world trade institute

MILE 14 Thesis | Fall 2014

The Nature of Decentralized Virtual Currencies: Benefits, Risks and Regulations.

Paul du Plessis

Supervisor: Prof. Dr. Kern Alexander

DECLARATION

This master thesis has been written in partial fulfilment of the Master of International Law and Economics Programme at the World Trade Institute. The ideas and opinions expressed in this paper are made independently, represent my own views and are based on my own research. I confirm that this work is my own and has not been submitted for academic credit in any other subject or course. I have acknowledged all material and sources used in this paper. I understand that my thesis may be made available in the World Trade Institute library.

ABSTRACT

Virtual currency schemes have proliferated in recent years and have become a focal point of media and regulators. The objective of this paper is to provide a description of the technical nature of Bitcoin and the reason for its existence. With an understanding of the basic workings of this new payment system, we can draw comparisons to fiat currency, analyze the associated risks and benefits, and effectively discusses the current regulatory framework.

TABLE OF CONTENTS

Page

1. Introduction

Virtual currency schemes have proliferated in recent years and have become a focal point of media and regulators. Virtual currencies are defined by the European Banking Authority as a digital representation of value that is neither issued by a central bank or public authority nor necessarily attached to fiat currencies, but is used as a means of exchange and can be transferred, stored or traded electronically. [1]

This paper focuses on Bitcoin, the first decentralized variation of virtual currency. In 2008 the Bitcoin white paper was published online by Satoshi Nakamoto, a pseudonymous person or likely a group people. The paper, "Bitcoin: A Peer-to-Peer Electronic Cash System" proposes a "purely peer-to-peer version of electronic cash would allow online payments to be sent directly from one party to another without going through a financial institution [..] a system for electronic transactions without relying on trust.[2] The open source Bitcoin software was released in January 2009, with an establishment of an exchange rate only on October 5, 2009 where 1 USD = 1,309 BTC. This initial value was calculated as the electricity exerted per bitcoin generated.[3] Since then, the system has grown to into a currency that is used for 60 – 80 thousand transactions per day, has a market capitalization of 5 billion USD, and trades 1 BTC = 380 USD.[4] Regardless of the extreme volatility in the exchange rate, an increasing number of suppliers are now accepting Bitcoin as a means of payment for a myriad of goods and services. Adopters include large multinationals companies such as eBay Inc's PayPal service, Dell Inc. (multinational technology corporation), DISH Network (pay-TV provider), CheapAir (airline) and Expedia Inc. (online travel agency, hotel bookings).[5]

The objective of this paper is to provide a description of the technical nature of Bitcoin and the reason for its existence. With an understanding of the basic workings of this new payment

---

[1] European Central Bank, 'EBA Opinion on 'virtual currencies', *EBA/Op/2014/08*. 2014.

[2] Nakamoto, S. 'Bitcoin: A Peer-to-Peer Electronic Cash system.', 2008, (accessed 30 September 2014), https://bitcoin.org/bitcoin.pdf

[3] 'New Liberty Standard', (accessed 10 October 2014), http://newlibertystandard.wikifoundry.com/page/2009+Exchange+Rate

[4] It must be noted that 1 BTC is arbitrarily divisible by up to 10^8. Thus, every bitcoin represents 100 million "satoshis"

[5] Morphy, E. 'Bitcoin? Yawn. CheapAir Is Now Taking Litecoin and Dogecoin.', *Forbes*, 2014, (accessed 30 September 2014), http://www.forbes.com/sites/erikamorphy/2014/09/03/bitcoin-yawn-cheapair-is-now-taking-litecoin-and-dogecoin/

'What can you buy with Bitcoins?', *Coindesk*, 2014, (accessed 29 September 2014), http://www.coindesk.com/information/what-can-you-buy-with-bitcoins/

system, we can draw comparisons to fiat currency, analyze the associated risks and benefits, and effectively discusses the current regulatory framework.

The second chapter introduces money theory. To understand Bitcoin, we require a basic understanding of the origin of money and role states and financial institutions play in the acceptance of money. It is accepted that the core objective of central banks is securing the stability of the national economy (price stability), and thus the stable value of a currency through maintaining public trust in the currency.[6] The bitcoin protocol autonomously determines how new bitcoins are created and the total possible number of bitcoins is fixed. This precludes the possibility of state intervention its supply and thus, questions the role of the state.

The third chapter describes and technical and economic nature of Bitcoin, drawing a comparison between its key properties to fiat currency systems. This chapter will provide a translation of the technical aspects of Bitcoin system which must be understood before its regulation can discussed.

The fourth chapter describes the potential economic and conceptual benefits of decentralized virtual currencies, followed by chapter five which will identify risks arising from the use of virtual currencies. Risks will be categorized according to the bearer of the risk (users, non-user market participants, financial integrity, etc.).[7]

Chapter six will discuss the regulation of virtual currencies. The regulatory vacuum Bitcoin once existed in is swiftly getting filled with varying sentiment, while most countries adopt a *permissive* stance, others outright ban it. Regulation is required to safeguard parties within the virtual currency ecosystem from various risks that accompanies its use. Decentralized virtual currencies face particularly challenging law enforcement predicaments because of their ability to disregard national borders while having no "owner" that controls the system, thus systems like Bitcoin, cannot be tied to any single jurisdiction.

Chapter seven concludes by mentioning noteworthy future applications of distributed ledger technology, and argues that the inventions underlying Bitcoin may change the world for the better.

---

[6] Committee on Payment and Settlement Systems, 'The role of central bank money in payment systems', *Bank for International Settlements*, 2003.

[7] European Central Bank, 'EBA Opinion on 'virtual currencies', *EBA/Op/2014/08*, 2014.

2. The evolution of money

2.1 Defining money

Money is a surprisingly elusive concept. Bamford(2011) stated that as with most attempts to define intellectual constructs, definitions of money describe what it does and some characteristics it has, instead of aiming to describe the thing itself.[8] In human societies throughout history, money has served as commodities or tokens that have value and is used as a medium of exchange.[9] Money's source of value stems from society's general agreement of what is seen acceptable tender in making payments and settling debt, rather than physical characteristics of the chosen media used.[10]

Classical economists agree that money mainly serves three functions within an economy. Firstly as a 'medium of exchange': An item that facilitates the exchange, something buyers give to sellers as payment for goods or services. Secondly as a 'unit of account': a benchmark used by people to measure and record economic numerically. Thirdly as a 'store of value': an item used to transfer purchasing power from the present into the future.[11]

Money that performs the abovementioned functions effectively usually has fairly uniform qualities. Jevons(1875) identifies properties such as: portability, must be convenient to store and transport; indestructability, must not deteriorate over time; homogeneity, units must be fungible; divisibility; and cognoscibility, units must be easily recognizable and secured from any counterfeiting.[12]

2.2 The Origin of Money

Money, as social institution, is used in almost every human society to facilitate trade. Trading allows standards of living that would not be possible if individuals were expected to independently produce every single commodity that they require. Before the existence of money, all exchanges had to take place through barter. Barter trade is typically a bilateral

---

[8] Bamford, C, *Principles of International Financial Law*, Oxford: Oxford University Press, 2011, pp. 10.

[9] Eatwell, J., Milgate, M., & Newman, P. (1994). *The new Palgrave dictionary of economics*, London:Macmillan, 2008, pp. 725.

[10] *Ibid.*

[11] Mankiw, N. G. & Taylor, P.M., *Economics. 2nd ed*. Andover : South-Western Cengage Learning, 2011, pp. 618.

[12] Jevons, W. S. 'Money and the Mechanism of Exchange'. *Library of Economics and Liberty.* 1876. (accessed 28 October 2014). http://www.econlib.org/library/YPDBooks/Jevons/jvnMME5.html

exercise, requiring that parties to the trade have a *double coincidence of wants*.[13] This means the chicken farmer can *only* acquire milk, if the cattle farmer wants eggs. This problem is theoretically solvable through multilateral barter (A supplies B, B supplies C and C supplies A), but as these trades could not practically all happen at a single point in time, this system would still require a central clearing house to keep track of balances of traders. In a multilateral barter system, traders would not be required to be balanced with every other trader, but due to the absence of money, each trader would have to be balanced in every commodity. Each trader would have to keep a portfolio of numerous goods which must not only be taken to each trading session, but must also be constantly synchronized by the clearing house.[14] This system would be clumsy, inefficient and extraordinarily complex.

Now we can consider how money acts as a lubrication to barter. By using money, traders are able to transfer purchasing power from one transaction to the next, overcoming the absence of *a double coincidence of wants* without a complex multilateral barter system. Traders have a reduced need for information and co-ordination and trades are subject to lower transaction costs. Buyers only need to know that sellers will accept money as payment. Money enables simpler pricing of goods, by allowing traders to assign a numerical value to each commodity in the common medium of exchange (as opposed to the value of each good being expressed in terms of a variety of other goods).[15]

Once in place, the benefits of a monetary trading system are apparent, but a paradox remains- the paradox of monetary trade. How do economies gravitate towards such a system? A system where a seller in a transaction gives up something desirable (goods or services) for something without immediate use (money), trusting the idea that a future sellers will do the same.[16] Starr(2003) summarizes the paradox:

> Inconvenience of barter is the reason why monetization of trade is efficient but it does not explain why monetary trade is a market equilibrium, the self-confirming behavior of rational self-interested economic buyers and sellers. No agent can choose individually to monetize; monetization is the common outcome of the equilibrium of the trading process. Monetary trade requires voluntary co-ordination among

[13] Jevons, W. S. 'Money and the Mechanism of Exchange'. *Library of Economics and Liberty.* 1876. (accessed 28 October 2014). http://www.econlib.org/library/YPDBooks/Jevons/jvnMME5.html

[14] Eatwell, J., Milgate, M., & Newman, P.,*The new Palgrave dictionary of economics*, London:Macmillan, 2008, pp. 725.

[15] *Ibid.*

[16] Starr, R. M, 'Why is there money? Endogenous derivation of "money" as the most liquid asset: A class of examples.', *Economic Theory, 21(2/3)*, 2003, pp. 455-474.

> households and firms. All must undertake to trade in the common medium. But it is by no means obvious that households and firms will voluntarily choose to trade in the commonly accepted money. [..] How can this arrangement be voluntarily sustained? [17]

There are two broad explanations for this paradoxical equilibrium- the Metallist(M) theory and the Chartalists(C) theory. These two views on the origin of money have been greatly debated in academia, and referred to as "the two concepts of money".[18]

2.3 The Two Concepts of Money

First the *Metallist* view, where a monetary trading system is the natural equilibrium resulting from the actions of self-interested parties in a free market barter economy, an endogenous process driven by the private sector with the purpose of minimizing the transaction costs related to trade.[19] Metallists focus on the medium of exchange function of money.[20]

The second theory is the *Chartelist* view, which argues that the state implements a monetary system as a means to facilitating the fiscal basis of government, money.[21] Chartalists recognize the power of the state to mandate that certain payments be made to it combined with the ability to determine the medium in which these payments must be made. The C theory provides a non-market-based theory where the currency is valued (and thus used) according to its usefulness in settling liabilities towards the state. Chartalists focus on the unit of account function of money. The state is the central force in the development of a monetary system, and the actual properties determining efficiency as a medium of exchange is irrelevant.[22]

M theory advocates most often quote the work of 19th century Austrian economist Carl Menger, which Starr(2001) refers to as a theory of market liquidity that forms the basis of

---

[17] Starr, R. M., 'Money: in transactions and finance'. *Dept. of Economics, University of California, San Diego*, pp. 13-15.

[18] Goodhart, C. A. E., 'The two concepts of money: Implications for the analysis of optimal currency areas.' *European journal of political economy, 14*(3). 1998., pp. 407-432.

[19] *Ibid.*

[20] Bell, S., 'The Hierarchy of Money'.*TheJerome Levy Economics Institute. Working paper No. 231.* 1998.

[21] Goodhart, C. A. E., 'The two concepts of money: Implications for the analysis of optimal currency areas.' *European journal of political economy, 14*(3), 1998, pp. 407-432.

[22] Bell, S. 'The Hierarchy of Money', *The Jerome Levy Economics Institute. Working paper No. 231,* 1998.

monetary theory. [23] Menger's theory stems from the concept that commodities in a barter economy have varying degrees of *saleableness* (meaning marketability or liquidity): "A commodity is more or less saleable according as we are able, with more or less prospect of success, to dispose of it at prices corresponding to the general economic situation, at economic prices."[24] Menger argues that since individuals within a barter economy recognize that certain commodities are relatively easier to trade compared to others, traders would acquire quantities of these commodities exceeding personal demand in order to better their chances of finding a suitable trading partner. These individuals' actions would have a network effect (increasing demand for the good results in further increasing demand) and further increase the *saleableness* of these commodities, further lowering the associated transaction costs. This process results in the most *saleable* commodity becoming accepted as a universal medium of exchange- the commodity with certain favorable characteristics, evolving into money.[25] Surda(2014) states:

> The core prerequisite for the classification as a medium of exchange is, for a casual observer maybe somewhat paradoxically, not the double coincidence of wants between the buyer and the seller with respect to the medium of exchange. Rather, it is the willingness of the buyer to hold it prior to the act of trading as a part of his liquidity portfolio.

The M perspective of the origin of money provides an explanation the process of how new commodities become a viable alternative medium of exchange. In a competitive environment that constantly strives towards lowering transaction costs, traders would naturally prefer a means of exchange which performs the functions of money more efficiently.[26]

While Menger attributes the origin of money to market forces, Menger recognizes the importance of the state in the historical development of money.[27] In Menger's monetary theory, state institutions aid the market with informational difficulties associated of using precious metals as money. Using precious metals in a raw form is inefficient as individuals are required to determine the true value of each unit they encounter. Through minting the raw

---

[23] Starr, R. M., 'Why Is There Money? Endogenous Derivation of "money" As the Most Liquid Asset: A Class of Examples.' *Economic Theory* 21.2/3. 2003, pp. 455-474.

[24] Menger, C., 'On the Origins of Money'. *Economic Journal, Vol 2*, 1892, pp. 239-255.

[25] *Ibid.*

[26] Olafsonn, I. A., 'Is Bitcoin Money?: An analysis from the Austrian school of economic thought'. *Haskoli Islands University*, 2014. pp 30.

[27] Ikeda, Y., 'Carl Menger's Monetary Theory: A Revisionist View'. *Keio University, Department of Economics*, 2008. pp 5.

materials into coins, traders are able to use trust the quality guarantee stamp of the mint, overcoming this informational difficulty.[28] Once the technology is available, the private sector is technically capable of minting yet the task is mostly a state-run operation.[29] The state plays this role for two reasons. Firstly, as public protector of law and order by means of force, the state is able to ensure the protection of the mint's inventory from theft. Secondly, in order to maintain trust in the quality of coins, the state ensures the value over time. A private mint operator "is bound to claim that the quality will be maintained forever, but in practice will always be tempted to debase the currency in pursuit of a quick and immediately larger return."[30] The state guaranteed the physical integrity of coins, solving the informational difficulties (lowering transaction costs) faced by individuals to trusting their real value.

