Blockchains and Bitcoin: regulatory responses to cryptocurrencies

Article (Published Version)

PEER-REVIEWED JOURNAL ON THE INTERNET

Volume 20, Number 12 - 7 December 2015

PEER-REVIEWED JOURNAL ON THE INTERNET

Blockchains and Bitcoin: Regulatory responses to cryptocurrencies

Andres Guadamuz and Chris Marsden

Abstract

This paper examines Bitcoin from a legal and regulatory perspective, answering several important questions.

We begin by explaining what Bitcoin is, and why it matters. We describe problems with Bitcoin as a method of implementing a cryptocurrency. This introduction to cryptocurrencies allows us eventually to ask the inevitable question: is it legal? What are the regulatory responses to the currency? Can it be regulated?

We make clear why virtual currencies are of interest, how self-regulation has failed, and what useful lessons can be learned. Finally, we produce useful and semi-permanent findings into the usefulness of virtual currencies in general, blockchains as a means of mining currency, and the profundity of Bitcoin as compared with the development of block chain technologies. We conclude that though Bitcoin may be the equivalent of Second Life a decade later, so blockchains may be the equivalent of Web 2.0 social networks, a truly transformative social technology.

Contents

---

1. Introduction: The hype about Bitcoin as a cryptocurrency

In 2008, the developed world banking system almost collapsed and had to be rescued by sovereign governments via takeovers of bad banks with bad loans, and the printing of money to loan to major banks, whether rescued or surviving. In the long recession of 2008 to 2014, governments supported their economies with a variety of means. With close to zero inflation and interest rates, governments had to find ways to stimulate some economic growth. They fell on three main solutions: limited stimulus via infrastructure spending, such as the American Reinvestment and Recovery Act of 2009; support for ICT-enabled, often environmentally sustainable industries to create new 'virtual' growth in the digital economy [1], some of it linked to the first option [2]; quantitative easing or the printing of money given to banks at low interest rates. Mason reports that the "[United States of] America and Britain did it first, in early 2009; Japan waded in massively in 2012 and the Eurozone finally did it, in the teeth of German resistance, in January this year." [3]

Reactions to the rescuing of banks were mixed, with many of those opposed to the policy either resorting to investment in commodities and bullion, for instance property and gold (which rose in value 350 percent 2006–12, and is still double 2006 levels at over US$1,100/ounce). Others chose a more radical path. Iceland bankrupted its banks and massively devalued its currency [4]. It then adopted a series of policies that alienated the population in a severe recession. In late 2015, the largest party by popular support is the Icelandic Pirate Party [5], which proposes far wider use of virtual currencies which would not rely on sovereign support. We should also note that throughout the years of recession (most developed economies regained 2008 levels of income after six years, with the notable exception of Greece and Iceland), the wealthiest quartile of the population invested massively in the "Apple economy", spending sovereign currency on a billion iPhones and other consumer electronics and services such as NetFlix movies and Amazon purchases. Rejection of the mass consumer economic model funded by debt is by no means universal or even a majority view.

In January 2011, an aspiring entrepreneur called Ross Ulbricht created an online marketplace called Silk Road [6]. This was not just another electronic commerce Web site, Silk Road was unique in almost all of its features. First, it was not available on the normal Web. It existed in an encrypted and secretive part of the Internet called the 'dark Net' [7]. Second, it offered a range of illegal merchandise not found on eBay or Amazon, mostly drugs, catering to discerning users by offering customer reviews and vendor ratings. Third, the

Silk Road was able to operate because it used a new virtual currency called Bitcoin that allowed users to remain anonymous and conduct transactions with little fear of interference by law enforcement.

While the Silk Road was eventually shut down and its creator arrested and convicted [8], the publicity that the case garnered for Bitcoin helped to establish it in the public's imagination as a powerful sign of the probabilities of the digital economy. The currency has even transcended the financial pages to be featured in popular television shows like *The Good Wife, Almost Human* and *The Simpsons*. Even the famous Winklevoss twins, of Facebook fame, have become heavy investors. Academics have published many social science papers about Bitcoin since 2011, with increasing regularity: six by the end of 2012, 19 in 2013 and 135 since the beginning of 2014 until August 2015 [9]. It is not merely an academic fashion: many books have been published in the period since we published a working paper on which this work is based [10], from the how-to-get-rich-quick variety [11] to the revolutionary [12] and its anti-thesis [13] to regulatory [14] and even academic [15]. Inevitably, a 'burst the bubble' anti-hype book concludes that: "There are fewer people using bitcoins to buy goods and services than there are members enrolled in Kuwait Airways frequent flyer program. And yet ... the blockchain technology behind bitcoin, is brilliant and will absolutely change the world." [16] We shared that conclusion in 2014 and continue to do so today.

This paper will look at Bitcoin from a legal and regulatory perspective, answering several important questions. We begin by explaining what Bitcoin is, and why it matters. In the following section, we explain problems with Bitcoin as a method of implementing a cryptocurrency. We are aware that the introductory section may seem extensive, and that including a very detailed description of currencies and Bitcoin may seem basic at this level. This is done on purpose, because in our experience whenever there is talk of Bitcoin and blockchains, non-technical audiences tend to miss the importance of some developments because they do not understand the basics. It is one of the goals of this article to be able to act as an easy introduction to cryptocurrencies. We ask the inevitable question for lawyers: is it legal? What are the regulatory responses to the currency? Can it be regulated? We explain why virtual currencies are of interest, how self-regulation has failed, and what useful lessons can be learned. Finally, we produce useful and semi-permanent findings into the usefulness of virtual currencies in general, block chains as a means of mining currency, and the profundity of 'media darling' currency Bitcoin as compared with the development of blockchain technologies [17]. We conclude that though Bitcoin may be the equivalent of Second Life, so blockchains may be the equivalent of Web 2.0 social networks, a truly transformative social technology.

2. Introduction to Bitcoin

2.1. Virtual currencies

There is a voluminous literature on regulation of virtual economies [18], virtual communities [19] and a fast emerging literature on Bitcoin itself [20]. From Facebook Credits to Bitcoin (BTC), virtual currencies have had a bumpy evolution. Virtual currencies are wildly successful in their 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 [21]. Amazon has announced that it will be launching its own virtual currency for their Kindle app store, Amazon Coins. 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. This replicates earlier uses of reward schemes to regular shoppers, from air miles and airline rewards, to Green Shield stamps in the 1960s and 1970s, to the Cooperative Society's dividends and stamps, and the now-ubiquitous reward programmes of online merchants.

Virtual communities can create social networks but also valuable goods and services for other users [22]. 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 U.S. dollars, though the largest social network Facebook uses sovereign currencies as do its third party games developers [23]. Most virtual community developers have historically claimed ownership of everything hosted in their servers, making them the 'sovereign' in the community [24]. 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 and other virtual communities [25]. Some virtual communities have gone further, developing virtual currencies that can be accepted in other communities.

