Bitcoin, the wrong implementation of the right idea at the right time

Andres Guadamuz and Chris Marsden (Sussex)

Table of Contents

This paper is an experimental investigation into virtual currencies conducted over three years[1], into the highly publicised and therefore highly contentious and bubbly atmosphere around virtual currencies. It uses the CAMPO methodology developed by social scientists in the Internet Science community, notably Moranda and Pavan[2]. In this paper, we provide the methodology in a table. We explain in CAMPO format why virtual currencies are of interest, how self-regulation has failed, and what useful lessons can be learned. We are hopeful that the full paper will produce useful and semi-permanent findings into the usefulness of virtual currencies in general,

[1] See Technollama (2011-14) at http://www.technollama.co.uk/?s=bitcoin
[2] See Marsden, C., Pavan E. et al (2013) Deliverable 6.1: Overview of user needs analysis, plus draft catalogue of design responses to needs analysis, Internet Science Consortium at http://www.internet-science.eu/biblio/reports

block chains as a means of mining currency, and the profundity of current 'media darling' currency Bitcoin as compared with the development of block chain generator Ethereum.

First, here is the summary of the method and conclusions.

Table 1: CAMPO framework applied to Bitcoin

CAMPO	Description	Added value in study
Context	Bitcoin peer-to-peer, client-based, completely distributed currency that does not depend on centralised issuing bodies (a 'sovereign') to operate, the value is created by the users, and the operation is distributed using an open source client	Study based on 3-year programme of observation and interaction with Bitcoin community and supporters. Virtual currencies in wider adoption than previously. Genuine potential for valuable critique of sovereign fiat currency. Cryptographic electronic payment system that purports to be the world's first cryptocurrency.
Actors	Invented by anonymous programmer, former largest exchange Mt Gox, Ghash.io largest miner, very few large Bitcoin owners. Widespread libertarian support based on both technology and political philosophy attacking fiat sovereign currencies.	Recent studies show very concentrated Bitcoin ownership in early adopters, especially in Mt Gox. Very unstable and illiquid market creates significant uncertainty and risk for late adopters.
Methods	BitCoin users have transparency of ownership but anonymity in many transactions. Studying community dynamics difficult due to anonymity. Journalistic accounts of BitCoin markets are subject to sensationalism, hype and inaccuracy, even more so than in the earlier hype cycle for SecondLife, exacerbated by anonymity.	Significant methodology challenges to researching this 'community', if BitCoin can even be said to have created a single community, as opposed to enabling an alternate method of exchange for potentially all virtual community transactions. Relatively little academic empirical study of virtual currencies in general, until relatively recently. Ethical implications similar problems as Tor, Anonymous, Lulzsec and other anonymous hacker communities.
Practices	Illustration of dynamics observed in each case study	Subject to slowly emerging regulation by financial authorities and police forces, which appears to be driving much of the early adopter community 'underground'. Community in 2016 may not bear much resemblance to that in 2012. Dynamism of the virtual currency environment in the face of the deepening mistrust of the financial system after the 2008 crisis, research conclusions must be provisional and transient.
Outcomes	Summary of the integration between online and offline dynamics	Alternative financial system separated from the real-world sovereign and which can use code regulation with limited enforcement from offline policing. Returns the study to the libertarian self-regulated environment of early 1990s MUDs. Prospect of a tool to evade the perils of 'private profit, socialized risk' which existing large financial institutions created in the 2008-12 disaster. Further research into virtual currencies based on blockchain mining, and for their usage by virtual communities, needed to solve methodology problems for exploring environment.

1. Context: Virtual currency and virtual property[3]

There is a voluminous literature on regulation of virtual communities[4] and a fast emerging literature on Bitcoin itself[5]. Virtual communities can create social networks but also valuable goods and services for other users[6]. This value is generally exchangeable for real world currencies, as in the largest role-player community World of Warcraft with an economy measurable in the billions of US dollars (USD), though the largest social network Facebook uses sovereign currencies as do its third party games developers[7]. Most virtual community developers have historically claim ownership of everything hosted in their servers, making them the 'sovereign' in the community[8]. This may include items with real-world value, such as virtual currency converted into real cash by the means of some exchange, as when players of online games purchase gold and in-game currencies from Chinese 'gold' farmers creating tools for World of Warcraft (WoW) and other virtual communities[9]. Some virtual communities have gone further, developing virtual currencies that can be accepted in other communities. Bitcoin has taken a yet further step, as it is a virtual currency that claims to be tradeable in exactly the same fashion as sovereign currencies, yet without a sovereign.

From Facebook Credits to Bitcoin (BTC), virtual currencies have had a bumpy evolution. Most of those analysts seem to be missing the point. Virtual currencies are wildly successful in their

[3]Technollama (2013) February 11 at http://www.technollama.co.uk/virtual-currency-and-virtual-property-revisited On regulation in virtual worlds see Fitzgerald, B, F. (1997) "Life in cyberspace: a simulating experience." Computer and Telecommunications Law Review. 3(3), 136-138; Bond, R (2009) "Business trends in virtual worlds and social networks - an overview of the legal and regulatory issues relating to intellectual property and money transactions." Entertainment Law Review 20(4), 121-128; James, S. (2008) "Social networking sites: regulating the online "Wild West" of Web 2.0" Entertainment Law Review 19(2), 17-50; Petrasic, K, L. (2013) "DATA's self-regulatory quest to legitimise virtual currencies" E-Finance & Payments Law & Policy 7(9), 6-7; Taylor, M. and Matteucci, M. (2009) "Virtual worlds" Computer and Telecommunications Law Review 15(5), 124-147; Regnard-Weinrabe, B., Taylor, M and Savary, R. (2013) "Virtual currencies, the risks and the regulatory radar" E-Finance & Payments Law & Policy 7(7), 10-11.

[4] See reviews of earlier literature in Balkin , J. M. and Noveck , B. S. (eds.) (2006) The State of Play: Law and Virtual Worlds, New York University Press, Davies , T . and Noveck , B. (eds.) (2006) Online Deliberation: Design, Research, and Practice, CSLI Publications/University of Chicago Press, Noveck , B. (2006) Architecture, law and virtual worlds , First Monday 10:11 , at www. firstmonday.org/issues/issue10_11/noveck/

[5] The vast recent literature on Bitcoin and its legal challenges includes Munck, M, G. (2011) "Future payments in a disruptive digital world." E-Finance & Payments Law & Policy. 5(4), 12-13; Alleyne, A. (2010) "Virtual currencies: can they classify as property?" E-Finance & Payments Law & Policy 4(5), 14-15; Tavan, D. (2013) "A brave new Bitcoin world?" Banker Aug, 74-76; Taylor, M., Savary, R. and Regnard-Weinrabe, B. (2013) "Virtual currencies." Computers & Law. 24(3), 31-34; Anderson, T, A. (2014) "Bitcoin - is it just a fad? History, current status and future of the cyber-currency revolution" Journal of International Banking Law and Regulation. 29(7), 428-435; Courtneidge, R. (2014) "Crypto currencies and the regulators: friends after all?" E-Finance Payments Law & Policy. 8(2), 8-9; Dixon, J (2013) "The importance of an effective Bitcoin exchange market." E-Finance & Payments Law & Policy. 7(6), 6-7; Jankelewitz, E., Nemirovsky, D., Reyhani, B, I. and Vaziri, A. (2014) "Regulators respond to the big questions posed by Bitcoin" E-Finance & Payments Law & Policy 8(4), 6-8; Meek, J. (2014) "Banks "killing" bitcoin industry, expert warns." Operational Risk & Regulation. 15(5), 10; Meek, J (2014) "Funny money" Operational Risk & Regulation. 15(2), 23-25.