Modern states guarantee the value of their own paper fiat money by declaring it as *legal tender* of the geographical area. Users are able to trust the government will accept fiat money as the only legal means of discharging financial obligations towards the state such as taxes or penalties. As long as tax obligations persist, the private sector will necessarily prefer fiat currency as payment in transactions.[31] Under the M approach, this property is seen an element to be considered by individuals choosing a preferred means of exchange. However, the combination of the state's ability to control the supply of fiat currency, and the power to impose taxes payable that fiat currency changes the role of the state in the equilibrium.

Here lies the core difference of the C perspective. The C theory views money as a *creature of the state* and views the state as the source of fiat money having value (rather than a contribution to its value), its value being primarily determined by its usefulness in extinguishing tax and other liabilities to the state.[32] Goodhart (1998) states:

> "[the] issue between the M and C theorists is how much of the subsequent acceptance of fiat money is due to the power of government, e.g., to impose taxes (C theory)., or to network factors and inertia encouraging people, without prompting from government, to stay with the existing currency (M theory) [..] Quite a number of economists combine the belief that M-form cost-minimization search theory

[28] Goodhart, C. A. E., 'The two concepts of money: Implications for the analysis of optimal currency areas', *European journal of political economy*, *14*(3), 1998, pp. 417-420.

[29] *Ibid:* In those cases where the mint has been run by the private sector, the government has in most cases both set the standards of fineness and extracted a rent, or seigniorage tax, that collected most of the available profits.

[30] Goodhart, C. A. E., 'The two concepts of money: Implications for the analysis of optimal currency areas', *European journal of political economy*, *14*(3), 1998, pp. 417-420.

[31] Bell, S. 'The Hierarchy of Money'.*TheJerome Levy Economics Institute. Working paper No. 231*. 1998.

[32] *Ibid.*

> explained the initial development of money, but that more recently, the State has clearly taken over the provision of fiat currency. So, whether, or not, they like the result, they accept that the C-form theory is at present, more realistic.[33]

Money is no longer something that exists independent of the state; it is now a pillar of the sovereign.[34] Modern C theorist Minksy (1986) views money as a ledger or two-sided balance sheet, where the creation of money is contingent to the acceptance of another's debt.[35] Bell states that only the C theory views the "creation of money as a two-sided balance sheet operation where the acceptance of another's debt is possible.[36] When a state declares that all payments to it must be made in a certain means of payment, it creates a potential debtor. The debtors demand for this specific money implies the creation of money and gives rise to a creditor.[37] The initial way to inject its fiat currency is through government spending. Therefore the C approach argues that the functions of money as a means of payment and media of exchange are a derived from the principle function as a unit of account in which state obligations must be paid.[38]

Both theories recognize the possibility of several types of money co-existing in a market. Under the M theory commodities are *all* seen as potential forms of money, each with varying degrees of liquidity. C theorists have noted the existence of a 'hierarchy of money' or a 'debt pyramid', where state issued currency ranks highest since as their imposed "liabilities reign supreme as the only promises in the hierarchy which cannot be refused."[39] As a technological innovation allows the introduction of virtual currency schemes, a new stateless variation of potential money enters the market, bringing new benefits and risks to the table.

2.4 What are Virtual currencies?

Virtual currency schemes have proliferated in recent years and have become a focal point of media and regulators. Virtual currencies are defined by as a digital representation of value that is neither issued by a central bank or public authority nor necessarily attached to fiat currencies, but is used as a means of exchange and can be transferred, stored or traded

---

[33] Goodhart, C. A. E., 'The two concepts of money: Implications for the analysis of optimal currency areas', *European journal of political economy*, *14*(3), 1998, pp. 417.

[34] *Ibid.*

[35] Bell, S. 'The Hierarchy of Money'.*TheJerome Levy Economics Institute. Working paper No. 231*. 1998.

[36] *Ibid.*

[37] *Ibid.*

[38] Semenova, A. 'The Origin of Money: Enhancing the Chartalist Perspective'. *CFEPS*. 2007.

[39] Bell (1998) summarizes the views of (Minsky, 1986; Foley, 1987; Wray, 1990)

electronically. In contrast to fiat currencies, virtual currencies are not legal tender but are nevertheless accepted by members within a virtual community as a medium of exchange and as a unit of account. Virtual currencies must also be distinguished from electronic money such as PayPal or Ven. In electronic money schemes the link between the electronic money and fiat currency is guaranteed through some legal foundation and funds are shown in the same unit of account (U.S. dollar, Euro, etc.).[40] Virtual currency schemes create an independent unit of account, which only exists in a digital form (Bitcoin, Litecoin, Ripple, etc.), which can be used as an alternative to fiat currency, or may be converted to fiat currency.[41]

In a broad sense there are two types of virtual currency schemes- centralized and decentralized. Centralized virtual currencies predate decentralized variations. Centralized virtual currencies have a centralized repository and is typically issued and controlled by a single organization. Decentralized virtual currencies have no central repository and are issued and operated in a decentralized manner. [42]

Centralized virtual currencies can be divided into three categories. Firstly, closed virtual currency schemes that are not convertible to fiat currencies (Frequent flyer miles, loyalty points and currencies typically used in online games such as World of Warcraft) and cannot be used for purchases outside the virtual community within which it exists. Secondly, unidirectional convertible virtual currencies (Linden Dollars or the Facebook credits) that are purchased at a fixed exchange rate (but cannot be converted back into fiat currency) and is typically used for the purchase of virtual goods or services. Thirdly, bidirectional convertible virtual currencies (Liberty Dollar, WebMoney, etc.) that allow buying and selling virtual currency according to the exchange rates with fiat currency. Bidirectional virtual currencies act similar to any other convertible currency and allows for the purchase of both virtual and real goods and services.[43]

The focus of this paper is on the decentralized variation of virtual currencies, the first variation of which emerged in 2009: Bitcoin. Through the innovative use of various

---

[40] European Central Bank,.'Virtual Currency Schemes', 2012, pp 11-14. (accessed 10 Ocotber 2014), http://www.ecb.europa.eu/pub/pdf/other/virtualcurrencyschemes201210en.pdf

[41] European Central Bank,.'Virtual Currency Schemes', 2012, pp 11-14. (accessed 10 Ocotber 2014), http://www.ecb.europa.eu/pub/pdf/other/virtualcurrencyschemes201210en.pdf

[42] FinCEN, 'Statement of Jennifer Shasky Calvery, Director Financial Crimes Enforcement Network United States Department of the Treasury', *United States Financial Crimes Enforcement Network*, 2013.

[43] European Central Bank. 2014. "EBA Opinion on 'virtual currencies'.

technologies, decentralized virtual currencies allow online payments to be sent directly from one party to another, using a system based on cryptographic proof instead of trust.[44]

3. Decentralized Cryptographic Virtual Currency: Bitcoin

3.1 What is Bitcoin?

Bitcoin is an invention of a computer programmer using the pseudonym Satoshi Nakamoto.[45] This invention is open source, meaning its underlying computer code is free and open to public viewing. Bitcoin is a peer-to-peer network that uses cryptography to allow the secure transfer of unique digital assets (bitcoin) between any two parties in a decentralized manner (independent of a trusted third party).[46] Within this system, each transfer of bitcoin is visible to the entire network and is the legitimacy of each transfer is unchallengeable.[47]

Centralized virtual currencies require trust on a third party to regulate the creation of new units, to verify transactions, and update the ledger of account balances. Bitcoin precludes the need to trust a third party, by providing a solution to two long-standing problems in computer science which have plagued past forms of electronic value transfer: the double-spending problem and the Byzantine Generals Problem.[48] The innovative solution that allow Bitcoin to function as a peer-to-peer payment system, is the use of a global public ledger (the block chain), which is maintained and secured by the collective processing power of individuals in network.

The basic functioning of the Bitcoin network will be described in section 2.2, followed by an analysis of bitcoin units and bitcoin transactions in section 2.3. With this basic understanding

---

[44] Nakamoto, S., 'Bitcoin: A Peer-to-Peer Electronic Cash system', 2008, (accessed 30 September 2014), https://bitcoin.org/bitcoin.pdf

Cryptography is a branch of mathematics based on the transformation of data, which provide high levels of security.

[45] This paper distinguishes between *Bitcoin* (with an uppercase 'B') which refers to the protocol, network, or the system as a whole, and *bitcoin* (with a lowercase 'b') for the currency units (abbreviated as BTC).

[46] 'Cryptography'. (accessed 5 October 2014), https://bitcoin.org/en/vocabulary

[47] Nakamoto, S. 'Bitcoin: A Peer-to-Peer Electronic Cash system.', 2008, (accessed 30 September 2014), https://bitcoin.org/bitcoin.pdf

[48] Dourado, E & Brito, J. 'Cryptocurrency, The New Palgrave Dictionary of Economics'. Eds. Steven N. Durlauf and Lawrence E. Blume, Palgrave Macmillan, 2014, *The New Palgrave Dictionary of Economics Online*, Palgrave Macmillan. 20 October 2014. (accessed 20 October 2014). http://www.dictionaryofeconomics.com/article?id=pde2014_C000625

of how the Bitcoin system functions, section 2.4 will address questions such as why people use this system as a means of exchange, while providing an outline of the associated risks and benefits.

3.2 The Bitcoin System: How is a Global Public Ledger Maintained through Distributed Consensus?

The double-spending problem exists in all payments apart from physical cash. Once physical cash changes hands between Alice and Bob, it is final and all parties are aware of whose money it is[49]. With any form of electronic value transfer (simply information) it is not as apparent: Alice could simply copy the information and use it as payment for several transactions, ensuring each recipient that they are the new rightful owner. Unless Bob can trust Alice's word that she has "deleted" the cash from her account, this system cannot function. Prior to Bitcoin, the double-spending problem was solved by entrusting a third party intermediary to maintain a ledger of all account balances and transactions. The trusted third party confirms identities and updates balances as Alice requested.

Bitcoin invented a way to transfer (not copy) digital assets through the innovative use of public-private key cryptography and a peer-to-peer networking system. Bitcoin provides a distributed ledger called the block chain, a public record of all Bitcoin transactions in chronological order. The block chain is not maintained by a central authority, but is instead maintained in an automated manner by using the network's combined computing power to verify balances and secure transactions.[50] Valid requested transactions form blocks which, once confirmed, are linearly added to the chain (every 10 minutes on average).[51] Transactions can only be requested by the party that holds the password (private key) associated with an account (public key).[52] After confirmation of every block, all nodes automatically update their version of the block chain.

But distributing the ledger between all nodes brings the second problem: The Byzantine Generals Problem. This problem is specifically about asynchronous communications:

---

[49] It is final in the sense that the only way to reverse the transaction would be that Bob give it back to the Alice.

[50] Anyone with internet access is able to download the open-source software and contribute processing power to the network.

[51] http://blockchain.info/blocks

[52] (accessed 5 October 2014), https://bitcoin.org/en/vocabulary

> The Byzantine Generals Problem is abstractly stated as: a set of generals must agree on a common battle plan using only messages to communicate; it is known that there may be traitors trying to sabotage the messages. The loyal generals must decide on the same plan of action. Moreover, the loyal generals should not be coerced into adopting a bad plan by the traitors. More concretely, a system must be reliable even with malfunctioning components.[53]

This problem applied to the Bitcoin network, raises the following questions. When nodes receive an updated version of the block chain, how can they be sure that it is not a falsified update? In other words, how can distributed parties who do not trust each other reach consensus on the current state of the block chain? [54] Bitcoin's solution is the process of "mining". Mining is a distributed consensus system that is used to confirm waiting transactions by including them in blocks added to the block chain.[55] This process of the network achieving consensus is called "mining" as it is also the source of newly minted coins, which serves as incentive to miners to dedicate resources to validate transactions and to secure the network.

Miners are defined as nodes in the network which provide processing power to collect valid transaction requests and assemble blocks that are added to the block chain. The miners function competitively, each receiving all transactions and independently attempting to assemble a valid block (1 miner succeeds approximately every 10 minutes).

The miner that "found" the valid block first, is rewarded for his processing power contribution. The incentive is two-fold: New coins that the Bitcoin protocol issues as a bounty, and transaction fees from all transactions included in the block.[56] The new coins rewarded by the protocol are the only way the coins in circulation increases. The total supply of bitoins is fixed at 21 million, and the coins enter circulation in a predetermined decreasing rate. The current reward is 25 BTC per block, and halves every 210,000 blocks (roughly every 4 years) until the reward equals 1 satoshi (the smallest possible part of a bitcoin, 0.00000001

---

[53] Lamport, L., Shostak, R and Pease, M., 'The Byzantine Generals Problem, ACM Transactions on Programming Languages and Systems', July 1982, pages 382-401, as summarized by Jacobson, E. (accessed 6 October 2014), http://pages.cs.wisc.edu/~swift/classes/cs739-sp11/blog/2011/02/the_byzantine_generals_problem.html

[54] Dourado, E & Brito, J. 'Cryptocurrency, The New Palgrave Dictionary of Economics'. Eds. Steven N. Durlauf and Lawrence E. Blume, Palgrave Macmillan, 2014, *The New Palgrave Dictionary of Economics Online*, Palgrave Macmillan, 2014, http://www.dictionaryofeconomics.com/article?id=pde2014_C000625

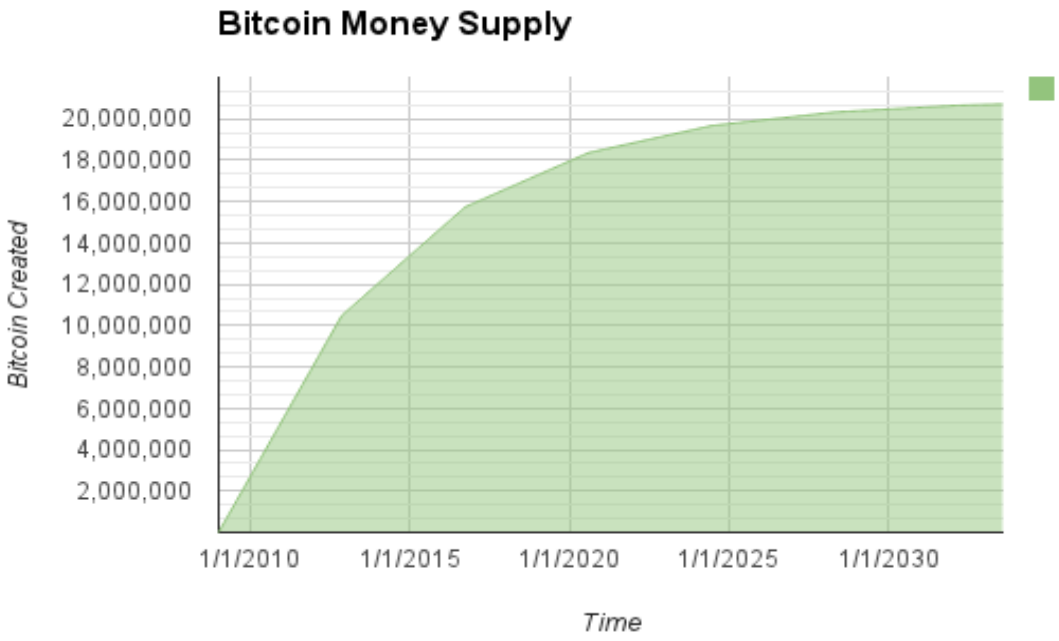
[55] 'How does Bitcoin work?' (accessed 10 October 2014). https://bitcoin.org/en/how-it-works

[56] (accessed 5 October 2014). https://en.bitcoin.it/wiki/How_bitcoin_works

BTC). After that block, roughly 2140, the reward will consist only of transaction fees. The supply of bitcoins is thus expanded at a decreasing rate, as shown in figure 1.

