Regulating Digital Currencies: A Study on Bitcoin

Research Project for Emerging Issues/Advanced Topics Course

Diploma in Investigative and Forensic Accounting Program

University of Toronto

Prepared by Vivian Shum

June 20, 2014

For Prof. Leonard Brooks

TABLE OF CONTENTS

1.0 INTRODUCTION

With Bloomberg providing their global subscribers pricing of the cryptocurrency Bitcoin[1] and the Standing Senate Committee on Banking, Trade, and Commerce authorized to examine and report on the use of digital currency, digital currencies are being recognized as an emerging issue; however, no government has yet defined "digital currency"[2]. Digital currencies, like bitcoin (BTC), have picked up momentum in the past few years in providing an alternative payment method for purchases, increasing its overall value. Hailed as the new way of facilitating purchases and transfer of funds without extra costs from banks, it has slowly become more of a high-risk investment product due to its volatility and increased popularity in the economic mainstream. The lack of regulation has been noted as its largest advantage and weakest link, as noted in the case of Mt. Gox, a Bitcoin exchange that filed for civil rehabilitation in February 2014 and bankruptcy soon after[3].

Governments are now being challenged with implementing laws that are suitable for digital currencies as they become more mainstream. Lack of regulation makes digital currencies the ideal vehicle for money laundering purposes, whereas excessive regulation will defeat the purpose of some digital currencies' market advantage. The lack of jurisdiction also adds onto the confusion: while Canada has taken the stance of it not

[1] Van Name, T. "Bitcoin Now on Bloomberg," *Bloomberg Now*, April 30, 2014, http://www.bloomberg.com/now/2014-04-30/bitcoin-now-bloomberg/ Accessed on May 1, 2014.
[2] Kinsella, N. A. "Committee Authorized to Study the Use of Digital Currency," *Debates of the Senate*, March 25, 2014, http://www.parl.gc.ca/Content/Sen/Chamber/412/Debates/pdf/043db_2014-03-25-e.pdf Accessed on April 22, 2014.
[3] Announcement the applicability of US Bankruptcy Code Chapter 15, *MtGox Co., Ltd.*, March 14, 2014, https://www.mtgox.com/img/pdf/20140314-announcement_chapter15.pdf Accessed on April 23, 2014.

being legal tender but still allowed for use[4], other countries have banned or have started taking serious thought in the regulation of digital currencies.

2.0 EXECUTIVE SUMMARY

2.1 Background

A transaction of what one would regard as "simple" has now grown to be complex due to the introduction of digital currencies. Instead of paying with cash, cheque, or with plastic (i.e. debit or credit card), the customer can now initiate a payment to the vendor while the vendor hands them their purchase, be it a virtual item in a game, tokens to be used to purchase tunes, or an exchange to digital coinage. The cryptocurrency bitcoin is now in the spotlight due to its decentralized nature, relieving users of transaction fees. However, its ability to provide anonymous transactions has made it an ideal currency for illicit transfers due to its ease in convertibility between bitcoin and real currency.

As discussions about regulating digital currencies become more prominent, some users have already started to counter their attempts, with software and applications like the Dark Wallet[5], where its main function is to launder bitcoins. Governments are cautious in quickly providing a response; while it is important to ensure that the risks relating to the usage of digital coinage are reduced, they also need to consider what users value from the currency: privacy. The concern on privacy raises issues on whether governments should regulate a currency that is intangible and not belonging to any jurisdictions, yet may have an effect on the economy.

---

[4] George-Cosh, D. "Canada Says Bitcoin Isn't Legal Tender," *The Wall Street Journal Canada*, January 16, 2014, http://blogs.wsj.com/canadarealtime/2014/01/16/canada-says-bitcoin-isnt-legal-tender/ Accessed on April 23, 2014

[5] *Dark Wallet*, http://darkwallet.is/ Accessed on May 5, 2014

2.2 Contents of the Report

The intention of this paper is to provide a basis of knowledge on digital currencies, issues that currently exist for the government and the possible effects that should be considered for its users.

Section 3 provides the basic definition of digital currencies including the different forms and a comparison between digital currencies versus real currencies, focusing on Bitcoin as the main type of digital currency to be examined. Section 4 provides a more in-depth analysis on what cryptocurrencies are considered as based on our current system of definitions. Once the digital currency has been defined based on the currently available definitions that matches current legislation, its ability for money laundering is discussed in Section 5.

Section 6 offers a glimpse of responses from different governments and also the responses from digital currency users to thwart government attempts at regulation. A proposal of potentially regulating the starting point of the transaction is considered in Section 7, with Section 8 presenting the implications on investigative forensic accountants (IFAs) based on their current treatment and the proposed treatment of digital currencies.

3.0 BACKGROUND DEFINITIONS

3.1 The Basics: What are Digital Currencies?

Digital currencies consist mainly of virtual currencies, electronic currencies, and cryptocurrencies. The main differences between the three types relate mostly to its convertibility between the digital currency and real currency as well as its centralization.

Value of the digital coinage is built on consumer confidence; if there is a demand, the item can then be quantified with a value.

3.1.1 Virtual Currencies

Virtual currencies can be used to purchase virtual or real goods and services; however, the currency is limited in use within the centralized systems, restricting its appeal to users (i.e. only game users will use the virtual coins). However, depending on the type of environment, it may also be converted back to a real currency. Using generic online games as an example, some types include:

1. Closed, isolated environment

   In a closed environment, the in-game currency can only be obtained through gameplay and can only be used to purchase virtual goods and services. As coins cannot be transferred between players and real currency cannot be used, there is no effect on the real world economy.

   However, gaming technology has advanced to allow interaction amongst players.

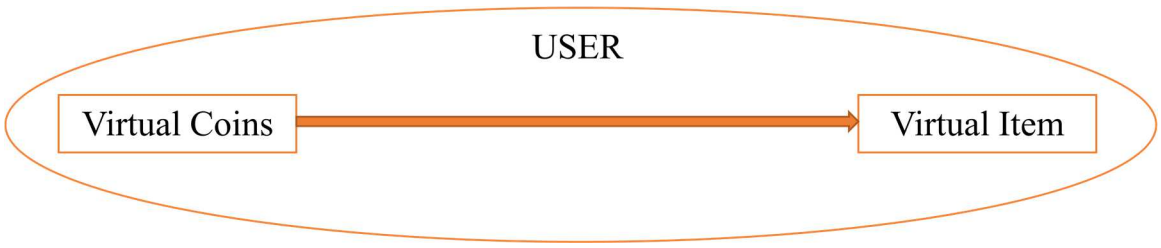

Figure 1: Illustration of a closed, isolated environment of a virtual currency. Each user's actions are isolated within their own environment. There is no currency convertibility.

2. Closed, interactive environment

   In a closed, interactive environment, players may include transfer of in-game currency and virtual items with other players. Although the virtual currency is still obtained through normal gameplay, users can take advantage of their efforts by using third party sites to sell their virtual coins or goods in exchange for real currency. The conversion between real versus virtual currency or good is decided by the selling user and is performed outside of the gaming environment.

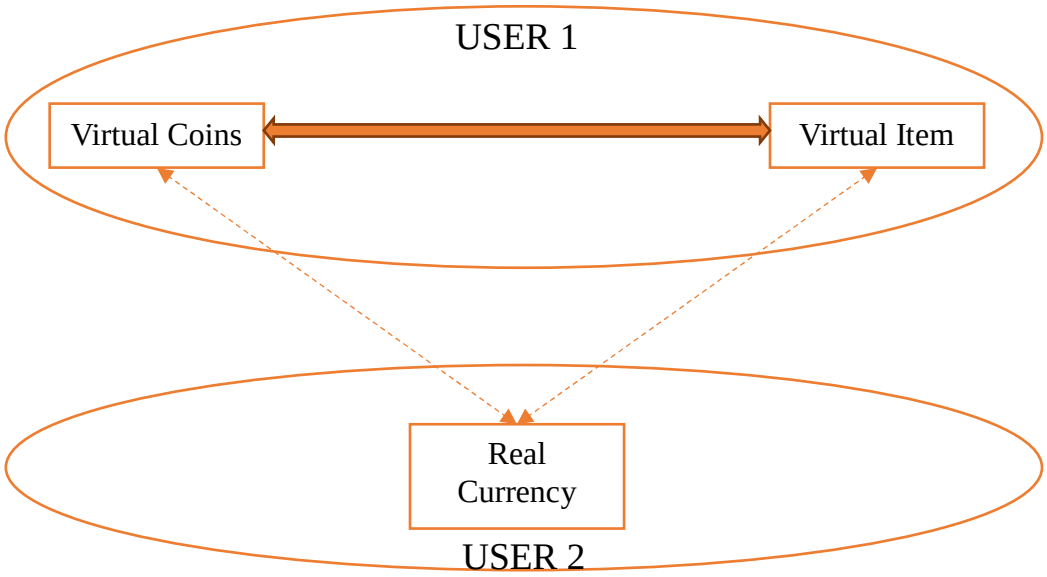

Figure 2: Illustration of a closed, interactive environment of a virtual currency. Exchanges amongst users are permitted, allowing real currency transactions to take place via a third party website. Currency convertibility is not limited.

3. Uni-directional environment

   In a uni-directional environment, real currency can be used to purchase virtual coins that can be used to purchase virtual goods and services. Once the virtual coins are purchased, it cannot leave the system (i.e. be transferred back to real currency). This type is different from the closed, interactive environment as developers encourage purchases through the game itself and prohibits transfers between players. The conversion between real versus virtual currency is decided by the developer.

   Another example would be a user purchasing credits from a website in order to purchase songs. While the songs cannot be converted back to credits, credits are not transferrable between users.

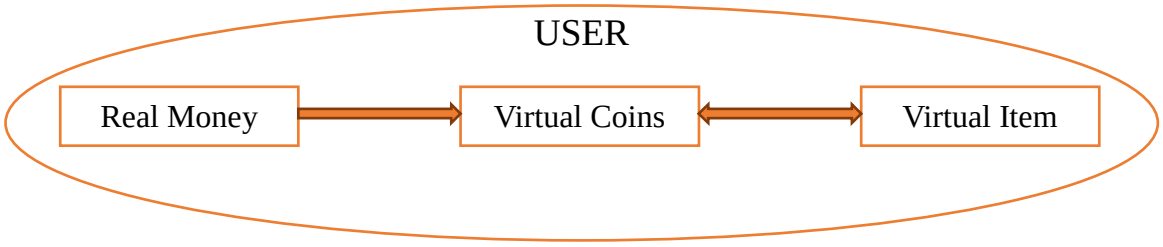

Figure 3: Illustration of a uni-directional flow of a virtual currency. Users can purchase virtual coins through the registered company, removing the incentive of purchasing through external means. Currency convertibility is limited.

4. Bi-directional environment

   In a bi-directional environment, real currency can be used to purchase virtual currency or the virtual good directly. Users can also sell their virtual good for virtual currency; alternatively, users can sell their virtual good or currency (as an item) for real currency, making the transaction bi-directional.