[6] See the review by SecondLife's co-founder Ondrejka, C. (2004) Aviators, Moguls, Fashionistas and Barons: Economics and Ownership in Second Life, at http://ssrn.com/abstract =614663

[7] On gaming and virtual currencies see Gervassis, N, J. (2004) "In search of the value of online electronic personae: commercial MMORPGs and the terms of participation in virtual communities" Journal of Information, Law & Technology 3; Anil, S., Jie, A, K, W., Min, J, S, H. and Xiu, Q, C, W. (2012) "Virtual property - a theoretical and empirical analysis" European Intellectual Property Review 34(3), 188-202; Courtneidge, R. and Lloyd, V. (2013) "Accepting Bitcoin as payment for online gambling services." World Online Gambling Law Report. 12(2), 3-4; Margaritov, D. (2014) "Bitcoin: on the frontier of online gambling innovation" World Online Gambling Law Report. 13(3), 8-9.

[8] On the role of social network gatekeepers, see Barzilai-Nahon, K. (2006) "Gatekeepers, virtual communities and the gated: multidimensional tensions in cyberspace." International Journal of Communications Law & Policy 11; Garrie, D, B. and Wong, R. (2010) "Social networking: opening the floodgates to "personal data" Computer and Telecommunications Law Review. 16(6), 167-175; Gonzalez, L, H. (2013) "Habeo Facebook ergo sum? Issues around privacy and the right to be forgotten and the freedom of expression on online social networks" Entertainment Law Review 24(3), 83-87; Gray, T., Zeggane, T. and Maxwell, W. (2008) "US and EU authorities review privacy threats on social networking sites" Entertainment Law Review 19(4), 69-74; Hicks, L. (2010) "Through the privacy wall" European Lawyer 98, 51.

[9] The existence of these exchanges is one of the premises of Neal Stephenson's novel *Reamde*, Harper Collins (2011).

respective in-game economies, they are used by millions to buy goods and services in limited virtual environments, and it has been proven that people will pay real cash to boost their online content. Take the successful FIFA series, where there is a thriving economy of card trading, where players purchase virtual cards of their favourite players. This can be done through virtual in-game currency which is earned by playing and winning games. But players can also use real money to obtain coins to boost their teams. Amazon has announced that it will be launching its own virtual currency for their Kindle app store, Amazon Coins. This move has baffled tech analysts everywhere. Why would Amazon try something that has been attempted and failed everywhere? Amazon Coins will almost certainly be used exclusively within the Kindle environment to buy content for the Kindle, such as books, music, movies and TV shows. If Amazon can even mildly replicate the most successful in-game currencies, then look for other companies to start adopting the model.

1.1 Currency basics[10]

Bitcoin is a non-fiat cryptographic electronic payment system that purports to be the world's first cryptocurrency. In other words, it is a peer-to-peer, client-based, completely distributed currency that does not depend on centralised issuing bodies (a 'sovereign') to operate, the value is created by the users, and the operation is distributed using an open source client that can be installed in any computer running Windows, Mac or Linux. In order to better understand Bitcoin, we will discuss currencies in general, and electronic currencies specifically.

Payment systems in general, and currency specifically, depend on value. Value is simply the desirability that someone allocates to something, generally material items according to our needs, such as food and shelter, or according to their scarcity, such as gold; we also give value to energy in the shape of labour. Finally, we value intangibles, such as experience, knowledge, creativity and know-how.

Currencies were invented as a means to transfer value. Initially, this was done through barter, and then people started allocating value in coins using metals that were considered inherently valuable for their scarcity. In the Renaissance in Europe[11], as coins became unwieldy, a more flexible system of value embedded in paper money was devised in order to make transactions easier, as carrying gold and silver around was insecure and expensive. The first paper notes worked as a promise to give the bearer the equivalent value in metal to the one inscribed in the document. Money therefore relied on the idea that the issuer had metal reserves that could be redeemed at any time, hence giving value to the currency. The problem with this system, called the gold or silver standard[12], is that it placed a limit on the amount of money that could be exchanged at any given time by the issuer to that which could be allocated to metal reserves, therefore creating an upper limit to the size of the economy that was equal to the available metal. When a country needed to issue more money than it had in metal reserves, such an during time of war, this would result in devaluation, as people would not trust that there were reserves that supported the money. During the 20th century the gold standard was abandoned, and a new monetary system was put in place that uses a country's wealth and economic trustworthiness as the basis for value. This is what is known as fiat[13] money.

---

[10] Technollama (2011) http://www.technollama.co.uk/is-bitcoin-legal

[11] Promissory notes developed, lost trust and were reintroduced at different periods in different societies with no exact date of introduction.

[12] Note that English 'pieces of eight' were an adaptation of 'peseta', a measure of silver in the Spanish Empire developed from its control over South American silver mines. In the Anglo-Saxon world, gold reserves discovered in Australia, South Africa, Yukon and California led to the long term adoption of the gold standard even in late capitalism, though this was reviled by populists, notably Presidential candidate William Jennings Bryan in his famous 'cross of gold' speech of 9 July 1896 calling for convertibility of gold to silver: http://historymatters.gmu.edu/d/5354/

[13] From the Latin "let it be done".

Modern fiat currencies have value based on the economic strength of the issuer. In some libertarian and anarchist circles, it is said that fiat money does not have any inherent value, but this fails to recognise that neither does the gold standard[14]. Gold does not have intrinsic value; under the right circumstances gold could be valueless except as an industrial input. In fact, there is no such thing as inherent value; all value is dependent on circumstances. The value in fiat money arises from the law, the currency has the support of the government as sovereign, and therefore, it is supported by the economy of the territory where it is accepted. Trusted governments support strongly valued currencies, though governments permitting hyperinflation can destroy that trust.

2. Actors in Bitcoin

BitCoin users have transparency of ownership but anonymity in many transactions, necessary for libertarians or outright criminals in such illicit markets as #SilkRoad. Studying community dynamics is therefore made much more difficult than even such pseudonymous or avatar based communities as Habbo Hotel, World of Warcraft or SecondLife. The ethical implications of studying such communities raise similar problems as those of Tor, Anonymous, Lulzsec and other anonymous hacker communities[15]. Journalistic accounts of BitCoin markets are largely subject to sensationalism, hype and inaccuracy, even more so than in the earlier hype cycle for SecondLife, exacerbated by the first issue of anonymity.

Bitcoin was developed in 2008 as a concept by an anonymous developer going by the pseudonym Satoshi Nakamoto, who posted a paper detailing the currency to a cryptography mailing list[16]. The paper details a decentralised system with no issuing authority that would serve as both a means of exchange but also as an anonymous and fully open log of all transactions (known as the blockchain). The value would be created by people running a client that would "mine" value by verifying transactions.

Bitcoin was devised as a non-fiat currency; in other words, its proponents claim that it has "real" value. The value arises from computing power, that is, the only way to create new coins is by allocating distributed CPU power through computer programs named "miners"; the miners create a block after a period of time that is worth an ever-decreasing amount of bitcoins in order to ensure scarcity. Each bitcoin consists of 100 million smaller units, called a satoshi. The operations performed to mine are precisely to authenticate other transactions, so the system both creates value and authenticates itself, an elegant and simple solution that is one of the appealing aspects of the currency. Once created, each Bitcoin (or 100 million satoshis) exists as a cryptographic address that is part of the block that gave birth to it. The person who mined the coin owns the address, and can transfer it by sending value to a another address, which is a "wallet" file stored in a computer. The blockchain is the public record of all transactions.

Bitcoin is simply allocating value arbitrarily to a program that performs the mathematical equations necessary to support the creation of a bitcoin. It is a self-referential and circular currency, and its only value is that which people give it, just like fiat money but with faith placed in computer programming not sovereign states.

---

[14] See Flint, D. (2014) "Computers and internet: are all modern currencies not virtual? - The Bitcoin phenomenon." Business Law Review. 35(2), 60-62; Folsom, R. and Cashman, M. (2014) "Digital currency: a primer." Computers & Law. 24(6), 27-30.

