

BEST PRACTICE FOR BITCOINS

**REGULATORY, LEGAL AND FINANCIAL APPROACHES TO VIRTUAL
CURRENCIES IN A HESITANT, GLOBAL ENVIRONMENT**

KELLY McCONNELL

SUPERVISOR: DR. EMMANUEL LARYEA

Best Practice For Bitcoin
Thesis – Kelly McConnell

DECLARATION PAGE

ABSTRACT

Decentralised virtual currencies may operate outside regulatory, legal and financial systems. Despite the risks that these currencies pose to stakeholders, including consumers, merchants, and investors and to the broader economy, their popularity continues to grow rapidly. Concerns regarding volatility, security and criminality can be addressed through the incorporation of virtual currencies into broader legal landscapes on a domestic and global scale. While most countries are hesitant to take the lead on virtual currency regulation, global action is required to ensure the continued effectiveness of existing regulations and provide consumer and investor protection in this new area of virtual currencies.

Bitcoin, the most widely adopted decentralised virtual currency is used as a case study in this thesis for reviewing regulation strategies in relation to virtual currencies and their associated risks. A 'best practice' regulatory approach is recommended for domestic and global authorities regarding Bitcoin regulation. This approach recommends Bitcoin regulation be incorporated into existing legal and financial frameworks in a way that balances the benefits that virtual currencies provide with the need to preserve a stable currency and economy.

Table of Contents

Declaration Page.....	2
Abstract	3
Chapter 1 - Introduction.....	6
I. Background.....	6
A. Non-Convertible VCs	6
B. Convertible VCs.....	7
1. Linden Dollars	8
2. E-Gold	8
3. Bitcoins	8
II. Concerns with Convertible Virtual Currencies.....	9
A. Criminal Law Enforcement	9
B. Regulatory Effectiveness.....	10
C. Consideration of Consumer Protection	10
III. Concerns with Regulating Decentralised Convertible Virtual Currencies.....	10
IV. Thesis Statement	11
V. Organisation of Thesis.....	12
Chapter 2 – The Bitcoin System	14
I. Features	14
A. Decentralisation	14
B. Mining	15
C. Public-ledger.....	16
II. Bitcoin Ecosystem	17
Chapter 3 – Bitcoin: Benefits and Uses	20
I. Benefits.....	20
A. Cost of Time	20
B. Accessibility and anonymity	20
II. Uses	21
III. Conclusion	23
Chapter 4 – Bitcoin: Potential Risks and Issues	24
I. Economic Risks	24
A. Short-Term Risks	24
1. Volatility	24
2. Ponzi-like	27
B. Long-Term Risks	29
II. Features	31
A. Anonymity.....	31
B. Legal Uncertainties Caused by Decentralisation	33
III. Security Risks.....	34
IV. Conclusion.....	36
Chapter 5 – Bitcoin: Current Regulatory Approaches.....	37
I. Banning Bitcoins Approach	37
II. Wait-And-See Approach.....	38
A. Characteristics.....	38

Best Practice For Bitcoin
Thesis – Kelly McConnell

B. Forms.....	39
III. Action Approach	40
Chapter 6 – Bitcoin: Why Should Bitcoin be Regulated?.....	41
Chapter 7 – Bitcoin: How Should It Be Regulated - Best Practices Recommendation	43
I. The Difficulties in Regulating Bitcoins.....	43
II. General Regulations	44
A. Actors.....	44
B. Global	44
C. Neutral and flexible	45
III. Specific Areas of Regulation	46
A. Public Law	46
B. Civil Law.....	49
1. Irreversibility	49
2. Consumer Protection.....	50
C. Bitcoin as part of the financial system	51
1. General financial services.....	52
2. Specific Regulations	53
a. Banking Regulations	53
b. Investments.....	53
i. Investments purchased with bitcoins.....	53
ii. <i>Investments in bitcoins</i>	54
c. Derivatives	54
3. Currency	55
a. Medium of Exchange.....	55
b. Global Currency Regulation.....	55
IV. Conclusion	56
Chapter 8 - Conclusion.....	57
Bibliography.....	58

CHAPTER 1

INTRODUCTION

I. BACKGROUND

Virtual currencies (VCs) have arisen with the digital age. VCs link the concept of money with advances in technology to challenge traditional perceptions of currency and introduce alternatives that exist purely in digital form. There are two basic types of VCs; non-convertible and convertible.¹

A. *Non-Convertible VCs*

Non-convertible VCs are specific to a particular domain or world and cannot be exchanged for a traditional currency. They can be divided into two types; closed and unilateral flow types.²

Closed VC scheme are usually only available in a virtual game. Users generally pay for a subscription and earn virtual money through their online performance. The VC can only be spent on virtual goods and services inside the community.³ An example of this type is World of Warcraft Gold.⁴

The second type of VC schemes are unidirectional flow VCs. This type of VCs can only flow from the real economy into a virtual community. Such VCs can be purchased directly using traditional currency at a specific exchange rate. These VCs cannot be converted back into traditional currency and can only be spent on virtual goods and services inside that community.⁵ An example of this type is Facebook Credits.⁶

¹ Financial Action Task Force, *FAFT report: virtual currencies- key definitions and potential AML/CFT Risks* (June 2014), FAFT, 4-5 <<http://www.fatf-gafi.org/media/fatf/documents/reports/Virtual-currency-key-definitions-and-potential-aml-cft-risks.pdf>>.

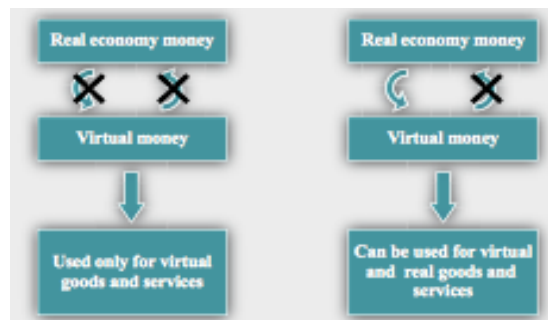
² European Central Bank, 'Virtual Currency Schemes' (Report, European Central Bank, October 2012), 13-15 <<http://www.ecb.europa.eu/pub/pdf/other/virtualcurrencyschemes201210en.pdf>>.

³ Ibid, 13.

⁴ World of Warcraft Gold is the VC used in the World of Warcraft online role-playing game designed by Blizzard Entertainment. The VC is a means of exchange in the game. Buying and selling the VC in the real world is strictly forbidden under the terms and conditions established by Blizzard Entertainment. See European Central Bank, 'Virtual Currency Schemes' (Report, European Central Bank, October 2012), above n 2, 13 <<http://www.ecb.europa.eu/pub/pdf/other/virtualcurrencyschemes201210en.pdf>>.

⁵ European Central Bank, 'Virtual Currency Schemes', above n 2, 14.

⁶ Facebook Credits are Facebook's virtual currency that allows users to buy virtual goods in any application on the Facebook platform. Facebook Credits were exchanges at a rate of FB 1 = USD 0.10.

Figure 1 emphasises the mechanism for non-convertible VC schemes⁷**B. Convertible VCs**

Convertible VCs, the focus of this thesis, have an equivalent value in real currency and can be exchanged back-and-forth for traditional currency.⁸ They allow users to buy and sell the VCs according to an exchange rate of the VC in relation to a traditional currency, similar to the purchase of any convertible currency.⁹ Users can use the VC to buy virtual and real good and services. A VC is convertible only if a market exists, some private participants must make offers and others must accept them. Convertibility is not guaranteed by law.¹⁰ There are many convertible VCs. This thesis will discuss three types, Linden Dollars, e-gold and Bitcoin in more detail below.

Figure 2 emphasises the mechanism for convertible VCs¹¹

The terms of the website did not provide for conversion back into US dollars. See European Central Bank, 'Virtual Currency Schemes' (Report, European Central Bank, October 2012), 14 <<http://www.ecb.europa.eu/pub/pdf/other/virtualcurrencyschemes201210en.pdf>>.

⁷ European Central Bank, 'Virtual Currency Schemes', above n 2, 15.

⁸ Section II in this chapter discusses the reasons why convertible VCs will be the focus of this thesis.

⁹ European Central Bank, 'Virtual Currency Schemes', above n 2, 14.

¹⁰ FAFT, *FAFT Report: virtual currencies*, above n 1, 4-5.

¹¹ European Central Bank, 'Virtual Currency Schemes', above n 2, 15.

Best Practice For Bitcoin
Thesis – Kelly McConnell1. *Linden Dollars*

Linden Dollars is a VC that was created by Linden Labs to purchase virtual goods and services in the virtual-game Second Life. Second Life has its own economy where users can buy and sell goods and services from and to each other. Linden Dollars are purchased with traditional currencies according to an exchange rate. They are convertible because users can sell their spare Linden Dollars in return for a traditional currency.¹²

2. *E-Gold*

E-gold is a VC that is operated by Gold & Silver Reserve Inc. The VC was 100% backed by physical gold (or other precious metals) held in locations around the world. Users opening an e-gold account were actually buying a quantity of gold, meaning the value of their account was linked to the price of gold. The system allowed transfers of money to other users and the selling of this VC against traditional currencies. In 2008 e-gold was suspected of violating U.S anti-money laundering regulations and two senior directors were charged with money laundering and operating an unlicensed money transfer business. E-gold is now defunct.¹³

3. *Bitcoins*

Bitcoins are created by the Bitcoin protocol. There is no central issuer for bitcoins; a distributed network of users creates them. The software that underlies it was designed and developed by Satoshi Nakamoto in 2009. Proponents argue that it possesses the 'positive characteristics of a backed currency without the perceived drawbacks of a traditional currency under the control of government'.¹⁴ The system is designed to be a peer-to-peer network, requiring no central issuer to create supply, no commercial bank to store and no trusted third party to transfer funds.¹⁵ Bitcoin uses cryptography¹⁶ and peer-to-peer

¹² European Central Bank, 'Virtual Currency Schemes', above n 2, 28.

¹³ Ibid, 13.

¹⁴ Kelsey L Penrose., 'Banking on Bitcoin: Applying Anti-Money Laundering and Money Transmitter Laws' (2014), 18 *North Carolina Banking Institute* 529, 531.

¹⁵ Nicholas A. Plassaras, 'Regulating Digital Currencies: Bringing Bitcoin within the Reach of the IMF' (2013-2014) 14 *Chicago International Law* 377, 379.

¹⁶ Cryptography is defined as the practice and study of techniques for secure communication in the presence of third parties. This area intersects the disciplines of mathematics, computer science and electrical engineering. Applications of cryptography include ATM cards, computer passwords and electronic commerce.

networking¹⁷ to bypass the usual players in the financial system.¹⁸ Bitcoins can be exchanged for traditional currencies.¹⁹

II. CONCERNS WITH CONVERTIBLE VIRTUAL CURRENCIES

The ability to convert the VC back into a traditional currency is the distinguishing feature and main concern associated with such schemes. The convertibility of such VCs means there is interaction between open-flow currencies and the real economy, multiplying the potential uses for convertible VCs. With this context in mind, there are three main concerns with convertible VCs. Firstly that the scheme can be used anonymously as a mechanism for illegal means, making it hard for law-enforcement agencies to track activities like money laundering and terrorist financing. Secondly convertible VCs may be used as the basis for financial products that may escape the reach of regulations, depriving investors of the rights normally associated with such products and undermining the effectiveness of financial regulations that protect these rights. And thirdly, convertible VCs may create legal uncertainties and risks for merchants and consumers who transact with them. These three concerns will be discussed below and are also used for the basis to justify why convertible VC regulation is important.

A. Criminal Law Enforcement

VC schemes can be used to anonymously conduct criminal activities like money laundering, drug trades and terrorist financing. Anti-money laundering and reporting regulations specifically exist to reduce these criminal activities. But an unregulated VC that does not require identifying information to transact and can be easily accessed anywhere in the world makes it difficult for law-enforcement agencies to track suspicious behaviour and enforce the law.²⁰ This undermines the goals of anti-money laundering and reporting regulations and their effectiveness. If regulations can capture VC users and strip the anonymity from these schemes, criminals acting through them will be caught and discouraged.²¹ Thus regulating VC

¹⁷ Peer to peer (P2P) networking is a distributed application architecture that partitions tasks or word loads between peers. Peers are equally privileged participants in the application.

¹⁸ Including central banks, commercial banks and payment providers.

¹⁹ Bitcoin will be the focus of this thesis and will be discussed in more detail in Chapter 2.

²⁰ Matthew Elias, *Bitcoin: Tempering the Digital Ring of Gyges or Implausible Pecuniary Privacy* (3 October 2011), Social Science Research Network
<http://papers.ssrn.com/sol3/papers.cfm?abstract_id=1937769>.

²¹ Perkins Coie, *Virtual Currencies: International Actions and Regulations* (September, 2014), Perkins Coie <<http://www.perkinscoie.com/virtual-currencies-international-actions-and-regulations/>>.

schemes will enable regulators to track criminal activity that they would otherwise be unable to.

B. *Regulatory Effectiveness*

Due to their interconnectedness of the real economy, convertible VC schemes can be used as the basis for a variety of financial products. If these VCs are unregulated, VC-based financial products circumvent financial regulations that would otherwise have to be complied with. This would undermine the goals and effectiveness of such regulations.²²

C. *Consideration of consumer protection*

Convertible VC schemes have many potential uses, including as a payment service, currency and investment. Merchants and consumers may transact in the VC, exposing themselves to legal uncertainties and risks that they may not be aware of, such as low liquidity and limited acceptance of the VC.²³ Though this may not warrant regulation, regulators need to consider the effects of such risks to transacting parties and whether consumers should be protected.

III. CONCERNS WITH REGULATING DECENTRALISED CONVERTIBLE VIRTUAL CURRENCIES

Convertible VCs have been regulated to address the concerns raised in Section II. There are no specific regulations for convertible VCs; existing regulations have been adapted to incorporate VCs according to how they are used. Regulators have been able to target the VC's central authority for compliance and enforcement. The arrest of e-gold's proprietors, Gold & Silver Reserve Inc. and its directors for violating money laundering regulations and knowingly allowing a transaction that purchased child pornography demonstrates the capacity for regulators to focus regulations on the use of the VC and target the VC's central body for enforcement.²⁴ This demonstrates how regulations have been able to be applied to convertible centralised VCs. However there has been an emergence of decentralised, convertible VCs that presents a difficulty for regulators and raises concerns about how these decentralised VCs can be regulated.

²² Penrose, 'Banking on Bitcoin: Applying Anti-Money Laundering and Money Transmitter Laws', above n 14.

²³ Pamela J. Martinson and Christopher P. Masterson, 'Bitcoin and the Secured Lender' (Report, Banking and Financial Services Policy Report, June 2014, 33.6) <<http://search.proquest.com.ezproxy.lib.monash.edu.au/docview/1540934291/abstract?accountid=12528>>.

²⁴ Grant Cross, 'Internet currency firm pleads guilty to money laundering', *The Industry Standard* (online), 22 July 2008 <<http://web.archive.org/web/20090414185759/http://www.thestandard.com/news/2008/07/22/internet-currency-firm-pleads-guilty-money-laundering>>.

Best Practice For Bitcoin
Thesis – Kelly McConnell

A decentralised, convertible VC does not have a central authority that issues new currency or processes transactions between users. A decentralised VC's system allows a distributed network of self-interested individuals to exclusively enable the creation of supply and transaction verification the system.²⁵ This decentralisation distinguishes Bitcoin and other decentralised VCs from centralised VCs like Linden Dollars and e-gold. Linden Dollars and e-gold have central authorities, similar to a central bank, Linden Labs and Gold & Silver Reserve Inc. respectively, for issuing currency and processing transactions between users.²⁶ The lack of a central authority makes it difficult for regulators to target decentralised VCs.

Bitcoin is the most well-known and developed decentralised VC. Other convertible, decentralised VCs include Litcecoins, Freecoins and Ripple. Litcecoins and Freecoins were built off the Bitcoin system and seek to address the deficiencies in the Bitcoin code.²⁷ Litecoins are more easily mined by regular consumers and are designed to be cheaper in value and easier to transact with than bitcoins and Freecoins, which charges a demurrage fee to encourage users to continually circulate the currency rather than hoard freecoins. Ripple is another virtual currency that has a distinct protocol and is a payment system and distributed currency exchange.²⁸ This thesis focuses on Bitcoin as a case study to demonstrate how regulations can target decentralised VCs. Bitcoin is used as a case study as it is the most well-known and developed decentralised VC. It has the highest degree of interest and use and has the most technological innovation, which is used to demonstrate the extensive variety of uses for VCs.²⁹

IV. THESIS STATEMENT

It is important to regulate convertible VCs to uphold the effectiveness of existing regulations. It is therefore necessary to determine a way to regulate decentralised VC. This thesis will focus upon regulating Bitcoin ('Bitcoin regulation') and will conclude that stakeholders in the Bitcoin system can be utilised to integrate Bitcoin into existing regulations even when there is no central issuer to target. The thesis will also make best practices recommendations on how Bitcoin should be regulated. These best practices recommendations will also provide guidance on how to regulate other decentralised VCs.

²⁵ Elias, 'Bitcoin: Tempering the Digital Ring of Gyges', above n 20.

²⁶ Ibid.

²⁷ These deficiencies will be discussed in further detail in Chapter 4.

²⁸ See Saumya Vaishampayan, *Five virtual currencies other than bitcoin* (18 November 2013), MarketWatch <<http://www.marketwatch.com/story/five-virtual-currencies-other-than-bitcoin-2013-11-18>>.

²⁹ European Central Bank, 'Virtual Currency Schemes', above n 2.

V. ORGANISATION OF THESIS

This thesis encompasses eight chapters including this introduction.

Chapter 1, the Introduction, provides background on the emergence of VC schemes and their different types. It identifies convertible VC schemes are the most likely to attract regulatory attention due to the VCs interconnectedness to the real economy. It further identifies that Bitcoin, as a decentralised, convertible VC scheme, presents a challenge for regulators due to its lack of a central authority. The Chapter concludes by identifying the importance of considering Bitcoin regulation.

Chapter 2 discusses Bitcoin's key features and outlines the players in the Bitcoin ecosystem, a distributed network of Bitcoin users that perform different functions to make up the Bitcoin economy.

Chapter 3 ponders the various benefits and uses for the Bitcoin system and Bitcoin-based products. It concludes that the uses for Bitcoin are varied and that regulators need to consider these diverse uses in Bitcoin regulation.

Chapter 4 discusses the risks and issues associated with Bitcoin use. These risks provide the background for the best practices recommendations.

Chapter 5 discusses the current regulatory frameworks that countries are taking to address Bitcoin, identifying countries are either banning, taking action or waiting to see what other nations will do before pursuing regulations. This chapter concludes that the take action approach is necessary and aims to encourage the countries taking 'wait and see' approach to overcome their apprehension to regulate Bitcoin.

Chapter 6 builds on the reasons for regulating Bitcoin. It discusses the benefits of regulating it and the detriments of failing to take action.

Chapter 7 recommends best practices for regulating Bitcoin that considers the difficulties presented by Bitcoin's decentralisation, diverse potential uses and global reach. It recommends targeting areas in the public law, consumer protection and financial regulations to incorporate Bitcoin regulation into existing regulations.

Best Practice For Bitcoin
Thesis – Kelly McConnell

It will be concluded that by targeting the stakeholders in the Bitcoin ecosystem and incorporating these stakeholders into existing regulations decentralised VCs can be regulated.