As the total supply and the rate at which the coins enter circulation are fixed, the system is protected from an oversupply of currency (hyperinflation). This has been referred to as digital scarcity.

Figure 1. Supply of bitcoins over time



The process of producing a valid block is intentionally difficult (time consuming), and is like a competition between miners to solve a complex mathematical puzzle (based on a cryptographic hash function). The solution to this puzzle, called "Proof-of-Work", forms part of each block and functions as evidence that the miner expended significant computing effort to produce the block.[57] The network automatically adjusts the difficulty so to ensure than an average of 6 blocks are found per hour (The more miners attempting a solve it, the more difficult it becomes), resulting in the predetermined rate of the expansion of the monetary supply. Cryptographic hash function puzzle have special qualities and can be described by a useful analogy drawn by Antonopolous (2014):

> [M]ining is like a giant competitive game of sudoku that resets every time someone finds a solution and whose difficulty automatically adjusts so that it takes approximately 10 minutes to find a solution. Imagine a giant sudoku puzzle, several thousand rows and columns in size. If I show you a completed puzzle you can verify it

[57] Antonopoulos, A. M. *Mastering Bitcoin: Unlocking digital crypto-currencies.* O'Reily Media. 2014.

> quite quickly. However, if the puzzle has a few squares filled and the rest is empty, it takes a lot of work to solve! The difficulty of the sudoku can be adjusted by changing its size (more or fewer rows and columns), but it can still be verified quite easily even if it is very large. The "puzzle" used in bitcoin is based on a cryptographic hash and exhibits similar characteristics: it is asymmetrically hard to solve but easy to verify, and its difficulty can be adjusted.[58]

This analogy provides a useful glimpse into the intricacies of Bitcoin's innovative use of cryptographic hash functions and helps explain the role of miners. The first miner to produce a valid block broadcasts it to the rest of the network which easily recognizes that the broadcasted block is valid, updates their copies of the block chain by adding the new block, and immediately starts working on the next.[59] One ingredient used in producing each block, is the previous block's fingerprint, and thus each block confirms the integrity its predecessor-all the way back to the genesis block.[60] If any changes would be made to any blocks, all subsequent blocks would no longer make sense and would instantly be spotted by other nodes, and simply not be accepted. This is the source of the networks security, as any changes to previous blocks would require to redo the Proof-of-Work for all subsequent blocks, which becomes exponentially difficult for each block that is added. The network views only the longest chain of blocks as valid, as it is the chain supported by the majority of the network's processing power. After a few blocks have been added, users can trust that transactions have taken place irreversibly and no question of ownership remains.[61]

But how does this solve the Byzantines Generals Problem? Imagine two miners solve the puzzle at almost exactly the same and each node in the network must decide which for themselves which the chain is the correct one that should be further extended. Nakamoto(2009) frames the problem and explains Bitcoin's solution:

---

[58] Antonopoulos, A. M., *Mastering Bitcoin: Unlocking digital crypto-currencies,* O'Reily Media, 2014, (accessed 14 October 2014), http://chimera.labs.oreilly.com/books/1234000001802/ch04.html#_public_key_cryptography_and_crypto_currency

[59] Pacia, C., 'Bitcoin Mining Explained Like You're Five: Part 1 – Incentives', 2014, (accessed 10 October 2014) http://chrispacia.wordpress.com/2013/09/02/bitcoin-mining-explained-like-youre-five-part-1-incentives/

[60] Antonopoulos, A. M. *Mastering Bitcoin: Unlocking digital crypto-currencies.* .O'Reily Media, 2014, (accessed 14 October 2014), http://chimera.labs.oreilly.com/books/1234000001802/ch04.html#_public_key_cryptography_and_crypto_currency

[61] Nakamoto, S. 'Bitcoin: A Peer-to-Peer Electronic Cash system.', 2008, (accessed 30 September 2014), https://bitcoin.org/bitcoin.pdf

> The problem is that the network is not instantaneous, and if two generals announce different plans at close to the same time, some may hear one first and others hear the other first.
>
> They use a proof-of-work chain to solve the problem. Once each general receives whatever plan he hears first, he sets his computer to solve a difficult hash-based proof-of-work problem that includes the plan in its hash. The proof-of-work is difficult enough that with all of them working at once, it's expected to take 10 minutes before one of them finds a solution and broadcasts it to the network. Once received, everyone adjusts the hash in their proof-of-work computation to include the first solution, so that when they find the next proof-of-work, it chains after the first one. If anyone was working on a different plan, they switch to this one, because its proof-of-work chain is now longer.[62]

In the sense of the Byzantines Generals Problem, a loyal miner can be trust the longest chain as the true order of events, since at least 51 percent of the loyal miners have already agreed upon it.

Thus, mining is the system that confirms waiting transactions, maintains the state of the ledger, protects the neutrality of the network, and also distributes new bitcoins in predetermined manner. The system is designed to incentivize individuals, acting as rational self-interested parties, to contribute processing power towards the operation and security of the network. These individuals are not required to trust each other, and through mining they are able to reach consensus.

It must be noted that the system itself is not a currency, but rather that the system (i.e. the block chain and mining) forms the basis on which bitcoins can be used as currency. The next questions are: what is a bitcoin (the unit that is transferable using the network)? ; how are bitcoins stored?; and what is a bitcoin transaction?

3.3 Wallets, bitcoins and Transactions

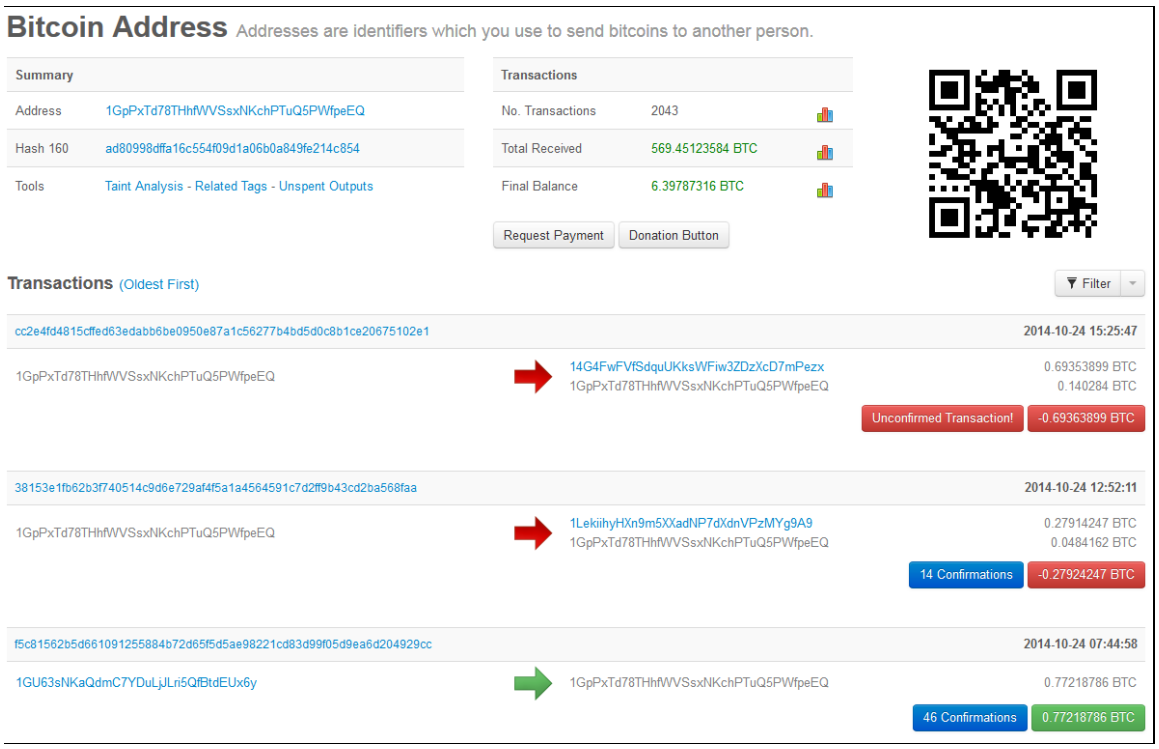
Nakamoto(2008) defines bitcoins as a chains of digital signatures.[63] Each owner transfers the bitcoin to the next, by digitally signing a hash of the previous transaction and the bitcoin address of the next owner and adding these to the end of the coin. The bitcoin address of the

[62] Bitcoin Forum Post by Satoshi Nakamoto, 2014, (accessed 15 October 2014), https://bitcointalk.org/index.php?topic=99631.0

[63] Nakamoto, S. 'Bitcoin: A Peer-to-Peer Electronic Cash system.', 2008, (accessed 30 September 2014), https://bitcoin.org/bitcoin.pdf

recipient is the only information the owner requires to initiate a transfer. Bitcoin addresses are public, anyone can see the entire transaction history and final balance on the block chain by using block chain explorer websites (figure 2). Bitcoin is said to be pseudonymous as Bitcoin addresses that are recorded in the block chain are not explicitly tied to anyone's identity. However, if a user makes a single transaction which links his/her identity to the address, it is easy to link the user's identity to all transactions associated with the address through the block chain.

Figure 2: Bitcoin address[64]



Source: https://blockchain.info/address/1GpPxTd78THhfWVSsxNKchPTuQ5PWfpeEQ

3.3.1 Digital keys, Addresses and Wallets

Addresses are derived from public keys, which are derived from private keys, and each derivation uses a one-way mathematical function. The public-private key pair is mathematically related in such a way that each private key has a unique public key. A private key is simply a randomly generated number, which is used to create digital signatures required to spend bitcoins.[65] Generating a unique private key is cost free, there are no limitations regarding to the amount of key pairs users can create, and does not even require an

[64] https://blockchain.info/address/1GpPxTd78THhfWVSsxNKchPTuQ5PWfpeEQ

[65] Antonopoulos, A. M. *Mastering Bitcoin: Unlocking digital crypto-currencies*, O'Reily Media, 2014, (accessed 14 October 2014). http://chimera.labs.oreilly.com/books/1234000001802/ch04.html#_public_key_cryptography_and_crypto_currency

internet connection.[66] Private keys must be kept secret and stored safely since funds that are held in associated addresses, can only be spent with the private key. If the private key is lost, the bitcoins held in addresses associated with it are locked in the address forever. As mentioned, a private key can be generated offline. This means that users do not really create a private key, but simply *chooses* one from the existing pool at random. The number of possible private keys is so immense (2^{256}, which is a 1 with 77 zeros) that it is virtually impossible to randomly generate the same private key twice.

A bitcoin address usually represents the owner of a private/public key pair, but can also represent something else such as a payment script.[67] Currently, the most commonly implemented type of payment script address is multi-signature addresses. Multi-signature addresses require a certain number of the parties associated with the address to sign transactions in order to spend the funds. Antonopoulos(2014) gives two examples of how multi-signature addresses can be used:

> […] could use multi-signature address requiring 1-of-2 signatures from a key belonging to him and a key belonging to his spouse, ensuring either of them could sign to spend a transaction output locked to this address. This would be similar to a "joint account" as implemented in traditional banking where either spouse can spend with a single signature.
>
> [...] a 2-of-3 multi-signature address for his business that ensures that no funds can be spent unless at least two of the business partners sign a transaction.[68]

This is just one example of addresses that can be used as to create a form of corporate governance control that can protect funds against theft or loss.[69]

Bitcoin users store their key pairs in wallets. Wallets can be either be self-managed and stored on a mobile device, desktop computer, hardware wallets or even paper wallets; or can be in a

---

[67] Antonopoulos, A. M. *Mastering Bitcoin: Unlocking digital crypto-currencies.* .O'Reily Media, 2014. (accessed 14 October 2014). http://chimera.labs.oreilly.com/books/1234000001802/ch04.html#_public_key_cryptography_and_crypto_currency

[68] *Ibid.*

[69] Antonopoulos, A. M., *Mastering Bitcoin: Unlocking digital crypto-currencies.* .O'Reily Media, 2014. (accessed 14 October 2014). http://chimera.labs.oreilly.com/books/1234000001802/ch05.html#p2sh

on a third party's server and accessed online. When storing a wallet on your home computer or mobile phone it must be kept in mind that bitcoins are like real money, and that there is no central party to reimburse you in case of loss or theft. Users keeping their coins on their computer or mobile device thus require the technical knowledge to secure their devices. For the average computer user who assumes there is no malicious software on his computer (because Norton's Antivirus declared it so), these self-managed software wallets will not suffice. The more user-friendly option is to use web wallet services, where a third party is entrusted to keep users keys secure and users simply log into their website or mobile application to access their wallet and in some cases the storage services even insures against theft and loss.[70]

Since Bitcoin acts similar to cash it is advised to only keep day-to-day funds in an online wallet, and the rest in offline hardware or paper wallets (cold storage). As previously mentioned, private keys can be generated offline, and be stored in a hardware wallet (Trezor) or a paper wallet. This way, users are able to create private keys that have never been connected to the internet and are never stored on hardware that will be connected to the internet, making their bitcoins immune to cyber-attacks. Bitcoins stored in cold storage require *at least* physical access to the wallet in order to control the funds.

3.3.2 bitcoins

The next step is to investigate the tokens that are storable and transferrable on the Bitcoin system: bitcoins. Due to a fixed eventual money supply of 21 million, bitcoins are scarce by design. Bitcoins are also impossible to counterfeit. This is an attractive property cited by advocates when comparing Bitcoin to fiat currencies: For example in the 2013-2014 fiscal year almost $90 million counterfeit U.S. dollars were seized by the secret service, who made 3,617 counterfeiting arrests.[71] Bitcoins can be transferred online or offline (by physically transferring keys). For online transfers transaction costs are voluntary (typically 0.0001 BTC ~ 0.04 USD), and unrelated to the recipient and amount transferred. Units are fungible- every unit (or subunit) is equivalent and identical to any other.[72] Every unit is divisible up to 8 decimal places (As 1 dollar is 100 cents, 1 bitcoin is 100, 000, 000 satoshis.)