[15] Soghoian, C. (2012) *Enforced Community Standards For Research on Users of the Tor Anonymity Network*, Center for Applied Cybersecurity Research, Indiana University, also at Financial Cryptography and Data Security: Lecture Notes in Computer Science Volume 7126, pp 146-153

[16] Nakamoto S, Bitcoin: A Peer-to-Peer Electronic Cash System, (2008), https://bitcoin.org/bitcoin.pdf.

2.1 Scarcity and Economic Value in Bitcoin

An important part of the concept behind Bitcoin is that it has built-in scarcity because mining for coins becomes more difficult as time goes by and the market grows[17]. The algorithms that produce new BTC coins increase the amount of processing power necessary to create each new block, so producing new money is more difficult as time goes by, and this difficulty is built into the system to try to keep the total amount of Bitcoins at a maximum of 21 million. The first block "mined" was at difficulty 1. By June 2011, there were 131,301 blocks, making a total BTC of 6,560,000, and a difficulty of 877,227. In June 2014, there were 303,162 blocks with a total 12,800,000 BTC in existence, and a difficulty of over 10 billion (10,455,720,138). That means, making a new block is more than 10 million times more difficult than it was for the initial block. This difficulty will only go up, so an individual cannot hope to have the processing power to develop new coins, and this can only be done currently through pool mining CPU resources.

While this model is trying to replicate scarcity in the market, it acts as a punishing disadvantage for late adopters, and means that early adopters have market power if they hoarded coins early. This may have regulatory repercussions.

During its recent history, the Bitcoin economy relied very heavily on one intermediary, a Tokyo-based company called Mt.Gox. Bitcoin relies on exchanges to operate: intermediaries that will accept your "normal" currency and exchange it into bitcoins, and vice versa. There have been dozens of exchanges, as in theory literally anyone could setup their own firm. Mt.Gox was famous (or infamous depending on your point of view) for having started out as an outfit to trade 'Magic the Gathering' cards, but then evolved to be the largest exchange. Ron and Shamir found that Mt.Gox had intervened in 90% of all Bitcoin transactions ever recorded[18]. In the same study, they found that there is some large accumulation of the bulk of Bitcoin activity, for example, one single user (Mt.Gox itself) had 156,722 different addresses. This level of centrality is not good for a supposedly decentralized currency. Many blips in price prior to the crash were caused precisely by DDoS attacks against Mt.Gox. Similarly, such reliance makes the entire system less resilient and prone to catastrophic failures. BTC has built-in problems from the economic standpoint as it: encourages hoarding; benefits disproportionately early adopters; is a deflationary currency.

We next examine the political motivation for BTC users and supporters, noting that sovereign currencies reflect a political sentiment accepting when not overtly supportive of nation-states.

2.2 Political libertarian philosophy and practice of BTC

From very early on, Bitcoin has been extremely popular in libertarian circles. Any visit to a Bitcoin discussion forum provides evidence that an important core of the BTC community consists of libertarian types of all stripes, from those who want to see the end of all fiat currencies, to slightly more moderate and pragmatic supporters. A libertarian tinge permeates the currency's proponents, who attack established fiat currencies, which they see as anathema to the system of value established by the Gold Standard. However, most seem to accept that coexistence will be prevalent. A growing number of Anonymous outlets support Bitcoin. The politics of Anonymous are more difficult to pinpoint, with communitarian positions in many issues, but an anarchic movement overall. Anarchic fear and loathing of government is shared

[17] This is not unlike gold, silver and diamond reserves, though new 'finds' in these commodities due to changing mining techniques and geopolitical conditions mean that greater liquidity can arise (e.g. with entry of Warsaw Pact and many new sub-Saharan African nations into global trading system since 1990).

[18] Reynolds R, "A Bit Too Far?" Terranova (June 10, 2011), http://bit.ly/1mJtwFj. Ron D and Shamir A, "Quantitative Analysis of the Full Bitcoin Transaction Graph", Cryptology ePrint Archive: Report 2012/584 (2012), http://eprint.iacr.org/2012/584

by Randian libertarians. The common denominator is distrust of any regulatory solution and the wish to see the end of the tools of power.

Ideally, a decentralized currency should be politically neutral, strive to be efficient. Any 'revolutionary effects' would be caused by its success, not as part of a plan to bring about a libertarian utopia[19]. There is a good reason why the gold standard was abandoned, the commodity's scarcity created more problems than other options. Bitcoin is an article of faith among a small cyber-elite but not a practical alternative to sovereign-issued currency.

3. Practices

The decentralised nature of Bitcoin and lack of a 'cast list' of actors may prompt some to think that it is not possible and/or desirable to attempt to regulate the electronic currency. The fact that there is no issuing body and no central authority in charge of the payment scheme may lead one to believe that it is not even possible to undertake any sort of regulatory effort. However, Bitcoin has some practices that make some form of regulation necessary if it becomes widespread, which we investigate in Section 3.

3.1 Transparency, Anonymity and Instability

One of the main selling points of Bitcoin is its transparency. The client itself is open source, and all the transactions are open to scrutiny because all transactions must be verified by the whole, so it is possible to look at each individual transaction[20] in the public blockchain to scrutinise the outgoing and incoming wallet addresses. The addresses do not identify the person, only the possessor of the key that unlocks the address. This makes it both anonymous and transparent at the same time, another neat feature that explains Bitcoin's popularity with the technical community (although the anonymity aspect is disputed by some studies).

Transparency is limited because the actual originator of the scheme remains anonymous. Bitcoin was created by a member of a cryptography mailing list under a pseudonym. This has made some people suspect that Bitcoin operates in a manner similar to a Ponzi scheme, where those early adopters at the top amassed large BTC stocks, so that the resulting coins can be easily manipulated. The barrier-to-entry is not only physically high (difficulty increases with time), but also it is a psychological investment for anyone who understands just how easy it would be to maliciously manipulate the market. There have been several examples of possible manipulation. There is evidence that bots have been involved in currency-price manipulation at a large scale, with a bot named Willy by analysts potentially responsible for inflating the price until it reached up to $1300 USD per 1 bitcoin. Some people have amassed large BTC fortunes and swayed and manipulated the market. For example, in 2013 there was a single transaction of 69,000 bitcoins.[21] Such transactions can have huge price effects.

The actual number of BTCs in circulation is considerably smaller than previously thought, with 78% of the entire BTC reserve (7,019,100 BTC) placed in "saving" addresses, and only 22% of all BTCs created (including the lost) in circulation. This confirms the suspicion that the system encourages hoarding and accumulation, which make it uniquely unsuitable as a currency. A large number of transactions appear to consist of operations between the same owner, where the coins are moved from one address to the other.

[19] This problem set of ideology and currency is discussed in depth in the EC FP7 D-Cent project.
[20] http://blockchain.info/.
[21] http://blockchain.info/tx/5d9ef693d41cb3bb4c6d98e70ea8b2cc91be29a804245a06ec8761d9cddc103c

Anonymity is the biggest selling point for Bitcoin. This was made evident after an article in The Atlantic[22] informed college students everywhere of the existence of Silk Road, a site where they could buy drugs using Bitcoins. Bitcoin's value exploded, usage shot up, and mining rigs went up using top-end GPUs. Because the currency is encrypted, there is theoretically no method to trace any given transaction to individual users. Reid and Harrigan in a recent paper[23] claim that Bitcoin's much-touted anonymity is seriously flawed. They explain:

> "Many organizations and services such as on-line stores that accept Bitcoins, exchanges, laundry services and mixers have access to identifying information regarding their users, e.g. e-mail addresses, shipping addresses, credit card and bank account details, IP addresses, etc. If any of this information was publicly available, or accessible by, say, law enforcement agencies, then the identities of users involved in related transactions may also be at risk."