Bitcoin has taken a further step, as it is a virtual currency that claims to be tradable in exactly the same fashion as sovereign currencies, yet without a sovereign. We now explain the basics of currencies before examining Bitcoin's challenges to that model.

2.2. Currency basics

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 users, and the operation is distributed using an open source client that can be installed on any computer or mobile device. 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 [26].

Currencies were invented as a means to transfer value. Initially, this was done through barter, and then people started allocating value to coins using metals that were considered inherently valuable for their scarcity. In the Renaissance in Europe [27], 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 bullion was insecure and expensive [28]. The first paper notes worked as a promise to give the bearer the equivalent value in metal to the one inscribed on 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 a given currency. The problem with this system, called the gold or silver standard [29], 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 (expansion of empire was often motivated and financed in part by the desire to gain gold and silver reserves, as for the Spanish and Portuguese in South America and British in South Africa). When a country needed to issue more money than it had in metal reserves, such as during time of war, this could result in devaluation, as people would not trust that there were reserves that supported the money.

During the twentieth 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 [30] money. 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 [31]. 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.

2.3. Bitcoin

Bitcoin was developed in 2008 as a concept by an anonymous developer going by the pseudonym of Satoshi Nakamoto, who posted a paper detailing the currency to a cryptography mailing list [32]. 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). People running a client that would "mine" value by verifying transactions would create the value, which encourages users to allocate processor time to confirm trades.

The paper gained some traction in cryptology circles, and it was coupled with the anonymous registration of the Bitcon.org domain, as well as the release on 9 January 2009 of the first version of the Bitcoin client [33]. The currency continued to become more popular, but it was not until the creation of the Silk Road in 2011 that it achieved more mainstream notice [34].

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, with each unit 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.

Another way of looking at the currency is that 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.

Why do people use Bitcoin and dedicate computing resources to mine them? One obvious element would be profit, but even before mining was profitable, there were thousands of people dedicating resources and efforts to the currency. 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 [35]. A libertarian tinge permeates some of the most vocal 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 more nuanced picture of the user base is beginning to emerge. Liu conducted a survey of over a thousand cryptocurrency enthusiasts in various Web sites, and found that the average BTC user is a 32-year-old libertarian male, motivated by curiosity, profit and politics [36]. Yelowitz and Wilson conducted a large study using Google Trends data from the United States, and found that computer science and illegal activity were some of the most prevalent topics linked with Bitcoin, with less correlation to political discourse and investment [37].

Bitcoin adoption may be motivated by a various number of features, including transparency, politics, anonymity and its use in illegal activities. Studying

community dynamics is therefore made much more difficult than even such pseudonymous or avatar based communities as Habbo Hotel, World of Warcraft or Second Life. The ethical implications of studying such communities raise similar problems as those of Tor, Anonymous [38], Lulzsec and other anonymous hacker communities [39]. Journalistic accounts of BitCoin markets are largely subject to sensationalism, hype and inaccuracy, even more so than in the earlier hype cycle for Second Life, exacerbated by the first issue of anonymity. Ideally, a decentralized currency should be politically neutral and 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 [40].

2.4. 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 [41]. The algorithms that produce new BTC coins increase the amount of processing power necessary to create each new block, so producing new coins is more difficult. This difficulty is built into the system to in order to keep the total amount of Bitcoins at a maximum of 21 million.

The first block "mined" was at difficulty 1, and this is known as the genesis block [42]. 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. At the time of writing (June 2015), there were 359,657 blocks and just over 14 million BTC had been mined, with a difficulty of over 47.5 billion.

That means, making a new block is more than 47 billion times more difficult than it was for the initial block, and four times more difficult than it was exactly one year before. 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 [43].

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. This may have regulatory repercussions in the future.

Because late adopters and interested individuals cannot hope to mine new coins, the BTC economy relies on users buying bitcoins with fiat currencies through exchanges. These are companies that hold bitcoins and are willing to sell them at an exchange rate. In other words, intermediaries will accept your "normal" currency and exchange it into bitcoins, and vice versa [44]. For most large part of its early history, Bitcoin relied very heavily on one intermediary, a Tokyo-based company called Mt. Gox. There have been dozens of exchanges, as in theory literally anyone could set up their own firm. Mt. Gox was famous 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 percent of all Bitcoin transactions ever recorded

[45]. 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 [46]. As we will discuss later, Mt. Gox became embroiled in serious fraud accusations. Similarly, such reliance makes the entire system less resilient and prone to catastrophic failures, but we will analyse those issues later.

2.5. Altcoins

Bitcoin has undoubtedly become the most talked about cryptocurrency, but it is easy to forget that it began mostly as a proof of concept. Because the software is completely open source [47], any developer can download it, modify it and create her own version of the software. This capability has led to an explosion of alternative bitcoin implementations, popularly known as altcoins. There are no limits to the number of altcoins that can be released, but in practice there are a few dozen real alternatives that implement minor or major changes; these are known as forks.

There is no single reason why a developer should fork the original code and create their own version. Some may do it to improve the code, to create better security, to modify some of the existing parameters, as a joke, or to attempt to convert altcoins into bitcoins [48].

Some of the most popular implementations are:

- *IxCoin (IXC):* The International eXchange Coin [49] is the first Bitcoin clone. It was released in 2011 and it can be mined at the same time as BTC. It also has a limit of 21 million coins, but much shorter mining period (all coins should have been mined in 2015).
- *Namecoin (NMC):* It is one of the most innovative altcoins [50]. It uses Bitcoin to create a decentralised domain name system outside of the existing international system operated by ICANN. The service allows the registration of domain names that cannot be shut down or taken over by law enforcement.
- *Litecoin (LTC):* This is one of the more popular Bitcoin alternatives [51], it was created specifically to fix perceived shortcomings in BTC, and it boasts faster transaction verification times and improved storage efficiency.
- *Ripple (XRP):* In the strict sense, Ripple is not a direct Bitcoin fork [52], but it borrows some of the main ideas of Bitcoin, such as being an open source decentralised ledger. It is a currency, but also it acts as an exchange protocol for existing currencies and altcoins.
- *Dogecoin:* This started as a joke BTC fork in 2013 [53], but quickly became a currency in its own right, with a 2015 estimated market capitalisation of over US$15 million [54], making it the fourth most popular altcoin. The name comes from Doge, the popular Internet meme [55].

- *Bitcoin XT:* This is a very recent and controversial fork [56] to the original Bitcoin source code that adds two main changes, the block size is increased and it removes the need to download the entire blockchain.

2.6. Key benefits

While it can be argued that Bitcoin has become better known in technology circles, at least at the time of writing, it still continues to fall short of wider recognition and dissemination. Even though the currency has achieved a non-negligible market capitalisation of US$3.2 billion in 2015 [57], this is still relatively small [58]. Similarly, the indicators for economic activity in the currency, such as trade volume, have remained relatively small [59]. Bitcoin continues on despite this relative obscurity, and some other problems that will be detailed later in this paper.