Through this thesis the phrase Bitcoin can be used to refer to the Bitcoin system, referred to as 'Bitcoin' and as the unit of account, referred to as 'bitcoin' or 'bitcoins'.

CHAPTER 2

THE BITCOIN SYSTEM

This chapter will address Bitcoin's features and outlines the players that make up the Bitcoin ecosystem. This knowledge is essential to understand how Bitcoin works and the consequences of this for regulatory action.

I. FEATURES

A. Decentralisation

One fundamental distinguishing feature of Bitcoin is that it is a decentralised system. It can therefore be used as a currency and as a payment system. In a centralised system, new currency is issued by a central bank such as the Reserve Bank of Australia. Centralised digital currencies are also operated by central authorities, for example E-gold's issuer was Gold & Silver Reserve Inc.³⁰ This central authority is entrusted with the management of the system's currency and money supply. Bitcoin, as a decentralised system issues new currency and allows for consistent money supply through a process called 'mining'. It also operates as a decentralised payment system that does not require a trusted third party to process and verify transactions. This resolves the need to protect user privacy while preventing doubling spending and enabling transaction verification. These elements are important in ensuring trust in the system. In a centralised payment system the register would belong to a trustworthy third party such as a bank or credit card company and the transaction and verification would occur through this intermediary.³¹ Bitcoin removes the need for a third-party intermediary, by making all Bitcoin transactions public in a 'public-ledger', removing all identifying information from the public record. Bitcoin utilises unique cryptography and peer-to-peer networking technology to enable these features. Another unique feature of the Bitcoin system is the way this technology is utilised to issue bitcoins and limit their production.

³⁰ E-Gold Ltd, *E-Gold Ltd and Gold & Silver Reserve (G&SR) Inc. bankruptcy announcement* (7 July 2008), Tools <<http://tools.rosinstrument.com/pb/m/12508.htm>>.

³¹ Rhys Bollen, 'The legal status of online currencies: are Bitcoins the future?' (December 2013), 24(4) *Journal of Banking and Finance Law and Practice* 272, 277.

B. Mining

A bitcoin is an encrypted computer file that contains identifying information and is created through a process called 'mining'.³² This is the Bitcoin system's method of issuing new currency. Users volunteer their computer's processing power to solve a complicated computer algorithm.³³ This can be time-consuming process, with the typical office computer taking anywhere from several months to a few years running non-stop to mine any bitcoin.³⁴ In many instances the cost of electricity would outweigh the value of the bitcoins generated.³⁵ There are six algorithms to be solved each hour, one every ten minutes. If a user is successful in solving the algorithm they are rewarded with 50 bitcoins. This provides a financial incentive for users to mine bitcoins, allowing for a consistent supply of bitcoin to be created.³⁶ Bitcoin is designed to be self-limiting; there are only 21 million bitcoins that can ever be mined. The reward for solving algorithms will halve every four years until supply eventually runs out.³⁷

Mining not only creates new bitcoins, but also runs the Bitcoin system. The completion of a complex algorithm creates lines of code that register every bitcoin transaction, ensuring a coin is not spent twice and preventing a transaction reversal.³⁸ The financial incentive of receiving bitcoins as a reward is used as the method to process, register and validate bitcoin transactions. When the new supply of bitcoins runs out, users will still be incentivised to volunteer their computer's processing power towards this method by charging fees to process bitcoin transactions.³⁹

³² Alan L Tyree and John Sheehan SC, 'Banking law and banking practice: Bitcoin' (2012) 23 *Journal of Banking and Finance Law and Practice* 139, 140.

³³ Plassaras, 'Regulating Digital Currencies', above n 15, 386.

³⁴ Ibid.

³⁵ Ibid.

³⁶ Juan Goncalves, 'Though unconventional, Bitcoin still a viable currency', *The Georgetown Voice* (online), 5 December 2013 <<http://georgetownvoice.com/2013/12/05/though-unconventional-bitcoin-still-viable-currency/>>.

³⁷ Reuben Grinberg, 'Bitcoin: An Innovative Alternative Digital Currency' (2011) 4 *Hastings Science & Technology Law Journal* 160, 163. There is no consistent data to confirm when supply will run out. Nakamoto estimated this would be in 2140 See Brian Patrick Eha, 'SecondMarket Establishes New Bitcoin Trust for Accredited Investors', *Entrepreneur* (online), 26 September 2013 <<http://www.entrepreneur.com/article/228597>>. Other estimates predict the supply running out as early as 2025 See Nicholas A. Plassaras, 'Regulating Digital Currencies: Bringing Bitcoin within the Reach of the IMF' (2013-2014) 14 *Chicago International Law* 377, 381.

³⁸ Goncalves, 'Though unconventional, Bitcoin still a viable currency', above n 36.

³⁹ Satoshi Nakamoto, *Bitcoin: a Peer-to-Peer Electronic Cash system* (2009), Bitcoin.org <<https://bitcoin.org/bitcoin.pdf>>.

C. *Public-ledger*

Bitcoin is a 'distributed system of trust'.⁴⁰ This means that the software is open-source, enabling anyone to download and use it. A user will then be connected over the Internet to a decentralised system of users. Downloading Bitcoin software generates two keys for the users; one private and one public.⁴¹ To maintain anonymity, the user may have an unlimited amount of public-keys. The public-key can be likened to a bank account number, an address that is available to other users to send bitcoins to you. The private-key is like a password, ensuring that only you can access your account or 'wallet'. Transactions cannot be authorised without this key.⁴² All transactions associated with a public-key are broadcast to the whole community on the public-ledger.⁴³ This public-ledger contains every single bitcoin transaction in history and is shared by all the computers in the system. Transactions occur within seconds and are verified within ten minutes to an hour.⁴⁴ Every 10 minutes a list of all bitcoin transactions and the time-stamps for each bitcoin⁴⁵ is recorded on the public-ledger. The public availability of transactions prevents double spending, and the lack of identifiable information maintains privacy. This method is a differentiating feature of Bitcoin and enables for a decentralised payment system that does not require a trusted party to process and verify its transactions. The Bitcoin system maintains integrity and protects from fraud⁴⁶ by requiring more processing power than the entire bitcoin network combined to fake a transaction.⁴⁷

⁴⁰ Norton Rose Fulbright, *Bitcoin and your business* (July 2014), Norton Rose Fulbright <<http://www.nortonrosefulbright.com/knowledge/publications/119023/bitcoin-and-your-business-what-you-need-to-know>>.

⁴¹ These keys are a digital signature in the form of chain of encrypted numbers.

⁴² When conducting a bitcoin transaction, a public-key encryption will generate two mathematically related keys. One key is retained by the payee as a private password and is used to access bitcoins kept in a payer's account and the other key is made public. The public-key is used to locate the payer's account. Funds can only be extracted from a payer's account when someone has the associated private key. The payer uses their own private-key to authorise the extraction of bitcoins from their account. See Anita Ramasastry, *Bitcoin: If you Can't Ban It, Should you Regulate it? The Merits of Legalization* (25 February 2014), Verdict <<http://verdict.justia.com/2014/02/25/bitcoin-cant-ban-regulate>>.

⁴³ Ibid.

⁴⁴ Bollen, 'The legal status of online currencies', above n 31, 277.

⁴⁵ The system protect from fraud by time-stamping bitcoins. This records when a bitcoin was created and how it is spent.

⁴⁶ The system itself is secure and unlikely to be vulnerable to fraud or hacking. This feature is cited as a demonstration of the system's self-regulation. See Jon Southurst, *Australian Lawyers, Bitcoin Groups Call for Clarity on Regulation* (18 July 2014), Coindesk <<http://www.coindesk.com/australian-lawyers-bitcoin-groups-call-clarity-regulation/>>.

⁴⁷ Plassaras, 'Regulating Digital Currencies', above n 15, 385.

II. BITCOIN ECOSYSTEM

A user can obtain bitcoins in three ways: mining bitcoins, selling goods or services in exchange for bitcoins, or exchanging bitcoins with other currencies on a bitcoin exchange. Bitcoins can be stored on the exchanges themselves, in the user's wallet (computer), in an online locker or they can be converted back into another currency.⁴⁸ A bitcoin has 'no intrinsic value and is not reliant on the existence of a physical or tangible good'.⁴⁹ The value of bitcoins is derived solely from the supply and demand of the currency and is dependent on the market's willingness to buy and sell them.

Though there is no central authority in the Bitcoin system, its ecosystem consists of a variety of players. The four main types of players are: miners who obtain economic incentives for creating bitcoins and processing transactions, individuals holding bitcoins, individuals and merchants engaging in commerce with bitcoins and bitcoin exchanges that offer exchange services for bitcoins into a variety of currencies.⁵⁰ As Bitcoin becomes more popular other players are getting involved. These include mining pools,⁵¹ remote wallets,⁵² transaction anonymisers,⁵³ market information providers⁵⁴ and investment vehicles.⁵⁵ There is currently no futures market for Bitcoin.⁵⁶ The Bitcoin ecosystem is like a set of operators leveraging the Bitcoin system.⁵⁷ Figure 1⁵⁸ provides a model of Bitcoin's position in the financial and real economy.

⁴⁸ Anita Ramasastry, *Bitcoin: If you Can't Ban It, Should you Regulate it? The Merits of Legalization* (25 February 2014), Verdict <<http://verdict.justia.com/2014/02/25/bitcoin-cant-ban-regulate>>.

⁴⁹ Norton Rose Fulbright, 'Bitcoin and your business', above n 40.

⁵⁰ Elias, 'Bitcoin: Tempering the Digital Ring of Gyges', above n 20.

⁵¹ As the mining for bitcoins becomes more competitive, it requires greater computing-processing power to compete. Miners have begun to pool into group to combine their processing power to compete to complete the mathematically algorithm. This makes it almost impossible for an individual to successfully compete with these pools and mine bitcoins.

⁵² Wallets present a security risk to users that will be discussed later in the Chapter 4. Remote wallets have been introduced as a way to protect user's bitcoins that are held in an online storage site from hackers.

⁵³ Bitcoin is an anonymous system. However its anonymity can be jeopardised by law-enforcement and regulatory actions to identify Bitcoin customers. These actions will be discussed in detail in Chapter 7. Bitcoin transaction anonymisers seek to create further anonymity for bitcoin users by removing all traces of previous ownership and transactions from bitcoins. The effect of this is that bitcoins are laundered.

⁵⁴ These sites provide market updates on bitcoin. Information they provide may be the spread of exchange rates for bitcoins offered by the various exchanges. An example of a market information provider is Blockchain.info (available at <<https://blockchain.info>>).

⁵⁵ An example of a bitcoin investment vehicle is the Winklevoss exchange-traded Bitcoin fund that the Winklevoss twins have registered with the SEC. This is an EFT that is denominated and operates in bitcoins.

⁵⁶ Igot.com now offers bitcoin futures so users can lock in a bitcoin value. See David Potts, 'Bit by bit, bitcoin is gaining currency', *The Age* (online), 1 October 2014 <<http://www.theage.com.au/money/bit-by-bit-bitcoin-is-gaining-currency-20140924-10jfmb.html>>.

⁵⁷ Malte Moser, Rainer Bohme and Dominic Breuker, 'Towards Risk Scoring of Bitcoin Transactions' (Discussion Paper, Department of Information System, University of Munster, Germany), 2 <http://fc14.ifca.ai/bitcoin/papers/bitcoin14_submission_15.pdf>.

⁵⁸ Ibid, 3.

Figure 3 Bitcoin in financial and real economies⁵⁹

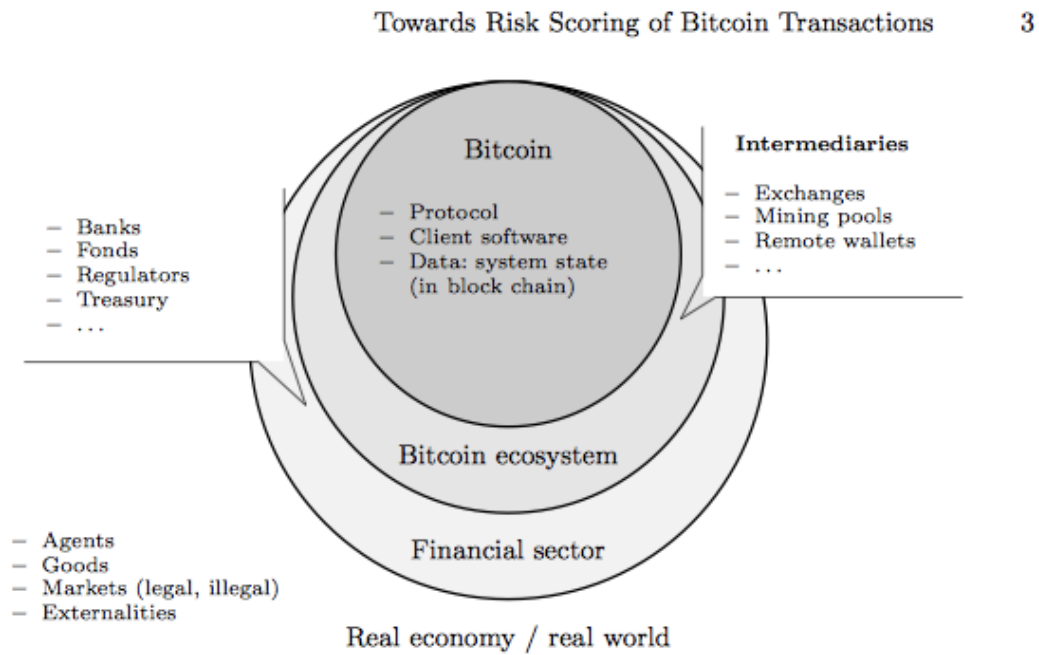


Fig. 1. Bitcoin's relation to the real world

⁵⁹ Ibid.

Best Practices for Bitcoin

There are a variety of technological innovations associated with Bitcoin and its ecosystem. Though this is not a conclusive list, Table 1 does give an impression of the variety and depth of Bitcoin innovations and the potential players in the ecosystem.

Table 1 Examples of Bitcoin innovations and players

Innovation/Player	Details
CoinBase ⁶⁰	Technology that allows individuals to buy and sell bitcoins with a U.S bank account and allows merchants to accept payment.
Bitcoin Investment Trust ⁶¹	SecondMarket introduced the first exclusively bitcoin based investment vehicle that allows institutional investors to put money into bitcoin without needing to hold the currency. It is only open to accredited investors with a minimum investment of US\$25,000.
Winklevoss Bitcoin Trust ⁶²	The Winklevoss twins applied to the U.S Securities Exchange Commission to publicly list a bitcoin trust on the stock exchange with shares available to everyone. Approval is pending on this application.
Mixer Services ⁶³	This technology caters to users wanting a greater anonymity guarantee. It works by mixing the encryption of public keys.
Bitcoin Watch ⁶⁴	This technology provides currency exchange value and volume charts offered by Bitcoin exchanges.
Bitcoin Block Explorer ⁶⁵	This technology allows individuals to search a public key address on the public ledger and see all transactions associated with that address.
Elliptic Vault ⁶⁶	A Bitcoin storage service covered by insurance is available. Lloyd's of London is the underwriter.

⁶⁰ Brian Patrick Eha, 'More Major Retails Are Getting Ready to Accept Bitcoin', *Entrepreneur* (online), 29 January 2014, <<http://www.entrepreneur.com/article/231134>>.

⁶¹ Brian Patrick Eha, 'SecondMarket Establishes New Bitcoin Trust for Accredited Investors', *Entrepreneur* (online), 26 September 2013 <<http://www.entrepreneur.com/article/228597>>.

⁶² Ibid.

⁶³ Simon Barber, Xavier Boyen, Elaine Shi et al, *Bitter to Better - How to Make Bitcoin a Better Currency*, Stanford.edu <<http://crypto.stanford.edu/~xb/fc12/bitcoin.pdf>>.

⁶⁴ Grinberg, 'Bitcoin: An Innovative Alternative Digital Currency', above n 37.

⁶⁵ Ibid.

⁶⁶ Norton Rose Fulbright, 'Bitcoin and your business', above n 40.

CHAPTER 3

BITCOIN: BENEFITS AND USES

I. BENEFITS

Bitcoin provides a quick, accessible, low-cost method of transacting over the Internet for users. These features facilitate a variety of benefits and potential uses for Bitcoin. This chapter will assist in gaining an understanding of the potential benefits and uses to Bitcoin, and demonstrates why regulatory action needs to be technology-neutral and non-specific to any one use of Bitcoin.

A. Cost and time

Bitcoin transactions are fast and cheap. A bitcoin transactions sent by a payer in Australia will be processed within seconds to anywhere in the world and will be verified within an hour.⁶⁷ Bitcoin provides an efficient alternative to international transactions that may take 2-5 days to process and may require accounts at both ends.⁶⁸ Furthermore, there can be substantial expense in making international transactions. Currently, Bitcoin miners are financially incentivised through the mining method to process bitcoin transactions, resulting in no transaction fees. Even when transaction fees are charged, Bitcoin is likely to remain a quicker and cheaper alternative to payments made through financial intermediaries.

B. Accessibility and anonymity

Bitcoin is also very accessible, requiring only an Internet connection to use. Ernie Allen, CEO of the International Centre of Missing and Exploited Children recognises the potential benefits of Bitcoin's accessibility, stating that virtual currencies can 'achieve social good by bringing real financial inclusion for the 2.5 billion adults today without access to banks, credits and the mainstream banking system'.⁶⁹ Bitcoin's real benefits may be realised in the developing world where Internet services access is increasing, but billions of people remain unable to access affordable traditional banking services.⁷⁰ Therefore it may be in the developing world that the benefits of Bitcoin can truly make an impact.⁷¹ In the developed world, Bitcoin's volatility may make it an 'unattractive

⁶⁷ Bollen, 'The legal status of online currencies', above n 31, 277.

⁶⁸ Western Union is an example of this. Tyree, 'Banking law and banking practice: Bitcoin', above n 32, 139.

⁶⁹ Brian Patrick Eha, 'Why Regulate Bitcoin', *The New Yorker* (online), 18 November 2013
<<http://www.newyorker.com/business/currency/why-regulate-bitcoin>>.

⁷⁰ Aaron Miller, *Bitcoin: A Currency Revolution* (22 September 2011), Academia.edu
<http://www.academia.edu/1024973/Bitcoin_A_Currency_Revolution>.

⁷¹ Ibid.

Best Practices for Bitcoin

investment for holding a significant portion of an individual's wealth'.⁷² However in countries where a government-issued currency is equally unstable, bitcoins may be an attractive investment.⁷³ This is particularly true in countries where people are living with an unpredictable national currency or where there are capital controls on the currency.⁷⁴ As Bitcoin is difficult for governments to control, thus provide a useful and anonymous alternative currency.⁷⁵ However, an unfortunate consequence of anonymous accessibility is that people and countries may be able to circumvent economic sanctions by transacting in bitcoins.⁷⁶

II. USES

The benefits of Bitcoin, stemming from its accessibility, anonymity and ability to conduct quick and cheap transactions via the Internet have given rise to a system that has multiple current and potential uses. Bitcoin has two main types of purposes, those that depend upon the system itself and products that developed from Bitcoin, and are dependent on it as the basis for their existence.