As a case study, they used a highly-publicised theft of 25,000 BTCs (with a value at the time of theft of approximately $500,000 USD). They were able to follow the involved transactions using their network tools, and charted these with high level of accuracy. They conclude that:

> "Using an appropriate network representation, it is possible to map many users to public-keys. This is performed using a passive analysis only. Active analyses, where an interested party can potentially deploy marked Bitcoins and collaborating users can discover even more information. We also believe that large centralized services such as the exchanges and wallet. Using an appropriate network representation, it is possible to map many users to public-keys. This is performed using a passive analysis only. Active analyses, where an interested party can potentially deploy marked Bitcoins and collaborating users can discover even more information. We also believe that large centralized services such as the exchanges and wallet."

Ownership concentration in the BTC network is confirmed by the data:

> "36% of all owners received fewer than one BTC (currently worth about 12 USD) each throughout their lifetime, 52% received fewer than 10 BTC's and 88% fewer than 100. At the other end of the distribution there are only four owners who received over 800,000 BTC's and 80 owners who received over 400,000."

The list of BTC owners includes a single unidentified user with 2,886,650 coins, or more than a quarter of all BTCs issued so far. This hints at hoarding by a few people. BTC is not being used as a payment system, but as a commodity where users exchange bitcoins for cash and vice versa.

Bitcoin has been tremendously unstable throughout its trading history. While generally the overall trend has been upward, the currency has crashed several times before, and the price continues to swing up and down. Such instability is one of the reasons why it is very unlikely to be a viable currency. Yglesias argues that it may continue to vary cyclically in price[24]:

> "if everyone's hoarding their Bitcoins, then the network is actually useless. Since it turns out to be useless, you get a crash. The funny thing is that once the upward spiral comes to an end, the technological virtues of the Bitcoin platform come to the fore again."

Imagine that you are a merchant who decides to accept BTC, and agree with the buyer to sell at the trading rate when the transaction was initiated. The first problem you would encounter is

---

[22] Madrigal A, "Libertarian Dream? A Site Where You Buy Drugs with Digital Dollars", The Atlantic (June 1 2011), http://theatln.tc/1pvw0IK.

[23] Reid F and Harrigan M, "An Analysis of Anonymity in the Bitcoin System", arXiv:1107.4524 (2012), http://arxiv.org/abs/1107.4524. They used network analysis to trace transactions down a chain of distribution, and discovered that by treating transactions as a links in a network, and sender and recipients were vertices, they could get a very good idea of who was doing what. Moreover, they claim that this information can be easily cross-referenced with information in public spaces and intermediaries, so anonymity would be seriously compromised.

[24] Yglesias M, "Bitcoin Will Spiral Up and Down Forever", Slate (April 10 2013), http://slate.me/1tZI4ni

that the transaction needs to be verified, and as there are more verifications taking place all the time, the process takes longer (about an hour). With wild variations in price, it is possible that you could lose money even before the transaction has been completed. Moreover, even a minor downward swing like those which were common in the days before the crash could wipe away any profit margin.

Fiat money is kept stable by all sorts of means, from fiscal policies to centralized decisions about interest rates. It is possible that stability can only be achieved through centralization.

3.2 Lack of Replicability

Bitcoins exist only as files in a computer or mobile device; these files have access to the private key used to secure the money. This creates one of the biggest issues with Bitcoin to date, which is the ease of losing one. If the wallet file is lost, then the bitcoins it contains are lost forever. There are ways to back up the keys, such as by keeping physical copies offline, and similarly the key files can be backed up. But if a backup fails, the value will be forever lost, it is simply irretrievable unless one breaks the very secure encryption built into the system. The public address still exists, but this can only be accessed by the private key, which has been deleted, and it would not be possible to recover the lost coins.

There are indications that there are large numbers of lost coins in the system. Ron and Shamir examined very old "dormant" addresses in the blockchain, and assumed that these were probably lost coins from the time when people were testing the technology and deleted their wallets[25]. The authors calculated the historical number of lost coins to be 1,657,480 bitcoins. Considering the certainty of later losses, the total value of lost coins could very well double that number. This has not been seen as a problem for enthusiasts, as they point out that each BTC is divisible up to 8 decimal points. It is also assumed that the fewer BTCs there are, the higher the value.

Defenders of Bitcoin point out that it is possible to lose real money as well. This seems disingenuous, as the finality of Bitcoin loss is absolute. People tend to know where their wallet is, but are less conscious about files in their computer. Similarly, normal consumers do not keep all their money stashed in one location. The lack of a failsafe when things inevitably go wrong is a serious issue with the scheme.

The solution to this concern is to keep wallets online, a centralized solution that has its own problems, chiefly that one has to rely on unregulated intermediary 'banks' holding the wallet. Some online wallets have had problems with security and lost coins, not to mention the real possibility of fraud.

3.3 Deflation

Bitcoin is built with scarcity in mind. The idea is that the scarcity will ensure upward valuation of the currency because there is no central bank that can print more money, as the economy requires it. The problem with deflation is that it encourages hoarding, in which case the currency is not being used as intended, namely to exchange goods and services[26]. Moderate

[25] Ron, D and Shamir, A. (2012) Quantitative Analysis of the Full Bitcoin Transaction Graph, Cryptology ePrint Archive: Report 2012/584, at http://eprint.iacr.org/2012/584. Note the "vigorous debate" over their methodology: http://www.reddit.com/r/Bitcoin/comments/1reuwq/vigorous_debate_over_shamirrons_supposedly

[26] If everyone kept their money and hid it under the mattress, then the economy would enter into a downward spiral, as businesses would have no revenue, so they could not employ people.

inflation is desired in a healthy economy because it encourages investment and spending, as shown in the recent deflationary crises in Japan and the Eurozone. When Bitcoin was experiencing its upward trend, many commentators noted that a rise in value meant that it had entered a hyper-deflationary spiral which made it uniquely unsuitable as a currency because there was no reason to spend BTCs if the price would continue to rise. In the early days of Bitcoin, an individual reportedly spent 10,000 bitcoins to buy a pizza. In a deflationary economy, this person feels that they lost greatly as the currency's value goes up, and would be less willing to part with their currency in the future.

A stable currency abhors deflationary, otherwise it ceases acting as a medium of exchange and becomes akin to scarce commodities such as diamonds.

3.4 Security and BTC Theft

Criminal lawyers have taken a very significant recent interest in Bitcoin[27]. An aspect of the trust in Bitcoin is its security, touted as a very secure and anonymous method of transferring value from one computer to the other. The currency works by allocating a public cryptographic key to arbitrary units of value held in a non-proprietary client. Because they are public, the keys can be inspected by everyone, but a private key is needed to make the transaction. These units of value are held in "wallets", small .dat files hosted in the computer. This serves two purposes: as long as the keys are secure, only the wallet's owner will be able to transfer the bitcoins to make a payment; the keys make the transactions anonymous.

As with many things online, the theory is often defeated by a combination of greed, laziness, ignorance, and simple intermediary failure. Bitcoin's cryptography is very strong, so a hacking attack would not be able to break the security. But a hacker doesn't need to defeat the SHA-256 cryptographic hash in order to remove bitcoins from the wallet, a simple $5 dollar wrench would suffice. Practice has been bearing this out, the Bitcoin client does not encrypt the wallet.dat file itself, which leaves the currency vulnerable. Similarly, hackers have been targeting the exchanges, the places where people pay in real money to buy bitcoins. Encryption does not protect against fraudsters and scam artists.

Bitcoin is deeply flawed. The actual encryption and some of the technical details are sound, but 'strong encryption does not a currency make'. People have been the subject of hacker attacks and robbery, creating a "blame the victim" mentality. The exchanges and wallets are indeed the weakest link in the chain. A currency that requires a high level of security and of user knowledge will never be widespread. Once the coins are gone, they´re really gone. No recourse to your bank, no legislative protection (UK law for example protects debit and credit card users quite well). The only BTC recourse is reputational: to go to the forums to complain.