There are various problems with existing financial markets and currencies that cryptocurrency is trying to address. Some of the benefits of cryptocurrrency are:

- *Transparency:* One of the key benefits of Bitcoin is that all transactions are publicly available and verifiable in the electronic ledger called the blockchain [60]. This provides an unprecedented level of transparency and peer verification; it is one of the features that transcends currency elements.
- *Security:* Bitcoin uses the 256-bit version of the secure hash algorithm (SHA), an encryption protocol designed by the U.S. National Security Agency. The protocol maintains the integrity of the blockchain, but is also used to sign and secure BTC wallets, providing a mathematical proof that transactions are performed from the owner of the wallet. The signature also prevents the transaction from being altered by anybody once it has been issued [61].
- *Lower transaction costs:* While in theory Bitcoin transactions could be free between all parties, the system usually has transaction fees that vary from one exchange to the other [62]. Usually, the transaction fee will go to the miner (as an incentive to miners), and these transaction fees are a function of difficulty [63]. Even with these fees, Bitcoin still boasts lower transaction costs when compared to other payment methods, with some merchants estimating that the average is at one percent, as opposed to other intermediary clearinghouses such as PayPal and Western Union, which charge from two to four percent [64]. However, it must be noted that some researchers believe that low transaction costs will not sustainable in the future [65].
- *Anonymity:* Bitcoin is theoretically anonymous. A person in possession of BTC in an encrypted wallet can spend it in any service without identification. While the anonymity aspect has clearly made it attractive as a means of payment for illegal goods and services [66], it could be used for less nefarious purposes, such as funding campaigners in authoritarian regimes [67].

- *Resilience:* Bitcoin is a decentralised currency with no central authority and no issuing body. This means that it is resilient to attacks, and in theory it also means that it cannot be brought down [68].
- *Engine for innovation:* While it is easy to ignore some grandiose claims made by some Bitcoin developers, such as the claim that it will destroy fiat currencies, or that it has the potential to combat poverty and oppression [69], it cannot be denied that its creation has given a much needed push towards innovation in the way in which we think about money, financial institutions and centrality. Anything that encourages innovation is to be welcomed.

This list is not exhaustive and only shows some of the most cited benefits of the virtual currency. There are some benefits that are more difficult to quantify. For example, there is little doubt that whatever may happen with Bitcoin, its creation has revolutionised how we think about money, value and payments in general. It is possible to be sceptical of Bitcoin, yet to be awed by its elegance and the ambitious nature of its implementation. Even if it were to disappear tomorrow, it is possible that some applications of the technology will survive. We will deal with these in the next section.

3. Problems with the current implementation

While it is clear that Bitcoin has some attractive features, it also has some serious problems that have translated into it not being adopted in the mainstream. Some of the main concerns are listed below, in no particular order.

3.1. Lack of transparency

A main selling points of Bitcoin is transparency. The client itself is open source and all transactions are open to scrutiny because all transactions must be verified by the whole, so it is possible to look at each individual transaction in the public blockchain to scrutinise 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, a feature that explains Bitcoin's popularity with the technical community.

However, this transparency is in practice limited when one considers the currency's origins. Satoshi Nakamoto, the fabled originator of the scheme, remains anonymous to this day. It is a matter of record that Bitcoin was created by a member (or members) of a cryptography mailing list using Nakamoto as a pseudonym. Some 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 a

psychological investment for anyone who understands how easy it would for an early adopter to maliciously manipulate the market.

The fact that some investors have amassed large BTC fortunes is an indication that this could be used to leverage the market. There have been several examples of possible market manipulation, with sudden large volumes in trade used to shift the price up or down [70]. There is also growing evidence that bots have been involved in currency-price manipulation on a large scale, with some analysts identifying a trading bot (nicknamed 'Willy') as being potentially responsible for inflating the price until it reached US$1,300 per bitcoin [71].

It seems increasingly indefensible for Satoshi Nakamoto to remain anonymous, particularly given the potential power of early adopters and the creators of the scheme. For such a transparent currency from a technical standpoint, this remains a rather difficult area for outsiders.

3.2. Failing anonymity

Anonymity is one of the biggest selling points for Bitcoin. This was made evident after an article in the *Atlantic* described Silk Road, a site where drugs could be acquired using Bitcoins [72]. BTC's value increased, usage increased and mining rigs were created using supercomputers and graphic cards. Because the currency is encrypted, there is theoretically no method to trace any given transaction to individual users. However, many papers express serious doubts on the much-heralded anonymity present in Bitcoin. Reid and Harrigan [73] warned that Bitcoin's much-touted anonymity was seriously flawed:

> "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." [74]

As a case study, they used a highly-publicised theft of 25,000 BTCs (with a value at the time of theft of approximately US$500,000). They were able to follow the involved transactions using their network tools, and charted these with high level of accuracy. They concluded that using network analysis and network representation it is possible to map many users to their public keys. Furthermore, an interested party could potentially try to find more information by targeting centralised services, such as exchanges and online wallet services [75].

Ober and Hamacher found that maximum anonymity is simply not possible, and that there are many points in which it would be possible for an 'adversary' to identify a party successfully [76]. This can be achieved because many

addresses are known in advance, such as addresses that originate from popular long-running mining pools. The number of operators in the Bitcoin economy has been increasing as a function of price, but the authors were able to identify some large players, allocating an identity to some BTC public key addresses [77]. It would be possible for an observer to start identifying addresses, continuously updating the list based on incoming transactions, and using merging of coins to identify two separate entities as a single one. Eventually it would be possible to identify large coin owners when they merge their coins.

Furthermore, Bitcoin users usually need to rely on intermediaries in order to purchase bitcoins, and most of these require identifying information to open an account. This data could be used to de-anonymise the user [78]. To respond to these threats, some services have been created that allows users to 'mix' their coins swapping them and changing them from one address to another, providing further anonymity, albeit with mixed results [79].

Bitcoin anonymity ultimately fails because users cannot help but operate in the real world. The arrest of Ross Ulbricht offers an excellent example of someone who had astounding levels of security and anonymity, but was eventually brought down because he made small mistakes that eventually accumulated, making it possible for law enforcement to find him [80]. This is not a problem in itself with BTC, but it serves as a timely reminder that online activity is eventually subject to regulation.

3.3. Instability

Bitcoin has been tremendously unstable throughout its trading history. While generally the overall trend has been upward if we compare today's value with that of four years ago [81], the currency has crashed several times and the price continues to swing up and down repeatedly. During its peak in December 2013, the price reached US$1,147 per 1BTC (higher in some exchanges), only to crash spectacularly to US$522 in just a few days. Needless to say, such instability is one of the reasons why it is very unlikely to be a viable currency. Imagine that you are a merchant who decides to accept BTC, and agree with a buyer to sell at the trading rate when the transaction was initiated. The first problem you would encounter is 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, which are too common throughout its trading history, could wipe away any profit.