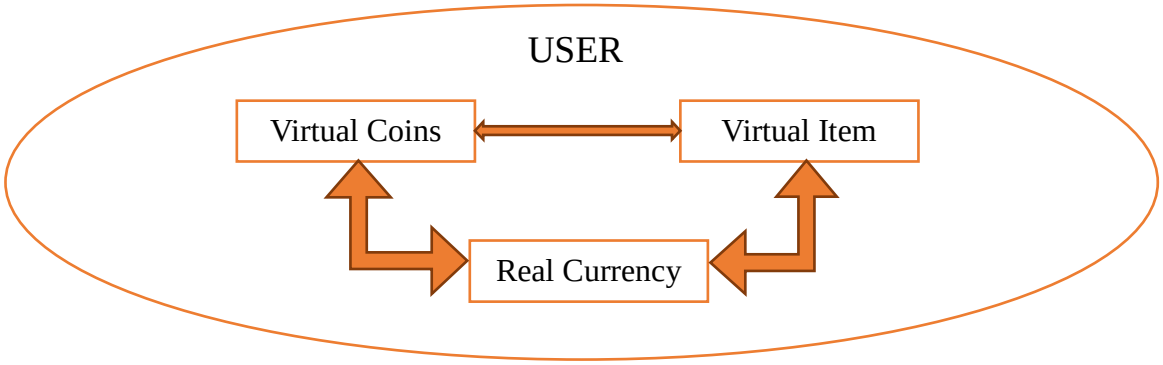

Figure 4: Illustration of a bi-directional flow of a virtual currency. Real currency can be used to purchase virtual coins or goods directly and can also sell the virtual items for real currency, exhibiting currency convertibility. Interaction between users occurs within the system without the need to use external means.

Aside from the closed, isolated environment, all other types have the potential to involve real currency, allowing a risk of potential money laundering to occur. The closed, interactive environment boosts the use of third party websites, making it difficult to centralize the more common way of offline exchanges. While the uni-directional environment locks the virtual currency used in the online world, this may cause difficulty to recovered laundered funds that were used to purchase virtual currencies without the ability to convert the funds back. Unlike the real world, online games are generally not

subject to the laws and regulations of the real world[6]. As online games usually only require a user-name and a valid e-mail address to start an account, transactions amongst users are hidden behind user-names. Third parties that support online purchases between users may contain more information, such as payment method instructions, which may assist in information gathering efforts in linking specific individuals to their gaming and payment accounts.

3.1.2 Electronic Monies

Electronic monies relates to currencies stored in a device that can then be used to exchange funds between users[7]. Systems such as Paypal or electronic funds transfers provide a method of transferring funds between users or financial intermediaries. Unlike some types of virtual currencies, convertibility is bi-directional, allowing the user to convert their electronic money back into real money.

Ability to open an account depends on the financial intermediary. In order to open an account, financial institutions require government identification, a matching physical address, and require an in-person meeting for confirmation. The Know Your Customer (KYC) refers to a process used to ascertain a potential customer's identity to ensure there is no identity theft through gathering and verifying records obtained through the customer. Through the verification of customer information and proper record keeping, the KYC process helps decrease the rate of fake accounts and provide their obtained information when any reproduction orders are requested. Depending on the sector, the

[6] Irwin, A S.M., J. Slay, R.C. Kim-Kwang, and L. Liu. "Are the financial transactions conducted inside virtual environments truly anonymous?" *Journal of Money Laundering Control, 16(1), 6-40*. December 11, 2012, http://dx.doi.org/10.1108/13685201311286832 Accessed on April 26, 2014.
[7] Johnson, E. "Digital Currency: legal and practical implications for forensic investigations and the forensic accountant." *University of Toronto*. June 20, 2007. p.9.

entity is required to keep proper record keeping and have proper due diligence in order to be compliant to the guidelines from the Financial Transactions and Reports Analysis Centre of Canada (FINTRAC).

Opening an online payment account such as Paypal does not require government identification although the user is suggested to enter their Social Insurance Number; however, it does requires a physical address, phone number, as well as either a bank account number or credit card number in order to perform transactions. While Paypal is not considered to be a bank in Canada, the information gathered from their preliminary forms indicate that they are attempting to link individuals to their accounts. For the user to send or receive funds, their account number and credit card number needs to be accurate; therefore, the identification of the users can be verified from the accounts. While for financial institutions, the Office of the Superintendent of Financial Institutions (OSFI) helps regulates banks to ensure they are compliant under the *Bank Act*[8], providing assurance for customers.

3.1.3 Cryptocurrencies

Using Bitcoin as the representative of cryptocurrency technology, "it is a decentralized peer-to-peer payment network that is powered by its users with no central authority or middlemen"[9]. Since Bitcoin is also the name of the technology, for the purposes of this paper, Bitcoin refers to the system whereas bitcoin or BTC will be used in reference of the cryptocurrency. As there are multiple types of software that can be chosen by users,

[8] Bank Act, *Government of Canada*. April 16, 2014, http://www.laws.justice.gc.ca/eng/acts/B-1.01/ Accessed on April 27, 2014.
[9] Frequently Asked Questions, *Bitcoin*, https://bitcoin.org/en/faq Accessed on May 3, 2014.

compatibility between software is essential as developers continue to improve the system. Bitcoin also boasts having a triple entry bookkeeping system[10].

A triple entry bookkeeping system involves providing information about the buyer and vendor. In a double entry bookkeeping system, the buyer would record a credit in cash and debit in the goods received, the vendor will record the opposite, a debit in cash and credit in goods sold, where the buyer and vendor recording their entries in their respective books. In a triple entry bookkeeping system, it records the transfer of funds in the same ledger, therefore linking the buyer and vendor's books together in a way to provide a full picture of location of funds and the identity of who received the funds while all sealed with cryptography, protecting the integrity and legitimacy of the transactions.

Peer-to-peer network provides protection on any attacks as each transaction is verified before being validated via digital signatures[11], which makes the transaction not instantaneous. The system is also a bi-directional system, allowing conversion between the cryptocurrency and real currency but the conversion is usually performed through a digital currency exchange. Bitcoin transactions are not reversible, disallowing reversal disputes.

For a transaction to occur, the seller provides the buyer a public key, the address that coins will be sent. The buyer accesses his own funds using a private key, and authorizes the transfer to the buyer's public key, initiating the verification process. Digital signatures are created through the use of the private key which is then used by the public key to verify the signature. The validation process helps ensure that the transaction is confirmed

[10] Ibid.
[11] Grinberg, R. "Bitcoin: An Innovative Alternative Digital Currency." November 11, 2011, http://hstlj.org/wp-content/uploads/2011/12/8-Grinberg-159-208.pdf Accessed on April 3, 2014.

with other users of the system, creating a transaction identification number (transaction ID) and completing the transfer. The seller can then access such funds through his own private key to the specific account. While transactions can be done between users, it can also be performed with digital currency exchanges or trading markets, where the user will be required to provide their public and private key to the trading markets in order for it to access funds for trading purposes. Unlike electronic monies and real currencies, users can be part of the creation process of the cryptocurrency through a process called mining.

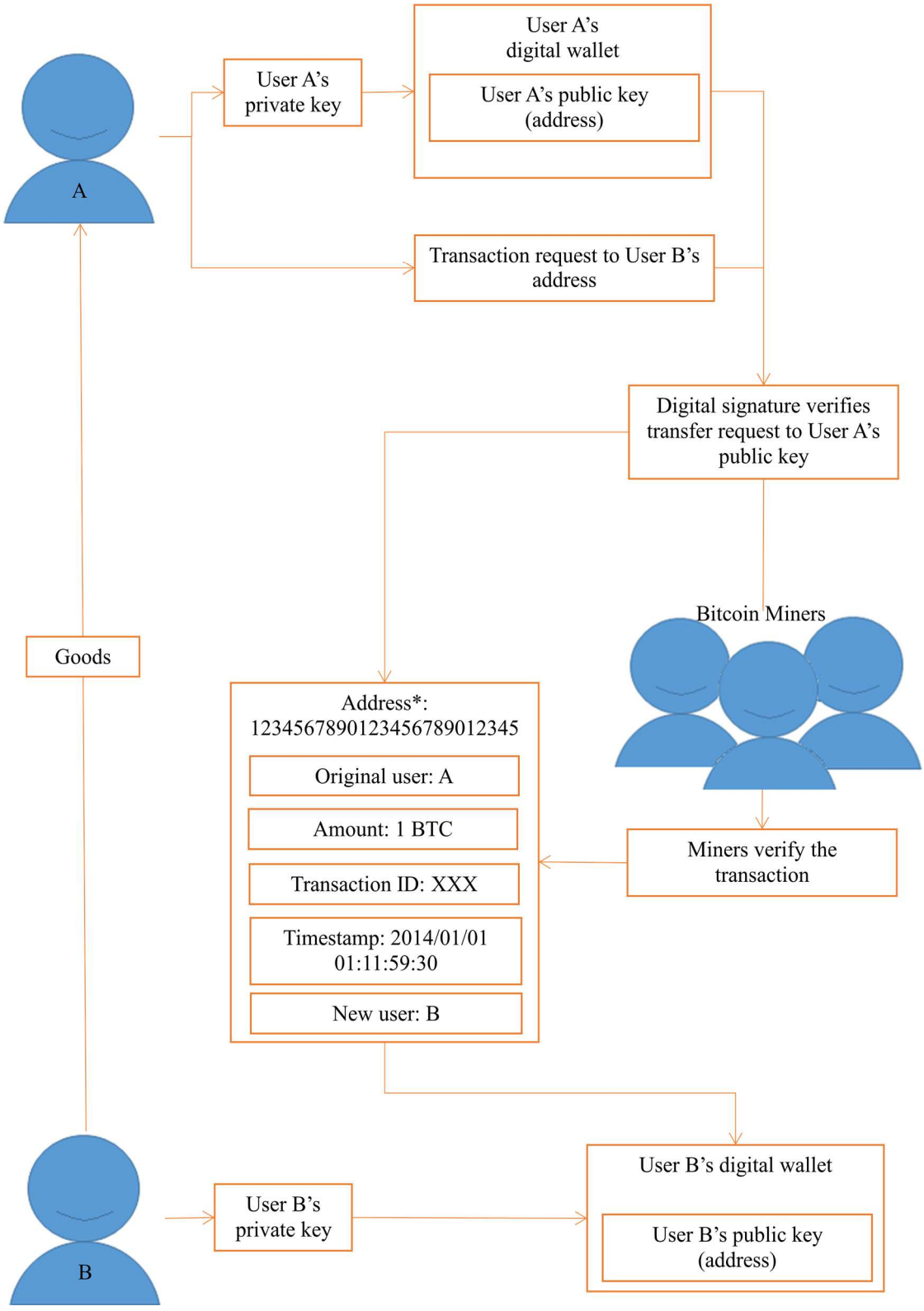
A
User A's private key
User A's digital wallet
User A's public key (address)
Transaction request to User B's address
Digital signature verifies transfer request to User A's public key
Bitcoin Miners
Goods
Address*: 1234567890123456789012345
Original user: A
Amount: 1 BTC
Transaction ID: XXX
Timestamp: 2014/01/01 01:11:59:30
New user: B
Miners verify the transaction
B
User B's private key
User B's digital wallet
User B's public key (address)

Figure 5[12]: A simplified illustration of a Bitcoin transaction. User B provides user A with their public key, in which User A requests a transaction of a certain amount of coins to be sent. Miners help verify the transaction and information relating to the transaction (i.e. users involved, amount, transaction ID, and timestamp) and is then added onto the coin history (the blockchain), with miners receiving an amount of BTC in return for their efforts. After the verification process, the amount will officially be confirmed in user B's public key in their digital wallet which can be accessed by User B with the associated private key.