Dealing specifically with cybercrime, network tools like social network analysis could have a large impact. Examples such as the above are precisely the type of uses that law enforcement

[27] On criminal law issues in using Bitcoin, see Birch, D. (2007) "Money laundering in virtual worlds: risk and reality." E-Commerce Law & Policy. 9(5), 12-13; Irwin, A, S, M., Slay, J., Choo, K, R. Lui, L. (2014) "Money laundering and terrorism financing in virtual environments: a feasibility study" Journal of Money Laundering Control. 17(1), 50-75; Jarvie, N. (2003) "Control of cybercrime - is an end to our privacy on the Internet a price worth paying? Part 1" Computer and Telecommunications Law Review 9(3), 76-81; Mok, F. and Tiah, K. (2014) "Singapore: money laundering - virtual currencies" Journal of International Banking Law and Regulation 29(7), N69; Ramage, S. (2014) "Bit coins - kiss of death to us all in the developed world" Criminal Lawyers 220, 1-2; Rees, M. and Willis, R. (2014) "Virtual currencies - virtual frauds?" Fraud Intelligence Feb/Mar, 17-19; Southall, E. and Taylor, M. (2013) "Bitcoins." Computer and Telecommunications Law Review. 19(6), 177-178; Stoeckert, B. and O'Brien, T. (2014) "Impossible to ignore - virtual currencies, the next challenge" Money Laundering Bulletin 214, 4-7; Stokes, R. (2012) "Virtual money laundering: the case of Bitcoin and the Linden dollar." Information & Communications Technology Law 21(3), 221-236; Straus, R, J. (2013) "The FinCEN virtual currency guidance: neutering Bitcoin?" E-Finance & Payments Law & Policy 7(4), 9; Stuber, W. (2014) "Brazil: virtual currencies - pyramid financial schemes." Journal of International Banking Law and Regulation 29(7), N66-N67; Varriale, G. (2013) "Bitcoin: regulating the wild west." International Financial Law Review 30(28), 17.

could employ to tackle high-tech online crime. Needless to say, when the price was going up there was a great incentive for hackers to create botnets that would mine bitcoins, or to engineer malware that would steal BTCs, these would be propagated by installing fake clients or by visiting infected sites. At some point there was also an increase in phishing sites trying to pass-off as Mt.Gox.[28]

Lack of regulation of the sector has translated into a fertile ground for fraudsters and scam artist, from the existence of phishing sites passing as exchanges, to online wallet services going bust, to the problem of Mt.Gox forced to file for bankruptcy in Japan after hackers allegedly managed to get into their system and steal $446 million USD worth of bitcoins. Some claim the site was riding a wave of speculation with coins that it did not have, accruing large amount of debt. This is precisely the type of practice that regulation is supposed to stem.

Law enforcement action is difficult because agencies may simply not understand the technology, and may not consider that this is worthy of prosecution. Until there are some arrests related to BTC fraud and hacking, serious investors might decide to stay away from Bitcoin because it simply is not safe enough, and it draws hackers like no other payment system. Bitcoin might therefore be suffering from lack of regulation, something that could be considered ironic, as one of its selling points is the distributed nature of the network, which makes it difficult to regulate in the first place.

In the following Method section, we explore proposed changes that may make the use of Bitcoin more effective.

3.5 Growing centrality

One of the foundational principles of Bitcoin is its decentralised nature. The idea is that value is issued by collaborative mining where all the parties are validating transactions in the blockchain. Assuming that thousands of people are mining separately, the system remains decentralised, and the prospect of a single entity gaining control of the network was seen as very remote. However, in June 2014 two computer scientists from Cornell University sounded the alarm,[29] stating that a large mining conglomerate was becoming too powerful, and had actually reached a 51% of all mining capacity for Bitcoin during a few hours. What this means is that for all intents and purposes, the system stops being decentralised. They commented that any person who controls 51% of the mining power can collect all of the Bitcoins mined at that time, but could also could cancel transactions, becoming a de facto monopoly.

The Bitcoin community went into a panic, with posts in forums and social media urging users of GHash.io, the mining conglomerate involved, to leave the pool to avoid it going over 51% again. Since the incident, Ghash.io has made a statement declaring that they will take steps to avoid becoming too dominant again.[30] At the time of writing, Ghash.io hovers around 30% of the hashrate distribution.[31]

Many Bitcoin enthusiasts have dismissed the centralisation concerns, they point out that the community polices itself adequately, and point to the fact that miners migrated to other pools as soon as the 51% threshold had been crossed.[32] More pragmatic developers have propsoed technical solutions, such as implementing an algorithm that would force nodes to srote the

[28] Dotson, K. "Mt. Gox Warns Bitcoin Popularity Attracting Increased Phishing Attacks", Silicon Angle (August 30, 2011), http://bit.ly/1nZes9A.
[29] Eyal, I. and Sirer, E. "It's Time for a Hard Bitcoin Fork", Hacking, Distributed (June 13, 2014), http://bit.ly/1nZezSx.
[30] See: https://ghash.io/ghashio_press_release.pdf.
[31] See: https://blockchain.info/pools.
[32] Faggart, E. "Bitcoin Mining Centralization: The Market is fixing itself", Coin Brief (2014), http://bit.ly/1nZia3a.

entire blockchain locally, which would help against a 51% conglomerate controlling the entire system.[33]

The truth is that until a long-term technical solution is reached, Bitcoin's decentralised nature relies entirely on the good will of miners. If Bitcoin in its present shape reached an important share of the financial market, it would be possible for an entity with substantial computing power to take over the entire system. The prospect of a government or corporation taking over Bitcoin would be a real threat.

4. Methods: Legal and regulatory issues

While virtual currencies can play a role in creating better trading conditions in virtual communities, despite the risks of non-sovereign issuance and therefore only regulation by code (Brown/Marsden 2013), the methodology used for JRA6 poses significant challenges to researching this 'community', if BitCoin can even be said to have created a single community, as opposed to enabling an alternate method of exchange for potentially all virtual community transactions.

First, BitCoin users have transparency of ownership but anonymity in many transactions, necessary for libertarians or outright criminals in such illicit markets as #SilkRoad. Studying community dynamics is therefore made much more difficult than even such pseudonymous or avatar based communities as Habbo Hotel, World of Warcraft or SecondLife. The ethical implications of studying such communities raise similar problems as those of Tor, Anonymous, Lulzsec and other anonymous hacker communities[34].

Second, the journalistic accounts of BitCoin markets are subject to sensationalism, hype and inaccuracy, even more so than in the earlier hype cycle for SecondLife, exacerbated by the first issue of anonymity.

Third, the virtual currency area is subject to slowly emerging regulation by financial authorities and police forces, which appears to be driving much of the early adopter community 'underground'. Thus, the community in 2016 may not bear much resemblance to that in 2012.

Fourth, there has been relatively little academic empirical study of the community, or indeed of virtual currencies in general, until relatively recently.

Fifth, the dynamism of the virtual currency environment in the face of the deepening mistrust of the financial system after the 2008 crisis is such that any research conclusions must by their nature be provisional and transient.

All these challenges, particularly the final three, also raise the motivation for research – an alternative financial system which is separated from the real-world sovereign and which can use code regulation with limited enforcement from offline policing, both returns the study to the libertarian self-regulated environment of early 1990s MUDs, and offers a tantalising prospect of a tool to evade the perils of 'private profit, socialized risk' which existing large financial institutions created in the 2008-12 disaster. The need for further research into virtual currencies based on blockchain mining, and for their usage by virtual communities, is thus pressing and should motivate researchers to solve the many problems in methodology for exploring such an environment.

[33] See: https://blog.ethereum.org/2014/06/19/mining/.