Bitcoin's price has stabilised somewhat in the last year, but it still can suffer swings of up to US$20 in price. This makes it too unstable and seems to be keeping away investors, making it an unreliable means of payment [82]. Price instability could be part of the decentralised nature of the technology. Yglesias argues that it may continue to vary cyclically in price [83]:

> "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."

Fiat money is kept stable by all sorts of means, from fiscal policies to centralized decisions about interest rates, with devaluation or revaluation largely managed by central banks and governments to ensure an orderly change of equilibrium. Panics were caused in 2008 with the sudden devaluation of the Swiss franc and Icelandic krona, or in 1998 with the devaluation of the Russian rouble and other currencies. It is possible that stability can only be achieved through centralization. Others have proposed more libertarian methods of creating stability [84], but at the moment there is no solution as long as the currency remains mostly a speculative vehicle, and not so much a currency for paying for goods and services.

3.4. Lack of replicability

In danger of over simplifying a complex issue, Bitcoin is nothing more than the ownership of a cryptographic address. In reality, most bitcoins exist only as files in a computer or mobile device; a wallet file has access to a private key used to secure the money. This creates one of the biggest issues with Bitcoin to date: the ease of losing one. If the wallet file is lost, then the bitcoins it contains are lost forever [85]. There are ways to back up the keys, such as by keeping physical copies off-line 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 a time when people were testing the technology and deleted their wallets [86]. 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. Developer John Ratcliff conducted a similar study of the blockchain, and identified a very large number of dormant coins, what he called 'zombie coins', which amount to 30 percent of all the Bitcoins ever mined [87]. While it is difficult to ascertain just how many of these coins are lost, this is evidence of a serious problem for the viability of Bitcoin.

It must be said that missing and lost coins has not been seen as a problem for enthusiasts, as they point out that each BTC is divisible up to eight decimal points. It is also assumed that the fewer BTCs there are, the higher the value. Defenders of Bitcoin also point out that it is possible to lose real money. 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 on 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 a given wallet. Some online wallets have had problems with security and lost coins, not to mention the real possibility of fraud.

3.5. 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 [88]. Moderate 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 deflation, otherwise it ceases acting as a medium of exchange and becomes akin to scarce commodities, such as diamonds. Furthermore, the decentralised nature of Bitcoin makes it uniquely unfit for banking [89], which would further encourage hoarding by individuals.

There is some evidence that hoarding is taking place. Ron and Shamir found that the actual number of BTCs in circulation was considerably smaller than previously thought, with 78 percent of the entire BTC reserve at the time (7,019,100 BTC) placed in "saving" addresses, and only 22 percent of all BTCs created (including those lost) in circulation [90]. 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 another. The data strongly indicates that there is considerable ownership concentration in the BTC network. Ron and Shamir found that:

> "Thirty-six percent of all owners received fewer than one BTC (currently worth about US$12) each throughout their lifetime, 52 percent received fewer than 10 BTCs and 88 percent fewer than 100. At the other end of the distribution there are only four owners who received over 800,000 BTCs and 80 owners who received over 400,000." [91]

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 just a few. BTC is not being used as a payment system, but as a commodity where users exchange bitcoins for cash and vice versa.

3.6. Security and BTC theft

Criminal lawyers and investigators have taken a very significant interest in Bitcoin [92]. 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 transactions anonymous.

As with many things online, theory is often defeated by a combination of greed, laziness, ignorance and simple intermediary failure. As stated earlier, 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 US$5 dollar wrench would suffice [93]. Practice has been bearing this out. For a long time, the Bitcoin client did not encrypt the wallet.dat file itself, which left the currency vulnerable to basic hacking attacks [94]. Similarly, hackers began successfully targeting the exchanges, managing to steal thousands of BTCs [95]. Strong encryption of the scheme does not protect against fraudsters and scam artists. The security issues with Bitcoin are hard to assess, but risk assessment of various aspects of Bitcoin undertaken by NEMODE, a U.K.-based research project, has concluded that there are various security issues with very high risk, such as general security, subversive miner strategies, loss of keys and man-in-the-middle attacks [96].

This is a serious problem with the currency. As exchanges and wallets are the weakest links in the chain, the currency requires some technical knowledge to operate securely, and this could affect average users from adopting the currency. This relative insecurity stands in stark contrast with existing protection given to traditional banking users [97]. The only BTC recourse is reputational: to go online to complain.

Law enforcement is difficult because agencies may simply not understand the technology, not considering it worthy of prosecution. Until there are arrests related to BTC fraud and hacking, serious investors might well decide to stay away from Bitcoin because it simply is not safe enough, as it draws hackers like no other payment system. Bitcoin might therefore be suffering from a 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.

3.7. 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 [98], stating that a large mining conglomerate was becoming too powerful, and had actually reached 51 percent of all mining capacity for Bitcoin during a few hours. Essentially the system was no longer decentralised. Any entity controlling 51 percent of the mining power would accrue all of the Bitcoins mined while in majority. The controlling mining conglomerate could send false information to the blockchain, which would amount to altering transaction history [99].

As a result, the Bitcoin community panicked, 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 percent again. Since the incident, Ghash.io made a statement declaring that they would take steps to avoid becoming too dominant again [100]. At the time of writing, Ghash.io use decreased to only two percent, but other large mining conglomerates have emerged with over 22 percent of total distribution [101].

Many Bitcoin enthusiasts have dismissed centralisation concerns, pointing out that the community polices itself adequately. They also note that miners migrated to other pools as soon as the 51 percent threshold was crossed [102]. More pragmatic developers have proposed technical solutions, such as implementing an algorithm that would force nodes to store the entire blockchain locally, which would help against a 51 percent conglomerate controlling the entire system [103].

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.

3.8. Computational inefficiency

A less-explored area of concern with Bitcoin is that, at least as currently implemented, it might be energy inefficient. Bitcoin generates value by requiring those who participate in the network to dedicate computing power to verify transactions. This presents two problems for the scalability of the network, namely the computational power required to mine BTC and the size of the blockchain itself.