* Within the public ledger, bitcoin addresses containing the coin is usually represented in a string of letters and numbers.

3.2 Comparison between Digital Currencies and Real Currency

The major concerns around BTC that have been noted by the Financial Consumer Agency of Canada include[13]:

1. Lack of coverage by deposit insurance by the federal or provincial governments
   For real currencies, the Canada Deposit Insurance Corporation (CDIC) covers deposits in Canadian dollars up to $100,000 in eligible deposits in case of failure from any of its members which include financial institutions[14]. Because of the insurance, consumers may be more inclined to trust financial institutions with their funds, therefore real currencies are considered more stable due to its government backing. Also, the government will also be able to produce more

[12] Romero, J., B. Palacio, Karlssonwilker Inc. "How a Bitcoin transaction works" *IEEE Spectrum*, http://spectrum.ieee.org/img/06Bitcoin-1338412974774.jpg Accessed on May 5, 2014
[13] Virtual Currencies, *Financial Consumer Agency of Canada.* April 1, 2014, http://www.fcac-acfc.gc.ca/Eng/forConsumers/topics/paymentOptions/Pages/Virtualc-Monnaies.aspx Accessed on April 27, 2014.
[14] Ibid.

currency in order to stabilize the system if needed. While it may not be the full amount in the account, it still provides more assurance than the digital currency. Digital currencies are not covered under the CDIC as digital currencies are not considered legal tender. Therefore, the risks associated with digital currencies are considered higher than real currencies.

2. Limited legal recourse

   In terms of real currencies, transactions are protected under their corresponding provincial Consumer Protection Acts where a paper complaint can be filed if goods are not received. Users can easily identify sellers at their physical locations and can report the seller to authorities if any issue arises.

   Due to the lack of government backing and its decentralized system, there will be difficulty in retrieving digital currencies from digital wallets if the holding institution goes bankrupt or even if goods are not received after funds have been transferred.

   Mt. Gox was a Bitcoin exchange based in Tokyo, Japan that has filed for bankruptcy in early 2014. Customers of the exchange have lost their digital coinage that was held with the exchange, unable to recover their funds. While bankruptcy proceedings are requesting proof of claims from customers in order to be included in any future legal distributions, there is no guarantee that that their claims will be accepted or the proceedings will have enough funds to provide back to its customers.

3. Exposure to consumer financial risk

   For real currencies, as everyone in the country is likely using legal tender for their transactions, it is relatively stable, with prices considered to be less volatile and not changing every day.

   Although digital currency users are growing day by day, the amount of users in comparison to the real world is still considered small; therefore, transactions that occur in the Bitcoin world that may seem small in the real world will be considered large, causing volatility. Due to the lack of stability, this increases the financial risks of its users.

4. Difficulty to get and use:

   Real currency is accepted everywhere and is easy to obtain via financial institutions.

   For digital currencies, there are currently limited ways to obtain BTC with the few mainstream ways listed below:

   i) Mining: Using the power from computer processors to assist in the maintenance of the currency system, the user is rewarded in BTC. Each coin is harder to mine than the last due to its requirement in verification in each algorithm; therefore, as the amount of coins increase, the algorithm becomes more complex. As the virtual environment increases, it becomes more difficult and time consuming for the user to mine enough coins to be worth the cost of usage (i.e. electricity, connection data) unless they are equipped with professional mining equipment.

ii) Purchase through Automated Teller Machines (ATMs) or currency exchanges: With Vancouver opening up the first Bitcoin ATM in Canada[15] and more vendors accepting BTC to be part of the digital currency movement, BTCs are becoming more accessible to the general public. However, the ability to obtain the coins through purchase is still incomparable to the real currency. Bitcoin exchanges such as the Canadian Virtual Exchange and Canadian Bitcoins also provide users the ability to purchase the digital coin.

iii) Accepting BTCs as a type of payment: As long as the vendor has a digital wallet that the customer can deposit amounts, BTCs can be collected in place of real currency without the difficulty of mining or through purchases. However, businesses that accept the digital currency as payment are still in the minority as the general public continue to observe the currency's stability before attempting use.

Usage of digital currencies is limited to its centralized system (in case of virtual currencies) and users with the application (for electronic monies). The difficulty for cryptocurrencies is its acceptability as it is on limited sites as well as limited vendors at stores.

5. Vulnerability to fraud, theft, and hackers

While Bitcoin boasts its currency's security, a thief may be able to steal the digital key to access funds in the corresponding digital wallet. Digital currencies are

[15] "World's first bitcoin ATM opens in Vancouver". *CBC*. October 29, 2013, http://www.cbc.ca/news/technology/world-s-first-bitcoin-atm-opens-in-vancouver-1.2286877 Accessed on May 3, 2014.

vulnerable to fraud as there is no way to track down the user if funds are improperly exchanged. Real currencies run the risk of counterfeits and external fraud by different users. While hacking can occur in both real currencies through bank sites, digital currencies have an advantage in that real currencies can also be physically stolen due its physical existence.

6. Privacy concerns

   Personal information obtained by financial institutions are regulated under the Privacy Act and the Personal Information Protection and Electronic Documents Act[16]. Although there is no regulation that requires digital currency exchangers to secure personal information, digital wallets only require a valid e-mail address; therefore, there is limited information that can be taken.

The comparison between a digital versus a real currency provides insight as to why a user would choose the digital route as it provides users with almost instantaneous transfers between locations without overbearing transaction fees and gives privacy that is lacking if the transfer is flowing through financial institutions. The next section analyzes the main characteristics of the most prevalent digital currency, Bitcoin, as an example of the advantages and disadvantages of the cryptocurrency.

[16] "Privacy Legislation in Canada." *Officer of the Privacy Commissioner of Canada*. March, 2009, http://www.priv.gc.ca/resource/fs-fi/02_05_d_15_e.asp Accessed on May 2, 2014.

3.3 An Analysis: The Advantages and Disadvantages of Bitcoin

Some of the main characteristics of Bitcoin include:

Issue	Advantage	Disadvantage
Lack of regulation	The lack of regulation allows quick transfer of funds between users without having to account for different jurisdictions.	Illicit use of the digital currency will find it easier as a way to hide illicit funds or to layer their funds with legitimate funds.
Lack of government backing	Its decentralized nature makes it difficult to hold someone accountable for the cryptocurrency, making it hard to pinpoint which jurisdiction it belongs to and subsequently, the corresponding laws it should follow.	Governments will print money as a way to stabilize the economic system; however, without the stabilization, BTC is considered to be a volatile currency as news relating to the system could cause major influx of transactions between users.
Anonymity	Increases privacy for users to send funds anonymously.	Illicit use of the digital currency due to its anonymity, making it harder for tracking funds. Although the transaction may be linked to an IP address, it can easily be blocked by programs such as Tor.

Impossible to counterfeit	Bitcoin's complex algorithm and logic makes it difficult for the coin to be counterfeited compared to a real currency as each "coin" has an identity and in order to counterfeit, the algorithm relating to the creation and transfer of the coin needs to be altered which requires more power than simply creating the coin in its legitimate manner.	
Transaction malleability		One of the issues relating to Bitcoin is transaction malleability, referring to its algorithm called a hash function. As transactions are sent, the process includes validation amongst other users that the transaction is legitimate which provides a transaction identification number; however, the transaction is malleable in that during the validation process, the

		algorithm may be changed slightly, resulting in a different identification number noted in the public general ledger[17]. The original sender will not see the expected identification number and may send another batch of funds in error.
Lack of consumer protection	Trust will be required in order to make up for the lack of government regulation to protect consumers, creating a community of users.	While protection usually leads to a loss of efficiencies[18], consumers will need to be more cautious in order to ensure that their transaction would be considered safe. Although the community of users is dependent on trust, there will always be ones that take advantage of such trust and without a way to trace back to the individual as long as they delete the public key given previously,

[17] King, R. "Transaction Malleability: Why nobody can withdraw bitcoins from one of the currency's largest exchanges." *Quartz*. February 10, 2014, http://qz.com/175565/why-nobody-can-withdraw-bitcoins-from-one-of-the-currencys-largest-exchanges/ Accessed on April 16, 2014.
[18] Gans, J. S. and Hanna Halaburda. "Some Economics of Private Digital Currency." *Bank of Canada.* November, 2013, http://epe.lac-bac.gc.ca/100/201/301/weekly_checklist/2013/internet/w13-46-U-E.html/collections/collection_2013/banque-bank-canada/FB3-2-113-38-eng.pdf Accessed on April 13, 2014.

		there is no way to stop a user from illicit behaviour.
Irrevocability		With the user unable to revoke the funds, users may not be able to prevent fraud, but can only act actively afterwards if the contracted goods or services are not received.
Lower transaction fees	Compared to real currencies, transaction fees help finance the investigation in potential reversals of transactions; however, Bitcoin can afford low transaction fees as it does not require financing to ensure it is following regulation (as it is not regulated) nor would it be required to investigate unusual transactions like financial institutions.	

As David S. Cohen has noted, "for consumers, anonymity and transaction irrevocability expose them to fraud or theft. And unlike FDIC insured banks and credit unions that guarantee the safety of deposits, there are no such safeguards provided to virtual wallets"[19]. The digital wallet is a place used to hold the keys of the user, like a bank account holding funds; however, there are minimal safeguards in protecting the keys inside aside from the basic protection from the wallet and the steps the user takes to secure it. The digital wallet needs to be examined to determine the effects of the lack of safeguard on users.

3.4 The Digital Wallet

Credentials required to open a digital wallet depends on the type of digital currency. In the case of Bitcoin, a valid e-mail address is all that is required to create a digital wallet. Like a bank account, "any person can maintain more than one wallet and in fact most users argue that it is more private to use a new wallet for each transaction thus making it somewhat harder for any third party to track another users' funds"[20]. Digital keys are stored in the digital wallet.

Digital keys allows access to the user's public address (for other users to send funds to) and sign transactions[21]. If the wallet is stolen, the user will lack the keys to access their funds, making their funds locked and inaccessible for anyone unless the user has the public key recorded elsewhere, the key and the amount may potentially be lost forever.