---

[70] Examples of web wallet services are: https://blockchain.info/wallet, http://mycelium.com/, https://www.coinbase.com/, https://www.elliptic.co/vault

[71] Wilber, D. Q., 'Woman With Printer Shows the Digital Ease of Bogus Cash', *Bloomberg*, 2014, (accessed 20 October 2014), http://www.bloomberg.com/news/2014-05-07/mom-with-hp-printer-shows-the-digital-ease-of-bogus-cash.html

[72] (accessed 25 October 2014). http://www.coindesk.com/bitcoin-fungibility-essential/

Users can acquire bitcoin through mining, purchasing bitcoin from other users through on bitcoin exchange, or by simply accepting bitcoin as payment for goods or services. However, mining has become a highly competitive affair and to enter to the market at this time would require significant investment in specialized bitcoin mining hardware.[73] The most common way to buy or sell bitcoins is through online bitcoin exchanges. There are currently 135 exchanges listed on the bitcoin wiki and facilitates bitcoin trading worldwide.[74] Using publicly posted prices and order books, bitcoin exchanges match customer orders directly and anonymously via automated algorithms. Bitcoin exchanges function similarly to stock exchanges, but different in the sense that users trade directly with one another and not through intermediary specialists as on NASDAQ or the New York Stock Exchange.[75] Another increasingly popular way of acquiring bitcoins is through a bitcoin ATM.[76]

Figure 3 – Bitcoin ATM Map by CoinDesk.com

Source: http://www.coindesk.com/bitcoin-atm-map/

3.3.3 A bitcoin Transaction

This section will describe the main steps of a bitcoin transaction by following a basic transaction between Alice the miner and Bob the merchant, from the moment of the decision to transfer the bitcoin, to the moment the network confirms the transaction.

---

[73] The network hashrate today is ~260,716,255 GH/s. If a miner were to decide to enter the market with enough computing power to have a 1 percent chance to solve the next block, the specialized hardware alone would cost approximately $ 2 million US$. (Not mentioning electricity costs).

[74] 'Exchanges'.(accessed 26 October 2014). https://en.bitcoin.it/wiki/Exchanges

[75] Lo, S. Wang, J. C. 'Bitcoin as Money?'. *Current Policy Perspectives, Federal Reserve Bank of Boston No 14-4.* 2014. pp 13.

[76] CoinDesk. 'Bitcoin ATM Map'. (accessed 26 October 2014). http://www.coindesk.com/bitcoin-atm-map/

Alice verified the last block and the network rewarded her with 25.5 BTC (25 new bitcoins and 0.5 in transaction fees from the block). Alice wants to buy more mining hardware from Bob, an online merchant selling the newest ASIC mining hardware. The new mining rig costs 5 BTC. Alice decides to purchase the new rig, and to add a transaction fee of 0.0001BTC.

Step 1 : Creating the Transaction

A transaction consists of inputs and outputs. The inputs are the address from which bitcoin will be sent and the outputs the addresses that will receive the bitcoin. The inputs and outputs are not necessarily equal; the difference being the transaction fees offered to the miner that verifies the transaction.

Antonopolous (2014) equates a transaction to a paper cheque: "Like a cheque, a transaction is an instrument that expresses the intent to transfer money and is not visible to the financial system until it is submitted for execution. […]While a cheque references a specific account as the source of the funds, a bitcoin transaction references a specific previous transaction as its source, rather than an account."[77]

Alice creates a transaction with the input as her address that contains 25.5 BTC, and the outputs are 5 BTC to Bob, 20.4999 to Alice (the 'change' from the transaction). The difference is 0.0001 and this is included as a miner's fee. After Alice created the transaction, she signs the transaction by encrypting it with her private key. This way anyone with Alice's public key can decrypt the transaction message, and verify that it was created by Alice. The transaction is now ready is now ready to be submitted for execution.

Step 2: Broadcasting the Transaction to the Network

Alice broadcasts the signed transaction to any node in the peer-to-peer network for verification. The node will validate that the inputs Alice used, are recognized previous outputs, and if valid, that node will broadcast the message to 3 – 4 nodes (each of which will independently validate the transaction and broadcast it to a further 3-4 nodes). Transactions with invalid inputs will never be rebroadcasted by the initial receiving node, and valid transaction will propagate in an exponentially expanding ripple across the entire network within seconds.[78]

---

[77] Antonopoulos, A. M. *Mastering Bitcoin: Unlocking digital crypto-currencies,* .O'Reily Media, 2014, (accessed 14 October 2014). http://chimera.labs.oreilly.com/books/1234000001802/ch05.html#tx_bcast

[78] Antonopoulos, A. M. *Mastering Bitcoin: Unlocking digital crypto-currencies.* .O'Reily Media, 2014. (accessed 14 October 2014). http://chimera.labs.oreilly.com/books/1234000001802/ch05.html#tx_bcast

Step 3: The Transaction is Included in a Block and Added to the Block Chain

After validating the transaction inputs, miners include the transaction in a block with other valid transactions coupled with demonstrated computational efforts through Proof-of-Work. Once a miner successfully verifies the block containing Alice's transaction, the miner is announces its find to the rest of the network. The other miners verify the validity of the new block, updates their versions of the global public ledger, and starts working of the next block. From this moment onwards, Bob is able to use the 5 BTC transaction output created by Alice, as an input in a new transaction.

3.4 The Current Economic State of Bitcoin (October 2014)

There are currently 13.5 million bitcoins in circulation, each valued at approximately 355 USD. Bitcoin is used in and the number of transactions per day ranges between 70,000 and 80,000. To put this into perspective: PayPal processes approximately 9.7 million transactions per day and Visa averages 150 million transactions per day.[79]

The price of bitcoin has been volatile. The first time a bitcoin traded for more than one USD was in April 2011. The price peaked in December 2013 at 1150 USD and throughout 2014 followed an overall downward trend with large fluctuations. Figure 4 shows the daily price variances of bitcoins and sterling expressed in terms of U.S. dollar.[80] While this comparison is a bit like comparing apples and oranges, this graph does indicate that the volatility of bitcoin is decreasing over time.

The Bank of England attributes Bitcoins price volatility mainly to the predetermined rate of supply and the fixed total supply. Since aggregate demand for money is volatile due to seasonal (Christmas shopping), cyclical (recessions) or structural (technological improvements) reasons, a money supply that is unable to respond accordingly will necessarily result in price volatility.[81]

---

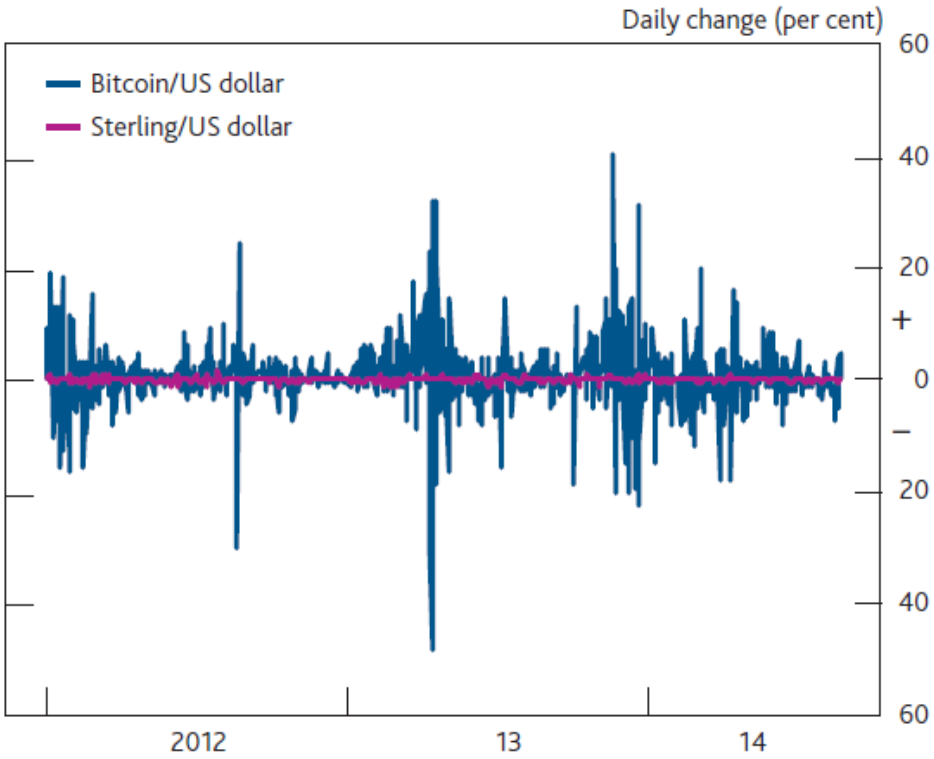
[79]Official webpages of Visa an Paypal, 2014, (accessed 25 October 2014)
http://usa.visa.com/merchants/industry-solutions/retail-visa-acceptance.jsp
https://www.paypal-media.com/about

[80] Ali, R. Barrdear, J. Clews, R. Southgate, J., 'The economics of digital currencies', *Bank of England Quarterly Bulletin2014 Q3*, 2014, (accessed 5 October 2014),
http://www.bankofengland.co.uk/publications/Documents/quarterlybulletin/2014/qb14q3digitalcurrenciesbitcoin2.pdf

[81] Ali, R. Barrdear, J. Clews, R. Southgate, J., 'The economics of digital currencies. *Bank of England Quarterly Bulletin2014 Q3*, 2014, (accessed 5 October 2014),

In a report issued by CoinDesk, 'State of Bitcoin Q3 2014', more positive statistics are shown regardless of the deterioration in price. For the period September 2013 to September 2014 the report showed the following: Merchants accepting bitcoin as a means of payment increased eightfold and now totals 76 000; The number of unique bitcoin addresses increased threefold and now totals 184,554; All time venture capitalist investment into bitcoin related firms increased tenfold and now totals $317 million; The Network Hash Rate (computational power securing the network) has increased 216-fold.[82]

Figure 4: Bitcoin Price Volatility Compared to Sterling



Source: Bank of England Quarterly Bulletin 2014 Q3.

The majority of merchants accept bitcoin exclusively as a means of exchange, and not as a unit of account (prices are USD converted to BTC) of a store of value (does not keep the payment in bitcoin form). Merchants typically accept bitcoin through payment processors such as BitPay or Coinbase, which handles and stores bitcoins on their behalf. Bitcoin

http://www.bankofengland.co.uk/publications/Documents/quarterlybulletin/2014/qb14q3digitalcurrenciesbitcoin2.pdf

[82] 'State of Bitcoin Q3 2014', CoinDesk, 2014, (Accessed 20 October 2014). http://www.slideshare.net/CoinDesk/state-of-bitcoin-q3-2014?qid=a856ddfe-f3e9-4f61-8fa1-b60ba2340d19&v=qf1&b=&from_search=1

payment processors also assume the volatility risk by offering merchants the option of immediate conversion of the bitcoin received into their local currency.[83]

4. The Benefits of Using Bitcoin as a payment system

The question is why anyone would want to use Bitcoin as a payment system instead of Visa or PayPal which are already commonly accepted.

As Bitcoin handles tasks usually entrusted to a central authority (verification of transactions, security of the system and regulation of the money supply) in a way that has never been used, the use of bitcoins as a means of exchange is radically different than everything that came before it. Its decentralized design grants users access to a payment system with no single point of failure. The network will process transactions unless all miners are forced to shut down their operations at once, this is a practical impossibility. In the absence of an intermediary to transactions, no mechanism for censorship or control exists. Anyone can easily create a Bitcoin address through which funds can instantly be received, and user's accounts cannot be "frozen". After a few confirmations, transactions are irreversible, and the only the holder of the private key of the receiving address has control over the coins.

The benefits to using Bitcoin as a payment system are economic (lower transaction costs, no cost of entry), practical (irreversible transactions in reasonably shot periods of time, geographical factors play no role) and conceptual (such as financial inclusion, censorship resistant). The following section will consider these benefits as they apply to different actors.

4.1 Economic Benefits

Due to the absence of an intermediary, Bitcoin transaction fees are generally significantly lower than that of other payment systems. Transaction fees are voluntarily added by the person initiating the transaction and the typical transaction fee is currently 0.0001 BTC (about 0.04 USD), regardless of the amount of the value being transferred, and regardless of the recipient. This contrasts against most payment systems, which usually charge a percentage of the transferred amount. Other economic benefits are that the acquisition of a Bitcoin address is free and instant; transaction processing time is 10 minutes on average; and that payments are irreversible.

[83] (accessed 25 October 2014). https://bitpay.com/features

Bitcoin can benefit merchants in several ways. For merchants, this process of setting up a Bitcoin address contrasts against the process for setting up an account with credit card payment systems like Visa or Mastercard. In order to accept credit and debit card payments, merchants must first obtain a merchant account by entering into an agreement with a member bank that has a processing relationship with Visa or Mastercard.[84] This agreement binds the merchant to the operating regulations as determined by the credit card company. Prior to the merchant account being granted, a merchant is subject to a comprehensive review of its business model and financial details, and smaller business owners must disclose their personal information and undergo a credit check.[85] The merchant account provider typically charges two fees per transaction: A per item flat rate as well as a percentage fee based on the total amount of the transaction (typically 2% to 5%). Merchants accepting credit card are also subject to chargebacks (the transaction is reversed) in cases where the card holder disputes a transaction on any ground (claims that card was stolen or that the merchant delivered unsatisfactorily).[86] Now consider a merchant accepting Bitcoin as payment: zero fees for creating a Bitcoin address, zero fees for accepting Bitcoin payments and zero risks of chargebacks.

Merchants thus not only benefit from lowered transaction costs, but also the reduced fraud risk. The Chairman of a large U.S. online retailer Overstock emphasizes that of the reduced fraud risks when using Bitcoin is benefits both merchant and customer:

> One, the merchant who is accepting bitcoin doesn't hold any meaningful personal identifiable information about the customer. If you purchase something on our site with bitcoins, yes you give us a shipping address, but you don't give us a credit card number or bank account details. On the off-chance someone hacked into our site, there is nothing there to target and steal. Two, we spend a lot of money and effort on fraud prevention, stopping the use of stolen credit cards, but we don't have to worry about that fraud prevention effort with bitcoin because there is no charge-back available.[87]

---

[84] 'How to Set Up a Merchant Account'. 2011. (Acessed 10 October 2014). http://paysimple.com/blog/2011/09/07/how-to-set-up-a-merchant-account/

[85] *Ibid.*

[86] Conde, J. 'Merchant Accounts 101'. 2013. (accessed 10 October 2014). http://www.merchant-account-services.org/article/merchant-accounts-101/11

[87] Wright, G., 'Is bitcoin good for business?', *Global Finance, 28*(6). 2014. (accessed 10 October). http://bitcoinchamberofcommerce.com/?p=448

Overstock started accepting bitcoins as payment in January 2014. In a statement to Reuters during August 2014, the CEO said Overstock has processed more $2 million worth or transactions in bitcoin, and expects total bitcoin sales of $6 million to $8 million in 2014.[88]

Lower transaction costs also allow micro-payments, giving businesses the opportunity to monetize low-cost goods or services sold online, which current transaction costs make unfeasible. For example a user could pay for a single song instead of purchasing an entire album, or pay to read a single article on a news-site instead of purchasing a monthly subscription.

There are also potential beneficiaries are on the other side of the financial spectrum: The "unbanked" and the international migrant remittances market.

