=338500>
- Chronicle Herald. (2015, June 23). CIBC: Banks will adapt to new financial tech such as Bitcoin. *Chronicle Herald*. Retrieved from <http://thechronicleherald.ca/business/1294814-cibc-banks-will-adapt-to-new-financial-tech-such-as-bitcoin>
- CoinDesk. (2015, May 22). Bitfinex warns customers to halt deposits after suspected hack. *CoinDesk*. Retrieved from <http://www.coindesk.com/bitfinex-warns-customers-to-halt-deposits-after-suspected-hack/>
- Croushore, D. (2006). *Money and banking: A policy-oriented approach*. Boston: Houghton Mifflin Company.
- CSBS. (2014, December 16). *CSBS policy on state virtual currency regulation*. Retrieved from <http://www.csbs.org/regulatory/ep/Documents/CSBS%20Policy%20on%20State%20Virtual%20Currency%20Regulation%20--%20Dec.%2016%202014.pdf>
- Department of Justice (DOJ). (2015, May 5). Ripple Labs Inc. resolves criminal investigation. *News Release, Office of Public Affairs*. Retrieved from <http://www.justice.gov/opa/pr/ripple-labs-inc-resolves-criminal-investigation>
- Dowd, K. (2014). New private monies: A bit-part player?. *Institute of Economic Affairs Monographs*. Retrieved from <http://ssrn.com/abstract=2535299>
- Euro Banking Association. (2015). *Cryptotechnologies, a major IT innovation and catalyst for change: 4 categories, 4 applications and 4 scenarios*. Retrieved from https://www.abe-eba.eu/downloads/knowledge-and-research/EBA_20150511_EBA_Cryptotechnologies_a_major_IT_innovation_v1.0.pdf
- European Central Bank (2012). Virtual currency schemes. *ECB Report 2012*. Retrieved from <https://www.ecb.europa.eu/pub/pdf/other/virtualcurrencyschemes201210en.pdf>

- European Central Bank (2015). Virtual currency schemes – a further analysis. *ECB Report 2015*. Retrieved from <https://www.ecb.europa.eu/pub/pdf/other/virtualcurrencyschemesen.pdf>
- FATF. (2015). Guidance for a risk-based approach to virtual currencies. *Financial Action Task Force Report*. Retrieved from <http://www.fatf-gafi.org/media/fatf/documents/reports/Guidance-RBA-Virtual-Currencies.pdf>
- Federal Reserve. (2005). Definition of M1, M2, M3. *The Federal Reserve System, Purposes and Functions*. Retrieved from http://www.federalreserve.gov/pf/pdf/pf_complete.pdf
- Federal Reserve (2015). Strategies for improving the U.S. payment system. *The Federal Reserve System*. Retrieved from <https://fedpaymentsimprovement.org/wp-content/uploads/strategies-improving-us-payment-system.pdf>
- Financial Times. (2015). Definition of M0, M1, M2, M3, M4. *Financial Times Lexicon*. Retrieved from <http://lexicon.ft.com/Term?term=m0,-m1,-m2,-m3,-m4>
- Flavelle, D. (2013, July 23). How credit card fees for merchants work. *The Star*. Retrieved from http://www.thestar.com/business/personal_finance/2013/07/23/how_credit_card_fees_for_merchants_work.html
- Graydon, C. (2014, August 30). Bitcoin's future: Proof-Of-Stake vs Proof-Of-Work. *CryptocoinNews*. Retrieved from <https://www.cryptocoinsnews.com/bitcoins-future-proof-of-stake-vs-proof-of-work/>
- Grinberg, R. (2011). Bitcoin: An innovative alternative digital currency. *Hastings Science & Technology Law Journal*, 4:160-181. Retrieved from <http://ssrn.com/abstract=1817857>
- Hayek, F. A. (1976). *Denationalization of Money: An analysis of the theory and practice of concurrent currencies*. London: Institute of Economic Affairs. Reprinted in Kresge, Stephen (ed). (1999) *The Collected Works of F.A.Hayek*. Retrieved from <https://mises.org/library/denationalisation-money-argument-refined>
- Herlin, P. (2015). *Apple, Bitcoin, Paypal, Google: La fin des banques?*. Paris: Les Éditions Eyrolles.
- HM Treasury. (2015). Digital currencies: response to the call for evidence. *HM Treasury*. Retrieved from https://www.gov.uk/government/uploads/system/uploads/attachment_data/file/414040/digital_currencies_response_to_call_for_information_final_changes.pdf