---

[19] Remarks From Under Secretary of Terrorism and Financial Intelligence David S. Cohen on "Addressing the Illicit Finance Risks of Virtual Currency". *U.S. Department of the Treasury*. March 18, 2014, http://www.treasury.gov/press-center/press-releases/Pages/jl236.aspx Accessed on April 15, 2014.
[20] Mullan, P.C. "The Digital Currency Challenge: Shaping Online Payment Systems Through U.S. Financial Regulations". 2014.
[21] "How to Store Your Bitcoins". *Coindesk*. May 1, 2014, http://www.coindesk.com/information/how-to-store-your-bitcoins/ Accessed on May 3, 2014.

In the real world, the user can go to their financial institution and regain access to their funds after a thorough review to ensure that the user is the owner of the account. However, in the digital world, the user must take active measures to ensure that their digital keys are kept private to avoid potential hacking and unauthorized transfer of funds out of their wallet.

A digital wallet is not required if an offline wallet is kept by printing the keys (i.e. a series of letters and numbers that is provided when a key is created and BTC are stored) and hiding the key in a secure, offline place. This type of situation may also be of concern if the user loses their keys. Losing one's keys is similar to losing a monetary bill from their pocket as there is no way a good Samaritan can trace the monetary bill back to its owner.

4.0 BITCOIN: DEFINING ITS PROPERTIES

Discussions about regulation have started to occur more frequently due to the bankruptcy of Mt. Gox, one of the largest known bitcoin exchanges. The lack of consumer protection indicates that some sort of protection such as regulation should be considered. However, the varying characteristics of digital currency make it difficult to define digital currencies.

Inspired by Grinberg's analysis on the potential label for digital currencies[22], an analysis based on Canadian regulations will be examined.

[22] Grinberg (p. 194-204).

4.1 Comparing the Definitions

Type	
Currency	Characteristics of money includes[23]: 1. Durability 2. Portability 3. Fungibility 4. Scarcity 5. Divisibility 6. Recognizability
Factors that agree with the definition	Durability: as the currency is in digital form, it would not suffer the wear and tear of real currency. Portability: BTCs can easily be transferred between users around the world as long as they have a digital wallet. However, the user must be connected to the internet in order to access their funds which might not be ideal in countries where the interest is not as accessible. Fungibility: All BTCs contain the same properties; therefore, there is no fungibility as there is no difference between each unit. Scarcity: BTCs are produced through a mining process and as the algorithm relating to the production of coins increases in difficulty, it would slow down the amount of coins in circulation. Known to have a limit of approximately 21 million BTC, it is not easily accessible for individuals to use the currency as a form of payment.

[23] Frequently Asked Questions. *Bitcoin*, https://bitcoin.org/en/faq Accessed on May 3, 2014.

	Divisibility: Each BTC is divisible by 8 units, allowing more for more units to be traded between users. Recognizability: Due to the algorithm system of Bitcoins, it would be impossible to produce counterfeit the cryptocurrency as the verification system will raise alerts on any potential usual activity.
Factors that disagree with the definition	Legal tender is defined in the currency of Canada if it was issued under the authority of the Royal Canadian Mint Act Section 15 notes that the definition of "sums" mentioned in the Constitution and Acts makes references to (a) a currency of a country other than Canada (b) a unit of account that is defined in the terms of currencies of two or more countries, (c) gold, or (d) a combination of any of the things mentioned in the paragraphs (a) to (c)[24] Digital currencies are not covered under any Constitution or Act as it does not pass the definition of "sums" since it does not belong to any country.

[24] Currency Act. *Government of Canada*. 1985, http://laws-lois.justice.gc.ca/eng/acts/c-52/page-1.html Accessed on April 16, 2014.

Commodity	Per definition provided in the Alberta Securities Act[25], commodity means: (i) any good, article, service, right or interest of which any unit is, from its nature or by mercantile custom, treated as the equivalent of any other unit; (ii) the currency of any jurisdiction; (iii) any gem, gemstone, or other precious stone; (iv) any other good, article, service, right or interest, or a class of any of these, that is under the designated order
Factors that agree with the definition	Like a type of stock, BTCs are traded between users through bitcoin exchanges. The volatility of BTC also reflects a high-risk stock, where holders of the stock may gain or lose depending on the price the item was valued at it was purchased versus the proceeds received when it was sold.
Factors that disagree with the definition	Commodities are tangible and considered to have inherent value[26]; however, BTC lacks inherent value as there is no government or alternate commodity backing. It would also be considered as an intangible item as there is no physical form of the coin. Bitcoin also does not meet the definition of "money" as it is not backed by any government.

[25] Alberta Securities Act. June 13, 2013, http://www.qp.alberta.ca/documents/Acts/s04.pdf, p. 11. Accessed on May 3, 2014.
[26] Grinberg (p. 200).

Precious metal	Metal that has high economic value and considered as rare[27]
Factors that agree with the definition	Bitcoin can be considered rare as not everyone has the ability to mine. Their economic value is questionable due to its volatility.
Factors that disagree with the definition	Bitcoins cannot be considered rare as in the case of real precious metals, land is explored and mined with the possibility of being rewarded for their efforts. For Bitcoins, there is only one exploration site to mine, decreasing its rarity as the user is guaranteed to be rewarded for their mining efforts; however, the reward is based on the mining effort and sizes of the mining group so the reward will likely decrease as the cryptocurrency gains popularity and more miners join the system.
Private currency	Currency issued by a private organization often backed by physical commodities[28]
Factors that agree with the definition	Bitcoins are issued by the mining community, not the government which can be seen as fitting the definition. Germany is one of the first countries to classify bitcoins as private currency[29].
Factors that disagree with	Bitcoins are issued by the mining community, not the government. However, the mining community may not be considered as a "private

[27] "Precious Metals". *Investopedia*, http://www.investopedia.com/terms/p/preciousmetal.asp Accessed on May 3, 2014.
[28] "Private currency". *Investopedia*, http://www.investopedia.com/terms/p/private-currency.asp Accessed on May 3, 2014.
[29] Regulation of Bitcoin in Selected Jurisdictions. The Law Library of Congress. January 2, 2014, http://www.loc.gov/law/help/bitcoin-survey/2014-010233%20Compiled%20Report_.pdf Accessed on April 9, 2014.

the definition	organization" as the community is not centralized.
Securities	In Canada, a Securities Act is produced by the provincial government. Under the Securities Act of Alberta, "securities" is defined[30].
Factors that agree with the definition	Per Grinberg, Bitcoins can be seen as a type of investment contract (which falls under the definition of "securities" in the Alberta Securities Act) as a person invests his money in a common enterprise and is led to expect profits solely from the efforts of the promoter or third party[31].
Factors that disagree with the definition	Bitcoin is not considered "money" due to its lack of government backing; therefore, based on the definitions from our current legislation, Bitcoins are likely exempt from this definition.
Digital casino chip	Characteristics of a casino chip includes it being immediate, irreversible, and private[32]
Factors that agree with the definition	Bitcoins can be transferred "immediately", based on the type required to confirm the transaction and is irreversible unless the receiving user agrees to return the amount. As discussed above, it can be considered that it is a private currency.
Factors that disagree with the definition	Casino chips are only usable within the controlled vicinity of the casino; if the analogy is extended to the Bitcoin community, it cannot be seen as a casino chip as the Bitcoin environment is not regulated tightly like a

[30] Alberta Securities Act. June 13, 2013, http://www.qp.alberta.ca/documents/Acts/s04.pdf, p. 20. Accessed on May 3, 2014.
[31] Grinberg (p. 196).
[32] Matonis, J. "Bitcoin Payments Could Quickly Become Competitive Wedge in Online Gaming". *Forbes*. June 27, 2013, http://www.forbes.com/sites/jonmatonis/2013/06/27/bitcoin-payments-could-quickly-become-competitive-wedge-in-online-gaming/ Accessed on April 15, 2014.

	casino. The conversion between real currencies and BTC does not only have to occur through designated currency exchanges but can be between users, cutting off the controlling factor.

Due to the lack of government backing, digital currencies have been quickly dismissed as much legislation defines currency with government backing. Without a proper classification, there is an inability to apply existing regulations, resulting in the side effect of money laundering because of the unregulated characteristics of the digital coin and also its lack of government control.

5.0 IMPLICATIONS ON MONEY LAUNDERING

Defined as "the process used to disguise the source of money or assets derived from criminal activity," the general three stages of money laundering includes: placement, layering, and integration.[33] However, because of the introduction of digital currencies, Stokes has defined what is considered "virtual laundering": the use of virtual currencies and/or virtual environments to launder criminal funds and bestow them with the appearance of legitimacy whilst simultaneously obscuring their actual, illicit origin[34].

5.1 Issues with Digital Currencies

Digital currencies allow quick transfers between jurisdictions without the watchful eye of the government, or any record in any financial institution. Without the ability to link the

[33] "What is money laundering"? *Financial Transactions and Reports Analysis Centre of Canada*, http://www.fintrac-canafe.gc.ca/fintrac-canafe/definitions/money-argent-eng.asp Accessed on May 10, 2014.
[34] Stokes (p.223).

user to the public address published, the public ledger that provides information on all transactions using BTC provides minimal information on the user.

Placement relates to placing proceeds of crime in the financial system whereas layering converts the funds into another form and creates layers of transactions, making it difficult to trace[35]. For virtual laundering, converting the illicit funds to BTC can be seen as a combination of placement and part of layering as it is placing funds with an exchange, a "financial system", and being converted into another form (BTC). Recipients of potential proceeds of crime include digital currency exchanges or another user if it is a private exchange of coins. Transfer of funds between users without going through exchanges remove the ability to observe the flow of funds, while anonymity provides coverage of a traceable audit trail.

One of the main issues with converting large amounts of BTC and back to real currency is the size of the transaction, as most transactions are small as the cryptocurrency is still in its growing stages with many users holding it for speculation purposes, larger transactions recorded in the public ledger will likely raise awareness from other Bitcoin users. With the public ledger publicizing all transactions, the launderer is more likely to exchange small amounts in order to stay under the radar of watchful Bitcoin users. After receiving BTC, the launderer can send funds to others in another jurisdiction or proceed to layer different transactions to disguise any trail of their public address.

Services such as Bitcoin Laundry and Zerocoin provide the launderer ways to make traceability more difficult. The purpose of such services is to disconnect bitcoins from the

[35] "What is money laundering"? *Financial Transactions and Reports Analysis Centre of Canada*, http://www.fintrac-canafe.gc.ca/fintrac-canafe/definitions/money-argent-eng.asp Accessed on May 10, 2014.

beginning and the end of the process, through cryptography or through mixing multiple users' funds together. While it can be argued that such services are providing criminals a way to conceal their digital currency obtained from illicit funds, legitimate users that value their privacy also consider the services useful.

Bitcoin advocates can choose to use a new public key for each transaction in order to cut connections between fund transfer of users. While using resources such as IP address tracking may provide clues to the identity of the user, users may opt to use software that shields their IP addresses, making it harder for their identities to be discovered.

Money laundering of digital coinage can also be compared to casino chips: illicit funds are converted into digital currency and used within the digital environment. Within the digital system, the funds could be transferred easily between users while layering coins that are converted from legitimate sources. The coins can then be redeemed for the same amount of currency or even more, potentially making a profit from the volatile conversion rates.