4.2 Financial Inclusion

Financial inclusion of the unbanked and the state of the international remittances market form the focus of the 2014 Global Financial Development Report released by the World Bank.[89] This report emphasizes the importance of financial inclusion for economic and social development.[90] The World Bank states that there is a growing worldwide recognition "that access to financial services has a critical role in reducing extreme poverty, boosting shared prosperity, and supporting inclusive and sustainable development."[91] So who are the unbanked? According to the report, approximately 50 percent of adults (2.5 billion) without access to a basic bank account, and while some have no demand for accounts, most are excluded due to barriers such as cost, distances, documentation requirement regulations or a

[88] Chavez-Dreyfuss, G., 'Exclusive: Overstock CEO says bitcoin sales to add 4 cents to 2014 EPS'. 2014. (Accessed 14 October 2014). http://www.reuters.com/article/2014/08/13/us-overstock-com-bitcoin-idUSKBN0GD21220140813

[89] World Bank,'Financial Inclusion', Global Financial Development Report, 2014. pp 21. (accessed 14 October 2014). http://econ.worldbank.org/WBSITE/EXTERNAL/EXTDEC/EXTGLOBALFINREPORT/0,,contentMDK:23489619~pagePK:64168182~piPK:64168060~theSitePK:8816097,00.html

[90] World Bank,.'Financial Inclusion'. *Global Financial Development Report 2014*. pp 21. (accessed 14 October 2014), http://econ.worldbank.org/WBSITE/EXTERNAL/EXTDEC/EXTGLOBALFINREPORT/0,,contentMDK:23489619~pagePK:64168182~piPK:64168060~theSitePK:8816097,00.html

[91] *Ibid.*

lack of trust in banks.[92] In the developing world, fixed transaction cost and annual fees make tend to make small transactions unaffordable. For example, total annual fees on a checking account in Sierra Leone are equivalent to 27 percent of GDP per capita.[93] High costs associated with opening and maintaining accounts in small developing countries are identified as a consequence of the lack of competition and underdeveloped physical or institutional infrastructures. The lack of bank branch penetration also explains the distance as being a major reason for exclusion. In Tanzania, 47 percent of the unbanked cite distance as the primary reason.[94] In Europe and Central Asia, 31 percent of the unbanked cite distrust in banks as a reason. Distrust can stem from "discrimination against certain segments of the population, past episodes of government expropriation of banks, or economic crises and uncertainty."[95]

Remittances are among the most important financial transactions for the populations that have limited access to formal banking services. The World Bank (2014) estimates that officially recorded international migrant remittances to developing countries totaled $401 billion. In 2012 the global average cost of remittance transactions was 8 percent of the amount transferred. While some countries enjoy lower fees, those who need it most are above. Approximately $60 billion in remittances was sent to the African continent in 2012, with an average cost per transaction of 11.89 percent. However, the more alarming part of this statistic is that transaction cost actually increased from 10.90 percent in 2011.[96]

The World Bank (2014) states: "Given the potential role of remittances in raising financial inclusion, it is important to make transfer systems less costly, more efficient, and more transparent."[97] Furthermore, the World Bank recognizes that technological innovations are able to make it easier and less expensive for people to use financial services, while increasing financial security. The technological innovations already exist to allow anyone with a mobile

---

[92] *Ibid*, pp. 34.

[93] *Ibid*, pp. 54.

[94] *Ibid*, pp. 55. Bank penetration in Tanzania averages less than 0.5 bank branches per 1,000 square kilometres.

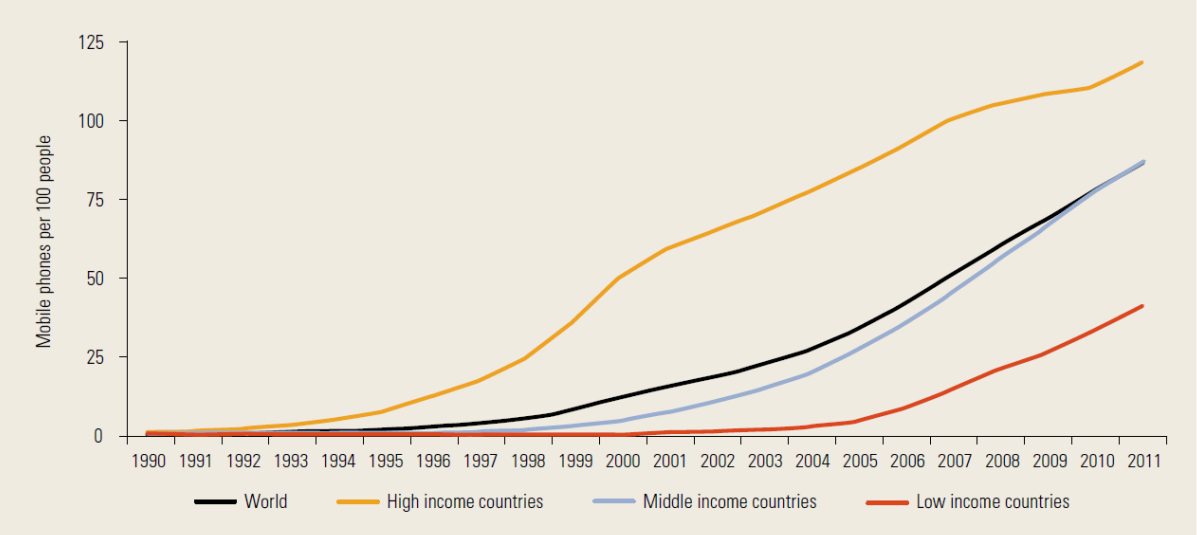
[95] *Ibid*, pp. 55.

[96] Cirasino, M., 'How can we cut the high costs of remittances to Africa', *World Bank Blog*, 2013., (Accessed 20 October 2014), http://blogs.worldbank.org/psd/how-can-we-cut-the-high-costs-of-remittances-to-africa

[97] World Bank, 'Financial Inclusion', *Global Financial Development Report 2014*, 2014. pp 76, (Accessed 14 October 2014), http://econ.worldbank.org/WBSITE/EXTERNAL/EXTDEC/EXTGLOBALFINREPORT/0,,contentMDK:23489619~pagePK:64168182~piPK:64168060~theSitePK:8816097,00.html

phone to utilize innovative payment systems such as Bitcoin. Fig. 2 shows the rapid increase of mobile phone technology adoption in the developing world.

Figure 2: Mobile Phones per 100 People, by Country Income Group, 1990–2011[98]



Source: World Development Indicators (database), World Bank, Washington, DC, http://data.worldbank.org/data-catalog/world-development-indicators.

Fig. 2 suggests that the developing world's unbanked and remittance paying migrants may be ripe for conceptual and economic benefits associated with innovative new payment systems. To harness the promise of new technologies, regulators need to allow competing financial service providers and consumers to take advantage of technological innovations . The World Bank states that regulators must ensure that "first, new technologies are adopted and, second, that they are priced and made available in a way that makes them accessible to the unbanked" by creating a regulatory framework which "create enabling conditions for the providers of technology-based financial services, while protecting the rights of consumers."[99]

5. Risks

There are many risks involved in the use of virtual currency schemes and most central authorities have issued warning statements regarding risks of use and speculation of bitcoin. This section will describe the risks involved for users, risks to financial integrity and risks to regulators.

[98] *Ibid.* pp 54.

[99] World Bank.'Financial Inclusion', *Global Financial Development Report 2014*, 2014. pp 76. (Acessed online 14 October) http://econ.worldbank.org/WBSITE/EXTERNAL/EXTDEC/EXTGLOBALFINREPORT/0,,contentMDK:23489619~pagePK:64168182~piPK:64168060~theSitePK:8816097,00.html

5.1 Risks to Users

In the absence of a central authority or intermediary, users of virtual currency enjoy less consumer protection than typically afforded by traditional banking and payment services. Bitcoin users are exposed to risks of theft or fraud, and price volatility. While Bitcoin is designed to function as a decentralized system that does not require users to trust or depend on third parties, in practice users often trust third parties such as exchange operators and wallet service providers to not act fraudulently and to have sufficient security safeguarding their systems.

Users that personally store their keys have the risk of permanently losing their funds if they lose their passwords/private key or if their hard drive containing their wallet crashes without having a backup. In this case the funds will be stuck in that address and can never be retrieved. Users also risk permanently losing their funds if their computer becomes infected with malicious software that steals their private keys. In the event of loss or theft, no recourse is available, since there is no central authority.

Users entrusting third party service providers such as exchanges or web wallet providers with their funds, risk loss as a result of fraudulent actors or pure mismanagement. Most companies built around virtual currencies are to be considered as startups which operate in unsure regulatory space. Startup companies have massive potential, but are also at high risk of mismanagement or even fraud, and thus failure. Many (if not most) exchanges have failed, and large amounts of users' funds have been lost. The most famous case is that of Mt.Gox, a Bitcoin exchange based in Tokyo, Japan. In February 2014 Mt. Gox, the largest and longest operating bitcoin exchange at the time, stopped trading and filed for bankruptcy after discovering that as many as 650,000 bitcoins (worth approximately US$465 million at the time) had been lost due to a security breach.[100] The Bitcoin community remains skeptical and many are of the opinion that the loss was due to gross negligence or even internal theft. In response to the failure of Mt. Gox, the Bitcoin Foundation stated: "This is certainly not the end of Bitcoin. As our industry matures, we are seeing a second wave of capable, responsible entrepreneurs and investors who are building reliable services for this ecosystem."[101] And indeed today the situation is different. The number of identifiably trustworthy actors has increased significantly. One example is Circle Internet Financial Inc. which is backed by

[100] 'Hackers hit web accounts of MtGox boss', *BBC Technology News*, 2014. (Accessed 20 October 2014). http://www.bbc.com/news/technology-26387800

[101] 'Bitcoin - Turbulent Waters - Part Seven', *Dorsey & Whitney LLP*, 2014. (Accessed 20 October 2014), http://www.dorsey.com/eu_cm_bitcoin_virtual_currency_pt7/

US$26 million in venture capital investment and boasts with a respectable management board. Circle Internet Financial allows customers to use credit cards to purchase bitcoins, provides a secure platform for users to send bitcoins to each other, and most unique in the Bitcoin ecosystem, all clients' funds stored on their system are fully insured at zero cost.[102]

When using bitcoins as a means of payment, there is little protection for the customer in the event that the counterparty fails to meet his contractual obligations. While merchants view chargebacks as a disadvantage, this measure of consumer protection is unavailable to users paying in bitcoin since there is no intermediary to appeal to. Thus, when making payments, users have more responsibility to verify the authenticity of the counterparty, as well as being more diligent in executing the transaction correctly. In the event of transferring bitcoins to a malicious party, or transferring bitcoins to an incorrect address, there is no recourse and the funds are lost.[103]

Users invested in Bitcoin are exposed to significant price volatility. The price of bitcoin experiences large and sudden fluctuations due to many factors which are generally uncontrollable, such as the extent of adoption and future expectations. Furthermore, the market depth is low, large buy/sell orders on exchanges cause noticeable fluctuations in the exchange rate.[104] The lack of a central bank combined with a fixed rate of supply is criticized by economists citing the need for macro-economic stabilization. Within the Bitcoin system, counter cyclical inflationary stimulus is impossible, and thus changes in demand for money will result in changes the price.[105]

Another risk faced by users is the possibility of Bitcoin losing all value if the network consensus is undermined. The existence Bitcoin's value relies on the uncompromised functioning of the protocol, and users' confidence that the network will remain functioning. Bitcoin's functioning could be compromised by '51% attack'- if the majority of the network's computational power is controlled by a malicious actor. If a single miner (or a pool of miners), controls the majority of the network's processing power it would be able to alter the current consensus over the rules of the network and could enable double spending or prevent

---

[102] Circle Financial Inc. website, 2014, (accessed 25 October 2014), https://www.circle.com/en

[103] European Central Bank. 'EBA Opinion on 'virtual currencies'. 2014. *EBA/Op/2014/08*. pp 23.

[104] *Ibid.*

[105] Dourado, E & Brito, J., 'Cryptocurrency, 'The New Palgrave Dictionary of Economics', Eds. Steven N. Durlauf and Lawrence E. Blume, Palgrave Macmillan, 2014, *The New Palgrave Dictionary of Economics Online*, Palgrave Macmillan. 20 October 2014. (accessed 20 October 2014). http://www.dictionaryofeconomics.com/article?id=pde2014_C000625

transactions from being included in blocks.[106] Bitcoin is designed that a 51% attack should never happen, since a profit seeking miner will always gain more by following the rules – by regularly solving blocks and receiving new bitcoins and transaction fees. If a 51% attack would be executed, it could destroy trust in the functioning of the network and which would nullify any proceeds attained through double spending. However, attackers might not be financially motivated and might attack the network for reasons outside the Bitcoin economy. An attacker controlling with 51% of the networks processing power could extend the block chain with empty blocks, and prevent any transactions from being confirmed. While honest miners (the 49%) will also find blocks, the attacker will simply keep extending his private version of the block chain which will eventually be longer than the honest block chain. When the attacker then eventually broadcasts its longer block chain, it will replace all blocks since the start of the attack with blocks excluding some (or all) transactions. This would result in some (or all) transactions that were confirmed during the attack, becoming unconfirmed. While these attacks could theoretically happen, the proceeds from the attack would never justify the immense investment required to perform it.[107]

5.2 Risks to Financial Integrity

Risks to financial integrity refer to exploitation of the pseudonymous nature of users and the borderless nature of the payment system.[108] Since addresses are not directly linked to individual identities, the system has the potential to be used for money laundering, terrorist financing and other financial crimes.[109]

The risk of facilitating money laundering and terrorist financing arises as Bitcoin transactions are carried out on peer-to-peer basis between parties without any identification requirements. Anti-money-laundering (AML) efforts face a more elusive target as it is not only more difficult to determine the identities of parties to a transaction, but the transaction itself is also unable to be interrupted. [110] While all transactions publicly recorded in block chain, the

[106] 'Weaknesses', 2014, (accessed 20 October 2014), https://en.bitcoin.it/wiki/Weaknesses#Attacker_has_a_lot_of_computing_power

[107] Trautman, L., 'Virtual Currencies Bitcoin & What Now After Liberty Reserve, Silk Road, and Mt. Gox? *Richmond Journal of Law & Technology. Volume XX(4),* 2014, pp 56. (accessed 28 October 2014). http://jolt.richmond.edu/v20i4/article13.pdf.

[108] European Central Bank, 'EBA Opinion on 'virtual currencies', 2014. *EBA/Op/2014/08*. pp 32.

[109] *Ibid.* pp 32.