[34] Soghoian, C. (2012) *Enforced Community Standards For Research on Users of the Tor Anonymity Network*, Center for Applied Cybersecurity Research, Indiana University, also at Financial Cryptography and Data Security: Lecture Notes in Computer Science Volume 7126, pp 146-153

4.1 Legalities of Bitcoin

Based on Mayer-Schönberger/Crowley[35], we construct four scenarios for virtual currencies:

(1) **'Virtual sovereigns'**: virtual currency providers will serve as regulators by enforcing the terms of their contracts with users to prevent cyber-fraud and ensure proper behaviour;

(2) **Prohibition**: governments could try to block their citizens from using virtual currencies that don't abide by government restrictions and regulations (governments have not been able to completely block access to websites nor will total prohibition on virtual currencies succeed);

(3) **Selective Prohibition**: government minimize the real-world impact of virtual currencies by, for instance, banning the sale of real-world goods for virtual currency; or

(4) **'Real-World Assisted Virtual Currency Self-Governance'**: governments provide support for mechanisms whereby users of virtual currencies can agree upon and enforce their own 'community standards' and rules of conduct.

Note the fifth 'do-nothing' option is a minor variant on Option 4[36].

Is Bitcoin legal? There are generally two types of currency from a legal perspective, legal tender and legal currency. Legal tender is simply currency that cannot be refused in the fulfilment of a debt. Legal currency is money that is recognised by the government as a legitimate manner to pay for goods and services. In most countries legal currency and legal tender are one and the same, but there are some exceptions. For example, in the most of the UK the Bank of England notes are legal tender, but in Scotland only coins are legal tender, there are notes issued by several banks, which act as legal currency. The same applies for Northern Ireland. It is also common to see economies with a weak local currency to accept international money as legal currency.

In the United States, only the US Dollar is legal tender (31 U.S.C. § 5103). Similarly, only the Mint and the Federal Reserve can produce coins and currency, which are the only means of legal tender. Title 31 of the US Code does not seem to make the distinction between legal currency and legal tender, so they appear to be treated in a similar fashion. This is corroborated by several official documents that indicate clearly that only the USD is allowed as the official currency of the United States. According to the FBI "it is a violation of federal law for individuals, [...] or organizations,[...] to create private coin or currency systems to compete with the official coinage and currency of the United States." In the US, it seems more likely that Bitcoin should be treated more like a speculative vehicle, more akin to securities or commodities, in which case its possible definition as a currency would not be necessary.

The picture is slightly clearer in the European Union, but there is still a lot of room for interpretation. Unlike the United States, the EU has implemented a legal framework for the regulation of electronic money. The Electronic Money Institutions Directive 2009/110/EC defines electronic money thus (paraphrased for clarity):

1. electronically, including magnetically, stored monetary value;
2. as represented by a claim on the issuer which is issued on receipt of funds for the purpose of making payment transactions;

---

[35] Mayer-Schönberger, V. and Crowley, J. (2006) *Napster's Second Life? The regulatory challenges of virtual worlds*, Northwestern University Law Review , 100 :4 , at www.vmsweb.net/attachments/pdf/NWLR100n4.pdf See also Gillen, M. (2007) "Managing virtual communities: time to turn the whetstone?" International Review of Law Computers & Technology 21(3), 211-220

[36] See further Marsden, C. (2011) *Internet Co-regulation*, Cambridge University Press, at pp.71-100 for virtual world regulation.

3. the transaction is an act, initiated by the payer or by the payee, of placing, transferring or withdrawing funds, irrespective of any underlying obligations between the payer and the payee;
4. which is accepted by a natural or legal person other than the electronic money issuer.

If a payment system fulfils these requirements, then it is considered electronic money, and only electronic money institutions can issue electronic value. There is a high threshold for an electronic money institution, as the EMI would have to fulfil quite a lot of requirements. The idea behind this stringent regulation is evident, as what is taking place is the issuing of value into the economy. Bitcoin would meet the legal definition to a certain extent, with the exception that it is not money that is issued in the sense that is meant by the Directive. As there is no central issuing authority, then it would be difficult to envision how financial services authorities in charge of regulating EMIs could intervene Bitcoin.

4.2 Regulatory actions to date

Bitcoin users are learning the hard way why financial markets and currencies are heavily regulated areas. Deposit taking, the keeping of accounts, management of payment transactions, the keeping of balances, all of these are functions of financial institutions that are of the utmost importance to businesses and consumers. The economy relies on financial intermediaries to operate, and regulation is designed to prevent damage to consumers.

Regulators have yet to tackle some of the legal questions explored above. Part of the appeal of the payment system is that it is completely decentralised. Just as with P2P file-sharing, you could shut down the entire Bitcoin operation tomorrow and the network would still run because it does not depend on a central system. Bitcoin may very well be illegal, but almost impossible to shut down in any efficient manner, as a distributed network.

Tax regulatory responses to Bitcoin have been very low-key[37]. In the United States, the Financial Crimes Enforcement Network (FinCEN) issued guidelines specified that decentralized currencies should comply with money laundering regulations[38]. In the UK, Her Majesty's Revenue and Customs (HMRC) has issued a briefing paper detailing the position on the tax treatment of income received from, and charges made in connection with, activities involving Bitcoin and other similar cryptocurrencies[39]. The HMRC recognises that this is an evolving regulatory area, and is expecting that at some point there will be some sort of EU-wide effort to define and clarify cryptocurrencies in general. Taking that into account, HMRC has decided to treat income from sales of goods and services through Bitcoin in the same manner as it does any other sales. With regards to other income, they issued the following guidelines for the time being:

1. "Income received from Bitcoin mining activities will generally be outside the scope of VAT on the basis that the activity does not constitute an economic activity for VAT purposes

[37] On Bitcoin, virtual currencies and taxation, see Asquith, R. (2014)"Bitcoin: too big not to tax." Accountancy 152(1447), 27; Atlas, A (2014) "Bitcoin: getting down to real business with virtual currency." E-Commerce Law & Policy 16(4), 5-6; Bal, A. (2013) "Stateless virtual money in the tax system" European Taxation 53(7), 351-356; Lambooij, M. (2014) "Retailers directly accepting Bitcoins: tricky tax issues?" Derivatives & Financial Instruments. 16(3), 138-144; Nemeczek, H. and Schies, C. (2013) "German Ministry clarifies where Bitcoin falls under German law." E-Finance & Payments Law & Policy 7(11), 10-11; Nuttall, G. (2007) "Income earning in virtual worlds: taxation issues." E-Commerce Law & Policy 9(5), 7-9.

[38] Financial Crimes Enforcement Network, FIN-2013-G001 (March 18, 2013) Application of FinCEN's Regulations to Persons Administering, Exchanging, or Using Virtual Currencies, http://1.usa.gov/1kWrsK7.

[39] Her Majesty's Revenue and Customs (2014) Tax treatment of activities involving Bitcoin and other similar cryptocurrencies, Revenue & Customs Brief 09/14, http://bit.ly/1kWrBgE.

because there is an insufficient link between any services provided and any consideration received.

2. Income received by miners for other activities, such as for the provision of services in connection with the verification of specific transactions for which specific charges are made, will be exempt from VAT under Article 135(1)(d) of the EU VAT Directive as falling within the definition of 'transactions, including negotiation, concerning deposit and current accounts, payments, transfers, debts, cheques and other negotiable instruments.'
3. When Bitcoin is exchanged for Sterling or for foreign currencies, such as Euros or Dollars, no VAT will be due on the value of the Bitcoins themselves.
4. Charges (in whatever form) made over and above the value of the Bitcoin for arranging or carrying out any transactions in Bitcoin will be exempt from VAT under Article 135(1)(d) as outlined at 2 above."

This brings it in line with other foreign currencies, and could be considered to be an official recognition of BTC's status as yet another currency in the eyes of the law. However, as it has been mentioned repeatedly, Bitcoin is not behaving like a currency, and it is more like a commodity fuelled by speculative investment. This is because Bitcoin's price continues to swing wildly, in the last 60 days the price has been in the range of $420-580 USD. Such currency instability has been one of the key features of the movement since its inception, and it is perhaps one of the greatest challenges to its wider acceptability as a currency.