The Bitcoin system itself is currently used as a currency, payment system and speculative investment. Though it is controversial whether Bitcoin fulfils the economic functions of a currency,⁷⁷ it can be used to purchase goods and services, the only limitation being the willingness of a

⁷² Jonathan B. Turpin, 'Bitcoin: the Economic Case for a Global Virtual Currency Operating in an Unexplored Legal Framework' (2014) 21 *Indiana Global Legal Studies* 335, 348.

⁷³ Ibid, 359.

⁷⁴ Joe Weisenthal, 'China May Be Preparing Harsh New Regulations on Bitcoin', *Business Insider Australia* (online), 2 April 2014 <<http://www.businessinsider.com.au/chinese-bitcoin-regulations-2014-4>>.

⁷⁵ This trend can be seen in Iran, where Iranians are moving their money to Bitcoin, enabling them to hold their wealth anonymously and electronically in response to economic sanctions and an unpredictable currency. The trend is also believed to have emerged following the announcement by the Cypriot President that the government would be taking a portion of the saving accounts held by Cypriot banks in March 2013. Two days following this announcement the price of bitcoins rose dramatically and there was a significant increased interest in Bitcoin on Internet search engines. See Jonathan B. Turpin, 'Bitcoin: the Economic Case for a Global Virtual Currency Operating in an Unexplored Legal Framework' (2014) 21 *Indiana Global Legal Studies* 335.

⁷⁶ Turpin, 'Bitcoin: the Economic Case for a Global Virtual Currency', above n 72, 360.

⁷⁷ The three economic functions of a currency are as a medium of exchange, unit of account and store of value. Some argue that for Bitcoin to be a useful currency it must fulfill these purposes. Bitcoin can most likely be used as medium of exchange, though the low liquidity in exchanging bitcoins and limited acceptance of it as a form of payment limits this function. Bitcoin however, is unlikely to fulfill the other two functions. Merchants must quote bitcoin prices in 4 to 5 decimal places with a leading zero, creating an unusual and unfriendly reference point for consumers, suggesting bitcoin makes a poor unit of account. Furthermore bitcoins cannot be stored in banks, they can only be stored in wallets or lockers that are vulnerable to hacking or theft. Though there is some forms of deposit insurance available for these wallets, the vast majority of bitcoins are not protected to the same levels as funds stored in traditional banks. Bitcoin is also extremely volatile, with its fluctuations not linked to macroeconomic events. This market uncertainty makes it difficult to hedge and manage risks. These features make bitcoin an unsafe and unreliable store of value. See European Central Bank, 'Virtual Currency Schemes' (Report, European Central Bank, October 2012), 10 <<http://www.ecb.europa.eu/pub/pdf/other/virtualcurrencyschemes201210en.pdf>>.

Best Practices for Bitcoin

merchant to accept bitcoins as a form of payment.⁷⁸ Bitcoins are not legal tender in any country,⁷⁹ therefore for the purposes of regulation; it is a form of money that depends upon a private agreement to accept it as such.⁸⁰ Bitcoin can also be used as a payment system where users can transact or transfer funds through the system.⁸¹ Bitcoins can be exchanged for traditional currencies, encouraging the use of Bitcoin as a quick and cheap way to transfer and transact internationally. Bitcoin can also be used as a speculative investment. Market speculators conduct 80-90% of all bitcoin transactions.⁸² It will be discussed in more detail in Chapter 4 why bitcoins are an attractive investment to some. Bitcoin also has the potential to be used for a variety of other purposes, including for crowd funding,⁸³ as an investment vehicle⁸⁴ and even as the basis for a validation protocol tool to validate information other than transactions, such as electronic votes.⁸⁵

Bitcoin also has the potential to be used as the basis for a variety of products. These products include investments,⁸⁶ to create debit and credit cards,⁸⁷ as the basis for derivatives and even to perform banking services.⁸⁸

⁷⁸ David Rountree, 'Champing at the Bitcoin: Bitcoin, Regulators and the Law (October 2013) 32 *Communications Law Bulletin* 5, 6.

⁷⁹ Perkins Coie, 'Virtual Currencies: International Actions and Regulations', above n 21.

⁸⁰ Franziska Boehm and Paulina Pesch, 'Bitcoin: a First Legal Analysis - with reference to German and US-American law' (Discussion Paper, Institute for Information, Telecommunication and Media Law, Leonardo-Campus 9, Germany) <http://fc14.ifca.ai/bitcoin/papers/bitcoin14_submission_7.pdf>.

⁸¹ Turpin, 'Bitcoin: the Economic Case for a Global Virtual Currency', above n 72. Some small businesses and large online retailers such as Amazon accept bitcoins as payment. See David Potts, 'Bit by bit, bitcoin is gaining currency', *The Age* (online), 1 October 2014 <<http://www.theage.com.au/money/bit-by-bit-bitcoin-is-gaining-currency-20140924-10jfmb.html>>. Paypal has also set up the infrastructure for retailers to receive payments in Bitcoin. See BBC, *New Paypal partnership enables limited Bitcoin payments* (24 September 2014), BBC <<http://www.bbc.com/news/technology-29341886>>.

⁸² David Yermack, 'Is Bitcoin a Real Currency? An economic appraisal' (Working Paper, No. 19747, NBER Working Papers, 2013) <<http://online.wsj.com/public/resources/documents/NBER.pdf>>.

⁸³ Phillipe Marini, 'Regulation & Innovation: Public Authorities and the Development of Virtual Currencies' (Report, Committee on Finance of the French Senate, 4 August 2014) <<http://www.senat.fr/rap/r13-767/r13-767-syn-en.pdf>>.

⁸⁴ David Yermack, 'Bitcoin Economics: the digital cash lacks most of the features economists value in a currency' (2014) 117 *Technology Review* 12.

⁸⁵ Marini, 'Regulation & Innovation: Public Authorities and the Development of Virtual Currencies', above n 83.

⁸⁶ The Bitcoin Investment Trust introduced by SecondMarket and the Winklevoss Bitcoin Trust, described in Chapter 2 demonstrate how Bitcoin can be used as an investment vehicle and the basis for a financial product.

⁸⁷ Bitplastic offers the world's only Bitcoin debt card, enabling a purchaser to convert Bitcoin to cash and withdraw it anonymously anywhere in the world. See Bitplastic.com <<https://bitplastic.com>>. CoinJar is also offering an experimental debt card that can be used in supermarkets or anywhere else that takes eftpos. The card can be swiped, and converts the bitcoins into a linked bank account. See David Potts, 'Bit by bit, bitcoin is gaining currency', *The Age* (online), 1 October 2014 <<http://www.theage.com.au/money/bit-by-bit-bitcoin-is-gaining-currency-20140924-10jfmb.html>>.

⁸⁸ BTCjam provides services for bitcoin loans. See Btcjam.com <<https://btcjam.com/borrow/overview>>. Circle is also providing services for a Bitcoin bank, allowing for the withdrawing, depositing, and storage of bitcoins. See Sharif Sakr, *Bitcoin bank entices mom and pop with insurance, fraud checks and no fees* (16 May 2014), Engadget <<http://www.engadget.com/2014/05/16/circle-bitcoin-bank/>>.

III. CONCLUSION

It is necessary only to note that money is a social construct, a tool that has evolved and adapted in character throughout history.⁸⁹ Bitcoin is designed to provide a 'new form of money using cryptography to create supply and control transactions'.⁹⁰ It challenges traditional notions of money but this does not undermine its growth in popularity or there many potential uses it. It is beyond the scope of this thesis to consider the viability of Bitcoin or bitcoin-based products; it is only necessary to outline their potential purposes and risks. The risks associated with Bitcoin and its uses will be discussed in Chapter 4. Chapter 4 will also outline some technological and economic ways to mitigate these risks. The regulations discussed in Chapter 7 will take into account the various current and potential uses of Bitcoin.

⁸⁹ European Central Bank, 'Virtual Currency Schemes', above n 2, 10.

⁹⁰ Bollen, 'The legal status of online currencies', above n 31, 274.

CHAPTER 4

BITCOIN: POTENTIAL RISKS AND ISSUES

Bitcoin poses risks to stakeholders including consumers, merchants and investors ('users') and central banks. These risks can be broadly characterised as economic risk, security risks and risks associated with Bitcoin's distinguishing features of anonymity and decentralisation. This chapter will outline the risks that Bitcoin stakeholders choose to bear in using the system and the challenges these risks can present to law enforcement. The chapter will also demonstrate technological and economic actions that stakeholders can take to mitigate these risks.

This chapter will use the history of Mt Gox, the world's largest Bitcoin exchange as a case study for the risks associated with Bitcoin.⁹¹ Several events in Mt Gox's history demonstrate these risks. These events include vulnerabilities exposing users to volatility and security risks, and Mt Gox's bankruptcy in February 2014, which left Mt Gox's users with limited legal recourse.

I. ECONOMIC RISKS

The economic risks associated with Bitcoin can be separated into short-term and long-term. The short-term risks are Bitcoin's volatility and its Ponzi-like features. The long-term risks are those that may arise if Bitcoin is widely adopted.

A. Short-Term Risks

1. Volatility

Bitcoin is highly volatile, with its value fluctuating based on a variety of factors that have no definitive link to the wider economy.⁹² The European Banking Commission (ECB) states that volatility depends on how many people are using Bitcoin, low-trading levels and the speculating activity associated with it.⁹³ Due to these factors Bitcoin's volatility is mostly linked to its own system. An

⁹¹ Mt Gox is an acronym for Magic: The Gathering Online eXchange, originally used for trading cards online (85),⁹¹. In July 2010 Jed McCaleb rebranded the site Mt Gox as a Bitcoin exchange. Mtgox.com was sold to Mark Karpeles in March 2011. Mt Gox in 2013 account for 80% of all bitcoin transaction. See Kate L, *The Rise and Fall of Mt Gox, Everything You Need to Know* (25 March 2014), CoinReport <<https://coinreport.net/editorial-rise-fall-mtgox/>>.

⁹² Bitcoin is not pegged to a real world currency or commodity. It is 10 times more volatile against the \$US than other major currencies such as the Euro and 3 to 4 times more volatile than common traded stocks⁹². Bitcoin's fluctuations are not linked to macroeconomic events and can primarily be attributed to events linked to its own system. See David Yermack, 'Bitcoin Economics: the digital cash lacks most of the features economists value in a currency' (2014) 117 *Technology Review* 12, 12.

⁹³ European Central Bank, 'Virtual Currency Schemes', above n 2, 38.

Best Practices for Bitcoin

example of this can be seen on 19th June 2011 when Mt Gox experienced its first hacker attack, causing 60,000 identities to be leaked, and 600 users having their balances stolen. This initiated a mass sell-off of bitcoins, causing the price to drop from US\$17.00 to \$0.01 in a matter of hours.⁹⁴ Bitcoin's volatility was also emphasised during Mt Gox's bankruptcy crisis. Prior to this announcement, the price of Bitcoin dropped 23% in the space of one day,⁹⁵ due to a mass selling-off of bitcoin at low-value by Mt Gox users who feared they could not liquidate their funds. This volatility can be seen in *Figure 4*.⁹⁶ *Figure 5*⁹⁷ further emphasises the volatility of bitcoins over a 12-month period.

Figure 4, the fall in Bitcoin's value on 25 February 2014, the day Mt Gox declared bankruptcy.⁹⁸



Bitcoin's price Monday night, as measured by Bitcoin news site and price tracker Coindesk.

⁹⁴ Kate L, *The Rise and Fall of Mt Gox, Everything You Need to Know* (25 March 2014), CoinReport
<<https://coinreport.net/editorial-rise-fall-mtgox/>>.

⁹⁵ Shirley Siluk, *Why are the feds seizing Mt. Gox and Dwolla funds* (15 May 2013), Coindesk
<<http://www.coindesk.com/why-are-the-feds-seizing-mt-gox-and-dwolla-funds/>>.

⁹⁶ *Ibid.*

⁹⁷ Blockchain, *Market Price (USD)* (20 September 2014), Blockchain.info
<https://blockchain.info/charts/market-price?timespan=all&showDataPoints=false&daysAverageString=1&show_header=true&scale=0&address=>>.

⁹⁸ Siluk, *Why are the feds seizing Mt. Gox and Dwolla funds*, above n 96.

Best Practices for Bitcoin

Figure 5, the price of bitcoins during a 12-month period ending September 2014, demonstrating its volatility.⁹⁹



It is extremely difficult to hedge or manage risk associated with Bitcoin's volatility.¹⁰⁰ This lessens the ability of businesses to use and accept Bitcoin as a major part of their operation. Bitcoin's volatility limits the capacity for merchants and consumers to use Bitcoin as a medium of exchange. As the exchange-price for bitcoins differs greatly depending on the exchange, this provides as a further risk to Bitcoin as a currency. During Mt Gox's popularity a premium of between \$23 and \$34 was charged due to the perceived stability in the exchange.¹⁰¹ The differences in exchange-prices can be seen in *Figure 5*.¹⁰² Although Bitcoin's volatility is a risk to consumers, merchants and investors, though some argue that Bitcoin is a resilient system that recovers from crashes.¹⁰³ A recommendation for avoiding this is to utilise a tool like BitPay to automatically convert received bitcoins into local currency, limiting exchange and volatility exposure.¹⁰⁴

⁹⁹ Blockchain, *Market Price (USD)*, above n 93.

¹⁰⁰ There is difficulty in hedging or managing risks associated with bitcoins. This is due to Bitcoin's extreme volatility that is not linked to any macroeconomic events. Bitcoins may experience swings in value very quickly with no external economic warnings. The value is unpredictable and vulnerable to disruptions in its own system. There are also counter-party risks as the derivatives market for bitcoins, even over-the-counter, is quite small. See Yermack, 'Is Bitcoin a Real Currency? An economic appraisal', above n 82.

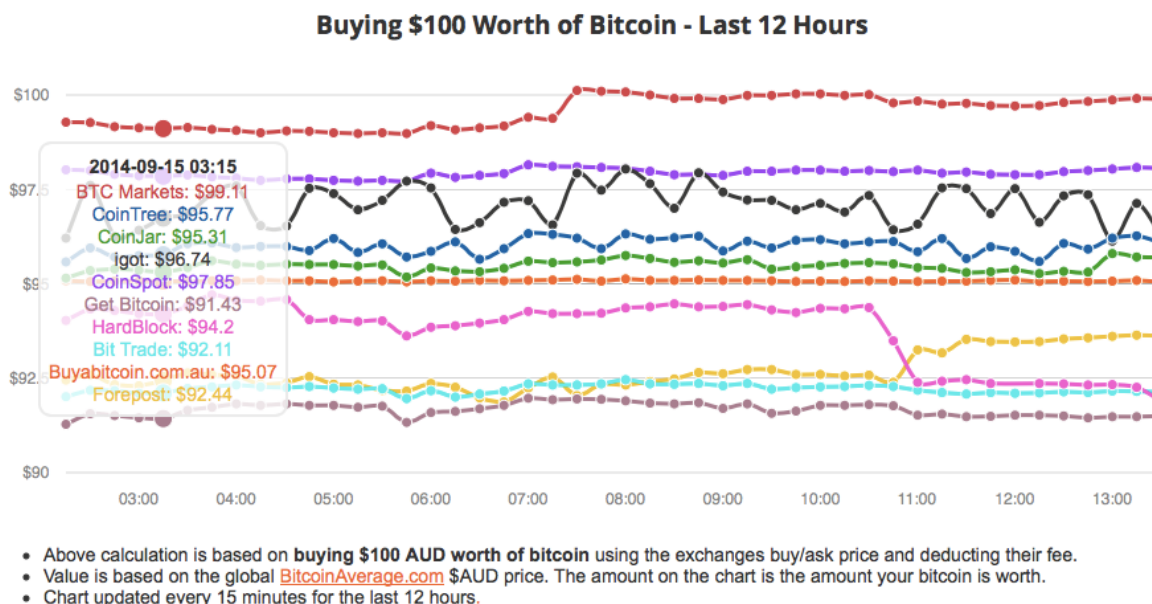
¹⁰¹ Kate L, *The Rise and Fall of Mt Gox, Everything You Need to Know*, above n 95.

¹⁰² Compare Bitcoin Exchanges, *Buying \$100 Worth of Bitcoin - Last 12 hours* (20 September 2014), Compare Bitcoins Australia <<http://comparebitcoins.net>>.

¹⁰³ Jeff Cox, 'Bitcoin's four steps to Wall Street acceptance', *CNBC* (online), 8 January 2014 <<http://www.cnbc.com/id/101320507>>.

¹⁰⁴ Moser, 'Towards Risk Scoring of Bitcoin Transactions', above n 57.

Figure 6, the differences in exchange-prices that can be received for US\$100, recorded during a 12-hour period on 15th September 2014.¹⁰⁵



2. Ponzi-like

Bitcoin is an attractive investment to speculators due to its potential appreciation-value. Bitcoin exchanges operate 24-hours-per-day and do not automatically close to prevent massive inflation.¹⁰⁶ There is also no guarantee that bitcoins will be exchanged into a traditional currency.¹⁰⁷ It is also an illiquid market that depends on broad bid-ask spreads.¹⁰⁸ Bitcoin is a risky investment, as it does not generate any income, and depends only on capital growth.¹⁰⁹ Investors may in the short-term lose part of or all of their investment if the value of bitcoins drops. An example of this is Mt Gox's bankruptcy, discussed above.¹¹⁰

¹⁰⁵ Compare Bitcoin Exchanges, *Buying \$100 Worth of Bitcoin - Last 12 hours* (20 September 2014), above n 87.

¹⁰⁶ Miller, *Bitcoin: A Currency Revolution*, above n 70.

¹⁰⁷ Perkin Coies, *Virtual Currencies: International Actions and Regulations*, above n 21.

¹⁰⁸ Yermack, 'Is Bitcoin a Real Currency? An economic appraisal', above n 82.

¹⁰⁹ McCullough Robertson Lawyers, *Can a self managed super fund invest in bitcoins?* (15 July 2014), McCullough Robertson Lawyers <http://www.mccullough.com.au/publications/f/View/Finance==Can_a_self_managed_super_fund_invest_in_bitcoins/>. Bitcoin was named one of the top 10 2013 threats to investors by NASAA 72, with some likening bitcoin to the 1990s Internet stocks. See David Yermack, 'Is Bitcoin a Real Currency? An economic appraisal' (Working Paper, No. 19747, NBER Working Papers, 2013) <<http://online.wsj.com/public/resources/documents/NBER.pdf>>.

¹¹⁰ Kate L, *The Rise and Fall of Mt Gox, Everything You Need to Know*, above n 95.