With more countries on board in examining digital currencies, "regulatory efforts, must then, focus on the stage where stored values moves from the virtual world into the real world"[36] as it is the gateway that provides the opportunity for regulations to present compliance guidelines.

[36] Stokes (p.230).

6.0 REGULATION

6.1 Purpose of Government Regulation

Due to Bitcoin's popularity through its increase in trade volume from approximately 9.2 million USD in July, 2013 to a peak of $72.1 million in December, 2013[37], governments cannot continue to delay their decision in regulation as more vendors are accepting the digital currency as payment which also creates an issue with income reporting. However, because of the inability to link accounts (i.e. digital wallets) to individuals, the main purpose of regulation should be examined.

6.1.1 Protect the Consumer

Without government backing, the consumer is exposed to more risk by using a currency that is volatile in value, nor will their monies be protected in the event of bankruptcy from the exchanger, such as the case of Mt. Gox. As noted by David Cohen, "for consumers, anonymity and transaction irrevocability expose them to fraud or theft. And unlike FDIC [Federal Deposit Insurance Corporation] insured banks and credit unions that guarantee the safety of deposits, there are no such safeguards provided to virtual wallets. Similarly, investors in virtual currency today lack the standard protections applied to the purchase of a security or a commodity."[38] Some form of regulation will be needed in order to properly protect the consumer.

By having regulation, it would reduce the incentive for criminals to use the currency for illicit purposes but it will also help boost consumer confidence in the digital currency by

[37] USD Exchange Trade Volume, *Blockchain*, http://blockchain.info/charts/trade-volume Accessed on June 11, 2014.
[38] Remarks From Under Secretary of Terrorism and Financial Intelligence David S. Cohen on "Addressing the Illicit Finance Risks of Virtual Currency". *U.S. Department of the Treasury*. March 18, 2014, http://www.treasury.gov/press-center/press-releases/Pages/jl236.aspx Accessed on April 15, 2014.

encouraging more conservative consumers to perform non-traditional transactions. To be able to regulate and determine whether the user will follow the rules, it will be beneficial for the digital currency as a whole to allow a form of regulation to warn potential users that illicit use will be made aware to the corresponding authorities.

Another issue to consider is whether the consumer should be protected as by using the digital currency, they are already aware of the risks involved. Although some consumers may appreciate the protection that regulations provide, some users that believe in the freedom of the digital currency will indicate that there is no need for protection as the Bitcoin community will continue to improve itself through each obstacle that occurs.

6.1.2 Protect the Economy

While governments would likely not be interested in protecting the digital environment, any effects on the real world will raise their awareness of the digital currency. As digital currencies gain consumer confidence and is promoted as a quick, low-costing alternative to real coinage, there may be repercussions on the economy if a material number of transactions are performed using digital currencies.

China's Q-coin provides an example where the digital currency was used as a substitute of the state-sponsored currency, resulting in the Chinese government banning exchanging mutual currencies for real goods and services[39]. While the usage of Bitcoins is spread amongst different jurisdictions, there may be countries that benefit from using the digital coin as a means of exchange such as Africa, avoiding the corrupt banks, bribery, and fluctuating currencies of their own countries[40].

[39] Gans and Halaburda (p.23).
[40] Varriale (p.3).

6.1.3 Protect the Currency

With the increase use of digital currencies, governments run the risk on the decrease use of their own currency and with a decrease of consumer use, it may lead to a decrease in consumer confidence, resulting in a potential loss of the currency. Consumer confidence provides value to digital currencies as it allows an item to be worth an amount by producing a demand. Governments may be interested in digital currencies in order for them to not disrupt the country's own currency, as in the case of the Q-coin.

6.1.4 Taxes

Through understanding the properties of digital currencies, governments can then determine the next course of action: how users should report any gains from its usage. Canada Revenue Agency has recently indicated that the gains and losses on digital currencies that have been purchased or sold may be liable as taxable income or capital[41], depending on the type of transaction. Regulation assists governments in ensuring that users are compliant to the law and any non-compliant users will be treated accordingly.

6.2 Recent Government Responses

The Law Library of Congress has recently released a document pertaining to regulation of bitcoin as of January, 2014[42]. While most countries are aware of the potential of digital currencies, there have been different stances taken, most notably Iceland where foreign

[41] "What you should know about digital currency". *Canada Revenue Agency*. November 5, 2013, http://www.cra-arc.gc.ca/nwsrm/fctshts/2013/m11/fs131105-eng.html Accessed on May 4, 2014

[42] Regulation of Bitcoin in Selected Jurisdictions, The Law Library of Congress, January 2, 2014, http://www.loc.gov/law/help/bitcoin-survey/2014-010233%20Compiled%20Report_.pdf Accessed on April 9, 2014.

exchange trading with Bitcoins are prohibited[43]. The following showcases the difference of treatment between some of the countries.

Canada

The Currency Act of Canada states that "money is a legal tender if it is made in coins … and in notes issued by the Bank of Canada[44]", indicating that it is not considered to be a currency. Transactions that involve digital currencies are considered to be a barter transaction: a transaction without using legal currency[45]. The Bank of Canada has released a study which indicated that digital currencies also exhibit network effects in that as the more people accept the currency, the more value there is to accepting it[46] as it gains consumer confidence. While it recognizes that the effect of digital currencies with the real economy is minimal[47], the use spans through different jurisdictions, making it difficult to regulate.

The introduction of House Government Bill C-31 in March, 2014 provides amendments to the *Proceeds of Crime (Money Laundering) and Terrorist Financing Act* (PCMLTFA) to extend the requirements for financial institutions and intermediaries to entities that deal with virtual currencies[48]. By treating digital currency dealers as an extension of a money service business, Canadian entities will be required to report any suspicious transactions accordingly.

---

[43] Ibid, p.11.
[44] Currency Act. *Government of Canada*. 1985, http://laws-lois.justice.gc.ca/eng/acts/c-52/page-1.html Accessed on April 16, 2014.
[45] "What you should know about digital currency". *Canada Revenue Agency*. November 5, 2013, http://www.cra-arc.gc.ca/nwsrm/fctshts/2013/m11/fs131105-eng.html Accessed on May 4, 2014.
[46] Gans and Halaburda.
[47] Ibid.
[48] Bill C-31, *House of Commons of Canada*. March 28, 2014, http://www.parl.gc.ca/HousePublications/Publication.aspx?Language=E&Mode=1&DocId=6495200&File=4, Division 19 Accessed on May 4, 2014.

As previously noted, income gained from digital currency exchanges or transactions are to be considered like a commodity, such that taxes will be considered taxable income or of a capital nature, depending on the transaction and intent.

United States of America

The Financial Crimes Enforcement Network (FinCEN) has provided guidance relating to digital currencies in indicating that it is "a medium of exchange that operates like a currency in some environments, but does not have all the attributes of real currency"[49]. Digital currency exchangers are considered to be providing money transmission services but not a foreign exchange provider as digital currencies are not considered to be legal tender.

The U.S. Department of the Treasury has indicated that financial transparency will help protect the consumers from illicit finance threats; basic controls such as KYC, record keeping, and provide reports necessary in order for law enforcement to take action if any abuse of the financial system occurs[50]. By guarding the entryway between digital currency and real currency through regulation of the digital exchanges, digital currencies are treated in a cash-like way as the requirement of requiring reports for any transactions over a certain amount (i.e. $10,000) is being considered.

[49] Application of FinCEN's Regulations to Persons Administering, Exchanging, or Using Virtual Currencies. *The Financial Crimes Enforcement Network*. March 18, 2014, http://fincen.gov/statutes_regs/guidance/html/FIN-2013-G001.html Accessed on April 13, 2014.
[50] Remarks From Under Secretary of Terrorism and Financial Intelligence David S. Cohen on "Addressing the Illicit Finance Risks of Virtual Currency". *U.S. Department of the Treasury*. March 18, 2014, http://www.treasury.gov/press-center/press-releases/Pages/jl236.aspx Accessed on April 15, 2014.

European Union

While the European Banking Authority (EBA) has acknowledged the increase of retailers accepting Bitcoin as a means of payment, a warning has been issued in December, 2013 to indicate concerns, including potential tax liabilities in the user's corresponding country[51]. A cross-sectoral taskforce has been established to determine whether virtual currencies can and ought to be regulated[52].

Japan

With Mt. Gox's headquarters located in Tokyo, Japan, the Japanese government was caught in the middle of accountability when the Bitcoin exchanger filed for bankruptcy. Their current stance indicates that the cryptocurrency should be treated more as a commodity, disabling the banks and securities firms in handling Bitcoin as part of their business[53]. The government has also noted that any regulation of the cryptocurrency should involve international cooperation to avoid loopholes[54].

Iceland

Iceland's Foreign Exchange Act restricts foreign exchange trading and capital movements between Iceland and other countries; therefore, use of bitcoins will be considered illegal. However, on March 25, 2014, 10.5 million Auroracoins, another type

[51] "EBA Consumer Trends Report 2014". *European Banking Authority*. February 28, 2014, http://www.eba.europa.eu/documents/10180/534414/EBA+Consumer+Trends+Report+2014.pdf Accessed on April 13, 2014.
[52] Ibid.
[53] Hirata, N. and Takaya Yamaguchi. "Japan may tax bitcoin deals, stop banks, brokerages from handling." *Reuters*, March 5, 2014, http://www.reuters.com/article/2014/03/05/bitcoin-mtgox-idUSL3N0M207R20140305 Accessed on April 9, 2014.
[54] Ibid.

of cryptocurrency, will be given provided to all citizens of Iceland[55] in an attempt to boost the economy. The effect of using cryptocurrency as an alternative to the country's own currency remains to be seen.There is a general consensus on wanting digital exchangers and transmitters to provide information on transactions that reach certain amount in the corresponding country's currency in order to ensure that the transactions are being made aware and considered. From the few examples noted above, each government has treated digital currencies differently. The U.S. state regulators are working on a bitcoin rule-book in order to provide guidance to users and regulators[56]; however, as digital currencies are not owned by any country, cooperation between countries is essential in order for compliance regulations to be successful as it would create issues if standards varied heavily between jurisdictions.

6.3 Non-Government Responses

While the governments are attempting to properly categorize digital currencies within their corresponding legislation, some digital currency supporters are taking matters into their own hands, whether it is to prove that self-regulation is possible, government cooperation is essential for digital currencies to be accepted, or increase stealth in the software to make governments recognize the weaknesses in their legislation and ensure privacy is kept through covering transaction tracks.

6.3.1 Bitcoin Police

With popular online forums being the best place to warn other users of any suspicious users, Douget has noted that the Bitcoin Police, a community-run organization, helps

[55] Southan.
[56] Miedema.

identify and warn others on trading with a scammer[57]. While self-regulation may be ideal in order to reduce government intervention, running an organization that requires cooperation among all trading platforms is unlikely to be successful as the digital economy grows and more resources are likely required to maintain quality investigations, increasing the cost. Government regulation will help provide proper punishment to scammers as the community would lack the ability. Prevention through warnings on forums may help decrease transactions with scammers; however, it also depends on active participation and awareness from its users to maintain being up to date with such information.