[110] Bryans, D., 'Bitcoin and Money Laundering: Mining for an Effective Solution', *Indiana Law Journal Vol. 89:441,* 2014, pp 445.

existence of bitcoin mixing services allow users to maintain anonymity if they want to. Bitcoin mixers provide services that obscure the flow of bitcoins from one address to the next, by mixing the large amounts of bitcoins through many transactions, and returning clean bitcoins to the user. Bryans (2014) states that Bitcoin could enable money launderers to "move illicit funds faster, cheaper, and more discretely than ever before."[111]

The anonymity afforded to users coupled with zero entry costs makes Bitcoin attractive for criminals as a means of payment for illegal commodities and services via hidden online marketplaces called "dark markets". Dark markets, similar to eBay, provide an infrastructure for sellers and buyers to trade over the internet. Dark markets are not accessible through normal internet browsers, but require the use of TOR ("The Onion Router") which conceals true IP addresses and thus the identities of the network participants.[112] Most vendors on these marketplaces only accept Bitcoin as payments, and some marketplaces even have automatic mixing services to ensure the anonymity of parties to each transaction. One such marketplace, called the Silk Road, was shut down in October 2013 by the FBI. Prior to being shut down, the Silk Road website was visited by hundreds of thousands of unique users from countries across the globe on a daily basis.[113] In September 2013, the website had approximately 13,000 listings of illegal goods (such as illegal substances, counterfeit US dollars, forged passports, weapons) and services (such as computer hacking and even assassinations).[114] The only form of payment that was accepted on Silk Road was bitcoins, and sellers would use the normal postage system to deliver goods. During the site's two and a half year existence, it facilitated illegal trades valuing roughly $1.2 billion, and generated $80 million in commissions. The FBI arrested the alleged creator of Silk Road, Ross Ulbricht, and seized his laptop which contained 144,336 bitcoins. A further 29,655 bitcoins were seized from a servers which were used to run the Silk Road website.[115] In July 2014, the U.S. Marshals auctioned off the 29,665 bitcoins (valued at approximately $17 million) in a public auction, with the winning bid from

---

[111] Bryans, D., 'Bitcoin and Money Laundering: Mining for an Effective Solution', *Indiana Law Journal Vol. 89:441,* 2014, pp 447.

[112] Ron, D. Shamir, A., 'How Did Dread Pirate Roberts Acquire and Protect His Bitcoin Wealth?', *Department of Computer Science and Applied Mathematics, The Weizmann Institute of Science, Israel,* 2013, pp. 1.

[113] *Ibid.*

[114] *Ibid.*

[115] Hern, A., 'US government prepares to auction $17m of seized Silk Road bitcoins', *The Guardian.* 2014. (Accessed 24 Octber 2014), http://www.theguardian.com/technology/2014/jun/24/us-auction-seized-silk-road-bitcoins

venture capitalist Tim Draper.[116] The auction is indicative that the U.S. recognizes the legality of Bitcoin. The remaining 144,336 bitcoins are still held by the authorities pending the outcome of the Ulbricht's trial which starts in January 2015.[117]

In the six months following the shut-down of Silk Road, new dark markets proliferated and the number of illicit goods and services listings totaled more than 32,000 by March 2014, almost triple the listings found on Silk Road in 2013.[118]

Previous virtual currencies used for illicit transactions have been shut down by the U.S. Department of Justice. The first was E-Gold, which operated within the U.S., and more recently Liberty Dollar, which was incorporated in Costa Rica. E-gold, founded in 1996, was a centralized virtual currency which was backed by precious metals. Before it was shut down it had more than $60 million dollars in deposits and more than 4 million user accounts. E-gold allowed users to create accounts without any identification requirements, and soon became a mechanism used by criminals for illicit transactions and money laundering.[119] In 2008 e-gold and its three directors pleaded guilty to charges of "conspiracy to engage in money laundering and the "operation of an unlicensed money transmitting business".[120] After the failure of E-Gold and the criminal conviction of those involved, defendant Arthur Budovsky immigrated to Costa Rica and incorporated Liberty Reserve, a payment system specifically designed to "succeed in eluding law enforcement outside the U.S."[121] Liberty Reserve was shut down in 2013 on the grounds that it facilitated money laundering in excess of $6 billion during its existence. Liberty Reserve required account holders to declare their

---

[116] Silk Road Bitcoin Auction Winner Tim Draper Won't Say How Many Millions He Paid. *Forbes,* 2014, (accessed 25 October 2014), http://www.forbes.com/sites/kashmirhill/2014/07/02/tim-draper-silk-road-bitcoin-auction/

[117] The funds are held in the following address: https://blockchain.info/address/1i7cZdoE9NcHSdAL5eGjmTJbBVqeQDwgw

[118] Wong, J. I., 'Dark Markets Grow Bigger and Bolder in Year Since Silk Road Bust', CoinDesk, 2014, (accessed 20 October 2014), http://www.coindesk.com/dark-markets-grow-bigger-bolder-year-since-silk-road-bust/

[119] Foley, S. 'Bitcoin needs to learn from past e-currency failures'. *The Financial Times.* 2014. (accessed 25 October 2014). http://www.ft.com/cms/s/2/6d51117e-5806-11e3-a2ed-00144feabdc0.html

[120] Wenzel, R. 'Bitcoiners: Remember What Happened to eGold'. *Economic Policy Journal.* 2013. (accessed 24 October 2014). http://www.economicpolicyjournal.com/2013/04/bitcoiners-remember-what-happened-to.html

[121] Trautman, L., 'Virtual Currencies Bitcoin & What Now After Liberty Reserve, Silk Road, and Mt. Gox?', *Richmond Journal of Law & Technology Volume XX(4),* 2014, pp 86, (accessed 28 October 2014). http://jolt.richmond.edu/v20i4/article13.pdf,

identity, address and birth date, yet did not require any documentation to support these declarations, and the content of the declaration had no effect on the validity of the account.[122]

Decentralized virtual currencies like Bitcoin present difficult law enforcement challenges since no central point can be targeted, and it is impossible to regulate the system itself and enforce obligatory registration or know your customer procedures. The online drug trade industry is developing at a rapid pace and presents new enforcement difficulties. James Martin(2014), a drugs trade researcher states:

> "With online drug trading, you have hidden financial transactions; the dealer and customer never meet in the same place; you have drugs arriving in the post [...] all of this breaks the 'business model' of conventional law enforcement."[123]

5.3 Risk to regulators

This section addresses the risks faced by regulatory authorities. At this early point in the existence of decentralized virtual currencies, most authorities regulate its use under existing legislation as either a currency or as an asset, depending on whether it is used as a means of exchange or as a speculative investment. If the acceptance of decentralized virtual currencies increase and amount to a greater economic significance, specific legislation and perhaps new regulatory bodies might be needed on account of the unique nature of these virtual currencies. Regulators face reputational risks, and risks regarding the competitive objectives within the economy.

Regulatory authorities face reputational risks. If the chosen regulatory response is ineffective the credibility of the regulators would be undermined. In the event of under-regulation, the risks faced by users and the threats to financial integrity would be unmitigated. Since virtual currencies offer the same services as traditional payment systems while falling outside current regulations applicable to payment systems, the regulators objective of ensuring well-functioning payment systems is undermined. [124]

In the case of over-regulation, states risk driving away technological innovation and the economic activity to other countries, given Bitcoin's borderless nature. It must be understood that Bitcoin is a protocol on which a currency is able to function, just as HTTP is the Internet protocol on which email is able to function. It is impossible to predict all future applications

[122] *Ibid.*

[123] *Ibid.*

[124] European Central Bank, 'EBA Opinion on 'virtual currencies'. *2014. EBA/Op/2014/08*. pp 36.

of the Bitcoin protocol or different implementations of block chain technology at this point in its development, just as it was impossible to predict all future applications of the internet in 1994.

5.4 Risk of undermining the State´s monopoly on currency.

In modern states using fiat currency systems, the state exerts control over the money supply and uses it to steer the economy and control inflation. Through central banks, states are able to actively strengthen and stabilize the economy through promoting employment, stable prices, and moderate long-term interest rates.[125] To effectively pursue these goals, Central banks require a high degree of control over the currency. The central banking institution exerts control over the money supply mainly through open market operations. Open market operations as the dominant form of monetary policy, refers to the central bank´s participation in the market for government bonds. By buying or selling bonds in the public market, the central bank is able to expand or contract the money supply, which influences the federal funds rate (the interest rate applicable on short term interbank loans). Changes in the federal funds rate has a cascading effect on the economy by influencing general interest rates.[126] Lower interest rates make borrowing money cheaper and saving money less profitable, and thus encourages borrowing over saving. Increased borrowing equates to increased spending and thus, increased economic activity. With lower interest rates, more money enters circulation, increasing economic growth and leads to an increased rate of inflation. A central bank aims to maintain a low, positive rate of inflation in order to discourage holding on to money. With a positive rate of inflation, money loses purchasing power over time and people are encouraged to spend and invest their money in order to increase (or at least maintain) their purchasing power. The state´s monopoly over the creation money is essential to this process, and competing or alternative currencies could undermine the effectivity of central banks.[127]

The existence and adoption of competing currencies undermines the powers of the state by creating doubt in the value of the fiat currency. This suggests the concern that competing currencies devalue the currency of the state, a process which is difficult to stop once it gains momentum.[128] States thus have an incentive to prevent competitive currencies.

---

[125] Cook, R. J., ´Bitcoins: Technological innovation or Emerging Threat?´. *The John Marshall Journal of Information Technology and Privacy Law. Volume 30(3) 535.(*2014), pp 550.

[126] *Ibid.*

[127] *Ibid.*

[128] Cook, R. J., ´Bitcoins: Technological innovation or Emerging Threat?´, *The John Marshall Journal of Information Technology and Privacy Law. Volume 30(3) 535*, 2014, pp 544.

An example of the state responding to a competing currency is the case of the Liberty Dollar in the U.S, a private commodity currency. A man named Bernard von NotHaus established the National Organization for the Repeal of the Federal Reserve and International Revenue Code (NORFED). NORFED aimed to circulate a commodity currency to serve as an alternative to the U.S. dollar called the Liberty Dollar, a private currency backed by precious metals which was launched in 1998. The purpose was to create an inflation-proof currency, which retains its purchasing power over time. As the price of silver increases over time the value of the currency increases, as opposed to fiat currency which loses value over time. The Liberty Dollar was shut down when Von NotHaus was charged for counterfeiting (due to similarities between the Liberty Dollar and the U.S dollar) in addition to charges under the U.S anti-competitive currency statute, 18 U.S.C. §486.[129] Von NotHaus was charged and convicted (2011), in part, due to his intention to compete with the U.S. dollar by circulating Liberty Dollars as if they were U.S. dollars.[130] At that time there was roughly $20 million Liberty Dollars in circulation.

When people turn to alternative currencies as a store of value instead of the local fiat currency, it reduces the overall demand for fiat currency, and thus the central banking institutions´ ability to stimulate demand.[131] If Bitcoin gains widespread adoption, it could pose a risk to the central banking institutions' ability to influence demand, and without a central authority to hold accountable or shut down, it is unclear what could be done in such a case.[132]

[129] Cook, R. J., ´Bitcoins: Technological innovation or Emerging Threat?´, *The John Marshall Journal of Information Technology and Privacy Law. Volume 30(3) 535*, 2014, pp 548.

[130] *Ibid.*

[131]Cook, R. J., ´Bitcoins: Technological innovation or Emerging Threat?´,*The John Marshall Journal of Information Technology and Privacy Law. Volume 30(3) 535*, 2014, pp 548.

[132] *Ibid.*

6. Regulation of Virtual Currencies

Due to Bitcoin's decentralized structure, pseudonymous nature of its users, and irreversibility of transactions, effective regulation of this rapidly emerging technology requires a novel approach. As Bitcoin is not created or controlled by any central entity, regulations typically applicable to the banking and the financial industry may not be suitable for Bitcoin and Bitcoin transactions.[133]

Regulators lack the ability to impose regulatory requirements (or impose accountability) upon a centralized entity that could assist with detection and prevention of illicit activity. It is not feasible to regulate senders and receivers of bitcoin since there is no requirement to exchange personally identifiable (PII) when making transactions. The costs of attempting to track all users who have not provided any PII, largely outweighs the benefit of exposing minor transactions.[134] In the event of regulation targeting users directly, it might result in users not only using methods to attain even greater anonymity, but also could cause users to lose confidence in the regulators. More efficient points of regulation are the entities within the Bitcoin economy where users are concentrated such as exchanges and payment processors. Regulation of exchanges could be feasible under existing laws that apply to money transmitters. Money transmitters are required to implement AML and KYC procedures, and obtain necessary licenses and complete registration procedures prior to being able to lawfully conduct business.[135]

Member of the Executive Board of the European Central Bank, Mr. Yves Mersch(2014) stated that given the economic size of virtual currency schemes in Europe: "virtual currencies do not pose a risk to price stability or financial stability, but do pose a risk for users. However, this user risk is more related to speculative investments and consumer protection, and not necessarily to payments."[136] This statement encapsulates the idea that regulations of this new technology should focus on mitigating risks faced by users, and regulators should be

[133] Gilbert, R. N. & Blye A. D. 'Bitcoin and Internet Payment Systems: Regulatory and Commercial Law Concerns', *Carlton Fields Jorden Burt*, 2014, (accessed 30 September 2014), http://www.cfjblaw.com/bitcoin-internet-payment-systems-regulatory-and-commercial-law-concerns/#_edn15

[134] Bryans, D. 'Bitcoin and Money Laundering: Mining for an Effective Solution. *Indiana Law Journal Vol. 89:441*. 2014. pp 472.

[135] Trautman, L. 'Virtual Currencies Bitcoin & What Now After Liberty Reserve, Silk Road, and Mt. Gox? *Richmond Journal of Law & Technology Vol.XX:4.* 2014. (accessed 28 October 2014). http://jolt.richmond.edu/v20i4/article13.pdf. pp 24.

[136] Mersch, Y. 'Efficient retail payments - key in strengthening the competitiveness and growth potential of the EU'. 2014. (accessed 25 October 2014). http://www.bis.org/review/r140324a.htm

cautious to not stifle innovation and prevent the realization of the greater economic benefits (for 'the unbanked' and the global remittances market) associated with decentralized virtual currencies.

In a survey conducted by the U.S. Law Library of congress, 40 countries were requested to provide comments of their official stances on Bitcoin.[137] The comments addressed three primary themes: That Bitcoin does not have legal tender status, aspects of consumer protection, and clarification regarding taxation.[138] The status and regulation of Bitcoin in a few notable countries will be discussed below.

Most countries have indicated that there no immediate intention to implement regulation of Bitcoin at this point in time. Many countries (Singapore, U.K., Germany, will be briefly discussed below) have provided clarification regarding tax obligations arising from the use of Bitcoin and, classifying it as an asset if it is speculated upon, and as income if used as a means of payment, but have not made specific legislation.[139] Few countries (China, Russia and Brazil will be briefly discussed below) have implemented virtual currency specific legislation, either effectively banning Bitcoin, or actively promoting its development.[140] Most recently, the U.S. Financial Crimes Enforcement Network (FinCEN) has announced that all virtual currency exchanges and payment processors may be required to obtain money services businesses licenses under U.S. Law.

In Singapore, the financial services regulator, The Monetary Authority of Singapore (MAS), does not directly regulate or interfere with Bitcoin, since virtual currencies are not considered legal tender or securities under the Securities and futures Act.[141] The MAS recognizes the potential money laundering and terrorist financing risks and consequently regulates virtual currency intermediaries (Bitcoin exchange operators and Bitcoin ATM machines) that trade or facilitate the trade of virtual currencies for fiat currencies to verify the identification of customers and to report suspicious transactions to the Commercial Affairs Department

---

[137] 'Regulation of Bitcoin in Selected Jurisdictions', *The Law Library of Congress, Global Legal Research Center,* 2014, (accessed 10 October 2014), http://www.loc.gov/law/help/bitcoin-survey/regulation-of-bitcoin.pdf

[138] Shaheen, K., 'Regulation of Bitcoin around the world´. *Lexology, Dentons,*2014, (accessed 18 October 2014), http://www.lexology.com/library/detail.aspx?g=d92a33fe-3f11-43f6-b0cf-d8476ca612b1

[139] Shaheen, K., 'Regulation of Bitcoin around the world´. *Lexology, Dentons.*2014, (accessed 18 October 2014), http://www.lexology.com/library/detail.aspx?g=d92a33fe-3f11-43f6-b0cf-d8476ca612b1

[140] *Ibid*.