Best Practices for Bitcoin

Bitcoin may also present a long-term risk to investors. Esontia,¹¹¹ France¹¹² and two American agencies, FINRA¹¹³ and the SEC¹¹⁴ have warned that Bitcoin may be a Ponzi scheme. This warning arises from the limited supply of bitcoins. The limited supply ensures users are financially invested in getting more people involved and the value of bitcoins continually appreciating. This makes 'today's buyers tomorrow's sellers'.¹¹⁵ Appreciation of bitcoins also encourages hoarding, which takes bitcoins out of circulation and drives their value up.¹¹⁶ Bitcoin's infrastructure is designed as a transaction system, rather than as a speculative investment vehicle. If bitcoins are taken out of circulation, the transaction volume will dwindle, making mining less profitable as supply decreases. If the circulation of bitcoins drops too much, it will likely result in a loss of interest in the system. Furthermore, if there are less users and miners, the effort devoted to verifying transactions diminishes, bringing the system to a halt and making it more vulnerable to attack.¹¹⁷ The appreciating value of bitcoins, its limited supply and the consequential hoarding that is encouraged by these features makes Bitcoin a risky investment. Furthermore, as the system is dependent upon bitcoin transactions and mining to remain secure, the features that discourage these activities could potentially damage the infrastructure that holds the system together and leave investments exposed to security risks and extreme volatility.¹¹⁸

A possible solution, suggested by Goldman Sachs 'is that the supply of bitcoins could be increased; only requiring 51% of computer power of the network to be dedicated towards adopting that change. Consensus could be reached through online developer forums and the changes made by the miners who maintain the system'.¹¹⁹ Increasing supply of bitcoins could ease inflationary concerns and discourage hoarding, although this places monetary decisions for the currency in the hands of

¹¹¹ Perkin Coies, *Virtual Currencies: International Actions and Regulations*, above n 21.

¹¹² Ibid.

¹¹³ The Financial Industry Regulatory Authority. U.S. Securities and Exchange Commission, 'Investor Alert: Bitcoin and other Virtual Currency-Related Investments' (Investor Alert, Securities and Exchange Commission, 7 May 2014) <http://www.sec.gov/oiea/investor-alerts-bulletins/investoralertsia_bitcoin.html#.VCCwmksk8dt>.

¹¹⁴ Securities Exchange Commission. U.S. Securities and Exchange Commission, 'Investor Alert: Ponzi Schemes Using Virtual Currencies' (Investor Alert, No. 153, SEC, Office of Investor Education and Advocacy) <http://www.sec.gov/investor/alerts/ia_virtualcurrencies.pdf>.

¹¹⁵ Stephen Kinsella, 'Once bitten twice shy, so stay away from Ponzi-like Bitcoins', *Independent.ie* (online), 19 November 2013 <<http://www.independent.ie/opinion/columnists/stephen-kinsella/stephen-kinsella-once-bitten-twice-shy-so-stay-away-from-ponzilike-bitcoins-29764982.html>>.

¹¹⁶ Miller, *Bitcoin: A Currency Revolution*, above n 70.

¹¹⁷ Bitcoin would be more vulnerable as less computer power would be needed to override the system, making it easier for an individual or group of miners to attack the system. See Simon Barber, Xavier Boyen, Elaine Shi et al, *Bitter to Better - How to Make Bitcoin a Better Currency*, Stanford.edu <<http://crypto.stanford.edu/~xb/fc12/bitcoin.pdf>>.

¹¹⁸ Miller, 'Bitcoin, a Currency Revolution', above n 70.

¹¹⁹ Yermack, 'Is Bitcoin a Real Currency? An economic appraisal', above n 82.

Best Practices for Bitcoin

an Internet forum, rather than a central bank.¹²⁰ This could lead to uncertainty and a loss of confidence in the system. Another possible solution to inflation is the introduction of bitcoin credit or a fractional-reserve bitcoin banking-system.¹²¹

If interest in Bitcoin falls, for whatever reason, investors left holding the coin will be exposed to a quick and permanent loss in value. This is a risk that investors need to be aware of and regulators should consider when forming regulatory strategies.

B. Long-Term Risks

There are long-term risks associated with Bitcoin if it is widely adopted.¹²² The issues and regulatory actions that arise from wide adoption of Bitcoin are now considered.

Supporters of Bitcoin argue that its limited supply and lack of governmental control gives Bitcoin a legitimacy that is absent in government-issued currencies.¹²³ Government-issued currencies are susceptible to influence from interest groups and economic concerns, such as the quantitative easing actions pursued by central banks following the global financial crisis.¹²⁴ Governments may print money and cause inflation, thereby harming the currency's stability. Bitcoin, it is argued, is stabilised by self-interested parties that have a financial incentive to keep the currency stable, ensuring there is no erosion in the purchasing power of bitcoins and enabling it to be a useful store of value.¹²⁵ The ECB argues that the 'theoretical roots' of Bitcoin can be found in an economic thought¹²⁶ that criticises traditional money, interventions taken by government in financial crisis and the fractional-reserve banking system as the current basis for our financial system.¹²⁷ The ECB also

¹²⁰ Ibid.

¹²¹ Craig K. Elwell, M. Maureen Murphy and Michael V. Zeitzinger, 'Bitcoin: Questions, Answers and Analysis of Legal Issues' (Congressional Report, Congressional Research Service, 15 July 2014), <<http://fas.org/sgp/crs/misc/R43339.pdf>>.

¹²² For Bitcoin to be widely adopted its daily value will likely need to stabilise so it can serve as a store of value and unit of account in the commercial markets. At the moment its volatility are more consistent with the behaviour of a speculative investment than a currency. See David Yermack, 'Is Bitcoin a Real Currency? An economic appraisal' (Working Paper, No. 19747, NBER Working Papers, 2013) <<http://online.wsj.com/public/resources/documents/NBER.pdf>>.

¹²³ Plassaras, 'Regulating Digital Currencies', above n 15, 389.

¹²⁴ Ibid.

¹²⁵ Elwell, 'Bitcoin: Questions, Answers and Analysis of Legal Issues', above n 122, 6.

¹²⁶ The Austrian School of Economics, led by Eugen von Bohm-Barwerk, Ludwig von Mises and Friedrich A. Hayak, argues that business cycles are the inevitable consequence of monetary interventions in the market by governments and call for the abolition of the fractional-reserve banking system and returning to money based on the gold standard, which cannot be easily manipulated by any authority. See European Central Bank, 'Virtual Currency Schemes', above n 2, 22.

¹²⁷ European Central Bank, 'Virtual Currency Schemes', above n 2, 22.

Best Practices for Bitcoin

states that Bitcoin is a direct testament to the monetary theory of Friedrich von Hayek,¹²⁸ concluding that proponents of Hayek's theory would argue Bitcoin is a 'positive move in the direction of ending monopoly of central banks' that introduces private currency in the post-global financial crisis era.¹²⁹ Nonetheless, Bitcoin is exposed to the same vulnerabilities as the gold standard, which showed that a fixed money supply is incompatible with a growth economy.¹³⁰ A Bitcoin-dominated economy would likely result in the need to accept pay cuts and a reduction in the prices of goods due to the deflationary effects of the limited supply of bitcoins.¹³¹ This deflationary effect presents an economic flaw that limits the ability for Bitcoin to be used widely as a currency.¹³²

Though Bitcoin is not current a threat to financial stability, it may be if widely adopted.¹³³ The ECB acknowledge that wide adoption could lessen the effectiveness of central banks as virtual currencies are outside their oversight but are connected to the real economy.¹³⁴ Critics to this argument suggest wide acceptance is not realistic, as most people will continue to exchange bitcoins for traditional currencies and because Bitcoin is not used as the basis for an economy in a country or currency area.¹³⁵ They argue that it is most likely that merchants will continue to accept other currencies and adapt prices to bitcoins.¹³⁶ However, even in a mature market, with 1% bitcoins and 99% USD, the purchasing power of bitcoins will increase over time as Bitcoin has no alternative but to appreciate tremendously.¹³⁷ The Federal Reserve¹³⁸ in this example would need to increase the number of dollars in circulation to accommodate economic growth. Their power would be limited due to the number of bitcoins circulating in the economy. Due to the interconnectedness of Bitcoin to the real economy, if there was wide adoption, financial stability and the effectiveness of central banks to perform their function could diminish.

As Bitcoin has global reach, the ECB also suggests that global monitoring and oversight is required.¹³⁹ The International Monetary Fund (IMF), as a global authority may have a role to play.¹⁴⁰ If Bitcoin

¹²⁸ Hayek's *Denationalisation of Money* argues that government monopoly of money must be abolished to stop recurring bouts of inflation and deflation. He argues that abolition is the cure for the more deep-seated disease of the recurring waves of depression and unemployment attributed to capitalism. See F. A. Hayek, *Denationalisation of Money – the Argument Refined* (The Institute of Economic Affairs), 3rd ed, 1990).

¹²⁹ European Central Bank, 'Virtual Currency Schemes', above n 2, 22.

¹³⁰ Yermack, 'Is Bitcoin a Real Currency? An economic appraisal', above n 82.

¹³¹ Ibid.

¹³² Ibid.

¹³³ European Central Bank, 'Virtual Currency Schemes', above n 2, 37-39.

¹³⁴ Ibid.

¹³⁵ Ibid.

¹³⁶ Ibid, 25.

¹³⁷ Barber, 'Bitter to Better – How to Make Bitcoin a Better Currency', above n 63.

¹³⁸ The United States of America central bank

¹³⁹ European Central Bank, 'Virtual Currency Schemes', above n 2.

¹⁴⁰ Plassaras, 'Regulating Digital Currencies', above n 15.

Best Practices for Bitcoin

becomes an important currency for international commerce it may pose a serious threat to economic stability in the foreign exchange markets. Under current regulations, if there was a speculative-attack¹⁴¹ on Bitcoin, it would be met with no recourse or defence, as it operates outside the domestic and global financial-system. One proposal would be to allow the IMF to obtain bitcoins to effectively-counter a speculative-attack.¹⁴² This emphasises the need to address this issue in the present, rather than in the future. Due to the appreciating value and finite supply of bitcoins, it would be more expensive for the IMF to acquire bitcoins for such a counter-attack later.¹⁴³ This proposal is one example that demonstrates the long-term consequences that Bitcoin and other virtual currencies may pose, and the risks that may arise to all stakeholders if regulatory action is delayed.

II. FEATURES

There are two key risks that arise from Bitcoin's features. These include Bitcoin's decentralisation and the anonymity that bitcoin transactions enable.

A. Anonymity

Bitcoin's anonymity presents a challenge to law-enforcement and a risk to legitimate users. Users can create and discard unlimited public keys,¹⁴⁴ can use bitcoin mixers for additional anonymity¹⁴⁵ and do not need to be physically present to receive money or register any identifying information to use Bitcoin. Authorities warn that these attributes make it attractive for Bitcoin to be used for criminal purposes.¹⁴⁶ The European Banking Authority (EBA) states that though 'bitcoin transactions are public, the owners and recipients are not'.¹⁴⁷ These transactions are largely untraceable and anonymous,¹⁴⁸ meaning criminals may be attracted to the system. The FBI warns that Bitcoin may attract transactions involving money-laundering, human trafficking, terrorist financing, illegal

¹⁴¹ A speculative attack occurs when an investor wishes to take advantage of a weak currency, a currency that has depreciated in value relative to other currencies. If left unchecked this successful attack can push a weak currency's value even lower, resulting in a destabilising of the international foreign exchange currency market. See Nicholas A. Plassaras, 'Regulating Digital Currencies: Bringing Bitcoin within the Reach of the IMF' (2013-2014) 14 *Chicago International Law* 377.

¹⁴² Plassaras, 'Regulating Digital Currencies', above n 15.

¹⁴³ Ibid, 381.

¹⁴⁴ David Vandervort, *Challenges and Opportunities associated with a bitcoin-based transaction rating systems*, Xerox <http://fc14.ifca.ai/bitcoin/papers/bitcoin14_submission_5.pdf>.

¹⁴⁵ Boehm, 'Bitcoin: a First Legal Analysis - with reference to German and US-American law', above n 80.

¹⁴⁶ Vietnam, Israel and the European Banking Authority. See Perkins Coie, *Virtual Currencies: International Actions and Regulations* (September, 2014), Perkins Coie <<http://www.perkinscoie.com/virtual-currencies-international-actions-and-regulations/>>.

¹⁴⁷ Dean Carroll, European Banking Authority to consider Bitcoin regulation (December 2013), Public Affairs Policy Review <<http://www.policyreview.eu/european-banking-authority-to-consider-bitcoin-regulation/>>.

¹⁴⁸ Ibid.

Best Practices for Bitcoin

gambling, child pornography and illicit drugs.¹⁴⁹ In October 2013, the FBI shut down Silk Road, a website that allowed people to buy drugs with bitcoins.¹⁵⁰ They also made an arrest and seized US\$13.5 million worth of bitcoin.¹⁵¹ Silk Road recorded US\$1 billion in transactions and accounted for 8% of all bitcoin transactions.¹⁵² The US Justice Department also arrested Charlie Shrem and Robert Faiella for operating BitInstant.com, a bitcoin-exchange that was used by the men to purchase large quantities of bitcoins to sell on Silk Road to users who wanted to buy drugs anonymously.¹⁵³ The men pleaded guilty to running an unlicensed money transmitting business.¹⁵⁴ These are examples of the criminal usage of Bitcoin and law-enforcement's reaction to it. Anonymity makes it difficult for law-enforcement to track and enforce laws against criminals using Bitcoin to conduct criminal activities. This also exposes legitimate users to risks of law-enforcement closing down platforms, making users unable to access their funds and users unknowingly transacting with criminals or holding bitcoins used in criminal activities.

Though Bitcoin's anonymity poses risks for legitimate users and law-enforcement, these risks do not justify its ban, as illegal market places will always emerge.¹⁵⁵ Bitcoin is not as anonymous as cash because all transactions are recorded and publically available. The issue is in attaching identities to public-keys, making Bitcoin pseudonymous rather than anonymous.¹⁵⁶ Bitcoin's anonymity is a 'relative metric that is assessed in comparison to the current technologies, methods of tracing Internet activity'¹⁵⁷ and regulations surrounding registration. The identities of users can be revealed with effort, using context discovery, flow analysis, common transactions in a circle of users and identifying information collected from exchanges.¹⁵⁸ Though identifying information cannot be collected from Bitcoin itself, regulators have focused on third-party bodies in the Bitcoin ecosystem, notably exchanges, to collect this information.¹⁵⁹ An example of how third-parties can be targeted is

¹⁴⁹ Ibid.

¹⁵⁰ Martinson, 'Bitcoin and the Secured Lender', above n 23.

¹⁵¹ Ibid.

¹⁵² Ibid.

¹⁵³ Juliana Kenny, 'Bitcoin regulation on the horizon', *Inside Counsel* (online), 4 February 2014

<<http://www.insidecounsel.com/2014/02/04/bitcoin-regulation-on-the-horizon>>.

¹⁵⁴ BBC News, 'Bitcoin trader admits unlicensed money transfers', *BBC News* (online), 4 September 2014

<<http://www.bbc.com/news/business-29072886>>.

¹⁵⁵ Ramasastry, 'Bitcoin: if you can't ban it, should you regulate it?', above n 48.

¹⁵⁶ Perianne Boring, 'Bitcoin Could Strengthen The World Economy If Washington Doesn't Destroy It', *Forbes* (online), 4 February 2014 <<http://www.forbes.com/sites/perianneboring/2014/04/02/bitcoin-could-strengthen-the-world-economy-if-washington-doesnt-destroy-it/>>.

¹⁵⁷ Elias, 'Bitcoin: Tempering the Digital Ring of Gyges', above n 20.

¹⁵⁸ Miller, *Bitcoin: A Currency Revolution*, above n 70. For more information on these techniques see Aaron Miller, *Bitcoin: A Currency Revolution* (22 September 2011), Academia.edu

<http://www.academia.edu/1024973/Bitcoin_A_Currency_Revolution>. How the exchanges will be targeted will be discussed in Chapter 7.

¹⁵⁹ This regulatory action will be discussed in more detail in Chapter 7.

Best Practices for Bitcoin

seen with Mt Gox when, in May 2013, it was charged in the US for operating as an unlicensed money transmitting business.¹⁶⁰ This charge led to Mt Gox complying with AML and 'know-your-customer' regulations, requiring verification on all accounts seeking deposit or withdrawal of currencies out of bitcoin. This meant that users would need to submit government-issued identifying-information to trade bitcoins for traditional-currencies.¹⁶¹ This severely limited the anonymity of Mt Gox users. Anonymity is not a 'prominent design goal of Bitcoin and can be overcome'.¹⁶²

B. Legal Uncertainties Caused by Decentralisation

Authorities cite Bitcoin's 'lack of a central-authority that administers and provides redress as a key risk'.¹⁶³ This lack of central-authority makes it impossible for Bitcoin to 'conduct due-diligence, monitor and report on suspicious activities, implement an AML program and accept or process legal requests like subpoenas'.¹⁶⁴ The US Justice Department was able to charge E-gold proprietors, a centralised virtual-currency, for violating money-laundering regulations and knowingly allowing a transaction to purchase child-pornography.¹⁶⁵ If Bitcoin is used for such transactions, regulators cannot directly target a central body. This makes it impossible to 'target a central location or company for investigative purposes or to shut down the system'.¹⁶⁶ Regulators' solution to this is to

¹⁶⁰ Kate L, *The Rise and Fall of Mt Gox, Everything You Need to Know*, above n 95.

¹⁶¹ Andy Greenberg, 'Not so Anonymous: Bitcoin Exchange Mt. Gox Tightens Identity Requirement', *Forbes* (online), 30 May 2013 <<http://www.forbes.com/sites/andygreenberg/2013/05/30/not-so-anonymous-bitcoin-exchange-mt-gox-tightens-identity-requirement/>>.

¹⁶² Fergal Reid, Martin Harrigan, 'An Analysis of Anonymity in the Bitcoin System' (Discussion Paper, Physics and Society, Cornell University Library, 7 May 2012). Some academics recommend blacklisting as the next step in policing the criminal element of Bitcoin. Blacklisting would involve writing-off bitcoins that have been used for criminal activities and would depend on the transaction history of that bitcoin. Though this would expose legitimate users to counter-party risk and take bitcoins out of circulation, it is the next step in reducing criminal-usage of Bitcoin and enabling it to be used by legitimate users safely and confidently. For more information on this technique see Malte Moser, Rainer Bohme and Dominic Breuker, 'Towards Risk Scoring of Bitcoin Transactions' (Discussion Paper, Department of Information System, University of Munster, Germany) <http://fc14.ifca.ai/bitcoin/papers/bitcoin14_submission_15.pdf>.

¹⁶³ Hungary, France, China and Brazil. Perkins Coie, *Virtual Currencies: International Actions and Regulations*, above n 21.

¹⁶⁴ Federal Bureau of Investigation - Intelligence Assessment, 'Bitcoin Virtual Currency: Unique Features Present Distinct Challenges for Deterring Illicit Activity' (Report, Federal Bureau of Investigation - Intelligence Assessment, 24 April 2012).

¹⁶⁵ The proprietors later plead guilty to money-laundering charges and allegations surrounding child pornography transactions were dropped. Cross, 'Internet currency firm pleads guilty to money laundering', above n 24 <<http://web.archive.org/web/20090414185759/http://www.thestandard.com/news/2008/07/22/internet-currency-firm-pleads-guilty-money-laundering>>.

¹⁶⁶ Federal Bureau of Investigation, 'Bitcoin virtual currency', above n 165.

Best Practices for Bitcoin

target third-party intermediaries such as Mt Gox to ensure compliance with relevant regulations.¹⁶⁷ Given Bitcoin's global reach, this may require international cooperation with different legal and regulatory regimes.