6.3.2 Multi-signature wallets

Digital exchanges require the private key of the user in order to perform trading transactions on their behalf; however, vulnerability in their security system allows hackers to obtain possession of the private keys and steal funds from the exchange. To enhance security and prevent hackers from stealing private keys, developers are creating multi-signature wallets, requiring more than one private key to authorize any movement of funds. Examples include requiring a couple to provide their keys to authorize transactions so that it prevents one from spending without another's knowledge or providing a security measure for the users of having an offline key if the user's computer was hacked. Requiring more than one signature provides higher assurance that the transaction is authentic and also disallowing unauthorized parties from accessing their funds.

[57] Doguet (p. 1145).

Multi-signature escrows such as Cosign Coin[58] acts as an intermediary between the buyer and seller by creating a multi-signature address and distributing the private keys required to access the funds amongst the buyer, the seller, and the escrow service. In this situation, only two out of the three keys are required in order for the funds to be accessed; therefore, if the buyer has sent the funds and receives the goods from the seller, the buyer can then provide the seller with the private key to allow the seller access. However, if the buyer insists that the goods has yet to be delivered, the escrow service will provide arbitration services and determine whether the funds goes back to the buyer or the seller. The seller will be required to provide documentation such as the mailing receipt and transit number in order for the escrow service to confirm and release its key to the seller.

Such services will require more effort from the users as it would be less time efficient if the funds are required right away but not enough keys are obtained. Services such as arbitration from the escrow services also come at a cost. Given that digital currency exchanges require the client's key to perform transactions, the speed of the transaction is decreased while providing an increased in security as the user can ensure that the transaction was approved under their own consent. While it does not prevent the hacker from taking private keys, it does prevent the hacker from using the funds as they lack the extra private key required to unlock access. If the hacker was successful in obtaining the user's public key (i.e. the location of the funds) and the private key held by the third party, the balance cannot be considered to be lost by the user since the amount can be found but just not accessed. To solve this issue, a hierarchy system in multi-signatures should be considered. Although the hierarchy system may prevent unwanted access, it

[58] *CoSign Coin*, http://cosign.co.in/ Accessed on May 10, 2014.

may also cause concern for law enforcements if they are able to identify the accounts but cannot access it without the required keys as criminals can then easily transfer the funds out to a different public key to escape, unable to grant law enforcements proper seizure of the funds.

Although the multi-signature feature will provide more security to protect its consumers, illicit transfers could still occur as there is no indication of it being an unusual transaction and not all transactions are required to go through intermediaries. This may also hinder law enforcements from recovering assets if the extra private keys cannot be found: while the criminal cannot access the funds, law enforcement will also be unable to secure it.

6.3.3 Dark Wallet

While some organizations have started to prepare for upcoming government regulations and attempting to provide compliancy, others attempt to defy government attempts through applications whose sole purpose is to protect the privacy of its users through laundering and mixing of funds. The Dark Wallet boasts its ability to use stealth addresses to hide the receiving user and also mixing coins between users performing simultaneous transactions[59]. Its deceptive nature provides the user with anonymity; however, it runs the risk of being non-compliant if regulations are designed to handle such circumstances. Another issue would include how to disallow the use of applications such as Dark Wallet if it is widely available.

While it is ideal to assume that users would want to perform transactions with exchanges that are regulated or use digital wallets that are government approved, providing security

[59] Greenberg, A. "'Dark Wallet' Is About to Make Bitcoin Money Laundering Easier Than Ever". *WIRED*. April 29, 2014, http://www.wired.com/2014/04/dark-wallet/ Accessed on May 6, 2014.

and insurance if major issue arises, the Dark Wallet can be loosely compared to an offshore account, where the digital wallet may be less secure and more prone to scrutiny if discovered.

6.3.4 Independent Efforts

A project to produce the world's first Bitcoin law book has been announced in May, 2014, to be spearheaded by Christine Duhaime of Duhaime Law[60]. With the assistance of experts from multiple fields, the book aims to provide knowledge on multiple topics covering jurisdictions including the United States of America, Asia, Europe, and Canada[61]. However, with the technology still at its growth stage, it will be difficult to ensure that information reported maintains its relevance through the ever-evolving legislations.

Although government regulation of digital currencies may be considered an obstruction of the regulation-free, decentralized system, digital currencies will also have to play by government rules to minimize its current scrutiny of being a black market currency. While one of the major concerns of regulation is the invasion of privacy and lack of freedom, with minimal regulation, the digital economy can continue promoting freedom of transactions but with easier ways of tracking available for law enforcement purposes.

By regulating the wallets and exchanges as a first step, it would provide law enforcements the ability to link keys associated with the wallets and wallets to individuals. The onus of KYC should be distributed between the wallet makers and

[60] "Canadian law firm takes lead in writing first Bitcoin law book." *Duhaime Law*. May 11, 2014, http://www.duhaimelaw.com/2014/05/11/christine-duhaime-authoring-first-legal-book-on-digital-currencies/ Accessed on June 8, 2014.
[61] Ibid.

exchanges. By guarding the entryway to the digital coinage, while it would not deny illegitimate users, it will at least provide a way to identify and prosecute if necessary.

7.0 PROPOSAL: REGULATE THE WALLETS

The main concern is at the stage at which conversion between real currency and digital currencies occur. Therefore, two types of regulations needs to be considered in order to capture users of digital currency exchanges as well as private exchanges.

7.1 A Proposal on Regulation of Digital Wallets

One of the major concerns associated with digital currencies is the anonymity of its transactions. While Bitcoin provides an open book to its users on transactions, little is known aside from the public keys listed to show the transfer of funds. To decrease anonymity and provide a link between the keys and the user, regulation that starts at the initial stage of the process, such as during the creation of the digital wallet, should be considered.

The current requirements to open a digital wallet are minimal: a valid e-mail address and a password is all that is required. Even if it requires more information, such as a physical address, there is nothing that will prevent the user from creating an invalid or fake address due to lack of verification. Therefore, some sort of verification process would be required to ensure that the information the user is entering is not fictitious and is correct.

Since wallets are made in order to keep the keys associated to the funds, if comparing to a normal transaction with real currency, the wallets would be most associated with accounts with financial institutions. Therefore, if the wallet producers, called “issuing facilities”, follow similar regulations as financial institutions such as obtaining

information relating to the individual through government verifiable documents, there is more assurance that the wallet can be linked to an individual. As the issuing facilities are the only holders of personal information, the user can still perform transactions anonymously with other users. A production order will need to be issued to the issuing facility in order for the personal information to be provided to a third party.

Regulation on digital wallets would assist law enforcements to link the individual to the user as well as detect other keys within the same wallet. Private exchanges amongst users that do not bypass the exchanges will then be detectable under such regulations. While the issuing facilities may disassociate by indicating that they are only providing the ability for users to use the currency, even if regulations on issuing facilities are not successful, the minimal requirement that the facilities should provide is the valid e-mail address linked to the digital wallet associated with the public key, and provide the addresses of other keys located within the wallet.

7.2 Regulating the Digital Currency Exchanges

The secondary point of conversion relates to digital currency exchanges where users convert their digital coinage to real currency and vice versa. FINTRAC, a financial intelligence unit that operates within the PCMLTFA has noted that for real currencies, money service businesses (MSB) include: foreign exchange dealing, money transfer service, and cashing or selling money orders, traveller's cheques or anything similar[62]. While digital currencies are not considered to be real currency, they do have similar characteristics and digital currency exchanges are conducting transactions similar to

[62] "Your Money Services Business in Canada: What you need to know". *Financial Transactions and Reports Analysis Centre of Canada*. April 1, 2014, http://www.fintrac-canafe.gc.ca/publications/brochure/2012-06/1-eng.asp Accessed on May 13, 2014.

foreign exchange dealings; therefore, by following regulations that apply to foreign exchanges and money transfer services, it should be considered as a new type of money services business. With digital currency exchanges following the obligations and responsibilities that are required by MSBs, the exchange will be required to ensure that their systems are properly able to track transactions between its clients and third parties and also client identification. The amount of regulation will also provide comfort to digital currency users for conversion or transfer services. If a production order is issued, the digital currency exchange will also be able to gather the information in a more timely fashion since the information should already have been obtained and properly verified through their own resources.

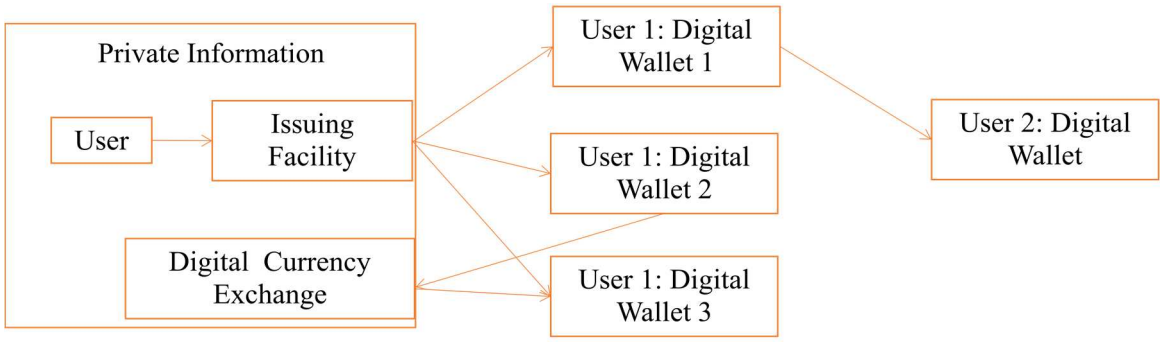

Figure 6: Illustration of the proposed structure. The box indicates where private information about the individual is known. Digital wallets associated with the user are kept anonymous within the system; however, under a document order, the issuing facility will provide authorities with the requested personal information of the user as well as the addresses of the known digital keys within the wallet. Digital exchanges will also collect personal information on its clients as part of the KYC process and to report any suspicious transactions to FINTRAC.

7.3 Issues

7.3.1 Accountability

Issuing facilities may argue that they are providing access to keys and as they hold no liability for the loss of funds or any illicit transfers, they do not require or care who uses their facilities. The transaction process needs to be examined to determine whether issuing facilities are to be accountable for receiving and validating the personal information provided by its users to determine whether it is accurate.

For digital currency exchanges, as they are providing services, accountability of any funds transferred that may be illegitimate needs to be known. While the exchange may deny that they are a MSB and therefore regulations do not apply, accountability needs to be identified if property of a user is held by a third party that also has access and can act on their behalf.

7.3.2 Privacy

Privacy will be sacrificed in that the wallet can be linked to an identifiable account. While anonymity will still be available between users, users should understand that exchanges and issuing facilities will be required to provide information obtained from the users if a production order arises.

7.3.3 Efficiency of Setup

The efficiency of being able to set up a wallet in mere minutes would be lost as the issuing institution will have to verify the provided documents before accepting the account as valid. However, it is more likely that they may accept the account before verification but disallow funds for release from the wallet until the validation process is completed.