[141] Monetary Authority of Singapore, 'Reply to Parliamentary Question on Virtual Currencies', Notice Paper 62, 2014, (accessed 30 September 2014), http://www.mas.gov.sg/news-and-publications/parliamentary-replies/2014/reply-to-parliamentary-question-on-virtual-currencies.aspx

(effectively treating it as money).[142] Regarding taxation, The Inland Revenue Authority of Singapore (IRAS) states that virtual currency is not treated as currency or goods, but as a 'supply of services'. When users purchase goods or services with virtual currency, the IRAS considers the transaction a 'barter trade' with two suppliers, both of which are taxed as service suppliers.[143]

The United Kingdom announced that it will treat Bitcoins like any other form of payment for tax purposes: Value Added Tax will be due in the normal way from suppliers of any goods or services sold in exchange for Bitcoins. The Bank of England has released two comprehensive reports regarding virtual currencies in which it concludes that Bitcoin currently does not "pose a material risk to monetary and financial stability in the U.K." given the small size when compared to the sterling. [144]

The German Ministry of Finance treats the commercial sale of bitcoins as a sale of 'other services' (subject to VAT) and does not recognize it as currency, legal tender or e-money in terms of payment supervision legislation.[145] [146] When Bitcoin is used by individuals as a money substitute, the Federal Financial Supervisory Authority (BaFin) qualifies bitcoins as "*Rechnungseinheiten*" (legally binding financial instrument in the category of units of account) that serves as a private means of payment in barter transactions, regardless of not being denominated in legal tender.[147] Germany's Fidor bank has integrated a virtual currency

---

[142] Monetary Authority of Singapore, 'MAS to Regulate Virtual Currency Intermediaries for Money Laundering and Terrorist Financing Risks', 2014, (accessed 30 September 2014), http://www.mas.gov.sg/news-and-publications/media-releases/2014/mas-to-regulate-virtual-currency-intermediaries-for-money-laundering-and-terrorist-financing-risks.aspx

[143] Inland Revenue Authority of Singapore, 'GST treatment for e-Commerce transactions: Sale of virtual currency', 2014, (accessed 30 September 2014), http://www.iras.gov.sg/irashome/page04.aspx?id=2276

[144]'Digital currencies: Quarterly Bulletin 2014 Q3 pre-release articles'. 2014. (accessed 15 October 2014). http://www.bankofengland.co.uk/publications/Pages/quarterlybulletin/2014/qb14q3prereleasedigitalcurrenciesbitcoin.aspx

[145] 'German Ministry of Finance declares Bitcoin payments sales-taxable', *The Bundesverband Bitcoin, German affiliate of the Bitcoin Foundation* , 2014, (accessed 30 September 2014), http://www.bundesverband-bitcoin.de/?p=221

[146]Payment Services Supervision Act of 25 June 2009 (Federal Law Gazette 1, p. 1506), as amended by Article 2 subsection (74) of the Act of 22 December 2011 (Federal Law Gazette I, p. 3044)

[147] German Federal Financial Supervisory Authority, 'BaFin Annual Report 2013', 2014 , pp.58. (accessed 30 September 2014), http://www.bafin.de/SharedDocs/Downloads/EN/Jahresbericht/dl_annualreport_2013.pdf?__blob=publicationFile

called Ripple. Since September 2014, Fidor allows customers to complete international wire transfers via the Ripple protocol.[148]

Countries that have banned or severely regulated virtual currencies include Russia and China. The Russian Ministry of Finance announced a legislation initiative that would "recognize the act of engaging in Bitcoin transactions as a misdemeanor and impose fines for "transactions with a cybercurrency and creation and distribution of software used for the issuance of monetary surrogates" in an amount up to the equivalent of $30,000."[149] In China, Bitcoin is treated as a special virtual commodity, and banks and payment institutions are prohibited from dealing in Bitcoin or providing services which are directly or indirectly related to Bitcoin.[150]

On the other side of the spectrum some countries have taken step towards recognition and regulation of Bitcoin as a valid currency. Brazil enacted legislation in late 2013 which created the possibility "for the normalization of mobile payment systems and the creation of electronic currencies" which includes Bitcoin.[151] The Brazilian tax authority have announced that as a financial asset- bitcoin transactions are subject to capital gains tax, but only if capital gains exceed $15,000. Such a framework is effective in collecting taxes from investors, without obstructing the activities of bitcoins users that use it as a means of payment.[152]

In the U.S., Bitcoin is regarded as a currency without legal tender status by the Financial Crimes Enforcement Network (FinCEN). Regarding taxation: When Bitcoin is received as payment for goods or services, it forms part of general income and is subject to taxation. Miners rewards are includible in gross income, and thus also subject to income tax.[153] Bitcoins are also treated as an asset which is subject to capital gains tax, but there is no exemption threshold as under the Brazilian legislation. On 27 October, 2014, FinCEN

[148] Carney, M., 'German's Fidor bank will begin using Ripple for international wire transfers next week.' *Pando Daily*.http://pando.com/2014/08/22/germans-fidor-bank-will-begin-using-ripple-for-international-wire-transfers-next-week/.

Fidor Bank, 2014, https://www.fidor.de/faq/ripple

[149] 'Russia: Fines for Bitcoin Transactions Will Be Introduced'. (accessed 25 October 2014). http://www.loc.gov/lawweb/servlet/lloc_news?disp3_l205404151_text

[150] 'Regulation of Bitcoin in Selected Jurisdictions'. *The Law Library of Congress, Global Legal Research Center.* 2014. (accessed 10 October 2014). http://www.loc.gov/law/help/bitcoin-survey/regulation-of-bitcoin.pdf

[151] *Ibid.*

[152] De Filipi, P., 'Bitcoin: a regulatory nightmare to a libertarian dream'. *Internet Policy Review Vol. 3:2.* 2014. (accessed 20 October 2014), http://policyreview.info/articles/analysis/bitcoin-regulatory-nightmare-libertarian-dream

[153] BitLegal. United States, 2014, (accessed 31 October 2014). http://bitlegal.io/nation/US.php

released new guidelines for Bitcoin related companies such as exchanges and payment processors.[154] The guidelines state that these companies may be considered money services businesses (MSB) under U.S. law. MSB must register with FinCEN to obtain money transmitter licenses, which are issued on a State level. This means that these companies must acquire a money transmitter license, for each state in which they do business. Acquiring money transmitter licenses for all 53 states is a costly and time consuming process. The estimated cost to become a licensed money transmitter in all 53 states amount to almost US$200,000 (surety bond fees, application fees, investigative fees etc.) and would take between one and three years.[155] These licensing requirements would greatly hamper the proliferation of these types of companies and limit entry into the market to those backed by large investors. As mentioned, these licenses are required for each state the company wishes to conduct business in. The New York Department of Financial Services (DFS) are actively developing a unique, virtual currency specific, called BitLicense. The DFS proposed the BitLicense regulatory framework in July 2014, which would require virtual currency businesses to be subject to specific capital requirements, financial examinations, recordkeeping and reporting requirements. The capital requirements include that the licensee must invest retained earnings and profits "only in high-quality, investment-grade permissible investments with maturities of up to one year and denominated in US dollars."[156] The BitLicense framework aims to impose AML and KYC requirements for virtual currency related companies, in order to aid law enforcement and also to improve consumer protection, while still encouraging innovation. The proposal was open to public comment until October 2014, and was heavily criticized by the virtual currency community. Circle Internet Financial Inc., one of the largest virtual currency businesses, stated:

> Circle believes there are numerous areas in the Proposed Rule, which could negatively impact consumers and businesses that wish to utilize digital currencies. There are several requirements that are so burdensome (and in some cases nearly impossible to

---

[154] FinCEN. 'Request for Administrative Ruling on the Application of FinCEN's Regulations to a Virtual Currency Payment System'.2014. http://www.fincen.gov/news_room/rp/rulings/pdf/FIN-2014-R012.pdf

[155] 'Money Transmitter Licensing'. *Grimes Law PPLC*,.2014, (accessed 30 October 2014), http://www.grimeslawaz.com/technology-and-licensing/money-transmitter-licensing/
To maintain the license would amount to approximately US$135,000 per annum.

[156] 'New York Proposes BitLicense Regulations for Virtual Currency Businesses', *Cleary Gottlieb*, 2014, (accessed 30 October 2014), http://www.cgsh.com/files/News/fb453ee8-2b46-404e-8922-c8e02d700c9e/Presentation/NewsAttachment/f3db9861-69e3-45bb-a7d4-ca408760ed24/New%20York%20Proposes%20BitLicense%20Regulations%20for%20Virtual%20Currency%20Businesses.pdf

> comply with) that if the Proposed Rule were to be enacted in its current form, Circle would have no choice but to exclude New York residents from its service.[157]

If the one of the largest virtual currency companies consider the requirements overly burdensome, there is little doubt that smaller companies would be able to comply. Voorhees states:

> "This will eliminate the college dorm room startup. It will eliminate the young entrepreneur who is willing to put in 100 hours per week, but who doesn't have $100,000 for his first two months of legal bills. It will make innovation the purview of large companies, which is to say, it will diminish innovation."[158]

Some Bitcoin related companies such as SatoshiBet, a large Bitcoin gambling website, have started excluding all U.S. citizens from accessing their services on account of the expected regulatory framework which is to be implemented in 2015.[159]

Regulators face a difficult task of mitigating the various risks associated with decentralized virtual currencies, and must find a way to protect consumers and prevent illegal activity that is not only cost-effective for regulators, but also allows the legitimate entities in the virtual currency economy to keep innovating and further developing these technologies.

7. Conclusion

Decentralized virtual currencies have rapidly become a reality and continues to evolve at an unprecedented rate. Bitcoin has emerged as potential new form of money which performs the functions of money in an innovative manner that does not rely on a central authority to facilitate transactions or confirm account balances. The absence of a central authority acting as an intermediary to transactions creates new opportunities, but also new potential risks. Users are able to independently, irreversibly and securely transfer value over the internet, with low transaction costs. With Bitcoin, the unbanked could become part of the global economy and the international migrant economy could be changed for the better. However, Bitcoin creates also complicated challenges for users and regulators, on due to its volatility and pseudonymous nature. On account of its pseudonymous nature, Bitcoin has been associated

[157] Tucker, M. 'Circle Submits Comments to NYDFS on Proposed BitLicense'. (accessed 30 October 2014). https://www.circle.com/en/2014/10/20/circle-submits-comments-nydfs-proposed-bitlicense

[158] 'Industry Reactions to New York's BitLicense Proposal', *CoinDesk* 2014, (accessed 30 October 2014), http://www.coindesk.com/new-york-bitlicense-views-inside-bitcoin-industry/

[159] 'SatoshiBet not planning to withdraw from more markets despite US exit', (accessed 31 October 2014), http://www.totallygaming.com/news/satoshibet-not-planning-withdraw-more-markets-despite-us-exit

with facilitating transactions for illicit goods and services, and could serve as a sophisticated tool for money laundering. Regulators have a difficult task of mitigating the risks associated with Bitcoin in a manner that does not drive technological innovation and the related economic development out of their borders.

Bitcoins primary innovation is the global public ledger, in which all transactions are recorded, and which is updated and secured by the entire network. This invention is still in early stages of its development: its evolution and future iterations cannot be accurately predicted. It is comparable how the internet was perceived in 1994. This analogy is formulated by Jimmy (2014) on Bit Blogger:

> Around 1994, the people that did anything on the internet at all were using it mostly for email. Some more savvy users maybe participated in newsgroups. A few very bleeding-edge people made web pages. You could have foreseen that there would be better versions of those things. What you couldn't foresee was stuff like VOIP [such as skype], Bittorrent [peer-to-peer downloads], video on demand or social networks. These are all technologies built on top of the internet and currently take up a large part of the traffic that goes through it.
>
> Email for most people in the 90′s was the first great killer app. It allowed people to communicate with each other without sending letters or making phone calls. Most people that knew about the internet in the early 90′s pointed to the post office as the first industry to get disrupted by the internet and to some degree they were right. What most people didn't see back then was that the internet would also disrupt the music store, the video rental store and to some degree, even the book store. In the same way, for most people bitcoin is a way to send money easily, so they point to Western Union and other money transmission businesses as the ones that will get disrupted. To a large degree they're right, but it's not the only one that'll get disrupted.[160]

Noteworthy applications that already exist include Counterparty (decentralized stock exchange based on block chain technology) , Ripple (decentralized money transfer), Storj.io (decentralized version of Dropbox), Proof of Existence (anonymously and securely store an online time-stamped distributed proof of existence for any document), BitPesa (remittance service for sending funds to Kenya), and OpenBazaar (open source, decentralized, cost free

[160] http://www.bitblogger.net/2014/07/10/the-great-unknown-bitcoin-killer-app/

marketplace). [161] Two exciting Swiss based projects that are yet to be launched include Ethereum and Monetas. Ethereum allows developers to build and publish their own distributed applications, potentially allowing decentralized secure forms of voting, domain name registries, financial exchanges, crowd-funding, company governance, smart contracts, intellectual property and even smart property through hardware integration. [162] Monetas, focused on financial inclusion, is developing a consumer mobile phone application to enable the unbanked masses to access to the global economy, as well as a "turnkey enterprise platform" that enables users to quickly and cheaply create businesses, complete with legal entity and payment system, all from a mobile phone.[163]

The invention of distributed ledger technologies will force various industries to become more competitive in the not-so-distant future. Tasks that up until the invention of Bitcoin required a trusted central authority can now be automated and become cheaper, quicker, more predictable and more secure than ever before. Block chain technology is here to stay, and while it is still relatively complicated and potentially risky to use, it is becoming more user friendly by the day. If mass consumer adoption becomes a reality, block chain applications could revolutionize the way we bank, transact and manage our assets.

[161] 'Startups around BlockChain technology`, 2014, (accessed on 30 October 2014), http://www.adesblog.com/startups-around-blockchain-technology/, http://counterparty.io/, https://ripple.com/, http://storj.io/, http://www.proofofexistence.com/, https://www.bitpesa.co/, https://openbazaar.org/.

[162] Ethereum, (accessed 25 October 2014), https://www.ethereum.org/

[163] Monetas Product Overview, (accessed 25 October 2014), http://monetas.net/products/

List of References

Ali, R. Barrdear, J. Clews, R. Southgate, J., 'The economics of digital currencies', *Bank of England Quarterly Bulletin2014 Q3,* 2014, (accessed 5 October 2014), http://www.bankofengland.co.uk/publications/Documents/quarterlybulletin/2014/qb14q3digitalcurrenciesbitcoin2.pdf

Antonopoulos, A. M., *Mastering Bitcoin: Unlocking digital crypto-currencies,* O'Reily Media, 2014.