There are also legal uncertainties surrounding Bitcoin that make it risky to users. Users need to be aware that Bitcoin does not enjoy specific protections afforded other financial services and products, for example, there is no deposit-insurance to insure losses, exchanges may have varying responsibility disclaimers and that there is no central-body to seek recourse from.¹⁶⁸ The EBA warns that VCs are currently unregulated and users are unprotected.¹⁶⁹ Mt Gox's bankruptcy is an example of the vulnerability users face if recourse is not available. Mt Gox halted all transactions and withdrawals in January 2014, making it impossible for users to access or withdraw their funds. 650,000 bitcoins belonging to users were lost and Mt Gox subsequently declared bankruptcy, requesting liquidation in April 2014.¹⁷⁰ Salachii LLP, a London-based law firm, has filed a claim against the CEO, Mark Karpeles and other executives, representing 200 claimants from 15 countries for breaches of contract.¹⁷¹ Users were left with little recourse but to join a pool of unsecured creditors by pursuing an action in court.

Bitcoin's decentralisation presents a challenge to regulators in the absence of a central authority to target and exposing users to the risks of being limited to pursuing third party intermediaries.

III. SECURITY RISKS

Bitcoin itself is a secure system,¹⁷² protected by the vastness of its computer-powered network and financial incentive to dedicate power towards mining.¹⁷³ Nevertheless, the storage of bitcoins is not as secure. Bitcoins need to be stored in digital wallets on personal devices, on an online storage

¹⁶⁷ This will be discussed in more detail in 7.

¹⁶⁸ United States Government Accountability Office, 'Virtual Currencies: Emerging Regulatory, Law Information and Consumer Protection Challenges' (Report, Report to the Committee on Homeland Security and Governmental Affairs, U.S. Senate, U.S. Government Accountability Office, May 2014) <<http://www.gao.gov/assets/670/663678.pdf>>.

¹⁶⁹ Carroll, 'European Banking Authority to consider Bitcoin regulation', above n 148.

¹⁷⁰ Kate L, *The Rise and Fall of Mt Gox, Everything You Need to Know*, above n 95. Mt Gox then filed for bankruptcy protection in the US, temporarily halting legal action by users and creditors alleging the operation was fraudulent. Karpeles, the CEO of Mt Gox refused to appear for a deposition or heed a subpoena relating to this case.

¹⁷¹ A US judge has since allowed a preliminary approval for Mt Gox creditors to reach a settlement with two executives of the exchange. The plan would have Sunlot Holdings Ltd, an investment company, buy Mt Gox for 1 bitcoin, to resurrect the exchange and compensate shareholders. Previous users to Mt Gox would receive a 16.5% equity stake. 200,000 bitcoins and \$20 million held by the administrator would be divided amongst the users. See Shirley Siluk, *CoinLab sues Mt. Gox in US court* (3 May 2013), Coindesk <<http://www.coindesk.com/coinlab-sues-mt-gox-in-us-court/>>.

¹⁷² Turpin, 'Bitcoin: the Economic Case for a Global Virtual Currency', above n 72, 339-40.

¹⁷³ The mining process was explained in detail in Chapter 2.

Best Practices for Bitcoin

locker or in an exchange. There are three security risks associated with bitcoins: loss, theft and fraud. Firstly, if you lose your private key, there is no way to access your bitcoins, as there is no central authority to issue you with a new password.¹⁷⁴ Lost bitcoins become unrecoverable zombie coins.¹⁷⁵ Secondly, unless your bitcoins are adequately protected by anti-virus or back-up measures, or the server you have trusted in has anti-theft measures, your bitcoins can be stolen through hacking.¹⁷⁶ There are many examples of this occurring, including the Mt Gox hacking discussed above.¹⁷⁷ The need to carefully consider the trust placed in a third-party exchange is emphasised in the Bitcoinica example. Bitcoinica was an exchange run by Zhou Tang who claimed 60,000 bitcoins were stolen. Though he promised to repay half, people suspected he stole the funds. A lawsuit was filed against him for breach of contract and negligence. The case is pending.¹⁷⁸ These examples emphasise the need to be aware of potential security risks in holding bitcoins and trusting exchanges. The last security risk associated with transacting in bitcoins is the potential for fraud. Fraud can manifest in two ways. Firstly, individuals can trick victims into giving away their bitcoins without compensation.¹⁷⁹ As transactions are irreversible, there is no central authority to mediate and identifying information may be limited, leaving victims with little recourse to recover their funds. The second way people may become victims of fraud is to be enticed into a Ponzi-like investment scheme, promising high returns with limited understanding of the risks involved.¹⁸⁰ This occurred where Trendon Shavers was charged with running a Ponzi scheme through Bitcoin Savings and Trust.¹⁸¹ He promised investors up to 7% weekly-interest based on Bitcoin market arbitrage activity. However, he was actually using bitcoins from new investors to make purported interest payments and cover investor withdrawals on outstanding investments.¹⁸² The SEC stated that 'fraudsters are not beyond their reach' because they used virtual currencies to mislead investors and violate federal securities laws'.¹⁸³ This emphasises that in the case of investment fraud, protections

¹⁷⁴ Norton Rose Fulbright, 'Bitcoin and your business', above n 40.

¹⁷⁵ Zombie coins cannot be replaced and result in a further shrinkage in the money base. Tens of thousands of bitcoins have reportedly become zombies. See Simon Barber, Xavier Boyen, Elaine Shi et al, *Bitter to Better - How to Make Bitcoin a Better Currency*, Stanford.edu <http://crypto.stanford.edu/~xb/fc12/bitcoin.pdf>.

¹⁷⁶ Turpin, 'Bitcoin: the Economic Case for a Global Virtual Currency', above n 72.

¹⁷⁷ Another example occurred in November 2013 when 4000 digital wallets in a Czech exchange Bitcash.cz were hacked and bitcoins stolen. In the same month a bitcoin bank in Australia was hacked and 4000 bitcoins (worth AUD\$1 million) were stolen, most belonging to users. See Cameron Fuller, 'Bit Licenses: How Will New York Regulate Bitcoins?', *International Business Times* (online), 30 January 2014 <<http://www.ibtimes.com/bit-licenses-how-will-new-york-regulate-bitcoins-1552078>>.

¹⁷⁸ Turpin, 'Bitcoin: the Economic Case for a Global Virtual Currency', above n 72, 346.

¹⁷⁹ Ibid.

¹⁸⁰ Ibid, 356.

¹⁸¹ U.S. Securities and Exchange Commission, *SEC Charges Texas Man with Running Bitcoin-Denominated Ponzi Scheme* (23 July 2013), U.S. Securities and Exchange Commission <<http://www.sec.gov/News/PressRelease/Detail/PressRelease/1370539730583#.VCC5TEsk8dt>>.

¹⁸² Ibid.

¹⁸³ Ibid.

Best Practices for Bitcoin

through securities laws may exist.¹⁸⁴ However, for other security risks there is limited or no legal recourse to theft, fraud or loss. To mitigate exposure to such risks users can carefully choose the exchange they engage with, check whether there is a responsibility disclaimer for fraud and theft, purchase insurance, and exercise caution through threshold cryptography and super-wallets.¹⁸⁵

IV. CONCLUSION

Bitcoin users often do not understand how the system works. They are exposed to complex risks and are vulnerable due to legal uncertainties. Bitcoin is easily downloaded and used, and actions can be taken to mitigate these risks. These risks need to be understood by users if they are to use Bitcoin responsibly, and should be a consideration to regulators when formulating regulatory strategies.

¹⁸⁴ This will be discussed in more detail in Chapter 7.

¹⁸⁵ Threshold cryptography splits private keys onto multiple devices, requiring devices to operate together to spend bitcoins. Super-wallets could be spread across multiple devices using this technology and still be user-friendly by enabling a sub-wallet with a nominal amount to be attached to a user's smart-phone. Thus if the sub-wallet is hacked not all the bitcoins are lost and it is much more difficult for the super-wallet to be hacked. See Simon Barber, Xavier Boyen, Elaine Shi et al, *Bitter to Better - How to Make Bitcoin a Better Currency*, Stanford.edu <<http://crypto.stanford.edu/~xb/fc12/bitcoin.pdf>>.

CHAPTER 5

BITCOIN: CURRENT REGULATORY APPROACHES

There is no consensus about how Bitcoin is defined or how it should be treated. Three regulatory approaches have emerged in response to the increase in Bitcoin's popularity. The first approach is to ban or severely restrict the use of Bitcoin. The second approach is to do nothing, issue warnings and 'wait and see' what action other countries take. The third approach is to take action and regulate virtual currencies. Irrespective of the approach taken inside a jurisdiction, Bitcoin actors including intermediaries are still bound by general commercial, contractual and criminal laws.¹⁸⁶

I. BANNING BITCOINS APPROACH

Several countries have banned or severely restricted the use of Bitcoin. This has been done in two ways. Firstly, countries such as Iceland and Russia have banned the acceptance of bitcoins as a currency. For example the Icelandic Exchange Act prohibits entities from engaging in the exchange of virtual currencies.¹⁸⁷ Russia has stated that the 'official currency is the ruble, and introduction of all other monetary units and money substitutes are prohibited'.¹⁸⁸ This prohibition extends to bitcoins.¹⁸⁹ Bolivia has also explicitly banned bitcoins in this way.¹⁹⁰ Secondly, the governments of China and Columbia have prohibited banks and third-party payment providers from accepting, using or selling virtual currencies, ensuring that financial and payment institutions cannot be involved in Bitcoin-related transactions.¹⁹¹ Though the use of bitcoins by merchants and consumers is still legal, its use is severely restricted.¹⁹² China states that this approach 'avoids harm to the public' and protects the legal monetary status of their official currency, the renminbi (RMB), which may be affected by the excessive speculation in Bitcoin.¹⁹³

Banning or restricting the use of bitcoins is not an effective approach to prevent Bitcoin use, protect users or obtain benefits in the Bitcoin system.¹⁹⁴ The reason is that Bitcoin's global, online and anonymous features mean that the ban may be easily circumvented. For example, criminals may

¹⁸⁶ Bollen, 'The legal status of online currencies', above n 31, 280.

¹⁸⁷ Perkins Coie, *Virtual Currencies: International Actions and Regulations*, above n 21.

¹⁸⁸ Ramasastry, 'Bitcoin: if you can't ban it, should you regulate it?', above n 48.

¹⁸⁹ Ibid.

¹⁹⁰ Perkins Coie, *Virtual Currencies: International Actions and Regulations*, above n 21.

¹⁹¹ Ibid.

¹⁹² Bloomberg View, 'Time for Smarter Rules on Digital Money', *Bloomberg Businessweek* (online), 27 February 2014 <<http://www.businessweek.com/articles/2014-02-27/bitcoin-exchange-mt-dot-goxt-collapse-shows-need-for-regulation>>.

¹⁹³ Ramasastry, 'Bitcoin: if you can't ban it, should you regulate it?', above n 48.

¹⁹⁴ The benefits and potential uses for Bitcoin were discussed in Chapter 3.

Best Practices for Bitcoin

take advantage of Bitcoin's anonymity to exchange Bitcoin for a traditional currency internationally. The ban's effectiveness is also limited due to Bitcoin's online and decentralised nature, which means that locating and penalising criminal is different for regulators. Furthermore, if the ban is ineffective in limiting the use of Bitcoin, by extension users of Bitcoin will still be exposed to the outlined risks without any protection.¹⁹⁵ Conversely, if the ban is effective, this will have the effect that the outlined benefits in the Bitcoin system cannot be obtained. Thus a national ban on Bitcoin is undermined by Bitcoin's global presence and anonymity and may not be effective to achieve the desired result of protecting the currency and citizens of a country. Even if effective, the ban may also put at risk the potential benefits to Bitcoin.

II. WAIT-AND-SEE APPROACH

Most countries are in 'wait-and-see' mode when it comes to Bitcoin regulation as reflected the current environment surrounding Bitcoin.¹⁹⁶ Given Bitcoin's newness, this hesitancy stems from uncertainty as to what Bitcoin is, how it is used and the risks it poses. There is also a regulatory trend that technological advances generally precede regulatory updates by a number of years.¹⁹⁷ Despite this, most countries have adopted regulations on how to tax Bitcoin-transactions, although these are inconsistent. For example, Canada has determined Bitcoin is not to be a currency but instead treats transactions involving it as barter trade; conversely Sweden treats bitcoins as assets to which capital gains tax is applicable.¹⁹⁸ As most countries have moved to tax Bitcoin in some way, Bitcoin taxation is not an area that will be discussed in regards to best-practice recommendations.

A. Characteristics

The 'wait-and-see' approach includes three main characteristics, any or all which might be employed by a country. These include the issuing of warnings to investors and consumers, the freedom of individuals and companies to choose to transact in bitcoins and bear the associated legal uncertainties and the belief that the Bitcoin's self-regulation is sufficient protection for users.

Firstly, most countries have issued warnings to investors and consumers about Bitcoin's risks.¹⁹⁹ The Netherlands has released consumer warnings regarding the use of virtual currencies, warning that it

¹⁹⁵ These risks were discussed in detail in Chapter 4.

¹⁹⁶ Ramasastry, 'Bitcoin: if you can't ban it, should you regulate it?', above n 48.

¹⁹⁷ Boehm, 'Bitcoin: a First Legal Analysis - with reference to German and US-American law', above n 80.

¹⁹⁸ Perkins Coie, *Virtual Currencies: International Actions and Regulations*, above n 21.

¹⁹⁹ Marini, 'Regulation & Innovation: Public Authorities and the Development of Virtual Currencies', above n 83.

Best Practices for Bitcoin

is like the Tulip-mania bubble.²⁰⁰ The European Union has issued a warning against virtual currencies, citing its legal uncertainty and other outlined risks.²⁰¹ These consumer and investor warnings caution Bitcoin's use due to the risks discussed in Chapter 4.

The second characteristic of this approach may be summed up by the statement that 'investors who are prepared to accept risk should be allowed to do so' as suggested by Glenn Stevens, the RBA's Governor.²⁰² This approach provides users and Bitcoin actors with the most freedom, enabling them to take advantage of Bitcoin's benefits and uses.

The third characteristic of this approach is the argument that Bitcoin is self-regulating, and this self-regulation provides sufficient protection to Bitcoin users. The Bitcoin system is secure, requiring someone to harness more computing power than the rest of the network combined to undermine the system's integrity.²⁰³ This protects the integrity of the system, however as Chapter 4 demonstrated, Bitcoin's self-regulation cannot mitigate the risks associated with Bitcoin, such as volatility and security risks in storing bitcoins. This demonstrates that Bitcoin's self-regulation is insufficient to mitigate the outlined risks to Bitcoin users.

B. Forms

The 'wait-and-see' approach can take two forms. States can explicitly state they will not regulate, as Hong Kong as done, or countries may observe and consider the possibilities of regulating.²⁰⁴ Israel is waiting to see how other countries address Bitcoin before taking action.²⁰⁵ Australia recognises that virtual currencies pose regulatory questions²⁰⁶ and the EU has stated that it is 'imperative' to look at possible regulation for Bitcoin and currencies like it.²⁰⁷ It is this 'wait-and-see' approach, representing apprehension but acknowledgment that Bitcoin regulation may be needed that this thesis is aimed at addressing.

²⁰⁰ Norton Rose Fulbright, 'Bitcoin and your business', above n 40. Tulip mania was a period in the Dutch Golden Age when contract prices for bulbs for the recently introduced tulip reaches extraordinarily high levels and then suddenly collapsed, leaving many people holding worthless tulip bulbs.

²⁰¹ Ibid.

²⁰² Perkins Coie, *Virtual Currencies: International Actions and Regulations*, above n 21.

²⁰³ Jon Southurst, *Australian Lawyers, Bitcoin Groups Call for Clarity on Regulation* (18 July 2014), Coindesk <<http://www.coindesk.com/australian-lawyers-bitcoin-groups-call-clarity-regulation/>>.

²⁰⁴ The Economist China, 'Bitcoin in Hong Kong: Still Different, the rule of law continues to appeal', *The Economist* (online), 7 June 2014 <<http://www.economist.com/news/china/21603499-rule-law-continues-appeal-still-different>>.

²⁰⁵ Perkins Coie, *Virtual Currencies: International Actions and Regulations*, above n 21.

²⁰⁶ Ibid.

²⁰⁷ Huw Jones, *EU executive to look at regulating Bitcoin currency* (4 July 2014), Reuters <<http://uk.reuters.com/article/2014/07/04/uk-eu-bitcoin-barnier-idUKKBN0F916I20140704>>.

III. ACTION APPROACH

Bitcoin regulation is still in its early days, with only a few countries taking steps to regulate it.²⁰⁸ The United States, the Czech Republic, Singapore, Canada and Italy have all begun to tackle the anonymity and criminality risks associated with Bitcoin through anti-money laundering and reporting regulations.²⁰⁹ Though only a few countries have pursued this action, there is consistency in their approaches and this gives some insights into where governments are best equipped to cope with Bitcoin regulation and supervision. In the public law area of tax law and regulation, countries are able to adapt traditional definitions and laws to incorporate Bitcoin into existing frameworks.²¹⁰ The action will be discussed in more detail in the following chapters and will form part of the best practice recommendations.

It is important to note that Bitcoin actors, including intermediaries are still bound by general commercial, contractual and criminal laws. For example, money laundering through the Bitcoin system is still a crime even if it is harder to trace.²¹¹ The difficulty is the ability for law-enforcement to track and enforce criminal activities through the Bitcoin system. Furthermore, an agreement between two parties to conduct a transaction in bitcoins will still attract contractual rights and responsibilities. There is, however, difficulties in enforcing these rights and responsibility on a Bitcoin account holder.²¹² Thus, irrespective of the approach taken inside a jurisdiction, general commercial and criminal laws will apply.²¹³

²⁰⁸ Bollen, 'The legal status of online currencies', above n 31.

²⁰⁹ Perkins Coie, *Virtual Currencies: International Actions and Regulations*, above n 21.

²¹⁰ Boehm, 'Bitcoin: a First Legal Analysis - with reference to German and US-American law', above n 80.

²¹¹ Norton Rose Fulbright, 'Bitcoin and your business', above n 40.

²¹² The difficulties of enforcing contractual rights and responsibilities are discussed in Chapter 7.

²¹³ Bollen, 'The legal status of online currencies', above n 31, 280.

CHAPTER 6

BITCOIN: WHY SHOULD BITCOIN BE REGULATED?

There are two reasons why action must be taken to regulate Bitcoin. Firstly there are risks to current users that cannot be resolved without regulations. These risks could be mitigated by the application of existing regulations to Bitcoin. And secondly there is hesitancy towards wider Bitcoin adoption due to these perceived risks. Bitcoin regulation will encourage the wider adoption of Bitcoin, which is necessary for the associated benefits and uses of Bitcoin to be fully realised.

Firstly there are risks to current users that cannot be resolved without regulation. As stated above, banning Bitcoin may be ineffective, thereby leaving users exposed to the risks outlined in Chapter 4. Similarly if a country employs a 'wait and see' approach users will be exposed to these same risks. It has been demonstrated that there are some risks that cannot be mitigated by action taken by users alone. Bitcoin users need to accept and bear the risks of bitcoin use, but there still remains the potential exposure to economic loss and lack of understanding about these risks that emphasises the need to issue warnings to users at a minimum. Furthermore, there are risks that Bitcoin will be used in criminal activity and in financial products that would normally attract the attention of regulators to supervise and enforce existing laws. Existing regulations cannot be applied directly to Bitcoin; they are ill equipped to handle the decentralised and anonymous features of Bitcoin use. There are therefore risks to current users and law enforcement agencies that cannot be mitigated without regulatory action.