7.3.4 Jurisdiction

To determine the jurisdiction of the digital wallets, two approaches should be considered: based on the issuing facility or based on the user's location. If the jurisdiction is based on the issuing facility, the difficulty lies with pinpointing the facility that may not be incorporated, accessible for all countries, and possibly produced by developers from multiple countries. If the jurisdiction is based on the user's location, there is a higher likelihood in locating the user as they will have to provide their personal information in order to open an account; therefore, the jurisdiction will belong to the country that the user has deemed to be their own.

7.3.5 Transaction Costs

While digital currencies boasts minimal transaction costs, one of the reasons for transaction costs in financial institutions is to support verification costs and investigating returns. If the issuing facility is required to obtain and maintain records of its users, potential expenses will likely be incurred by its users in order to cover such costs, with the amount of expenses depending on the issuing facility's policies. For existing exchanges where trust and company brand is known, continuing lower transaction costs may be difficult in the short term but it would help deter new exchanges from rising as new companies face the difficulty of competing with existing exchanges.

7.4 Linking the Digital Wallet back to the User: The Case of Mt. Gox

Although Bitcoin has indicated that their transactions are not anonymous as all transactions are stored publicly[63], using a Bitcoin address only once removes the trail of

[63] "Some things you need to know". *Bitcoin*, https://bitcoin.org/en/you-need-to-know Accessed on May 3, 2014.

funds, making it difficult to reconstruct the balance of the wallet connected to the address. The discussion surrounding anonymity is usually one-sided; what if the user wants to be linked to the account?

Mt. Gox has recently released an announcement indicating that proof of claims is required from users in order to be part of the bankruptcy proceedings[64]. Common details required in the filing of the proof of claim likely include name, address, and amount of claim[65]. However, unless sufficient records were kept by the user, the challenge may exist for the bankruptcy trustee to ensure that the proofs of claim are accurate in order for distribution to occur. Another issue is that even if the user has all their information, including the private key, if another user provided the same private key as theirs (i.e. a hacker), the bankruptcy trustee will have issues in confirming the true owner of the funds. If there was more linkage between the digital wallet and user, the process may be easier for the user to file their proof of claim as the company would already possess information, especially in terms of locating their clients of the bankruptcy proceedings.

As digital currencies become more mainstream, businesses trading in the digital world may require the assistance of forensic accountants when the need arises. The ability to track the digital flow of the transaction will become pertinent for the forensic accountant to be successful in providing credible information that is also admissible for court purposes.

[64] "Announcement of Commencement of Bankruptcy Proceedings". *MtGox Co,, Ltd.* April 24, 2014, https://www.mtgox.com/img/pdf/20140424_announce_qa_en.pdf Accessed on May 3, 2014.
[65] Ibid, p.3.

8.0 A FORENSIC PERSPECTIVE: TRACKING THE DIGITAL FLOW

With digital currencies acting as an alternative payment for goods and services, the tracking of transactions will also be moved to the digital platform, requiring increase computer knowledge from forensic accountants in order to understand the basic concepts of the digital flow. While Bitcoin boasts transparency through their public ledger, IFAs will also need to be able to explain such concepts to the court in order for their report to be credible. The developing regulations also provides a challenge as what may be noted in reports may become obsolete by updates from government regulators.

8.1 Transparency: The Blockchain

While digital currencies all have different methods of providing users security in their transactions, Bitcoin has provided a publicized ledger for users, known as a block chain. The block chain is a shared public ledger on which the entire Bitcoin network relies, with the integrity and the chronological order of the block chain enforced through cryptography[66]. Each transaction is validated within a certain amount of time (i.e. approximately ten minutes) where the transfer is added as a new block to the existing blocks that the block came from. By doing so, all public keys are listed in the ledger in order for users to see the chain of possession of the coins, providing transparency. The validation process also ensures that there would not be double-spending on the same coins; therefore, the buyer cannot buy two items with the same coin. Timestamps are added to ensure that if double-spending of the same coin occurs, the earlier transaction takes precedent.

[66] "How does Bitcoin work?" *Bitcoin*, https://bitcoin.org/en/how-it-works Accessed on May 11, 2014.

Despite the public availability of the transaction ledger, an IFA requires a way to link the published public key to an individual to identify the user. Reid and Harrigan has indicated that through a passive analysis, it is possible to link users to public keys[67]. As exchanges have access to its clients' public keys, it may be possible that the information from digital currency exchanges contains information that links the key to the real identity of the user, provided that the user uses exchange services to convert their digital coinage to real currency. If most conversions occur within digital currency exchanges, regulation would enhance the reasoning for exchanges to collect personal data not to only protect themselves from suspicious clients but also protect the client in knowing that the exchange is following due diligence within their industry and can be trusted.

Another method of conversion may not require the assistance of a digital exchange service, as long as the seller is willing to accept BTC and provide the buyer with real currency directly. The level of trust required for such transactions are higher, although it would escape the scrutiny of potential government regulations if the exchange is between users, unattached to larger organizations. A method is required to at least capture such transactions so that if required, there will be clues available to associate the user with its public keys. A potential solution would be to track wallets, as mentioned previously, in order to capture such transfers.

The legitimacy of the ledgers made public by Bitcoin may be questioned. While the concept of the cryptocurrency can be analyzed, it would be difficult for IFAs to vouch that the ledger is accurate and can be relied on.

[67] Reid and Harrigan (p.26).

8.2 Following the Digital Transaction

Using a simple transaction as an example, imagine a buyer purchasing a book from a vendor in exchange for a certain amount of digital coins. While the transaction looks simple, with all transactions converted to the digital world, the difficulty for IFAs lies in showing and proving each step of the transaction.

Buyer passes amount to Vendor

In a real currency transaction, the buyer provides the vendor with real currency. While the cash may be recorded by the vendor in their records, the vendor will provide a receipt to indicate that the amount has been received and recorded. A decrease in the bank balance and a receipt obtained from the Buyer will provide the forensic accountant evidence that the cash relates to the receipt.

For digital currencies, the Vendor provides the public key address to the Buyer to enclose the funds in, likely via an e-mail. The transaction ID produced by the transfer of funds can also be confirmed through the public ledger. By having information on the public key produced by the Vendor and the transaction ID produced from the transfer of funds, the IFA can confirm the link of the transfer to the public key. Depending on the vendor, a confirmation from the Vendor to indicate that the funds were accepted may be received by the Buyer, acting as a receipt.

Through access of e-mail addresses, the IFA should be able to obtain enough information to confirm the transfer of digital coins between users. If the Buyer does not have information on how the Vendor's public key address is obtained, the lack of a paper trail will make it difficult to determine whether the Buyer truly sent the funds to the correct

address as there could be human error when typing in the address that the funds are to be sent. Another issue that is out of forensic accountant's expertise is determining whether the public ledger of Bitcoin is accurate and can be used as the basis for confirming transactions. Approval on the transfer also provides a challenge as theoretically, the Buyer should be the only one with access to the private key to access the funds; however, if someone else also had access to the private key such as a hacker or an exchange, it would be hard to determine whether the approval was given by the actual user if there were any disputes between the user and the intermediary that they have provided access to their funds.

Vendor provides goods/services to Buyer

In a real currency transaction, the goods or services provided by the Vendor will be given to the Buyer in-person or sent through the mail. To prove that the Vendor has sent the goods, a tracking number for the package may be provided to the Buyer. Once again, e-mail confirmation is likely the most convenient way of producing such information. If the transaction is private, there is likely no sales invoice given to the Buyer and to keep costs at a minimum, the Buyer might not even receive a tracking number for their goods. Issues rise if the Vendor did not send their goods after receiving the coins. With only user-names and an e-mail address that may only be set up for such behaviour, the forensic accountant may have difficulty in finding the Vendor's true identity.

Aside from the public key that the Vendor has provided, information of the Vendor is limited. With the current lack of information on users not using exchanges, factors such as an e-mail used specifically for swindling by the Vendor or the Vendor transferring the

funds out from the given public key and laundering the funds through multiple keys will deter the ability of identifying the user.

With the ability to link the wallet keys to the corresponding wallet, the information required to associate an actual individual to the wallet will provide forensic accountants the confirmation required to support their findings.

8.3 Tracking Wallets

As mentioned in Section 7, if the KYC process also exists at the beginning stages of opening a wallet, this would help identify users with the wallets that are used to keep their public keys. However, by requiring filling out of personal information and having the information validated before a wallet can be open will likely be considered onerous for the user as it removes the efficiency value of using BTC instead of real currency.

Lack of privacy will also be a concern since personal information will likely be stored by the issuing facilities; therefore, the issuing facility must also prove that the data obtained from its users are stored safely to minimize hacking efforts.

8.4 Mutual Legal Assistance Treaty

In order to identify the individual, the public keys that are under suspect needs to be identified. While production orders are issued to financial institutions to obtain information on individuals, assuming that a pattern was established that the user frequently performs transactions with a digital currency exchange, an equivalent type of production order should be issued to the digital currency exchange as they would have to obtain personal information of the user to mitigate fraud risks associated with the

company. If the individual is found to be outside the jurisdiction of Canada, special assistance is required to obtain the information.

As money laundering offences are found under the Criminal Code, the Mutual Legal Assistance in Criminal Matters Act provides for the implementation of treaties for assistance in criminal matters. Section 9.3 (4) notes that a registered order filed will have the same effect as a warrant for seizure of proceeds of crime, restraint of proceeds of crime, and seizure and restraint of offence-related property[68]. For digital currencies where physical seizure of funds is not possible due to its intangible form, seizure of the private keys to access the associated coins will be considered as a type of seizure of offence-related property.

The borderless ability of digital currencies requires universal cooperation in order for seizure of digital coinage purchased with proceeds of crime to be successful. The lack of jurisdiction may provide a basis for countries to ignore such requests. However, as the information that can be gathered will be considered privileged under Section 44, the information can be used as evidence in court if required and will likely be admissible.

8.5 Requiring Expert Assistance

With technology relating to digital currencies evolving at such a rapid pace, expert assistance in analysis and obtaining information is essential in order to build a case that will be admissible for litigation purposes. Acquiring help from information technology experts and information systems analysts can help ensure that information is properly extracted from computers without damage and alterations to the original files which are

[68] *Criminal Code*. *Justice Laws Website*. May 14, 2014, http://laws-lois.justice.gc.ca/eng/acts/C-46/FullText.html Accessed on June 8, 2014.

essential to prove the authenticity of the documents. Unless the IFA is also skilled with computers and extracting data, the use of experts is covered under Standard Practices Section 400.14-16[69]; therefore, the IFA must ensure that the work of the experts are at an acceptable standard and communication between the expert and the IFA is necessary so that interpretations are communicated thoroughly as the strength of the IFA's report is dependent on the information provided and its findings.

Not only do computer experts need to be continuously updated with the technology of digital currencies, IFAs also need to maintain the basic understanding and updates on the issue in order to understand the expert reports. As regulations are still evolving, engagements relating to digital currencies needs to be executed keeping potential regulation updates in mind as well as the affected jurisdictions as governments are still determining the best treatment.