The fact that there is little evidence of any growth in the use of BTC as a currency may be the reason why there have been minimal attempts to regulate it. But perhaps more surprising is the fact that neither the Security and Exchange Commission nor the Commodity Futures Trade Commission in the US have made any attempts to regulate it either. The reason for this could be simply that the BTC market is just too small to warrant any wide-ranging regulatory effort. It is also possible that regulators simply do not understand the technology and its implications, and are awaiting any further developments to act.

Other countries have taken this wait-and-see approach. Japanese authorities have also stated[40] that they will monitor for illegal activity with Bitcoins, but will not regulate it for the time being. Canadian regulators explain:

> "There could be potential risks to overall financial stability if Bitcoin became a significant means of payment and the Bitcoin system remained unstable… users need to be aware of the potential financial risks to which they might be exposed, in light of the ongoing volatility of bitcoin prices and the risk of failure of Bitcoin exchanges."[41]

One of the most important regulatory developments recently has taken place in France with the publication of a report by the Minister of Finance, Michel Sapin.[42] While French authorities admit that Bitcoin does not pose a threat to financial markets, they have recognised that there is clearly room for concern with regards to criminal activity and fraud. These concerns are mostly concerned with the anonymity of transactions, which could have tax and money laundering implications. Therefore, France is the first country to make clear regulatory actions with regards to virtual currencies. These are:

1. Limit anonymity by making it mandatory for intermediaries and exchanges to require proof of identity upon opening an account.

[40] http://japandailypress.com/japan-to-monitor-illegal-bitcoin-activity-stops-short-of-regulation-1548441/.
[41] http://www.bankofcanada.ca/wp-content/uploads/2014/05/boc-review-spring14-fung.pdf.
[42] http://www.economie.gouv.fr/rapport-sur-monnaies-virtuelles-2014.

2. Clarify the taxation of virtual currencies with the publication of a set of instructions for consumers and regulators.
3. Propose a European-wide approach to Value Added Tax (VAT).
4. Propose, after discussion with industry, to cap payments in virtual currencies, similar to existing caps on cash payments.
5. Regulate at European level platforms that exchange virtual currencies against the official currency.

These measures are substantial and substantive, particularly with regards to anonymity and the requirement for identification. It will be interesting to see if such measures act as a deterrent against the creation of new intermediaries in France. It will be also vital to see if European regulators will follow the French lead and try to harmonise some of the above proposals. Given that financial markets are heavily regulated to combat money laundering, such a development would not come as a surprise. Undoubtedly, we are just starting to see the first of a flood of regulatory attempts in the near future.

5. Outcomes

Money is a unit of account, a store of value, and a medium of exchange. Bitcoin is none of those things (in any serious sense). Bitcoin has too many problems to be the solution. An anonymous and decentralized payment system could indeed revolutionise the economy, it could help to end the disproportionate power of fat-cat banking systems, and would democratise monetary exchange. A system created by an anonymous cryptographer may not be the way of the future, true openness is needed for the next experiment to be successful.

The most interesting development arising from Bitcoin has nothing to do with the currency itself, or with regulation. It is an idea proposed by a group of developers that turns the blockchain, Bitcoin's proof-of-transaction open log, into a platform for creating a smart contract decentralised platform called Ethereum.[43] The project will allow the creation of a transaction log (blockchain) with a built-in Turing-complete programming language, allowing anyone to write smart contracts and decentralized applications where they can create their own arbitrary rules for ownership, transaction formats and state transition functions.

Bitcoin is a great idea in achieving decentralisation, but suffers from the current implementation based on libertarian economic dogma. Ethereum could bring everything that is good about Bitcoin and translate it into decentralised applications. This will certainly merit further monitoring.

References

Alleyne, A. (2010) "Virtual currencies: can they classify as property?" E-Finance & Payments Law & Policy 4(5), 14-15

Anderson, T, A. (2014) "Bitcoin - is it just a fad? History, current status and future of the cyber-currency revolution" Journal of International Banking Law and Regulation. 29(7), 428-435

Anil, S., Jie, A, K, W., Min, J, S, H. and Xiu, Q, C, W. (2012) "Virtual property - a theoretical and empirical analysis" European Intellectual Property Review 34(3), 188-202

Asquith, R. (2014)"Bitcoin: too big not to tax." Accountancy 152(1447), 27;

Atlas, A (2014) "Bitcoin: getting down to real business with virtual currency." E-Commerce Law & Policy 16(4), 5-6;

Bal, A. (2013) "Stateless virtual money in the tax system" European Taxation 53(7), 351-356;

[43] https://www.ethereum.org/

Balkin , J. M. and Noveck , B. S. (eds.) (2006) The State of Play: Law and Virtual Worlds, New York University Press

Barzilai-Nahon, K. (2006) "Gatekeepers, virtual communities and the gated: multidimensional tensions in cyberspace." International Journal of Communications Law & Policy 11

Birch, D. (2007) "Money laundering in virtual worlds: risk and reality." E-Commerce Law & Policy. 9(5), 12-13

Bond, R (2009) "Business trends in virtual worlds and social networks - an overview of the legal and regulatory issues relating to intellectual property and money transactions." Entertainment Law Review 20(4), 121-128

Bryan William Jennings (1896) 9 July calling for convertibility of gold to silver: http://historymatters.gmu.edu/d/5354/

Courtneidge, R. (2014) "Crypto currencies and the regulators: friends after all?" E-Finance Payments Law & Policy. 8(2), 8-9

Courtneidge, R. and Lloyd, V. (2013) "Accepting Bitcoin as payment for online gambling services." World Online Gambling Law Report. 12(2), 3-4

Davies , T . and Noveck , B. (eds.) (2006) Online Deliberation: Design, Research, and Practice, CSLI Publications/University of Chicago Press

De Filippi P "Bitcoin: a regulatory nightmare to a libertarian dream", 3(2) *Internet Policy Review* (2014), doi:10.14763/2014.2.286. http://bit.ly/1teQq8l.

Dixon, J (2013) "The importance of an effective Bitcoin exchange market." E-Finance & Payments Law & Policy. 7(6), 6-7

Dotson, K. "Mt. Gox Warns Bitcoin Popularity Attracting Increased Phishing Attacks", Silicon Angle (August 30, 2011), http://bit.ly/1nZes9A.

Eyal, I. and Sirer, E. "It's Time for a Hard Bitcoin Fork", Hacking, Distributed (June 13, 2014), http://bit.ly/1nZezSx.

Faggart, E. "Bitcoin Mining Centralization: The Market is fixing itself", Coin Brief (2014), http://bit.ly/1nZia3a.

Financial Crimes Enforcement Network, FIN-2013-G001 (March 18, 2013) Application of FinCEN's Regulations to Persons Administering, Exchanging, or Using Virtual Currencies, http://1.usa.gov/1kWrsK7.

Fitzgerald, B, F. (1997) "Life in cyberspace: a simulating experience." Computer and Telecommunications Law Review. 3(3), 136-138

Flint, D. (2014) "Computers and internet: are all modern currencies not virtual? - The Bitcoin phenomenon." Business Law Review. 35(2), 60-62

Folsom, R. and Cashman, M. (2014) "Digital currency: a primer." Computers & Law. 24(6), 27-30.