Secondly, there is hesitancy towards wider adoption of Bitcoin due to these perceived risks. In the present unregulated environment stakeholders use Bitcoin at their own risk. Investors and consumers are warned of the risks associated with Bitcoin but there is no action taken by regulators to resolve these risks. Many people may feel uncomfortable with being exposed to the risks associated with an unregulated Bitcoin system. This is reflected in the percentage of Bitcoin transactions that are speculative, rather than transactional in nature.²¹⁴ Therefore in order for Bitcoin to be widely utilised and its associated benefits and uses more fully realised, adequate regulation that reduces these risks and encourages wider adoption is necessary. Furthermore, if Bitcoin is widely adopted, there are associated long-term economic risks that regulators must consider, in turn providing another reason for regulatory action.²¹⁵

²¹⁴ Yermack, 'Is Bitcoin a Real Currency? An economic appraisal', above n 82.

²¹⁵ As discussed in Chapter 4.

Best Practices for Bitcoin

Thus, if Bitcoin remains unregulated it is likely that there will not be wider adoption of the system. But this leaves current and potential future users exposed to risks that only regulators can resolve. Regulatory action can reduce criminality and address volatility and security risks associated with Bitcoin, however existing regulations in these areas cannot be applied to Bitcoin. The reduction in risks and the incorporation of Bitcoin into existing regulations will lead to the legitimisation and wider acceptance and adoption of Bitcoin.²¹⁶ Thus, regulating Bitcoin will provide a reduction in the risks to current and future stakeholders and incorporate the Bitcoin ecosystem into current regulations, while encouraging wider adoption and realisation of the benefits of Bitcoin.

²¹⁶ Cox, 'Bitcoin's four steps to Wall Street acceptance', above n 104.

CHAPTER 7**BITCOIN: HOW SHOULD IT BE REGULATED?****BEST PRACTICES RECOMMENDATIONS**

This Chapter addresses the difficulties in regulating Bitcoin and proposes general and specific actions to be taken to regulate Bitcoin and other decentralised virtual currencies.

I. THE DIFFICULTIES IN REGULATING BITCOIN

There are three aspects of Bitcoin that make it difficult to regulate, Bitcoin's decentralised, global presence and its diverse current and potential uses.

Firstly, Bitcoin is a decentralised, distributed network that exists as a system solely on the Internet. There is no central company or location for regulators to target; this makes it difficult to regulate the Bitcoin system.²¹⁷

Secondly, Bitcoin can be accessed from anywhere in the world as long as a person has an Internet connection. This makes it relatively futile for single-countries to implement regulations as they will be ineffective unless similar regulations worldwide.²¹⁸ Bitcoin stakeholders, especially criminals, may use Bitcoin's easy access aspect to circumvent harsher regulations, resulting to regulatory arbitrage and forum shopping and undermining the effectiveness of single-country regulations.²¹⁹

Thirdly, Bitcoin has many current and potential uses. These uses vary greatly and have specific particular risks and concerns that regulators should consider. To create Bitcoin-specific regulation for one use or actor will stifle innovation or leave other Bitcoin uses unregulated.²²⁰ It would also be expensive and time-consuming process for regulators to create specific regulations for each Bitcoin player and potential use. Such regulations would be inflexible and expensive, undermining their effectiveness and demonstrating the difficulty of focusing on regulations that would specifically apply to Bitcoin, its ecosystem and uses.

²¹⁷ Steven Russolillo, 'Yellen on Bitcoin: Fed Doesn't Have Authority to Regulate It in Any Way', *The Wall Street Journal* (online), 27 February 2014 <<http://blogs.wsj.com/moneybeat/2014/02/27/yellen-on-bitcoin-fed-doesnt-have-authority-to-regulate-it-in-any-way/>>.

²¹⁸ Marini, 'Regulation & Innovation: Public Authorities and the Development of Virtual Currencies', above n 83.

²¹⁹ Elias, 'Bitcoin: Tempering the Digital Ring of Gyges', above n 20.

²²⁰ Southurst, 'Australian Lawyers, Bitcoin Groups Call for Clarity on Regulation', above n 204.

II. GENERAL REGULATIONS

To address the three difficulties outlined above, the following general features should be included in Bitcoin regulation.

A. Actors

The Bitcoin ecosystem is made up of various actors, specifically: miners, Bitcoin exchangers, those holding bitcoins and those engaging in commerce using bitcoins. As it is difficult for the Bitcoin system itself to be regulated, the players in the ecosystem can be targeted. Individuals holding bitcoins are the hardest to target, as it is unknown who owns bitcoins and how much they possess.²²¹ The easiest targets are Bitcoin exchanges, trading floors and other financial entities developing around Bitcoin that act as the link between Bitcoin and the broader economy.²²² As most users will need to purchase bitcoins through these exchanges, rather than mining or receiving bitcoins in exchange for goods, the exchanges also are an avenue to regulate a large proportion of Bitcoin users. Regulations introduced by the U.S have targeted Bitcoin exchanges such as Mt. Gox. These regulations have also targeted miners who exchange their mined bitcoins for traditional currencies, demonstrating that it is not who you are in the Bitcoin ecosystem, but what you do with bitcoins that will affect whether regulations touch you.²²³ Individuals, who hold, transact or mine bitcoins for their own use are specifically excluded from these regulations.²²⁴ Bitcoin exchanges and other players who enable transactions that interact with the real economy and are utilised by a large proportion of Bitcoin users, are the best and easiest targets for Bitcoin regulation and will be the focus of the best practice recommendations.

B. Global

The French Senate has acknowledged that it is 'relatively futile' to establish different national policies given Bitcoin's nature.²²⁵ National regulation of Bitcoin may be ineffective as stakeholders can 'forum-shop' for the best location to conduct their business, not bound by the geographical limitations of national governments.²²⁶ Where one country's regulations are harsh, a criminal for example may transact in bitcoins located in the U.S, but exchange their bitcoins for a traditional

²²¹ Elias, 'Bitcoin: Tempering the Digital Ring of Gyges', above n 20.

²²² Ibid.

²²³ Penrose, 'Banking on Bitcoin: Applying Anti-Money Laundering and Money Transmitter Laws', above n 14.

²²⁴ Ibid, 529.

²²⁵ Marini, 'Regulation & Innovation: Public Authorities and the Development of Virtual Currencies', above n 83.

²²⁶ Elias, 'Bitcoin: Tempering the Digital Ring of Gyges', above n 20.

Best Practices for Bitcoin

currency in a country with lighter or no regulations. This would circumvent the purpose of regulations and pose continued risks to stakeholders.²²⁷ Canada has attempted to address this difficulty by capturing foreign Bitcoin companies if they direct services at persons or entities in Canada.²²⁸ Yet these regulations still do not extend to transactions and stakeholders outside of Canada that have no connection with it, leaving other users exposed to the outlined risks and encouraging regulatory arbitrage to 'friendlier' countries. The French Senate recommends a regulatory framework be established at an international level.²²⁹ Bitcoin's growth and global reach demonstrates the international cooperation and consistency that is needed in Bitcoin regulation. The national sovereignty principle that lays at the heart of the international political system may make this difficult. Though international cooperation to regulate financial systems has occurred,²³⁰ adoption of such recommendations is generally dependent on individual countries incorporating them into their own legal systems. With this context in mind, the best practice recommendations will focus on adopting consistent regulations into national legal systems, in the understanding that consistent regulations will reduce the risk of regulatory arbitrage.

C. Neutral and flexible

Bitcoin has multiple potential uses, each of which is different. Bitcoin regulation must be neutral and flexible to adapt to future innovations and inventions in Bitcoin technology. Regulations must find the balance between protecting stakeholders and the economy, while not stifling innovation to ensure that the benefits and uses of Bitcoin can be realised. Bitcoin-specific regulation may not take into account the various uses to Bitcoin. It would be time-intensive for regulators to adopt regulations specific to each Bitcoin use. It will further be shown that existing regulations can be adapted to include Bitcoin. This demonstrates that regulation can be flexible, neutral, balanced and adaptable without requiring fundamental shifts in regulatory approaches to financial systems and currencies.

To address the difficulties Bitcoin presents to regulators, it has been established that regulators should seek international cooperation. Regulations should be consistent across borders, neutral and flexible, taking into account the diverse uses of Bitcoin. Furthermore, Bitcoin regulation should target the intermediaries and exchanges in Bitcoin's decentralised system. It will also be shown that

²²⁷ Ibid.

²²⁸ Former Writer, *O Canada! Regulating Bitcoin at the National Level* (23 June 2014), NEWSBTC <<http://newsbtc.com/2014/06/23/canada-regulation-at-national-level/>>.

²²⁹ Marini, 'Regulation & Innovation: Public Authorities and the Development of Virtual Currencies', above n 83.

²³⁰ The international cooperation that created the Basel III recommendations is an example of this.

Best Practices for Bitcoin

regulators do not need to fundamentally shift regulations to incorporate Bitcoin. Bitcoin-specific regulations are not necessary, as existing regulations can be adapted to include it.

III. SPECIFIC AREAS OF REGULATION

With these central features in mind, there are three specific areas of regulation that require consideration. These three areas include public law, civil law and consumer protections and the laws surrounding financial systems.

A. Public Law

It is in the area of public law²³¹ that countries have been able to cope with the emergence of Bitcoin.²³² This thesis does not focus upon taxation law. It concentrates on the actions of countries to regulate Bitcoin in relation to with anti-money laundering and reporting.

An immediate concern of regulators is the potential use of Bitcoin's anonymity by criminals to conduct untraceable transactions globally and with ease.²³³ Regulators have targeted Bitcoin exchanges to require identifying information from users to hold accounts and conduct transactions as a way to remove the anonymity from public-keys.²³⁴ This takes advantage of the public history of all bitcoin transactions to hold criminals accountable to the law and protect legitimate users. An example of this is the move by the U.S Treasury Department's Financial Crimes Enforcement Network (FinCEN) to require all VC firms to be regulated as money transmitters.²³⁵ This requires all bitcoin companies, excluding those who use bitcoin for personal use to do four things.²³⁶ Firstly, companies need to register with the government. Failure to register will make companies liable to operating as an unregistered money-transmitting business. Mt Gox was found to be in this situation, consequently having accounts frozen until they complied. Secondly, companies need to record and report transactions. This includes filing Currency Transaction Reports (CRTs) for each deposit, withdrawal and exchange of currency involved in a transaction with more than \$10,000. Companies also need to file Suspicious Activity Reports (SARs) for any questionable transactions relevant to the

²³¹ Public law refers to the established rules for the relationship between the government and its citizens. See Franziska Boehm and Paulina Pesch, 'Bitcoin: a First Legal Analysis - with reference to German and US-American law' (Discussion Paper, Institute for Information, Telecommunication and Media Law, Leonardo-Campus 9, Germany) < http://fc14.ifca.ai/bitcoin/papers/bitcoin14_submission_7.pdf>.

²³² Boehm, 'Bitcoin: a First Legal Analysis - with reference to German and US-American law', above n 80.

²³³ Bryan Cronan, 'How New York state wants to regulate', *Alaska Dispatch News* (online), 21 July 2014 <<http://www.adn.com/article/20140721/how-new-york-state-wants-regulate-bitcoin>>

²³⁴ Federal Bureau of Investigation, 'Bitcoin virtual currency', above n 165.

²³⁵ Penrose, 'Banking on Bitcoin: Applying Anti-Money Laundering and Money Transmitter Laws', above n 14.

²³⁶ Ibid. Companies are required to comply with the Bank Secrecy Act 1970 and the Title III of the USA Patriot Act 2001.

Best Practices for Bitcoin

possible violation of a law or regulation, irrelevant of the sum of money involved. CRTs and SARs allow law-enforcement to track suspicious and large sums of money potentially used for illegal purposes by identifying the source, volume and movement of currency.²³⁷ Thirdly, companies must implement anti-money laundering procedures, with individuals or businesses that knowingly process dirty money, make a profit from those transactions and do nothing to stop processing them, guilty of money laundering.²³⁸ Fourthly, companies must obtain identifying information about customers and properly identify the people conducting these transactions.²³⁹ Companies must comply with due diligence standards to verify customer identity, including documenting the customer's name, address, date of birth, passport number and whether they are on a terrorist list.²⁴⁰ Without such information companies cannot allow persons to open an account.

Mt Gox complied with these requirements by introducing three different account levels.²⁴¹ Level 0 required no verification but users could only transact in bitcoins. Level 1 required individuals to provide identifying information, including a government-issued photo ID and a less than 6-month-old proof of residence before allowing them to deposit or withdraw any real currency into their account. Level 2 was designed for day-traders, professionals and companies that needed higher withdrawal limits, requiring, in addition to the Level 1 identifying-information, notarised certificates of incorporation, valid copies of government-issued photo ID for shareholder entities with 10% or more voting rights and a copy of the company's constitution.²⁴²

The Mt Gox example demonstrates how these regulations can be complied with by an exchange. It also reveals how regulations can be enforced. These requirements ensure exchanges have personal information about their customers. This provides law-enforcement agencies with the ability to combine the history of transactions on the public-ledger with the identifying-information from exchanges if there is any suspicious activity, allowing them to identify users and follow transactions.²⁴³

These regulations will assist in removing the anonymity from Bitcoin, will hold criminals accountable to the law and will likely discourage the use of Bitcoin for criminal purposes. With the additional information these regulations require, exchanges and law-enforcement will be in a better position to

²³⁷ Ibid, 537.

²³⁸ Ibid.

²³⁹ Ibid, 538.

²⁴⁰ These are part of FinCEN's 'Know Your Customer' guidelines.

²⁴¹ Penrose, 'Banking on Bitcoin: Applying Anti-Money Laundering and Money Transmitter Laws', above n 14, 544.

²⁴² Ibid.

²⁴³ United States Government Accountability Office, 'Virtual Currencies: Emerging Regulatory, Law Information and Consumer Protection Challenges', above n 169.

Best Practices for Bitcoin

track the use of Bitcoin for criminal purposes, including; terrorist financing, illegal drugs, money-laundering, theft²⁴⁴ and fraud. Though a user does not need to register any identifying information to use or mine bitcoins, to covert bitcoins into another currency they will more than likely need to use an exchange. It is at this point that regulators can identify and target criminals.

Bitcoin regulation should require exchanges and other intermediaries in the Bitcoin ecosystem to collect identifying information about its customers, denying them the ability to open an account and convert currency without this information, report suspicious transactions and create an anti-money laundering program. The FinCEN regulations were adapted to Bitcoin, incorporating it into existing laws applicable to financial institutions and banks. Similar regulations have been adopted in other countries.²⁴⁵ It is recommended that all countries require Bitcoin exchanges and intermediaries in the Bitcoin ecosystem to comply with that country's relevant reporting and anti-money laundering regulations. To prevent regulatory arbitrage it is recommended that standards of reporting and customer identification be consistent across countries. Implementing this recommendation will address the key risk of anonymity and subsequent criminal usage of the Bitcoin system, and will not require fundamental shifts in a country's regulatory approach to anti-money laundering and reporting laws.

²⁴⁴ There remains an issue in the definition of virtual currencies such as Bitcoin in the criminal law. The Netherlands' Supreme Court has classified virtual goods as property and sentenced a teenager for stealing virtual money and virtual goods in an online fantasy role-playing game. However in German law the scope of the criminal law would need to be extended to cover the theft of bitcoins. Bitcoins and virtual currencies are increasingly popular and the economic meaning of theft of virtual currencies is identical to the theft of legal tender or a payment card, but the theft of virtual currency may be punishable as such. This legal uncertainty leaves users exposed to the risks of theft and fraud and encourages criminals to pursue such actions without fear of recourse. With the enhancement of identifying information from exchanges, law-enforcement agencies will be able to track and identify thieves and fraudsters, but they can only do this if the activity is a crime. This action is required to protect users and reduce the criminal activity associated with Bitcoin. See Franziska Boehm and Paulina Pesch, 'Bitcoin: a First Legal Analysis - with reference to German and US-American law' (Discussion Paper, Institute for Information, Telecommunication and Media Law, Leonardo-Campus 9, Germany).

²⁴⁵ Singapore, Canada and the Czech Republic have adopted variations of these regulations and the European Union has also expressed interest in regulations that target money laundering and terrorist financing activities.

B. Civil Law

Bitcoin is a form of intangible, transferable private property. A bitcoin is a valuable asset to their current owner and can be transferred to another person if they accept this form of payment. Therefore, bitcoins are the circulation of valuable rights, but do not amount to a right to cash, rather it is a right to be transferred a valuable asset irrevocably and immediately.²⁴⁶ The two issues in the civil law to consider in regulating Bitcoin are the consequences of irreversibility and the possibilities of consumer protection.

1. Irreversibility

A key feature of the Bitcoin system is that transactions are irreversible and there is no central authority to mediate between parties or reverse transactions.²⁴⁷ This exposes a user to counter-party risk if they are defrauded or have their bitcoins stolen, as there is no way to reverse a transfer of bitcoins without the permission of the owner of those bitcoins.²⁴⁸ This makes Bitcoin different to other payment systems and places the responsibility on users to protect their bitcoins and take the appropriate checks before they complete a transaction. It is unlikely they will be able to recover their bitcoins if they need to. General contract principles apply to transactions involving bitcoins, but there is no third party that can mediate disputes or enforce a court order for the return of bitcoins to the original owner.²⁴⁹ Bitcoins remain in control of the party holding the private key, making it difficult and expensive to execute a legal process to control and access these funds. There are a number of reasons why this would be difficult. Firstly, a party or court would need to identify who is holding the bitcoins. This may require access to identifying information that only exchanges possess, information that exchanges will not likely share without a court order. Secondly, a user can easily create other public keys and accounts to transfer these funds, making it even more difficult to trace.²⁵⁰ Thirdly, this user may be in a different country, with the transaction occurring over the Internet. This complicates the process of enforcement, by requiring conflict of law principles to be considered. Lastly, if the user can be identified and an order served against them, enforcement may be difficult because they will need to perform the return of funds or compensation for the equivalent amount of bitcoins they received. Only the owner of the private key only can perform this transfer. An enforcement order cannot be served against a third party. This poses a counter-party

²⁴⁶ Bollen, 'The legal status of online currencies', above n 31, 283.

²⁴⁷ Ibid.

²⁴⁸ Ibid.

²⁴⁹ Ibid.

²⁵⁰ When funds are transferred from one bitcoin account to another bitcoin account, it can become difficult to track these transfers.

Best Practices for Bitcoin

risk to consumers and merchants in transactions and severely limits the ability of Bitcoin to be used as credit or collateral.²⁵¹ This restricts the ability for Bitcoin to become a trusted, and user-friendly payment system. There are no clear regulations that can resolve this issue, so users must bear these risks themselves when holding and transacting in bitcoins.

2. Consumer Protection

Another risk to consumers is the lack of legal recourse and consistency amongst the exchanges that form a fundamental part of the Bitcoin ecosystem. Regulations that ensure exchanges comply with anti-money laundering and reporting requirements do not extend to the soundness and safety of these exchanges.²⁵² Mt Gox was registered under the FinCEN regulations and complied with all necessary conditions, yet it still went bankrupt and left users unable to recover their funds. It is not the responsibility of regulators to promise the safety of a user's funds,²⁵³ but nevertheless, users may entrust substantial funds to these exchanges and could lose it all. The level of protection afforded to consumers where there is such financial exposure is generally higher than the protection afforded in other circumstances.²⁵⁴ There are economic consequences to users losing substantial funds that warrant consideration of how consumer protection can be afforded to these users.