The computational power dedicated to mining has continued to increase over time. In Bitcoin, computing power is called the hash rate, and the unit of measure is the hash/second, meaning a calculation per second. Ten tera hashes per second (Thash/s) means that the network is performing 10 trillion

calculations per second, with the hash rate at the time of writing standing at over 410 thousand Thash/s. Whichever way you measure it, that is an astounding amount of computing power used to produce value. O'Dwyer and Malone found that the entire Bitcoin network uses energy equal to that consumed in all of Ireland [104]. Even under normal circumstances, such a staggering amount of energy expenditure might prompt questions about Bitcoin's carbon footprint and other related environmental problems. Even if we ignore environmental issues, it is difficult to justify such consumption on economic grounds. O'Dwyer and Malone concluded in 2014 that "the cost of Bitcoin mining on commodity hardware now exceeds the value of the rewards". [105]

Another issue is that the size of the blockchain is starting to become a problem. At the time of writing it was reaching 40 gigabytes [106]. This has some practical implications for BTC as a currency, as the size of the blockchain may hinder the speed at which transactions are verified. Average transaction times vary a lot depending on network loads, but currently it ranges from 6–12 minutes per transaction [107]. As the blockchain size increases with more transactions, hosting of the entire blockchain could become a problem as well, as it is thought that the blockchain may reach three terabytes in size within 10 years [108].

4. Legal and regulatory issues

The decentralised nature of Bitcoin and a lack of a clear set of actors may prompt some to think that it is not possible 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.

4.1. The legal nature of Bitcoin

In an episode of the popular TV series *The Good Wife*, appropriately entitled 'Bitcoin for dummies', a person who acts on behalf of 'Mr. Bitcoin', the anonymous and mysterious inventor of the cryptocurrency, hires the protagonist's law firm to defend him against a government action. The premise of the episode is that the U.S. Department of the Treasury wants to find the creator of Bitcoin because the digital currency is illegal in the United States. Although a crude depiction of the legalities of currency and commodities surrounding Bitcoin, the episode pinpoints some of the most pressing legal issues regarding their use. What is their legal status? Are they a currency? Are they a commodity? Are they a security? In short, is Bitcoin legal?

There are generally two types of currency from a legal perspective, legal tender and legal currency [109]. Legal tender is simply currency that cannot be refused in the fulfillment 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 [110]. For example, there is something called a local currency, which is a currency that is usually accepted for payment in a local area, within a small number of participating stores [111]. Similarly, in the most of the U.K. the Bank of England notes are legal tender, but in Scotland and Northern Ireland, there are notes issued by several banks which act as legal currency. It is also common to see economies with a weak local currency accept international reserve currencies (for instance U.S. dollars or Euros) as legal currency [112].

4.1.1. United States regulatory response

In the United States, only the U.S. dollar is legal tender [113]. 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 U.S. 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 U.S. dollar is allowed as the official currency of the United States. According to the F.B.I. “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.” [114] It would seem clear that local currencies that may compete with the dollar are not allowed, but the question of whether Bitcoin can be considered a currency for these purposes is not clear. There does not appear to be consensus that BTC would fall foul of regulation designed to protect the U.S. dollar as legal tender [115]. On the contrary, there have been electronic payment systems in existence for over a decade and there have not been attempts to curb them by using counterfeiting legislation [116].

However, all of the above does not mean that Bitcoin is illegal in the U.S. Because of many of the problems highlighted earlier, BTC is not currently used as a currency, perhaps with the exception of Web sites dealing in illegal goods in the ‘dark Web’ [117]. 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. Yang [118] makes a very strong case that Bitcoin can be considered a security under U.S. law, particularly because the definitions of a security present in the Securities Act of 1933 and the Securities Exchange Act of 1934 are broad enough to include all sort of bonds, debentures and certificates of interest as well as investment contracts. The very open definition was eventually used to classify as a security unusual investment contracts, such as citrus trees and earthworms [119]. The U.S. Supreme Court [120] has specifically defined an investment contract as an agreement that must involve “(1) an investment of money; (2) a common enterprise; and (3) an expectation of profits to derive solely from the efforts of others.” [121] Yang argues that Bitcoin fulfills all of these three requirements, and therefore can easily be classified as a security, at least until

the law changes to classify it more adequately. It would also be easy for Bitcoin to be treated as a commodity under the broad definition present in the Commodity Exchange Act 1936, which offers a long list of goods that ends with the phrase “and all other goods and articles” [122].

4.1.2. European regulatory response

The situation in Europe and the U.K. is less ambiguous than in the U.S. First, there is considerably more regulatory acceptance for alternative currencies to those issued by central banks authorities, as evidenced by the aforementioned example of national legal currencies in the U.K., and a generally forgiving position for local currencies, such as the Bristol Pound, Brixton Pound and Lewes Pound [123]. These are very small payment schemes where a few participating retailers accept a note which acts more like a voucher and it is usually of very limited circulation. While BTC is larger by many degrees of magnitude, there does not seem to be any indication from regulators and central banking authorities in Europe that there will be a crackdown on Bitcoin over its legal status [124].

Second, Europe has already in place a legal framework for the regulation of electronic money, which could be used to cover virtual currencies such as Bitcoin. The Electronic Money Institutions Directive 2009/110/EC [125] contains rules for all sorts of electronic purses that can be used to store value in an electronic format, be it via a computer, a mobile device or online. The Directive 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;
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 (EMI) can issue electronic value. There is a high threshold for an electronic money institution, as the EMI would have to fulfil quite a number 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 with regards to Bitcoin. If Bitcoins are not an EMI in Europe, then their status as currency is in doubt. The European Banking Authority (EBA) has opined that virtual currencies (VCs) do not fulfil many of the requirements of a currency, and therefore should not be considered legal tender:

> "VCs are not legal tender, which means the following features are not fulfilled: (a) mandatory acceptance, *i.e.*, that the creditor of a payment obligation cannot refuse currency unless the parties have agreed on other means of payment; (b) acceptance at full face value, *i.e.*, the monetary value is equal to the amount indicated; and (c) that the currency has the power to discharge debtors from their payment obligations." [126]

While it does not state directly, the EBA opinion infers Bitcoin being a commodity that can be exchanged for fiat money.

4.2. Regulatory actions to date

As some of the legalities surrounding Bitcoin are still not fully clear, there is still considerable scope for legislators and regulators to try to tackle the problems that might arise from the use of virtual currencies. 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, 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 been cautious in tackling some of the legal questions exposed by the emergence of cryptocurrencies. 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 intermediaries 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 [127].

So what could regulators do? Based on Mayer-Schönberger and Crowley [128], 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 Web sites 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. This section would also cover the banning and/or criminalisation of the use of the currency to pay for illegal activities or for money laundering.
4. *Selective regulation:* regulators impose some restrictions to specific aspects of virtual currencies, such as taxation and the regulation of intermediaries.

5. *'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 that 'do-nothing' option is a minor variant on Option 4 [129].

4.2.1. Virtual sovereigns

During the first few years of the existence of cryptocurrencies, the lack of any meaningful regulation or enforcement meant that intermediaries were left to self-regulate through terms of use and policies [130]. Interestingly, some commentators and participants in the economy advocate for either minimal regulation or to continue with the virtual sovereign approach [131]. The problem with this is that at the moment self-regulation has been translated into economic losses for unsuspecting users, as many exchanges and intermediaries were operating haphazardly or even fraudulently.