9.0 CONCLUSION

While users object to regulation as it defeats one of the attractions of digital currencies, government regulations should not only be seen as a hindrance to the growth of Bitcoin but also serving the purpose of protecting its consumers from users using illicit funds. Users will likely be more willing to compromise as long as government regulators clearly shows that the purpose is to only obtain information when necessary, not for any other purposes that would inappropriately invade the privacy of its users.

[69] Standards Committee, *Standard Practices for Investigative and Forensic Accounting Engagements*. Toronto: Alliance for Excellence in Investigative and Forensic Accounting, CICA. November, 2006.

Although Bitcoin may be one of the main digital currencies taking precedence at the moment, countries like Iceland with interest in Auroracoin and China's Q-Coin provides evidence that the interest in digital currencies is only rising. Regulations should not only be considered for cryptocurrencies but for digital currencies in general as it is likely that there will be more uses of digital currencies in the future and adjusting existing legislation to fit what the current definition of digital currencies will not be enough for the evolving technology. Regulators need to consider not only the existing uses but also the future potential of digital coinage in order to produce guidance that will further the growth of digital currencies and digitalizing real currencies.

10.0 REFERENCES

Alberta Securities Act. June 13, 2013, http://www.qp.alberta.ca/documents/Acts/s04.pdf Accessed on May 3, 2014

"Announcement of Commencement of Bankruptcy Proceedings". *MtGox Co., Ltd.* April 24, 2014, https://www.mtgox.com/img/pdf/20140424_announce_qa_en.pdf Accessed on May 3, 2014.

Announcement the applicability of US Bankruptcy Code Chapter 15, *MtGox Co., Ltd.*, March 14, 2014, https://www.mtgox.com/img/pdf/20140314-announcement_chapter15.pdf Accessed on April 23, 2014.

Application of FinCEN's Regulations to Persons Administering, Exchanging, or Using Virtual Currencies. *The Financial Crimes Enforcement Network*. March 18, 2014, http://fincen.gov/statutes_regs/guidance/html/FIN-2013-G001.html Accessed on April 13, 2014

Bank Act, Government of Canada. April 16, 2014, http://www.laws.justice.gc.ca/eng/acts/B-1.01/ Accessed on April 27, 2014.

Bill C-31, *House of Commons of Canada*. March 28, 2014, http://www.parl.gc.ca/HousePublications/Publication.aspx?Language=E&Mode=1&DocId=6495200&File=4, Division 19 Accessed on May 4, 2014.

"Canadian law firm takes lead in writing first Bitcoin law book." *Duhaime Law*. May 11, 2014, http://www.duhaimelaw.com/2014/05/11/christine-duhaime-authoring-first-legal-book-on-digital-currencies/ Accessed on June 8, 2014.

CoSign Coin, http://cosign.co.in/ Accessed on May 10, 2014.

Currency Act. *Government of Canada*. 1985, http://laws-lois.justice.gc.ca/eng/acts/c-52/page-1.html Accessed on April 16, 2014.

Dark Wallet, http://darkwallet.is/ Accessed on May 5, 2014.

Doguet, J. J. "The Nature of the Form: Legal and Regulatory Issues Surrounding the Bitcoin Digital Currency System". *Louisiana Law Review*. 2013, http://digitalcommons.law.lsu.edu/cgi/viewcontent.cgi?article=6425&context=lalrev Accessed on April 15, 2014.

"EBA Consumer Trends Report 2014". *European Banking Authority*. February 28, 2014, http://www.eba.europa.eu/documents/10180/534414/EBA+Consumer+Trends+Report+2014.pdf Accessed on April 13, 2014.

Frequently Asked Questions. *Bitcoin*, https://bitcoin.org/en/faq Accessed on May 3, 2014.

Gans, J. S. and Hanna Halaburda. "Some Economics of Private Digital Currency." *Bank of Canada*. November, 2013, http://epe.lac-bac.gc.ca/100/201/301/weekly_checklist/2013/internet/w13-46-U-E.html/collections/collection_2013/banque-bank-canada/FB3-2-113-38-eng.pdf Accessed on April 13, 2014.

George-Cosh, D. "Canada Says Bitcoin Isn't Legal Tender," *The Wall Street Journal Canada*, January 16, 2014, http://blogs.wsj.com/canadarealtime/2014/01/16/canada-says-bitcoin-isnt-legal-tender/ Accessed on April 23, 2014.

Greenberg, A. "'Dark Wallet' Is About to Make Bitcoin Money Laundering Easier Than Ever". *WIRED*. April 29, 2014, http://www.wired.com/2014/04/dark-wallet/ Accessed on May 6, 2014.

Grinberg, R. “Bitcoin: An Innovative Alternative Digital Currency”. November 11, 2011, http://hstlj.org/wp-content/uploads/2011/12/8-Grinberg-159-208.pdf Accessed on April 3, 2014.

Hirata, N. and Takaya Yamaguchi. “Japan may tax bitcoin deals, stop banks, brokerages from handling.” *Reuters*, March 5, 2014, http://www.reuters.com/article/2014/03/05/bitcoin-mtgox-idUSL3N0M207R20140305 Accessed on April 9, 2014.

“How does Bitcoin work?” *Bitcoin*. Accessed on May 11, 2014 from https://bitcoin.org/en/how-it-works

“How to Store Your Bitcoins”. *Coindesk*. May 1, 2014, http://www.coindesk.com/information/how-to-store-your-bitcoins/ Accessed on May 3, 2014.

Irwin, A S.M., J. Slay, R.C. Kim-Kwang, and L. Liu. “Are the financial transactions conducted inside virtual environments truly anonymous?” *Journal of Money Laundering Control*, *16(1), 6-40*. December 11, 2012, http://dx.doi.org/10.1108/13685201311286832 Accessed on April 26, 2014

Johnson, E. “Digital Currency: legal and practical implications for forensic investigations and the forensic accountant.” *University of Toronto*. June 20, 2007. P9.

King, R. “Transaction Malleability: Why nobody can withdraw bitcoins from one of the currency’s largest exchanges.” *Quartz*. February 10, 2014, http://qz.com/175565/why-nobody-can-withdraw-bitcoins-from-one-of-the-currencys-largest-exchanges/ Accessed on April 16, 2014.

Kinsella, N. A. "Committee Authorized to Study the Use of Digital Currency," *Debates of the Senate*, March 25, 2014, http://www.parl.gc.ca/Content/Sen/Chamber/412/Debates/pdf/043db_2014-03-25-e.pdf Accessed on April 22, 2014.

Matonis, J. “Bitcoin Payments Could Quickly Become Competitive Wedge in Online Gaming”. *Forbes*. June 27, 2013, http://www.forbes.com/sites/jonmatonis/2013/06/27/bitcoin-payments-could-quickly-become-competitive-wedge-in-online-gaming/ Accessed on April 15, 2014.

Miedema, D. “U.S. states take lead in writing bitcoin rules.” *Reuters*. May 17, 2014, http://www.reuters.com/article/2014/05/17/us-bitcoin-rules-idUSBREA4G08P20140517 Accessed on May 24, 2014.

Mullan, P.C. “The Digital Currency Challenge: Shaping Online Payment Systems Through U.S. Financial Regulations”. 2014.

“Precious Metals”. *Investopedia*, http://www.investopedia.com/terms/p/preciousmetal.asp Accessed on May 3, 2014.

“Privacy Legislation in Canada.” *Officer of the Privacy Commissioner of Canada*. March, 2009, http://www.priv.gc.ca/resource/fs-fi/02_05_d_15_e.asp Accessed on May 2, 2014.

“Private currency”. *Investopedia*, http://www.investopedia.com/terms/p/private-currency.asp Accessed on May 3, 2014.

Regulation of Bitcoin in Selected Jurisdictions. The Law Library of Congress. January 2, 2014, http://www.loc.gov/law/help/bitcoin-survey/2014-010233%20Compiled%20Report_.pdf Accessed on April 9, 2014.

Reid, F. and Martin Harrigan. An Analysis of Anonymity in the Bitcoin System. *Cornell University Library*. July 22, 2011, http://arxiv.org/pdf/1107.4524.pdf?origin=publication_detail Accessed on April 27, 2014.

Remarks From Under Secretary of Terrorism and Financial Intelligence David S. Cohen on "Addressing the Illicit Finance Risks of Virtual Currency". *U.S. Department of the Treasury*. March 18, 2014, http://www.treasury.gov/press-center/press-releases/Pages/jl236.aspx Accessed on April 15, 2014.

Romero, J., B. Palacio, Karlssonwilker Inc. "How a Bitcoin transaction works" *IEEE Spectrum*, http://spectrum.ieee.org/img/06Bitcoin-1338412974774.jpg Accessed on May 5, 2014

"Some things you need to know". *Bitcoin*, https://bitcoin.org/en/you-need-to-know Accessed on May 3, 2014.

Southan, J. "Into the light: Iceland's capital is bouncing back thanks to its natural assets and creative citizens." *Business Traveller* March, 2014. *Academic OneFile*. Accessed on May 24, 2014.

Stokes, R. Virtual money laundering: The case of bitcoin and the linden dollar. *Information & Communications Technology Law*, *21*(3). October, 2012. 221-236.

USD Exchange Trade Volume, *Blockchain*, http://blockchain.info/charts/trade-volume Accessed on June 11, 2014.

Van Name, T. “Bitcoin Now on Bloomberg,” *Bloomberg Now*, April 30, 2014, http://www.bloomberg.com/now/2014-04-30/bitcoin-now-bloomberg/ Accessed on May 1, 2014.

Varriale, G. “Bitcoin: how to regulate a virtual currency”. *Perkins Coie*. August 20, 2013, http://www.perkinscoie.com/files/upload/08_20_2013_Bitcoin_IFLR.PDF Accessed on April 15, 2014.

Virtual Currencies, Financial Consumer Agency of Canada. April 1, 2014, http://www.fcac-acfc.gc.ca/Eng/forConsumers/topics/paymentOptions/Pages/Virtualc-Monnaies.aspx Accessed on April 27, 2014.

“What is money laundering”? *Financial Transactions and Reports Analysis Centre of Canada*, http://www.fintrac-canafe.gc.ca/fintrac-canafe/definitions/money-argent-eng.asp Accessed on May 10, 2014.

“What you should know about digital currency”. *Canada Revenue Agency*. November 5, 2013, http://www.cra-arc.gc.ca/nwsrm/fctshts/2013/m11/fs131105-eng.html Accessed on May 4, 2014.

“World’s first bitcoin ATM opens in Vancouver”. *CBC*. October 29, 2013, http://www.cbc.ca/news/technology/world-s-first-bitcoin-atm-opens-in-vancouver-1.2286877 Accessed on May 3, 2014.

“Your Money Services Business in Canada: What you need to know”. *Financial Transactions and Reports Analysis Centre of Canada*. April 1, 2014, http://www.fintrac-canafe.gc.ca/publications/brochure/2012-06/1-eng.asp Accessed on May 13, 2014.