Bamford, C., *Principles of International Financial Law*, Oxford: Oxford University Press, 2011.

Bell, S., 'The Hierarchy of Money', *The Jerome Levy Economics Institute. Working paper No. 231.* 1998.

'Bitcoin - Turbulent Waters - Part Seven', *Dorsey & Whitney LLP,* 2014. (Accessed 20 October 2014), http://www.dorsey.com/eu_cm_bitcoin_virtual_currency_pt7/

BitLegal. United States, 2014, (accessed 31 October 2014). http://bitlegal.io/nation/US.php

'Blocks', (accessed 25 October 2014), http://blockchain.info/blocks

Bryans, D., 'Bitcoin and Money Laundering: Mining for an Effective Solution', *Indiana Law Journal Vol. 89:441*, 2014.

Carney, M. 'German's Fidor bank will begin using Ripple for international wire transfers next week.' *Pando Daily*.http://pando.com/2014/08/22/germans-fidor-bank-will-begin-using-ripple-for-international-wire-transfers-next-week/.

Chavez-Dreyfuss, G. 'Exclusive: Overstock CEO says bitcoin sales to add 4 cents to 2014 EPS'. 2014. (Accessed 14 October 2014). http://www.reuters.com/article/2014/08/13/us-overstock-com-bitcoin-idUSKBN0GD21220140813

Cirasino, M. 'How can we cut the high costs of remittances to Africa)'. 2013. (Accessed 20 October 2014), http://blogs.worldbank.org/psd/how-can-we-cut-the-high-costs-of-remittances-to-africa

Circle Financial Inc, 2014, (accessed on 25 October 2014), https://www.circle.com/en

Committee on Payment and Settlement Systems, 'The role of central bank money in payment systems', *Bank for International Settlements*, 2003.

CoinDesk. 'Bitcoin ATM Map'. (accessed on 26 October 2014). http://www.coindesk.com/bitcoin-atm-map/

Conde, J. 'Merchant Accounts 101'. 2013. (accessed 10 October 2014). http://www.merchant-account-services.org/article/merchant-accounts-101/11

Cook, R. J., ´Bitcoins: Technological innovation or Emerging Threat?´. *The John Marshall Journal of Information Technology and Privacy Law. Volume 30(3) 535.* 2014.

De Filipi, P., 'Bitcoin: a regulatory nightmare to a libertarian dream'. *Internet Policy Review Vol. 3:2.* 2014. (accessed 20 October 2014), http://policyreview.info/articles/analysis/bitcoin-regulatory-nightmare-libertarian-dream

'Digital currencies: Quarterly Bulletin 2014 Q3 pre-release articles'. 2014. (accessed on 15 October 2014). http://www.bankofengland.co.uk/publications/Pages/quarterlybulletin/2014/qb14q3prereleasedigitalcurrenciesbitcoin.aspx

Dourado, E & Brito, J., 'Cryptocurrency, The New Palgrave Dictionary of Economics'. Eds. Steven N. Durlauf and Lawrence E. Blume, Palgrave Macmillan, 2014, (accessed 20 October 2014). http://www.dictionaryofeconomics.com/article?id=pde2014_C000625

Eatwell, J., Milgate, M., & Newman, P.*The new Palgrave dictionary of economics*, London:Macmillan, 2008.

Ethereum, (accessed 25 October 2014), https://www.ethereum.org/

European Central Bank, 'Virtual Currency Schemes'. 2012. (accessed 10 October 2014), http://www.ecb.europa.eu/pub/pdf/other/virtualcurrencyschemes201210en.pdf

European Central Bank, 'EBA Opinion on 'virtual currencies', *EBA/Op/2014/08*, 2014.

'Exchanges',(accessed 25 October 2014)https://en.bitcoin.it/wiki/Exchanges

Fidor Bank. 2014. https://www.fidor.de/faq/ripple

FinCEN. 'Request for Administrative Ruling on the Application of FinCEN's Regulations to a Virtual Currency Payment System'.2014. http://www.fincen.gov/news_room/rp/rulings/pdf/FIN-2014-R012.pdf

FinCEN. 'Statement of Jennifer Shasky Calvery, Director Financial Crimes Enforcement Network United States Department of the Treasury'. *United States Financial Crimes Enforcement Network.* 2013.

Foley, S. 'Bitcoin needs to learn from past e-currency failures'. *The Financial Times.* 2014. (accessed 25 October 2014). http://www.ft.com/cms/s/2/6d51117e-5806-11e3-a2ed-00144feabdc0.html

'German Ministry of Finance declares Bitcoin payments sales-taxable', *The Bundesverband Bitcoin, German affiliate of the Bitcoin Foundation* , 2014, (accessed 30 September 2014), http://www.bundesverband-bitcoin.de/?p=221

German Federal Financial Supervisory Authority, 'BaFin Annual Report 2013', 2014 , pp.58. (accessed 30 September 2014), http://www.bafin.de/SharedDocs/Downloads/EN/Jahresbericht/dl_annualreport_2013.pdf?__blob=publicationFile

Gilbert, R. N. & Blye A. D. 'Bitcoin and Internet Payment Systems: Regulatory and Commercial Law Concerns', *Carlton Fields Jorden Burt*, 2014, (accessed 30 September 2014), http://www.cfjblaw.com/bitcoin-internet-payment-systems-regulatory-and-commercial-law-concerns/#_edn15

Goodhart, C. A. E., 'The two concepts of money: Implications for the analysis of optimal currency areas.' *European journal of political economy*, *14*(3). 1998.

'Hackers hit web accounts of MtGox boss', *BBC Technology News,* 2014. (Accessed 20 October 2014). http://www.bbc.com/news/technology-26387800

Hern, A., 'US government prepares to auction $17m of seized Silk Road bitcoins', *The Guardian.* 2014. (Accessed 24 Octber 2014), http://www.theguardian.com/technology/2014/jun/24/us-auction-seized-silk-road-bitcoins

How to Set Up a Merchant Account'. 2011. (Accessed 10 October 2014). http://paysimple.com/blog/2011/09/07/how-to-set-up-a-merchant-account/

'How it Works, (accessed 25 October 2014),https://bitcoin.org/en/how-it-works

'How Bitcoin Works, (accessed 25 October 2014), https://en.bitcoin.it/wiki/How_bitcoin_works

Inland Revenue Authority of Singapore. 'GST treatment for e-Commerce transactions: Sale of virtual currency', 2014, (accessed 30 September 2014), http://www.iras.gov.sg/irashome/page04.aspx?id=2276

'Industry Reactions to New York's BitLicense Proposal', *CoinDesk* 2014, (accessed 30 October 2014), http://www.coindesk.com/new-york-bitlicense-views-inside-bitcoin-industry/

Ikeda, Y., 'Carl Menger's Monetary Theory: A Revisionist View'. *Keio University, Department of Economics,* 2008.

Jevons, W. S. 'Money and the Mechanism of Exchange'. *Library of Economics and Liberty.* 1876. (accessed on 28 October 2014). http://www.econlib.org/library/YPDBooks/Jevons/jvnMME5.html

Jimmy, 'The Great Unknown Bitcoin Killer App', 2014, (accessed 30 October 2014), http://www.bitblogger.net/2014/07/10/the-great-unknown-bitcoin-killer-app/

Lamport, L., Shostak, R and Pease, M., 'The Byzantine Generals Problem, ACM Transactions on Programming Languages and Systems', July 1982, pages 382-401, as summarized by Jacobson, E. (accessed 6 October 2014), http://pages.cs.wisc.edu/~swift/classes/cs739-sp11/blog/2011/02/the_byzantine_generals_problem.html

Lo, S. Wang, J. C. 'Bitcoin as Money?'. *Current Policy Perspectives, Federal Reserve Bank of Boston No 14-4.* 2014.

Mankiw, N. G. & Taylor, P.M., *Economics. 2nd ed.* Andover : South-Western Cengage Learning, 2011.

Menger, C., 'On the Origins of Money'. *Economic Journal, Vol 2*, 1892, pp. 239-255.

Mersch, Y. 'Efficient retail payments - key in strengthening the competitiveness and growth potential of the EU'. 2014. (accessed on 25 October 2014). http://www.bis.org/review/r140324a.htm

Monetary Authority of Singapore, 'MAS to Regulate Virtual Currency Intermediaries for Money Laundering and Terrorist Financing Risks', 2014. (accessed 30 September 2014), http://www.mas.gov.sg/news-and-publications/media-releases/2014/mas-to-regulate-virtual-currency-intermediaries-for-money-laundering-and-terrorist-financing-risks.aspx

Monetas Product Overview, (accessed 25 October 2014), http://monetas.net/products/

'Money Transmitter Licensing'. *Grimes Law PPLC,*.2014, (accessed 30 October 2014), http://www.grimeslawaz.com/technology-and-licensing/money-transmitter-licensing/

Morphy, E., 'Bitcoin? Yawn. CheapAir Is Now Taking Litecoin and Dogecoin.', *Forbes*, 2014, (accessed 30 September 2014), http://www.forbes.com/sites/erikamorphy/2014/09/03/bitcoin-yawn-cheapair-is-now-taking-litecoin-and-dogecoin/

Nakamoto, S., 'Bitcoin: A Peer-to-Peer Electronic Cash system.', 2008, (accessed 30 September 2014), https://bitcoin.org/bitcoin.pdf

Nakamoto, S., Bitcoin Forum Post, 2009 (accessed 15 October 2014), https://bitcointalk.org/index.php?topic=99631.0

'New York Proposes BitLicense Regulations for Virtual Currency Businesses', *Cleary Gottlieb*, 2014, (accessed on 30 October 2014), http://www.cgsh.com/files/News/fb453ee8-2b46-404e-8922-c8e02d700c9e/Presentation/NewsAttachment/f3db9861-69e3-45bb-a7d4-ca408760ed24/New%20York%20Proposes%20BitLicense%20Regulations%20for%20Virtual%20Currency%20Businesses.pdf

Olafsonn, I. A., 'Is Bitcoin Money?: An analysis from the Austrian school of economic thought'. *Haskoli Islands University*, 2014.

Pacia, C., 'Bitcoin Mining Explained Like You're Five: Part 1 – Incentives', 2014, (accessed 10 October 2014) http://chrispacia.wordpress.com/2013/09/02/bitcoin-mining-explained-like-youre-five-part-1-incentives/
Payment Services Supervision Act of 25 June 2009 (Federal Law Gazette 1, p. 1506), as amended by Article 2 subsection (74) of the Act of 22 December 2011 (Federal Law Gazette I, p. 3044)

'Regulation of Bitcoin in Selected Jurisdictions'. *The Law Library of Congress, Global Legal Research Center.* 2014. (accessed on 10 October 2014). http://www.loc.gov/law/help/bitcoin-survey/regulation-of-bitcoin.pdf

'Regulation of Bitcoin in Selected Jurisdictions'. *The Law Library of Congress, Global Legal Research Center.* 2014. (accessed 10 October 2014). http://www.loc.gov/law/help/bitcoin-survey/regulation-of-bitcoin.pdf

Ron, D. Shamir, A., 'How Did Dread Pirate Roberts Acquire and Protect His Bitcoin Wealth?', *Department of Computer Science and Applied Mathematics, The Weizmann Institute of Science, Israel*, 2013.

'Russia: Fines for Bitcoin Transactions Will Be Introduced'. (accessed 25 October 2014). http://www.loc.gov/lawweb/servlet/lloc_news?disp3_l205404151_text

'SatoshiBet not planning to withdraw from more markets despite US exit', (accessed 31 October 2014), http://www.totallygaming.com/news/satoshibet-not-planning-withdraw-more-markets-despite-us-exit

Semenova, A. 'The Origin of Money: Enhancing the Chartalist Perspective'. *CFEPS*. 2007.
Shaheen, K. 'Regulation of Bitcoin around the world´. *Lexology, Dentons.*2014. (accessed on 18 October 2014). http://www.lexology.com/library/detail.aspx?g=d92a33fe-3f11-43f6-b0cf-d8476ca612b1

Silk Road Bitcoin Auction Winner Tim Draper Won't Say How Many Millions He Paid. *Forbes.* 2014. (accessed 25 October 2014). http://www.forbes.com/sites/kashmirhill/2014/07/02/tim-draper-silk-road-bitcoin-auction/

Starr, R. M., 'Why is there money? Endogenous derivation of "money" as the most liquid asset: A class of examples.', *Economic Theory, 21(2/3),* 2003.
Starr, R. M., 'Money: in transactions and finance'. *Dept. of Economics, University of California, San Diego*. 1998.

'State of Bitcoin Q3 2014', CoinDesk, 2014, (accessed 20 October 2014). http://www.slideshare.net/CoinDesk/state-of-bitcoin-q3-2014?qid=a856ddfe-f3e9-4f61-8fa1-b60ba2340d19&v=qf1&b=&from_search=1

Trautman, L., 'Virtual Currencies Bitcoin & What Now After Liberty Reserve, Silk Road, and Mt. Gox?', *Richmond Journal of Law & Technology Volume XX(4),* 2014, pp 86, (Accessed 28 October 2014). http://jolt.richmond.edu/v20i4/article13.pdf.

Tucker, M. 'Circle Submits Comments to NYDFS on Proposed BitLicense'. (accessed 30 October 2014). https://www.circle.com/en/2014/10/20/circle-submits-comments-nydfs-proposed-bitlicense

'Vocabulary', (accessed 25 October 2014),https://bitcoin.org/en/vocabulary

'Weaknesses',(accessed 25 October 2014), https://en.bitcoin.it/wiki/Weaknesses#Attacker_has_a_lot_of_computing_power

Wenzel, R. 'Bitcoiners: Remember What Happened to eGold'. *Economic Policy Journal.* 2013. (accessed 24 October 2014). http://www.economicpolicyjournal.com/2013/04/bitcoiners-remember-what-happened-to.html

Wilber, D. Q., 'Woman With Printer Shows the Digital Ease of Bogus Cash', *Bloomberg*, 2014, (accessed 20 October 2014), http://www.bloomberg.com/news/2014-05-07/mom-with-hp-printer-shows-the-digital-ease-of-bogus-cash.html

'What can you buy with Bitcoins?',*Coindesk,* 2014, (accessed 29 September 2014), http://www.coindesk.com/information/what-can-you-buy-with-bitcoins/
Wong, J. I., 'Dark Markets Grow Bigger and Bolder in Year Since Silk Road Bust', CoinDesk, 2014, (accessed 20 October 2014), http://www.coindesk.com/dark-markets-grow-bigger-bolder-year-since-silk-road-bust/

World Bank, 'Financial Inclusion'. Global Financial Development Report 2014. (acessed 14 October 2014). http://econ.worldbank.org/WBSITE/EXTERNAL/EXTDEC/EXTGLOBALFINREPORT/0,,contentMDK:23489619~pagePK:64168182~piPK:64168060~theSitePK:8816097,00.html

Wright, G. 'Is bitcoin good for business?' *Global Finance, 28*(6). 2014. (accessed 10 October). http://bitcoinchamberofcommerce.com/?p=448