Lack of regulation of the sector has translated into a fertile ground for fraudsters and scam artists, from the existence of phishing sites passing off as exchanges [132], to online wallet services going bust. But the biggest example of the failure of self-regulation has to be the case of Mt. Gox. Mt. Gox was forced to file for bankruptcy in Japan after hackers allegedly managed to get into their system and steal US$446 million worth of bitcoins [133]. Some claim the site was riding a wave of speculation with coins that it did not have, accruing a large amount of debt. This is precisely the type of practice that regulation is supposed to stem.

4.2.2. Prohibition and selective prohibition

It should not be surprising that there has not been a regulatory push towards outright outlawing of Bitcoin, or any other cryptocurrency for that matter. There is no reason to suspect that governments feel threatened enough by Bitcoin at this time to warrant some form of ban, but most importantly, such an action could prove futile given the currency's decentralised nature [134].

Attempts at some partial prohibition of specific elements of the technology have been made. Thailand has attempted an outright ban on Bitcoin, although unsuccessfully. In 2013 a Thai company called Bitcoin Co. Ltd. was trying to register to operate in Thailand exchanging local currency for BTC, but the Foreign Exchange Administration and Policy Department declared that selling, buying, trading, exchanging and transferring bitcoins outside or within the country were illegal activities [135]. However, trading was re-opened six months later when the Bank of Thailand decided that the Foreign Exchange Administration lacked competence to ban BTC trading [136]. Russian regulators made some noise about cracking down on BTC trading but these never really materialised [137]. China has been the only jurisdiction to successfully attempt a major crackdown of Bitcoin. In December 2013, responding to claims of theft and fraud to Chinese nationals using BTC, the People's Bank of China made an announcement regarding Bitcoin in order to

“protect the public’s property rights, to protect RMB’s official currency status, to prevent money laundering risk and to protect financial stability.” [138] The statement contains two very interesting measures. Firstly, it classifies BTC as a commodity and clearly disavows it as any type of currency. Then it seriously curbs its viability by restricting the way in which financial institutions may use it. The statement reads:

> “At this stage, all financial institutions and payment institutions must not use Bitcoin to set price for product or services, not buy or sell Bitcoins, not act as a market maker for Bitcoins, not underwrite insurance related to Bitcoin or cover Bitcoin in insurance, not directly or indirectly provide other Bitcoin related services, including registering, trading, clearing, settlement; not accept Bitcoin or use Bitcoin as payment tool; not start a Bitcoin and RMB or foreign currency exchange; not start a Bitcoin saving, trust or mortgage service; not issue Bitcoin related financial services; not use Bitcoin as the investment in trusts or funds.”

While this is not a prohibition, it effectively restricted most of the currency-like functions of Bitcoin, as it could not be used to clear settlements or to make payments. The above meant that BTC operators could mostly trade it as a commodity, leaving out most other functions. It is curious that the announcement coincided with BTC’s highest trading month and helped to push down prices considerably, heralding a crash that halved the price in less than a month [139].

It must be said that while the Chinese crackdown had some adverse effects on the use of Bitcoin as a currency [140], it is still being traded in China and the most active exchange is Chinese [141]. The yuan has overtaken the dollar as the top traded exchange currency in the Bitcoin economy [142]. The reason for this might be counterintuitive if we think of Bitcoin as a currency, but it makes sense if we see it as a commodity. BTC’s popularity in China may be attributed to for domestic investors because, according to some analysts, “[t]here is not much else one can invest in.” [143]

4.2.3. Selective regulation

Most of the regulatory responses so far have been related to taxation, and even these have been rather low key in comparison to the Chinese experiment [144]. In the United States, the Financial Crimes Enforcement Network (FinCEN) issued guidelines specified that decentralized currencies should comply with money laundering regulations [145]. In the U.K., Her Majesty’s Revenue and Customs (HMRC) issued a briefing paper detailing its position on the tax treatment of income received from, and charges made in connection with, activities involving Bitcoin and other similar cryptocurrencies [146]. 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. HMRC has in the interim 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 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, continuing to behave mostly like a commodity.

This would bring it under the umbrella of securities and commodities regulators, such as the Security and Exchange Commission (SEC) or the Commodity Futures Trade Commission (CFTC) in the U.S. While these entities have not made any attempts to regulate Bitcoin directly, the SEC has imposed sanctions on unauthorised traders operating securities online for Bitcoin and Litecoin [147]. The SEC is also studying the approval of several securities companies operating as mutual fund and other Bitcoin-related financial instruments [148]. Finally, the SEC has issued a strongly worded statement warning investors interested in Bitcoin [149]. In it they point out some of the issues that we have enumerated earlier, such as the problem with the potential for losing bitcoins, lack of recourse if something goes wrong, and security concerns. They comment:

> “Both fraudsters and promoters of high-risk investment schemes may target Bitcoin users. The exchange rate of U.S. dollars to bitcoins has fluctuated dramatically since the first bitcoins were created. As the exchange rate of Bitcoin is significantly higher

> today, many early adopters of Bitcoin may have experienced an unexpected increase in wealth, making them attractive targets for fraudsters as well as promoters of high-risk investment opportunities."

European authorities seems to echo the warnings to consumers, with the European Banking Authority issuing a detailed list of potential risks for both consumers and investors that include many of those cited already, including monetary loss due to fraud, price instability, theft and the user's inexperience, which makes consumers unable to assess risk adequately [150].

4.2.5. Do nothing

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. 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, awaiting any further developments to act.

Many regulators seem to be adopting the wait-and-see approach. Japanese authorities have stated [151] that they will monitor for illegal activity with Bitcoins, but will not regulate them for the time being. Similarly, 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." [152]

However, there is concern that not taking any action will backfire on regulators. There are stories about illegal activities using Bitcoins, which eventually may prompt some form of action, at least to be seen as doing something to discourage blatant criminal activities. Similarly, news about fraud and exchanges becoming insolvent might also prompt some sort of action. Having provided a long list of risks for investors, users and financial institutions, the European Banking Authority issued the following warning to regulators against doing nothing:

> "Regulators themselves incur risks regardless of whether or not they do anything at all, deliberately decide not to regulate or decide to regulate but the approach fails. The risks may be of a legal nature, of a reputational nature or because the activity undermines one or more of the regulator's objectives. Unlike the risks in the previous categories, the mitigation of the risks listed below is firmly in the hands of the regulators." [153]

The argument from the European Banking Authority is that regulators could see their reputation diminished if they allow illegal or fraudulent activity to go unchecked, but they would also be facing legal action due to inactivity. The choice then is to take some form of regulation.

4.2.6. Specific regulation proposals

A few specific regulatory proposals of note have been drafted. The California legislature is considering a virtual currency bill [154], which mostly creates a requirement for registration to the relevant regulator body for any person or institution wishing to engage in any virtual currency business. The bill defines virtual currency as "any type of digital unit that is used as a medium of exchange or a form of digitally stored", but excludes units used in online games, or other digital units that "cannot be converted into, or redeemed for, fiat currency." This would tend to exclude vouchers, loyalty points and air miles. Bodies trading in digital currencies must obtain a licence to operate.