- International Monetary Fund. (2000). Chapter 6: Money, Credit, and Debt. In International Monetary Fund (Ed.), *Monetary and Financial Statistics Manual* (pp.57-71). Retrieved from <http://www.imf.org/external/pubs/ft/mfs/manual/pdf/mmfsch6.pdf>
- International Monetary Fund. (2009). Lessons of the financial crisis for future regulation of financial institutions and markets and for liquidity management. *IMF*. Retrieved from <http://www.imf.org/external/np/pp/eng/2009/020409.pdf>
- Internal Revenue Service (IRS). (2014). Notice 2014-21: Virtual Currency. *Internal Revenue Service*. Retrieved from <http://www.irs.gov/pub/irs-drop/n-14-21.pdf>
- Kelly, J. (2015, July 22). Betting on blockchain: firms seek fortune in bitcoin's plumbing. *UK Reuters*. Retrieved from <http://uk.reuters.com/article/2015/07/22/us-tech-bitcoin-blockchain-idUKKCN0PW1RT20150722>
- Library of Congress (2014). Regulation of Bitcoin in selected jurisdictions. *Library of Congress*. Retrieved from http://www.loc.gov/law/help/bitcoin-survey/#skip_menu
- Llewellyn, D. (1996). Banking in the 21st century: The transformation of an industry. *Reserve Bank of Australia*. Retrieved from <http://www.rba.gov.au/publications/confs/1996/pdf/llewellyn.pdf>
- Lo, S., Wang, C. (2014). Current perspectives: Bitcoin as money?. *Federal Reserve Bank of Boston*. (14-4). Retrieved from <http://www.bostonfed.org/economic/current-policy-perspectives/2014/cpp1404.pdf>
- Luther, W. J. and Olson, J. (2013). Bitcoin is memory. *Journal of Prices & Markets*, 3(3): 22-33. Retrieved from <http://ssrn.com/abstract=2275730> or <http://dx.doi.org/10.2139/ssrn.2275730>
- Marian, O.Y. (2013). Are cryptocurrencies 'Super' tax havens? *112 Michigan Law Review First Impressions*, 38 (2013). Retrieved from: <http://ssrn.com/abstract=2305863>
- McLeay, M., Radia, A., Thomas, R. (2014). Money in the modern economy: an introduction. *Bank of England Quarterly Bulletin*. Retrieved from <http://www.bankofengland.co.uk/publications/Documents/quarterlybulletin/2014/qb14q101.pdf>
- Menger, C. (1871). *Grundsätze*. Alabama: Ludwig Von Mises Institute. Retrieved from http://docs.mises.de/Menger/Menger_Grundsaeetze.pdf (in English: https://mises.org/system/tdf/Principles%20of%20Economics_5.pdf?file=1&type=document).

- Menger, C. (1892). On the origin of money. In Wiley (Ed.) on behalf of the Royal Economic Society, *The Economic Journal*, 2(6): 239-255. DOI: 10.2307/2956146
- O'Brien, Y.Y.C (2007). Table 1 summary of types and compositions of the monetary aggregates in the EMU and fifteen non-EU countries (p.5). *The Federal Reserve System*. Retrieved from <http://www.federalreserve.gov/pubs/feds/2007/200702/200702pap.pdf>
- Raeder, C. L. (2013). Hayek on the role of reason in human affairs. *First Principles Journal*. Retrieved from <http://www.firstprinciplesjournal.com/articles.aspx?article=1513&theme=home&page=1&loc=b&type=ctbf>.
- Richards, C. (2015, June 22). Barclays signs 'Proof of Concept' with Safello to explore blockchain advantages. *The CoinTelegraph*. Retrieved from <http://cointelegraph.com/news/114645/barclays-signs-proof-of-concept-with-safello-to-explore-blockchain-advantages>
- Rolnick, A.J., Weber, D.E. (1997). Money, inflation, and output under fiat and commodity standards. *Journal of Political Economy*, 105(6): 1308-1321. DOI: 10.1086/516394
- Security Exchange Commission (SEC). (2015, March 25). SEC adopts rules to facilitate smaller companies' access to capital. *Press Release* Retrieved from <http://www.sec.gov/news/pressrelease/2015-49.html#.VRReYjvF94j>
- Senate, Standing Senate Committee on Banking, Trade and Commerce. (2015). Digital Currency: You can't flip this coin!. *Report of the Standing Senate Committee on Banking, Trade and Commerce*. Retrieved from <http://www.parl.gc.ca/Content/SEN/Committee/412/banc/rep/rep12jun15-e.pdf>
- Shubber, K. (2014, May 1). Hyper-anonymising Bitcoin Service 'Dark Wallet' launches today. *CoinDesk*. Retrieved from <http://www.coindesk.com/hyper-anonymising-bitcoin-service-dark-wallet-launches-today/>
- Sidley Austin LLP. (2013, March 26). FinCEN issues guidance on application of Bank Secrecy Act regulations to virtual currencies. *News and Insights: Sidley Austin LLP*. Retrieved from <http://www.sidley.com/news/fincen-issues-guidance-on-application-of-bank-secrecy-act-regulations-to-virtual-currencies-03-26-2013>
- Solomon, E. H. (1997). *Virtual money: Understanding the power and risks of money's high-speed journey into electronic space*. New York: Oxford University Press.

- Stafford, P. (2015, May 26). NASDAQ to step up blockchain trials. *Financial Times*. Retrieved from <http://www.ft.com/intl/cms/s/0/81b6145c-0309-11e5-b31d-00144feabdc0.html#axzz3bM5re5uc>
- Stanley, J.W. (1876). *Money and the Mechanism of Exchange*. New York: D. Appleton and Co.
- Securities Exchange Commission (SEC). (2015). *SEC adopts rules to facilitate smaller companies' access to capital*. Press Release, SEC. Retrieved from <http://www.sec.gov/news/pressrelease/2015-49.html#.VRReYjvF94j>
- White, L.H. (1984). Competitive payments systems and the unit of account. In American Economic Association (Ed.), *The American Economic Review* (pp.699-712). Retrieved from <http://www.jstor.org/stable/1805134>
- World Bank (2015). *Money and quasi money (M2) as % of GDP*. Retrieved from <http://data.worldbank.org/indicator/FM.LBL.MQMY.GD.ZS>