Regulatory action has not yet been considered in this area, with the only acknowledgement of these risks in the form of consumer warnings to users. The Japanese approach may provide a move towards consumer protection that does not impose burdens upon regulators. The Japan Authority of Digital Asset (JADA) is a bitcoin business-only body intended to establish standards and codes of conduct for its members.²⁵⁵ JADA has the backing of the Japanese government and will softly-monitor its members without requiring any legislative changes.²⁵⁶ JADA advises its members on best practices and is an attempt to prevent another Mt Gox-like bankruptcy from occurring.²⁵⁷ JADA is a

²⁵¹ Martinson, 'Bitcoin and the Secured Lender', above n 23.

²⁵² Sanat Vallikappen, 'Singapore to Regulate Bitcoin Operators for Laundering Risk', *Bloomberg* (online), 14 March 2014 <<http://www.bloomberg.com/news/2014-03-13/singapore-to-regulate-bitcoin-operators-for-money-laundering.html>>.

²⁵³ These exchanges are private companies that compete in a free economy and consumers can choose to interact with. It is not the responsibility of governments and regulators to ensure the soundness of an exchange or the safety of user's funds. Even the banks, which play an integral part of the economy have been criticised for being too big to fail.

²⁵⁴ These increased levels of protection are due to the risk of consumers and investors losing substantial funds, but also the potential systemic consequences of a financial institution, that is linked to the broader economy, failing.

²⁵⁵ Deepak Tiwar, *The Japan Authority of Digital Asset (JADA) to Establish Standards and Codes of Conduct* (11 July 2014), *Forex Minute* <<http://www.forexminute.com/bitcoin/the-japan-authority-of-digital-asset-jada-to-establish-standards-and-codes-of-conduct-38202>>.

²⁵⁶ *Ibid.*

²⁵⁷ *Ibid.*

Best Practices for Bitcoin

step in the right direction to establishing consistency with Bitcoin businesses, but it is limited by not possessing the capability to monitor all business or enforce regulation against them.²⁵⁸ It is noted however that regulators do not often possess the supervisory and enforcement powers to monitor all businesses either.²⁵⁹ A vehicle like JADA, which is a self-policing body of Bitcoin businesses, may secure consistent standards across domestic and potentially international Bitcoin businesses and protect users through the implementation of these standards. Just as there was a Mt Gox premium for its perceived secure and stable system, higher minimum standards will create an expectation on businesses and exchanges to act responsibly and reduce risks to users if they hope to attract customers and stay in business. These bodies could recommend best practices for anti-money laundering policies, the collection and retention of customer information, security protections and anti-fraud measures. All bitcoin businesses are vested in the wider acceptance and adoption of Bitcoin, and the encouragement of its use for legitimate means. Introducing a competitive incentive for Bitcoin exchanges to improve their standards will increase consumer protection and likely result in more people being prepared to accept the risks associated with bitcoin transacting, in turn creating a wider market for bitcoin services.

This approach may mitigate volatility and security risks by securing standards across Bitcoin businesses, including exchanges. However, unless these standards can be adopted and enforced on a global scale, there will still be Bitcoin businesses that operate outside of these standards. Though global implementation is the most desirable outcome, the ability to self-police Bitcoin businesses through a vehicle like JADA is an excellent starting point to introduce some checks and standards on Bitcoin businesses, even if not all businesses adhere to them. The competitive nature of the industry will attract users to the safest and most reliable exchanges, ensuring that to survive businesses will need to adapt and adopt higher standards. This recommendation utilises the existing players inside the Bitcoin ecosystem and maintains an open legal environment to mitigate the risks to users and encourage the wider adoption of Bitcoin, making it an integral part of the best practice recommendations.

C. Bitcoin as part of the financial system

Bitcoin has many potential uses, as a currency, payment system investment and in the creation financial products such as derivatives and bitcoin-denominated credit cards. Bitcoin's interaction with a country's financial systems and exposure to investors and consumers requires consideration into the regulations that may attach to Bitcoin and its products. The areas of financial and economic

²⁵⁸ Ibid.

²⁵⁹ Ibid.

Best Practices for Bitcoin

regulation to be considered are general financial services, specific regulations and currency regulations.

1. *General financial services*

Most countries have regimes to deal with broad consumer protection and market integrity issues in the financial services industry.²⁶⁰ These regimes generally regulate payment products and electronic money.²⁶¹ Financial products and services that attach to the Bitcoin system, such as a Bitcoin exchange, would be regulated financial services under the Australian *Corporations Act 2001* (Cth) or a country's relevant financial services regulations.²⁶² However the Bitcoin system itself cannot be regulated in this area. There are two key elements that prevent this.

Firstly there must be an issuer that can issue the financial service or product.²⁶³ Bitcoin does not have a central body that can be a counterparty to coins, who is obliged to honour them or perform obligations owed under them. Bitcoin cannot be regulated under general financial services regulation and does not need to issue a Product Disclosure statement to set out its features, risks, fees and charges.²⁶⁴ There is again no central authority to target for such requirements.

Secondly, most e-money regulations require certain features that Bitcoin lacks.²⁶⁵ For example, the EU Payment Services Directive 2000/12/EC determines that a product is e-money if it needs an electronic device, on which the value recorded was that originally issued in return for funds equal to or exceeding the stored value and must be accepted by issuers.²⁶⁶ Bitcoin has its own unit of account (it is not tied to a traditional currency) and so does not fulfil the criteria to be an e-money product under the EU directives. This leaves it unregulated by current e-money laws.

Therefore, due to Bitcoin's own unit of account and lack of central body as an issuer, the Bitcoin system will not be regulated under general financial services regulations. Players in the Bitcoin ecosystem such as exchanges and intermediaries will be regulated like other financial services firms,

²⁶⁰ An example of such a regime is the work carried out by the Australian Securities and Investment Commission (ASIC), that is responsible for monitoring and promoting market integrity and consumer protection in relation to the Australian financial system.

²⁶¹ Bollen, 'The legal status of online currencies', above n 31, 283-4.

²⁶² *Ibid*, 284.

²⁶³ *Ibid*.

²⁶⁴ *Ibid*.

²⁶⁵ *Ibid*, 286.

²⁶⁶ *Ibid*.

Best Practices for Bitcoin

being required to comply with licensing, anti-money laundering and reporting standards.²⁶⁷ But users and the system itself will remain unregulated.

2. *Specific Regulations*

The Bitcoin ecosystem consists of a vast array of players, and promises many different uses for the system as a currency, investment, payment system, and broader financial product. Bitcoin-based financial products can be regulated in the same way as other financial products of its type:

a. Banking regulations

The Bitcoin system does not accept deposits, make payments on behalf of clients or make loans to third parties, therefore it is not a deposit-taking institution that will attract banking regulations. Issuing or distributing Bitcoins is not sufficient to run a bank.²⁶⁸ However if a person were to take deposits or make loans that were denominated in bitcoins, such services would likely attract the interest of banking regulators.²⁶⁹ This approach ensures that regulations are adept to deal with the risks associated with banking activities and protect consumers, incorporating activities denominated in bitcoins into existing regulations.

b. Investments

Investments involving bitcoins may take two forms, investments purchased with bitcoins and investment in bitcoins.²⁷⁰

i. Investments purchased with bitcoins

In *Securities and Exchange Commission (SEC) v Shavers*,²⁷¹ the court questioned the subject matter jurisdiction of a possible Ponzi scheme where investments were purchased with bitcoins. Shavers argued that because the investments were purchased with bitcoins, financial product regulations were not applicable. The court needed to determine whether investing in bitcoins amounted to an investment of money, a necessary element for the product to be an investment contract. The court found that bitcoins can be used to purchase goods or services, or even to pay for individual living expenses, thus investors wishing to invest in the trust with bitcoins provided an investment of

²⁶⁷ Ibid.

²⁶⁸ Ibid, 287-90.

²⁶⁹ Ibid.

²⁷⁰ Elwell, 'Bitcoin: Questions, Answers and Analysis of Legal Issues', above n 122, 14.

²⁷¹ *Securities and Exchange Commission v Shavers*, No. 4:13-CV-416 E.D. Tex. Aug. 6, 2013.

Best Practices for Bitcoin

money.²⁷² Despite the controversial significance of a court recognising bitcoins as money, the outcome of this case was not controversial to the application of federal securities law.²⁷³ The result was that investments purchased with bitcoins were still investments that attracted the oversight of financial product regulations to protect investors.²⁷⁴

Investments should not be exempt from financial product regulation purely because they were purchased with bitcoins, they remain products that people have invested in and should attract the same protections as other investments. Investments purchased with bitcoins should be regulated like any other investment or financial product.

ii. Investments in bitcoins

Investments products that are denominated in bitcoins, such as the Winklevoss public exchange-traded fund, remain investments that should attract the attention of financial product regulators. There is nothing that differentiates them from other financial products except that they are based in bitcoins rather than US dollars or another traditional currency.²⁷⁵

The only example of where an investment in bitcoins will not attract the attention of regulators is if a person has bought a large amount of bitcoins and is holding them hoping that the value will appreciate. This is a decision that a person has made to buy a currency, and is not a financial product that one person has offered to another. A similar action, such as a person purchasing a large amount of US dollars were bought anticipating an appreciation in value, would also not attract regulator attention.

If an investment in bitcoins involves an investment or financial product that would otherwise attract the attention of regulators, it should be covered by financial product regulation.

c. Derivatives

As bitcoins act like a commodity, with sharp fluctuations in price and limited supply, it is likely that bitcoin-based derivative products will emerge.²⁷⁶ Just as an investment in bitcoins should attract the

²⁷² Rountree, 'Champing at the Bitcoin: Bitcoin, Regulators and the Law, above n 78, 6.

²⁷³ Elwell, 'Bitcoin: Questions, Answers and Analysis of Legal Issues', above n 122, 15.

²⁷⁴ Ibid.

²⁷⁵ Ibid.

²⁷⁶ Ibid, 16.

Best Practices for Bitcoin

relevant regulator's attention; Bitcoin-derivative products should be regulated as if they were any other derivative product.²⁷⁷

If a person uses Bitcoin for their own purposes, such as an investment to store wealth or transact, they do so at their own risk. However Bitcoin-denominated financial products and services are no different from other financial products and services. If bitcoins are used in a banking activity, as an investment or as part of a derivative it should be regulated by the relevant regulations for that activity. There is nothing in the characteristics of Bitcoin-denominated financial products that undermine the necessity to protect consumers and investors of such products, or prevents regulators from targeting the relevant issuer.²⁷⁸ Thus, specific regulation should attach to bitcoins depending upon their usage and not because they are bitcoin-based.

3. Currency

a. Medium of exchange

Legal tender is generally a government-issued currency that comes with the promise that it is a legitimate means of transacting business in that country.²⁷⁹ For example in Australia the AUD is legal tender for all debts, public and private. Bitcoins do not have the status of legal tender in any country and its acceptance as a payment of debt depends upon the agreement between the parties to transact this way.²⁸⁰ Bitcoins are not banned by currency legislation in any country, and people are free to transact in them, but there is no right for bitcoin to be accepted as a means of payment. Users buy and transact in bitcoins at their own risk, and these activities do not attract the attention of regulations and as already outlined.²⁸¹ As discussed, there are also limitations to the enforcement of such transactions through the application of the general law.

b. Global currency regulation

If Bitcoin gains wide adoption and international use, there is a threat of a speculative attack on the currency that could destabilise the foreign currency exchange markets.²⁸² The IMF can restrict the flow of a currency it deems scarce and apportion its allocation accordingly. This makes it the body best equipped to deal with speculative attacks on traditional and virtual currencies. It is recommended that the IMF Articles of Agreement be changed to enable the IMF to utilise these

²⁷⁷ Ibid.

²⁷⁸ Ibid.

²⁷⁹ Bollen, 'The legal status of online currencies', above n 31, 291.

²⁸⁰ Ibid.

²⁸¹ Ibid, 290-92.

²⁸² This threat was discussed in more detail in Chapter 4.

Best Practices for Bitcoin

methods to deal with a speculative attack on bitcoins in the future.²⁸³ Nicholas Plassaras recommends that the Articles could be altered in two ways, by granting the IMF indirect control over Bitcoin through expanding the interpretation of 'separate currencies' in Article IV Section 5 or by providing the IMF direct control over Bitcoin by granting it quasi-membership status.²⁸⁴ It is beyond the scope of this thesis to consider the practicalities of these alterations; Plassaras' article gives further details on this.²⁸⁵ It is recommended that if Bitcoin is widely adopted and Bitcoin becomes an integral part of international trade and commerce, a shift to incorporate it into the influence of the IMF is necessary. This will equip the IMF with the ability to deal with speculative attacks on the currency and mitigate the risks to broader economic and financial instability.

IV. CONCLUSION

Bitcoin is difficult to regulate, however this chapter demonstrates that it is possible. To overcome Bitcoin's decentralisation regulations should target Bitcoin exchanges and other intermediaries that provide the link between Bitcoin and the real. These exchanges are run by central authorities and can be the target of regulatory enforcement. Bitcoin has many current and potential uses that must be considered by regulators. To address this issue it is recommended that regulators look to the use of Bitcoin or a Bitcoin-based product to consider specific regulations. This will ensure the effectiveness of existing regulations is not undermined by the existence of unregulated Bitcoin-based products and ensures regulations have taken into account the risks and specific concerns of that use. Lastly, to circumvent regulatory arbitrage and the undermining of a single country's regulatory efforts it is recommended as a desirable outcome that regulations, though focusing on action at a national level, be consistently adopted as standards worldwide.

Regulations are targeted at ensuring that existing regulations and laws are not undermined by the existence of the Bitcoin system. It therefore focuses upon incorporating Bitcoin and its uses into existing regulatory regimes. This demonstrates an incorporation of technological advances into existing public law and financial regulations. Measures discussed to extend regulations to consumer protection are less defined. There are potential risks to Bitcoin users that they personally must take responsibility for. Regulators in this area should focus on alerting users to these potential risks. They should also encourage the creation of JADA-like vehicles to competitively improve the standards of Bitcoin exchanges.

²⁸³ Plassaras, 'Regulating Digital Currencies', above n 15.

²⁸⁴ Ibid, 400-5.

²⁸⁵ See Nicholas A. Plassaras, 'Regulating Digital Currencies: Bringing Bitcoin within the Reach of the IMF' (2013-2014) 14 *Chicago International Law* 377.

CHAPTER 8

CONCLUSION

Bitcoin has various current and potential uses. The Bitcoin system is fundamentally a payment system that can be used to conduct transactions internationally and a currency that can be used as the basis for financial products and services. These diverse uses demonstrate the need to be technology-neutral in approaching regulatory action for Bitcoin. An unregulated Bitcoin system would present a risk to the effectiveness of existing regulations, particularly as it can be used as a mechanism for illegal means. This thesis made best practice recommendations to all countries on how to regulate the decentralised, convertible virtual currency. Countries that are in 'wait and see' mode should take note of these recommendations and act quickly to bridge the gap between existing regulations and developing technologies to prevent circumvention of regulations. Countries should also issue warnings to all current and prospective Bitcoin users of the legal and economic uncertainties surrounding Bitcoin. Consumer protection action can be extended to encourage higher standards of responsibility, safety and soundness in Bitcoin exchanges.

It is unknown whether Bitcoin will prevail in the long-term. However, given the emergence of VCs that have improved on the Bitcoin system and the growing acceptance of Bitcoin, it is likely that virtual currencies are here to stay. The more Bitcoin is widely adopted and incorporated as a currency and financial product into the broader economy, the less controversial it will become. It is important that governments continue to adapt their technical capacity to trace, monitor and regulate VCs as people take advantage of the technological innovations and opportunities that VCs provide.

BIBLIOGRAPHY

A. Articles/Reports

i. Articles

Bollen, Rhys, 'Best practice in the regulation of non-cash payment services' (2011) 22 *Journal of Banking and Finance Law and Practice* 147.

Bollen, Rhys, 'The legal status of online currencies: are Bitcoins the future?' (December 2013), 24(4) *Journal of Banking and Finance Law and Practice* 272.

Grinberg, Reuben, 'Bitcoin: An Innovative Alternative Digital Currency' (2011) 4 *Hastings Science & Technology Law Journal* 160.

Little, Emily M., 'Bitcoin' (2014) 21(5) *The Investment Lawyer* 22

Penrose, Kelsey L., 'Banking on Bitcoin: Applying Anti-Money Laundering and Money Transmitter Laws' (2014), 18 *North Carolina Banking Institute* 529.

Plassaras, Nicholas A., 'Regulating Digital Currencies: Bringing Bitcoin within the Reach of the IMF' (2013-2014) 14 *Chicago International Law* 377.

Rountree, David, 'Champing at the Bitcoin: Bitcoin, Regulators and the Law (October 2013) 32 *Communications Law Bulletin* 5.

Turpin, Jonathan B., 'Bitcoin: the Economic Case for a Global Virtual Currency Operating in an Unexplored Legal Framework' (2014) 21 *Indiana Global Legal Studies* 335.

Tyree, Alan L. and John Sheehan SC, 'Banking law and banking practice: Bitcoin' (2012) 23 *Journal of Banking and Finance Law and Practice* 139.

Vandezande, Niels, 'Between Bitcoins and mobile payments: will the European Commission's new proposal provide more legal certainty?' (2014) 22 *International Journal and Law and Information Technology* 295.

Yermack, David, 'Bitcoin Economics: the digital cash lacks most of the features economists value in a currency' (2014) 117 *Technology Review* 12.

ii. Working Papers

Babaioff, Moshe, Shahar Dobzinski, Sigal Oren et al, 'On Bitcoin and Red Ballons' (Conference report, ACM Conference on Electronic Commerce, June 2012)
<<http://research.microsoft.com/apps/pubs/default.aspx?id=156072>>

Boehm, Franziska and Paulina Pesch, 'Bitcoin: a First Legal Analysis - with reference to German and US-American law' (Discussion Paper, Institute for Information, Telecommunication and Media Law, Leonardo-Campus 9, Germany) < http://fc14.ifca.ai/bitcoin/papers/bitcoin14_submission_7.pdf>

Best Practices for Bitcoin

Elwell, Craig K., M. Maureen Murphy and Michael V. Zeitzinger, 'Bitcoin: Questions, Answers and Analysis of Legal Issues' (Congressional Report, Congressional Research Service, 15 July 2014)
<<http://fas.org/sgp/crs/misc/R43339.pdf>>

European Central Bank, 'Virtual Currency Schemes' (Report, European Central Bank, October 2012)
<<http://www.ecb.europa.eu/pub/pdf/other/virtualcurrencyschemes201210en.pdf>>

Federal Bureau of Investigation - Intelligence Assessment, 'Bitcoin Virtual Currency: Unique Features Present Distinct Challenges for Deterring Illicit Activity' (Report, Federal Bureau of Investigation - Intelligence Assessment, 24 April 2012).