Garrie, D, B. and Wong, R. (2010) "Social networking: opening the floodgates to "personal data" Computer and Telecommunications Law Review. 16(6), 167-175

Gervassis, N, J. (2004) "In search of the value of online electronic personae: commercial MMORPGs and the terms of participation in virtual communities" Journal of Information, Law & Technology 3

Gillen, M. (2007) "Managing virtual communities: time to turn the whetstone?" International Review of Law Computers & Technology 21(3), 211-220

Gonzalez, L, H. (2013) "Habeo Facebook ergo sum? Issues around privacy and the right to be forgotten and the freedom of expression on online social networks" Entertainment Law Review 24(3), 83-87

Gray, T., Zeggane, T. and Maxwell, W. (2008) "US and EU authorities review privacy threats on social networking sites" Entertainment Law Review 19(4), 69-74

Her Majesty's Revenue and Customs (2014) Tax treatment of activities involving Bitcoin and other similar cryptocurrencies, Revenue & Customs Brief 09/14, http://bit.ly/1kWrBgE.

Hicks, L. (2010) "Through the privacy wall" European Lawyer 98, 51.

Irwin, A, S, M., Slay, J., Choo, K, R. Lui, L. (2014) "Money laundering and terrorism financing in virtual environments: a feasibility study" Journal of Money Laundering Control. 17(1), 50-75

James, S. (2008) "Social networking sites: regulating the online "Wild West" of Web 2.0" Entertainment Law Review 19(2), 17-50

Jankelewitz, E., Nemirovsky, D., Reyhani, B, I. and Vaziri, A. (2014) "Regulators respond to the big questions posed by Bitcoin" E-Finance & Payments Law & Policy 8(4), 6-8

Jarvie, N. (2003) "Control of cybercrime - is an end to our privacy on the Internet a price worth paying? Part 1" Computer and Telecommunications Law Review 9(3), 76-81

Lambooij, M. (2014) "Retailers directly accepting Bitcoins: tricky tax issues?" Derivatives & Financial Instruments. 16(3), 138-144;

Madrigal A, (2011) "Libertarian Dream? A Site Where You Buy Drugs with Digital Dollars", The Atlantic June 1 http://theatln.tc/1pvw0IK.

Mallard A, Méadel C, and Musiani F, "The Paradoxes of Distributed Trust: Peer-to-Peer Architecture and User Confidence in Bitcoin", 4 *Journal of Peer Production* (2014), http://bit.ly/1gvL2gv.

Margaritov, D. (2014) "Bitcoin: on the frontier of online gambling innovation" World Online Gambling Law Report. 13(3), 8-9.

Marsden, C. (2011) Internet Co-regulation, Cambridge University Press, at pp.71-100 for virtual world regulation.

Marsden, C., Pavan E. et al (2013) Deliverable 6.1: Overview of user needs analysis, plus draft catalogue of design responses to needs analysis, Internet Science Consortium at http://www.internet-science.eu/biblio/reports

Mayer-Schönberger, V. and Crowley, J. (2006) Napster's Second Life? The regulatory challenges of virtual worlds, Northwestern University Law Review , 100 :4 , at www.vmsweb.net/attachments/pdf/NWLR100n4.pdf

Meek, J (2014) "Funny money" Operational Risk & Regulation. 15(2), 23-25.

Meek, J. (2014) "Banks "killing" bitcoin industry, expert warns." Operational Risk & Regulation. 15(5), 10

Mok, F. and Tiah, K. (2014) "Singapore: money laundering - virtual currencies" Journal of International Banking Law and Regulation 29(7), N69

Munck, M, G. (2011) "Future payments in a disruptive digital world." E-Finance & Payments Law & Policy. 5(4), 12-13

Nemeczek, H. and Schies, C. (2013) "German Ministry clarifies where Bitcoin falls under German law." E-Finance & Payments Law & Policy 7(11), 10-11;

Noveck , B. (2006) Architecture, law and virtual worlds , First Monday 10:11 , at www. firstmonday.org/issues/issue10_11/noveck/

Nuttall, G. (2007) "Income earning in virtual worlds: taxation issues." E-Commerce Law & Policy 9(5), 7-9.

Ondrejka, C. (2004) Aviators, Moguls, Fashionistas and Barons: Economics and Ownership in Second Life, at http://ssrn.com/abstract =614663

Petrasic, K, L. (2013) "DATA's self-regulatory quest to legitimise virtual currencies" E-Finance & Payments Law & Policy 7(9), 6-7

Ramage, S. (2014) "Bit coins - kiss of death to us all in the developed world" Criminal Lawyers 220, 1-2

Rees, M. and Willis, R. (2014) "Virtual currencies - virtual frauds?" Fraud Intelligence Feb/Mar, 17-19;

Regnard-Weinrabe, B., Taylor, M and Savary, R. (2013) "Virtual currencies, the risks and the regulatory radar" E-Finance & Payments Law & Policy 7(7), 10-11.

Reid F and Harrigan M (2012) "An Analysis of Anonymity in the Bitcoin System", arXiv:1107.4524 http://arxiv.org/abs/1107.4524

Reynolds R, “A Bit Too Far?” Terranova (June 10, 2011), http://bit.ly/1mJtwFj

Ron D and Shamir A, “Quantitative Analysis of the Full Bitcoin Transaction Graph”, Cryptology ePrint Archive: Report 2012/584 (2012), http://eprint.iacr.org/2012/584

Ron, D and Shamir, A. (2012) Quantitative Analysis of the Full Bitcoin Transaction Graph, Cryptology ePrint Archive: Report 2012/584, at http://eprint.iacr.org/2012/584.

Soghoian, C. (2012) Enforced Community Standards For Research on Users of the Tor Anonymity Network, Center for Applied Cybersecurity Research, Indiana University, also at Financial Cryptography and Data Security: Lecture Notes in Computer Science Volume 7126, pp 146-153 Nakamoto S, Bitcoin: A Peer-to-Peer Electronic Cash System, (2008), https://bitcoin.org/bitcoin.pdf.

Soghoian, C. (2012) Enforced Community Standards For Research on Users of the Tor Anonymity Network, Center for Applied Cybersecurity Research, Indiana University, also at Financial Cryptography and Data Security: Lecture Notes in Computer Science Volume 7126, pp 146-153

Southall, E. and Taylor, M. (2013) "Bitcoins." Computer and Telecommunications Law Review. 19(6), 177-178

Stephenson Neal (2011) Reamde, Harper Collins

Stoeckert, B. and O'Brien, T. (2014) "Impossible to ignore - virtual currencies, the next challenge" Money Laundering Bulletin 214, 4-7

Stokes, R. (2012) "Virtual money laundering: the case of Bitcoin and the Linden dollar." Information & Communications Technology Law 21(3), 221-236;

Straus, R, J. (2013) "The FinCEN virtual currency guidance: neutering Bitcoin?" E-Finance & Payments Law & Policy 7(4), 9;

Stuber, W. (2014) "Brazil: virtual currencies - pyramid financial schemes." Journal of International Banking Law and Regulation 29(7), N66-N67;

Tavan, D. (2013) "A brave new Bitcoin world?" Banker Aug, 74-76

Taylor, M. and Matteucci, M. (2009) "Virtual worlds" Computer and Telecommunications Law Review 15(5), 124-147

Taylor, M., Savary, R. and Regnard-Weinrabe, B. (2013) "Virtual currencies." Computers & Law. 24(3), 31-34

Technollama (2011) http://www.technollama.co.uk/is-bitcoin-legal

Technollama (2011-14) at http://www.technollama.co.uk/?s=bitcoin

Technollama (2013) February 11 at http://www.technollama.co.uk/virtual-currency-and-virtual-property-revisited

The Willy Report (May 25, 2014), “Proof of massive fraudulent trading activity at Mt. Gox, and how it has affected the price of Bitcoin”, http://bit.ly/1nFIA82.

Varriale, G. (2013) "Bitcoin: regulating the wild west." International Financial Law Review 30(28), 17.

Weber B, “Can Bitcoin Compete with Money?” 4 *Journal of Peer Production* (2014), http://bit.ly/1gvL6Ng.

Yglesias M, “Bitcoin Will Spiral Up and Down Forever”, Slate (April 10 2013), http://slate.me/1tZI4ni