One of the most important regulatory developments in France was a 2014 report by the Minister of Finance, Michel Sapin [155]. 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 about the anonymity of transactions, which could have tax and money laundering implications. Therefore, France has made clear regulatory direction 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.
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.

The European Banking Authority followed the lead of the French recommendations. In their aforementioned report on virtual currencies, they also listed a detailed number of possible regulatory responses to the challenges posed by virtual currencies [156]. Some of the main proposals include the following:

- *Creation of a scheme governance authority.* This will be a non-governmental entity that will be accountable to regulators and it will institution that will be a mandatory requirement for virtual currencies,

which will therefore operate as a financial institution. The authority will act as a central body that will have the responsibility of maintaining the public ledger and manage the currency's protocol(s).

- *Customer due diligence (CDD) requirements.* Exchanges and other consumer-facing intermediaries will have to collect identifying information.
- *Fitness and probity standards.* To diminish the chance of fraudulent activity, participating entities and individuals will have to pass probity standards present in other financial sector entities.
- *Mandatory incorporation.* Participating entities must be incorporated to ensure accountability and liability.
- *Transparent price formation and requirements against market abuse.* To avoid market manipulation and insider trading, intermediaries must comply with existing regulation against such practices in the financial sector.
- *Authorisation requirements.* Market participants must register to the relevant regulator and/or scheme governance authority, and must be authorised to operate.
- *A global regulatory approach.* Because of the international nature of VCs, there needs to be a coordinated international response by regulators around the world.
- *Evidence of secure IT systems.* Self-explanatory and required by independent audit.
- *Other standard procedures in financial institutions.* There are various proposals that are standard requirement for financial institutions. These include having a corporate governance scheme, operating with minimum required funds and separating client account currency from their own VCs.

Some of these proposals are nothing more than an attempt to bring VC institutions into the fold of the wider regulatory framework already in existence in the financial sector in general. Some of these could be easily adopted in the existing Bitcoin economy, such as requiring exchanges to register to authorities. Some will be more difficult to achieve and might very well destroy some of the unique features present in cryptocurrencies that make them so appealing to some in the first place. Needless to say, requiring the existence of a central body is anathema to the ethos of cryptocurrencies. Similarly, increased scrutiny comes at a price; these suggestions might increase transaction costs as well.

It is not possible at the moment to foresee what will happen next. If cryptocurrencies remain a niche interest by the technical elites, then it is difficult to foresee that any of the above recommendations will be implemented. If on the other hand Bitcoin and other VCs finally become widespread, then there will surely be some sort of regulation at some point.

5. Alternative uses of blockchain protocols

A blockchain is quite simply any open, cryptographic, decentralised ledger, so in theory it can be implemented into any sort of scheme, financial or not, that requires a record of transactions. As has been stated repeatedly, in Bitcoin the ledger is public and decentralised. Since anyone can check past, present and proposed transactions, there is increased reliability in the system. The main function of the blockchain in Bitcoin is to avoid the potential of double-spending money. However, the blockchain idea is independent of the existence of Bitcoin. In the off-line world, barring counterfeiting, it is impossible to double-spend money as people hold limited amounts of physical currency. Monetary transactions however more often occur as the digital movement of value from one account to the other [157]. The idea is for the holding institution to contain a master ledger, in other words a record of the money in all of the accounts, making it possible to follow movements from one to the other [158].

In order to have a viable blockchain alternative outside of the Bitcoin implementation, a developer can use existing protocols and open source code to create a verification mechanism that must fulfil three important functions key to any blockchain distribution. These are:

- *Proof of work.* The proof of work (POW) is the way in which Bitcoin rewards miners for conducting transaction verification operations, which are expensive computational transactions. Any blockchain alternative will have to have an alternative POW pay-out if the intention of the technology is not monetary. This could be social, such as solving mathematical equations or finding prime numbers [159].
- *Authentication.* This is the main function of a blockchain, the implementation must be designed to validate transactions securely and unequivocally [160].
- *Decentralization.* The blockchain must be decentralized, so copies of the entire ledger cannot be held centrally. This presents a few technical problems, such as the increasingly unmanageable size of the blockchain as more transactions accumulate [161].

There are hundreds of such potential applications in the financial markets, such as bonds, stocks and derivatives [162]; but it would also be possible to apply the same type of technology to automated contracts [163], or even copyright licensing agreements [164]. The idea is to attempt to bypass the difficulties of contract formation and other legal transactions by allocating rights and responsibilities through electronic tokens that then would be recorded in a common ledger. A recent report explains:

> "While all of the high-value applications of the first wave of blockchain innovation are explicitly financial, this is not the case for the second wave of blockchain innovation, which primarily rests on the idea of a 'smart contract.' Put simply, a smart contract uses software code to implement human intentions by dynamically carrying out instructions embedded in

> tokens associated with a contract, rather than relying on legal texts interpreted by courts, regulatory bodies or other legal institutions." [165]

But this would not only apply to contracts, but also to distributing and allocating rights within decentralised organizations themselves [166].

There are already a number of tools that are being developed to take advantage of the blockchain beyond payment systems and cryptocurrencies. One of the most publicised has been Project Ethereum [167] which creates "a 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." [168] In other words, Ethereum is a protocol for smart open ledgers where users can allocate their own rules and values. Ethereum has released an open source mining application to the public, directed mostly at developers, and users can mine its own currency called "ether" by allocating processing power to validate transactions. The system allows users to create legal documents that can be validated through the blockchain while at the same time allowing users to mine the new currency.

D-CENT (Decentralised Citizens ENgagement Technologies) is an European Union (http://dcentproject.eu/) project that has proposed the creation of a social blockchain toolset that will allow adopters to generate their own alternative currency. The interesting part of this scheme is that it changes the economically-minded proof of work with a social one, which will be decided upon by the community [169]. Another project called Chain [170] is proposing to use blockchain protocols to pay for mobile minutes, verify energy credits, store loyalty points and scrutinise securities. Many other projects are being announced routinely, with applications as varied as smart solar panels [171] and assistance to operate stock markets [172].

While these proposals are very interesting, IT law is replete with grandiose claims of life-changing technologies that will revolutionise lives. It is often too easy to fall prey to the latest meme adopted by some commentator [173]. Talk of the blockchain is reaching the level that previous technologies received, such as the cloud and 3D printing. While the reach of these is indeed great, we cannot lose sight of the limitations that exist within the Bitcoin environment. Furthermore, the idea of conducting legal transactions automatically by means of smart contracts and intelligent agents is not new [174]. Every generation brings a new crop of suggestions, claiming that we are about to make lawyers a thing of the past, with most transactions completed by computers, yet the legal profession persists [175].