Global Legal Research Directorate Staff, 'Regulation of Bitcoin in Selected Jurisdictions' (Report, The Law Library of Congress, Global Legal Research Center, January 2014)
<<http://www.loc.gov/law/help/bitcoin-survey/regulation-of-bitcoin.pdf>>

Marini, Phillipe, 'Regulation & Innovation: Public Authorities and the Development of Virtual Currencies' (Report, Committee on Finance of the French Senate, 4 August 2014)
<<http://www.senat.fr/rap/r13-767/r13-767-syn-en.pdf>>

Martinson, Pamela J. and Christopher P. Masterson, 'Bitcoin and the Secured Lender' (Report, Banking and Financial Services Policy Report, June 2014, 33.6)
<<http://search.proquest.com.ezproxy.lib.monash.edu.au/docview/1540934291/abstract?accountid=12528>>

Moser, Malte, Rainer Bohme and Dominic Breuker, 'Towards Risk Scoring of Bitcoin Transactions' (Discussion Paper, Department of Information System, University of Munster, Germany)
<http://fc14.ifca.ai/bitcoin/papers/bitcoin14_submission_15.pdf>

Reid, Fergal, Martin Harrigan, 'An Analysis of Anonymity in the Bitcoin System' (Discussion Paper, Physics and Society, Cornell University Library, 7 May 2012)

United States Government Accountability Office, 'Virtual Currencies: Emerging Regulatory, Law Information and Consumer Protection Challenges' (Report, Report to the Committee on Homeland Security and Governmental Affairs, U.S. Senate, U.S. Government Accountability Office, May 2014)
<<http://www.gao.gov/assets/670/663678.pdf>>

United States Securities and Exchange Commission, 'Investor Alert: Bitcoin and other Virtual Currency-Related Investments' (Investor Alert, Securities and Exchange Commission, 7 May 2014)
<http://www.sec.gov/oiea/investor-alerts-bulletins/investoralertsia_bitcoin.html#.VCCwmksk8dt>

United States Securities and Exchange Commission, 'Investor Alert: Ponzi Schemes Using Virtual Currencies' (Investor Alert, No. 153, SEC, Office of Investor Education and Advocacy)
<http://www.sec.gov/investor/alerts/ia_virtualcurrencies.pdf>

Yermack, David, 'Is Bitcoin a Real Currency? An economic appraisal' (Working Paper, No. 19747, NBER Working Papers, 2013) <<http://online.wsj.com/public/resources/documents/NBER.pdf>>

Best Practices for Bitcoin

iii. Newspaper reports

AAP, 'Singapore to regulate Bitcoin exchanges', *SBS News* (online), 14 March 2014
<<http://www.sbs.com.au/news/article/2014/03/14/singapore-regulate-bitcoin-exchanges>>

Ando, Ritsuko, 'Japan Says it Won't be Regulating Bitcoin Any Time Soon', *Business Insider* (online), 19 June 2014 <<http://www.businessinsider.com.au/r-japans-ruling-party-says-wont-regulate-bitcoin-for-now-2014-19>>

BBC News, 'Bitcoin trader admits unlicensed money transfers', *BBC News* (online), 4 September 2014
<<http://www.bbc.com/news/business-29072886>>

BBC News, 'New Paypal partnership enables limited Bitcoin payments', *BBC News* (online), (24 September 2014 <<http://www.bbc.com/news/technology-29341886>>

Berson, Susan A., 'Some basic rules for using "bitcoin" as virtual money' (2013) *American Bar Association Journal*
<http://www.abajournal.com/magazine/article/some_basic_rules_for_using_bitcoin_as_virtual_money/>

Bloomberg View, 'Time for Smarter Rules on Digital Money', *Bloomberg Businessweek* (online), 27 February 2014 <<http://www.businessweek.com/articles/2014-02-27/bitcoin-exchange-mt-dot-gox-collapse-shows-need-for-regulation>>

Boring, Perianne, 'Bitcoin Could Strengthen The World Economy If Washington Doesn't Destroy It', *Forbes* (online), 4 February 2014
<<http://www.forbes.com/sites/perianneboring/2014/04/02/bitcoin-could-strengthen-the-world-economy-if-washington-doesnt-destroy-it/>>

Carson, Ed, 'China Bans Bitcoin Trades by Banks, not Individuals', *Investor's Business Daily* (online), 5 December 2013
<<http://search.proquest.com.ezproxy.lib.monash.edu.au/docview/1465065754?accountid=12528>>

Cox, Jeff, 'Bitcoin's four steps to Wall Street acceptance', *CNBC* (online), 8 January 2014
<<http://www.cnn.com/id/101320507>>

Cronan, Bryan, 'How New York state wants to regulate', *Alaska Dispatch News* (online), 21 July 2014
<<http://www.adn.com/article/20140721/how-new-york-state-wants-regulate-bitcoin>>

Cross, Grant, 'Internet currency firm pleads guilty to money laundering', *The Industry Standard* (online), 22 July 2008
<<http://web.archive.org/web/20090414185759/http://www.thestandard.com/news/2008/07/22/internet-currency-firm-pleads-guilty-money-laundering>>

The Economist China, 'Bitcoin in Hong Kong: Still Different, the rule of law continues to appeal', *The Economist* (online), 7 June 2014 <<http://www.economist.com/news/china/21603499-rule-law-continues-appeal-still-different>>

Best Practices for Bitcoin

Eha, Brian Patrick, 'At Regulatory Hearing, Prosecutors Admit Bitcoin Is a Technological Breakthrough', *Entrepreneur* (online), 30 January 2014
<<http://www.entrepreneur.com/article/231167>>

Eha, Brian Patrick, 'How the World's Richest Nation's Are Regulating Bitcoin', *Entrepreneur* (online), 6 February 2014 <http://www.entrepreneur.com/article/231167>>

Eha, Brian Patrick, 'More Major Retails Are Getting Ready to Accept Bitcoin', *Entrepreneur* (online), 29 January 2014, <<http://www.entrepreneur.com/article/231134>>

Eha, Brian Patrick, 'SecondMarket CEO: Wall Street Will Put "Hundreds of Millions" Into Bitcoin', *Entrepreneur* (online), 11 December 2013 <http://www.entrepreneur.com/article/230346>>

Eha, Brian Patrick, 'SecondMarket Establishes New Bitcoin Trust for Accredited Investors', *Entrepreneur* (online), 26 September 2013 <<http://www.entrepreneur.com/article/228597>>

Eha, Brian Patrick, 'Why Regulate Bitcoin', *The New Yorker* (online), 18 November 2013
<http://www.newyorker.com/business/currency/why-regulate-bitcoin>>

Former Writer, *O Canada! Regulating Bitcoin at the National Level* (23 June 2014), NEWSBTC
<<http://newsbtc.com/2014/06/23/canada-regulation-at-national-level/>>

Fuller, Cameron, 'Bit Licenses: How Will New York Regulate Bitcoins?', *International Business Times* (online), 30 January 2014 <<http://www.ibtimes.com/bit-licenses-how-will-new-york-regulate-bitcoins-1552078>>

Greenemeier, Larry, 'What Is Bitcoin and Its Current Crisis', *Scientific American* (online), 25 February 2014 <<http://www.scientificamerican.com/article/what-is-bitcoin-and-its-current-crisis/>>

Goncalves, Juan, 'Though unconventional, Bitcoin still a viable currency', *The Georgetown Voice* (online), 5 December 2013 <<http://georgetownvoice.com/2013/12/05/though-unconventional-bitcoin-still-viable-currency/>>

Henning, Peter J., 'More Bitcoin Regulation Is Inevitable', *The New York Times* (online), 3 February 2014 <http://dealbook.nytimes.com/2014/02/03/more-bitcoin-regulation-is-inevitable/?_php=true&_type=blogs&_php=true&_type=blogs&_r=1>

Hill, Kashmir, 'Bitcoin's Legality around the world' *Forbes* (online), 31 January 2014, *Forbes*
<http://www.forbes.com/sites/kashmirhill/2014/01/31/bitcoins-legality-around-the-world/>>

Kenny, Juliana, 'Bitcoin gains legal, financial interest', *Inside Counsel* (online), 30 January 2014
<<http://www.insidecounsel.com/2014/01/30/bitcoin-gains-legal-financial-interest>>

Kenny, Juliana, 'Bitcoin regulation on the horizon', *Inside Counsel* (online), 4 February 2014
<http://www.insidecounsel.com/2014/02/04/bitcoin-regulation-on-the-horizon>>

Kinsella, Stephen, 'Once bitten twice shy, so stay away from Ponzi-like Bitcoins', *Independent.ie* (online), 19 November 2013 <<http://www.independent.ie/opinion/columnists/stephen-kinsella/stephen-kinsella-once-bitten-twice-shy-so-stay-away-from-ponzilike-bitcoins-29764982.html>>

Best Practices for Bitcoin

Pagliery, Jose, 'JP Morgan patents Bitcoin-like payment system', *CNN Money* (online), 11 December 2013 <<http://money.cnn.com/2013/12/10/technology/bitcoin-jpmorgan/index.html?iid=EL>>

Perez, Evan, 'Holder: Bitcoin raises law enforcement concerns', *CNN Money* (online), 8 April 2014 <<http://money.cnn.com/2014/04/08/technology/bitcoin-holder/>>

Petroff, Alanna, 'EU regulator warns on dangers of Bitcoin', *CNN Money* (online), 13 December 2013 <<http://money.cnn.com/2013/12/13/technology/bitcoin-europe-regulation/>>

Potts, David, 'Bit by bit, bitcoin is gaining currency', *The Age* (online), 1 October 2014 <<http://www.theage.com.au/money/bit-by-bit-bitcoin-is-gaining-currency-20140924-10jfmb.html>>

Reason.com, 'The Future of Bitcoin', *Reason.com* (online), June 2014 <<http://reason.com/archives/2014/06/01/the-future-of-bitcoin>>

Russolillo, Steven, 'Yellen on Bitcoin: Fed Doesn't Have Authority to Regulate It in Any Way', *The Wall Street Journal* (online), 27 February 2014 <<http://blogs.wsj.com/moneybeat/2014/02/27/yellen-on-bitcoin-fed-doesnt-have-authority-to-regulate-it-in-any-way/>>

Simonite, Tom, 'Academic Spy Weaknesses in Bitcoin's Foundations', *MIT Technology Review* (online), 24 March 2014 <<http://www.technologyreview.com/news/525676/academics-spy-weaknesses-in-bitcoins-foundations/>>

Stripe, Malleya, 'Regulating Down Under: Australian Taxation Office Preparing Bitcoin Guidelines', *Cointelegraph* (online), 30 April 2014 <http://cointelegraph.com/news/111328/regulating_down_under_australian_taxation_office_preparing_bitcoin_guidelines>

Toren, Matthew, 'Bitcoin: The Good, the Bad and the Ugly', *Entrepreneur* (online), 16 December 2013 <<http://www.entrepreneur.com/article/230354>>

Vallikappen, Sanat, 'Singapore to Regulate Bitcoin Operators for Laundering Risk', *Bloomberg* (online), 14 March 2014 <<http://www.bloomberg.com/news/2014-03-13/singapore-to-regulate-bitcoin-operators-for-money-laundering.html>>

Weisenthal, Joe, 'China May Be Preparing Harsh New Regulations on Bitcoin', *Business Insider Australia* (online), 2 April 2014 <<http://www.businessinsider.com.au/chinese-bitcoin-regulations-2014-4>>

B. Cases

Securities and Exchange Commission v Shavers, No. 4:13-CV-416 E.D. Tex. Aug. 6, 2013

C. Other

Aguiler, M., *Bitcoin and other virtual currencies finally get some regulation* (22 March 2013), Gizmodo <<http://gizmodo.com/5991951/bitcoin-and-other-virtual-currencies-finally-get-some-regulation>>

Best Practices for Bitcoin

Baijal, Shwetika, *What is Bitcoin? Regulating Bitcoin Legitimizes it as a New Currency* (17 May 2013), Policy.Mic <<http://mic.com/articles/42707/what-is-bitcoin-regulating-bitcoin-legitimizes-it-as-a-new-currency>>

Barber, Simon, Xavier Boyen, Elaine Shi et al, *Bitter to Better - How to Make Bitcoin a Better Currency*, Stanford.edu <<http://crypto.stanford.edu/~xb/fc12/bitcoin.pdf>>

Blockchain, *Market Price (USD)* (20 September 2014), Blockchain.info <https://blockchain.info/charts/market-price?timespan=all&showDataPoints=false&daysAverageString=1&show_header=true&scale=0&address=>

Carroll, Dean, European Banking Authority to consider Bitcoin regulation (December 2013), Public Affairs Policy Review <<http://www.policyreview.eu/european-banking-authority-to-consider-bitcoin-regulation/>>

Compare Bitcoin Exchanges, *Buying \$100 Worth of Bitcoin - Last 12 hours* (20 September 2014), Compare Bitcoins Australia <<http://comparebitcoins.net>>

Durden, Tyler, *JPMorgan's "Bitcoin Alternative" Patent Rejected (175 times)* (15 December 2013), Zerohedge <<http://www.zerohedge.com/news/2013-12-15/jpmorgans-bitcoin-alternative-patent-rejected-175-times>>

E-Gold Ltd, *E-Gold Ltd and Gold & Silver Reserve (G&SR) Inc. bankruptcy announcement* (7 July 2008), Tools <<http://tools.rosinstrument.com/pb/m/12508.htm>>

Elias, Matthew, *Bitcoin: Tempering the Digital Ring of Gyges or Implausible Pecuniary Privacy* (3 October 2011), Social Science Research Network <http://papers.ssrn.com/sol3/papers.cfm?abstract_id=1937769>

Financial Action Task Force, *FAFT report: virtual currencies- key definitions and potential AML/CFT Risks* (June 2014), FAFT <<http://www.fatf-gafi.org/media/fatf/documents/reports/Virtual-currency-key-definitions-and-potential-aml-cft-risks.pdf>>

Greenberg, Andy, 'Not so Anonymous: Bitcoin Exchange Mt. Gox Tightens Identity Requirement', *Forbes* (online), 30 May 2013 <<http://www.forbes.com/sites/andygreenberg/2013/05/30/not-so-anonymous-bitcoin-exchange-mt-gox-tightens-identity-requirement/>>

Jones, Huw, *EU executive to look at regulating Bitcoin currency* (4 July 2014), Reuters <<http://uk.reuters.com/article/2014/07/04/uk-eu-bitcoin-barnier-idUKKBN0F916I20140704>>

L, Kate, *The Rise and Fall of Mt Gox, Everything You Need to Know* (25 March 2014), CoinReport <<https://coinreport.net/editorial-rise-fall-mtgox/>>

Le Conte, Marie, *France Inches Closer to Bitcoin Regulation* (4 August 2014), Coindesk <<http://www.coindesk.com/france-inches-closer-bitcoin-regulation/>>

M, Sid, *Mt Gox Creditors Given the Preliminary Ok to Revive the Fallen Exchange* (9 May 2014), CoinReport <<https://coinreport.net/mtgox-creditors-ok-revive-exchange/>>

Best Practices for Bitcoin

Mann, Jasmine and Tola Lawal, *Regulating Bitcoin* (June 2011), Stanford

<<http://cs.stanford.edu/people/eroberts/cs181/projects/2010-11/Bitcoins/regulating-bitcoin.html>>

Matonis, Jon, *Market-Based Reactions to New Bitcoin Regulation* (23 February 2014), Coindesk

<<http://www.coindesk.com/market-based-reactions-new-bitcoin-regulation/>>

McCullough Robertson Lawyers, *Can a self managed super fund invest in bitcoins?* (15 July 2014),

McCullough Robertson Lawyers <http://www.mccullough.com.au/publications/f/View/Finance=-Can_a_self_managed_super_fund_invest_in_bitcoins/>

Miller, Aaron, *Bitcoin: A Currency Revolution* (22 September 2011), Academia.edu

<http://www.academia.edu/1024973/Bitcoin_A_Currency_Revolution>

Nakamoto, Satoshi, *Bitcoin: a Peer-to-Peer Electronic Cash system* (2009), Bitcoin.org

<<https://bitcoin.org/bitcoin.pdf>>

Norton Rose Fulbright, *Bitcoin and your business* (July 2014), Norton Rose Fulbright

<<http://www.nortonrosefulbright.com/knowledge/publications/119023/bitcoin-and-your-business-what-you-need-to-know>>

Perkins Coie, *Virtual Currencies: International Actions and Regulations* (September, 2014), Perkins

Coie <<http://www.perkinscoie.com/virtual-currencies-international-actions-and-regulations/>>

Ramasastri, Anita, *Bitcoin: If you Can't Ban It, Should you Regulate it? The Merits of Legalization* (25

February 2014), Verdict <<http://verdict.justia.com/2014/02/25/bitcoin-cant-ban-regulate>>

Raton, Boca, *U.S. swaps watchdog says considering bitcoin regulation* (11 March 2014), Reuters

<<http://www.reuters.com/article/2014/03/11/us-bitcoin-regulation-idUSBREA2A1W020140311>>

Roberts, Jeff John, *Feds seized \$2.9M in Bitcoin funds from Mt. Gox, court docs show* (19 August

2013), Gigaom <<https://gigaom.com/2013/08/19/feds-seized-2-9m-in-bitcoin-funds-from-mt-gox-court-docs-show/>>

Sharif Sakr, *Bitcoin bank entices mom and pop with insurance, fraud checks and no fees* (16 May

2014), Engadget <<http://www.engadget.com/2014/05/16/circle-bitcoin-bank/>>

Siluk, Shirley, *CoinLab sues Mt. Gox in US court* (3 May 2013), Coindesk

<<http://www.coindesk.com/coinlab-sues-mt-gox-in-us-court/>>

Southurst, Jon, *Australian Lawyers, Bitcoin Groups Call for Clarity on Regulation* (18 July 2014),

Coindesk <<http://www.coindesk.com/australian-lawyers-bitcoin-groups-call-clarity-regulation/>>

Southurst, Jon, *Peter Thiel: Bitcoin Payment System Badly Lacking* (12 September 2014), Coindesk

<<http://www.coindesk.com/peter-thiel-bitcoin-payment-system-badly-lacking/>>

Think Tanks, *IEA - Bitcoin will open the floodgates to a tidal wave of private money* (18 June 2014),

Wiredgov <[http://www.wired-](http://www.wired-gov.net/wg/news.nsf/articles/IEA+Bitcoin+will+open+the+floodgates+to+a+tidal+wave+of+private+money+18062014095000?open)

[gov.net/wg/news.nsf/articles/IEA+Bitcoin+will+open+the+floodgates+to+a+tidal+wave+of+private+money+18062014095000?open](http://www.wired-gov.net/wg/news.nsf/articles/IEA+Bitcoin+will+open+the+floodgates+to+a+tidal+wave+of+private+money+18062014095000?open)>

Best Practices for Bitcoin

Tiwar, Deepak, *The Japan Authority of Digital Asset (JADA) to Establish Standards and Codes of Conduct* (11 July 2014), Forex Minute <<http://www.forexminute.com/bitcoin/the-japan-authority-of-digital-asset-jada-to-establish-standards-and-codes-of-conduct-38202>>

United States Securities and Exchange Commission, *SEC Charges Texas Man with Running Bitcoin-Denominated Ponzi Scheme* (23 July 2013), U.S. Securities and Exchange Commission <<http://www.sec.gov/News/PressRelease/Detail/PressRelease/1370539730583#.VCC5TEsk8dt>>

Vaishampayan, Saumya, *Five virtual currencies other than bitcoin* (18 November 2013), MarketWatch <<http://www.marketwatch.com/story/five-virtual-currencies-other-than-bitcoin-2013-11-18>>

Vandervort, David, *Challenges and Opportunities associated with a bitcoin-based transaction rating systems*, Xerox <http://fc14.ifca.ai/bitcoin/papers/bitcoin14_submission_5.pdf>