Despite this critique of the Bitcoin meme hype, the blockchain itself has immense potential, particularly for transactions that require transparency, resilience and decentralisation.

6. Conclusions

This paper examined several areas related to cryptocurrencies. First, we outlined the basics of cryptocurrencies for a non-specialist audience. Second, we looked at the advantages presented by Bitcoin and examined problems with implementation. We then turned in depth to the practical and regulatory challenges presented by Bitcoin and crypto-currencies in general.

We conclude that though Bitcoin may be the equivalent of Second Life a decade later, a liberating technology that is overhyped and poorly executed, so blockchains may be the equivalent of Web 2.0 social networks, a truly transformative social technology. In the last year there has been a marked shift in the rhetoric emerging from the Bitcoin camp. While there are still (and probably will ever be) a core group of enthusiasts who believe in the cryptocurrency with a fervour matched only by the Free Software movement, Bitcoin has not matched the expectations of some proponents. Various crashes, and wave after wave of scandals and allegations of fraud have decidedly dented the perception that Bitcoin is the currency of the future. The relative difficulty in acquiring and spending BTC has meant that it has continued to elude mainstream acceptance. At the same, there are other electronic payment methods such as Apple Pay [176], launched in 2015. While Bitcoin may well recede from the public imagination in the future as a virtual currency, one aspect of the scheme is gaining momentum. It is the idea of a transparent, distributed and decentralised transaction ledger: the blockchain.

It is decreasingly accurate to call Bitcoin a currency. Money is a unit of account, store of value and medium of exchange. Bitcoin is none of those, in any serious sense. Bitcoin has too many problems to be the solution. An anonymous and decentralized payment system could indeed revolutionise the economy, help to end the disproportionate power of some banking systems and 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 that turns the blockchain, Bitcoin's proof-of-transaction open log, into a platform for creating a smart contract decentralised platform. We may very well be talking about blockchain in the future with Bitcoin as the first implementation of an open ledger.

Bitcoin is a revolutionary idea in achieving decentralisation, but the current implementation suffers from libertarian economic dogma and critical mistakes, such as the potential for a large entity with access to large computing power to control the public records. The blockchain could bring everything that is good about Bitcoin and translate it into decentralised applications. This will certainly merit further disinterested independent

research in the future, separated from the hype and financial self-interest of the Bitcoin community.

The wider research questions relate to the future of fiat currencies and the possibility of social production and sharing based on blockchains as the basis for the record of exchange [177]. Some proponents of blockchains and social production suggest it may supplant increasingly distrusted sovereign currencies [178]. Our research has been more limited to a critical exploration of the use of the first widely adopted non-proprietorial virtual currency, Bitcoin. We must remember that in the late nineteenth century that there was a fierce, agriculturally based mass resistance to fiat money, which failed. Overblown claims about blockchain enabled virtual currencies may similarly fall by the wayside with less mass mobilisation online or off-line. As a site of resistance to free market dogma, virtual currencies may be limited, but as an organising principle for cooperative sharing alongside the sovereign fiat currency capitalist market, it may have a stronger, if niche, future, just as cooperative movements gained coexistence with mass consumer capitalism in the previous 150 years. A new form of cooperative commons online may be enabled by blockchains, but it will most likely not be built on Bitcoins for the reasons we have identified in this paper. 

About the authors

Andres Guadamuz is Senior Lecturer in Intellectual Property Law, School of Law, Politics and Sociology at the University of Sussex.
E-mail: a [dot] guadamuz [at] sussex [dot] ac [dot] uk

Chris Marsden is Professor of Media Law, School of Law, Politics and Sociology at the University of Sussex.
E-mail: c [dot] marsden [at] sussex [dot] ac [dot] uk

Acknowledgements

The first draft of this paper was case study prepared for Joint Research Area: Virtual Communities of the European Internet Science Consortium 7th Framework Programme, Network of Excellence, under Grant No. FP7–288021, in which network we collaborated with Dr. Jonathan Cave (Warwick), Dr. Alison Powell and Dr. Paolo Dini (LSE), Dr. Melanie de Rosnay (CNRS), Professor Juan Carlos de Martin (UNIBO) and others. Research was also funded by the European Commission JUST/2013/ACTION GRANTS Grant Agreement Number 4562 Openlaws, in which network we collaborated with Dr. Paolo Dini and colleagues at the London School of Economics, and others, on the application of virtual currencies to legal reputational markets. All errors and omissions remain our own.

Notes

1. See European Commission, 2010. "Digital agenda for Europe: Communication from the Commission" (26 August), at http://ec.europa.eu/digital-agenda/en/news/digital-agenda-europe-communication-commission-26082010.

2. Broadband infrastructure in rural areas was a focus of the American Recovery and Reinvestment Act of 2009. In Europe, for instance, industry 4.0, the Internet of things, intelligent transportation systems and smart cities are all initiatives using ICT-enabled innovations in respectively manufacturing, inventory control, distribution, urban planning and environment: see http://ec.europa.eu/europe2020/europe-2020-in-a-nutshell/flagship-initiatives/index_en.htm.

3. P. Mason, 2015. "China's currency gambit and Labour's debate about quantitative easing: Old and new ways to cope with economic crisis," *Guardian* (16 August), at http://www.theguardian.com/commentisfree/2015/aug/16/china-labour-debate-currency-economic-crisis.

4. Icelandic krona have declined by almost 40 percent in value compared to £Sterling during 2008, and has maintained that 40 percent devaluation since: see http://www.xe.com/currencycharts/.

5. Robert Zoé, 2015. "Pirates largest party fourth month in row," *Iceland Review* (4 August), at http://icelandreview.com/news/2015/08/04/pirates-largest-party-fourth-month-row.

6. J. Bearman, 2015. "The untold story of Silk Road," *Wired*, at http://wrd.cm/1L6svlW.

7. J. Bartlett, 2014. *The dark net: Inside the digital underworld*. London: William Heinemann.

8. J. Mullin, 2015. "Sunk: How Ross Ulbricht ended up in prison for life," *Ars Technica* (29 May), at http://bit.ly/1M7ChnP.

9. Based on a search of 'Bitcoin' in the *Social Science Research Network* (http://papers.ssrn.com last accessed 19 August 2015). The original academic law review article was downloaded 11,140 times in four years until 19 August 2015: R. Grinberg, 2012. "Bitcoin: An innovative alternative digital currency," *Hastings Science & Technology Law Journal*, volume 4, number 1, pp. 159–207, at http://uchstlj.org/wp-content/uploads/2015/10/Bitcoin-An-Innovative-Alternative-Digital-Currency.pdf.

10. A. Guadamuz and C. Marsden, 2014. "Bitcoin: The wrong implementation of the right idea at the right time" (18 June), at http://ssrn.com/abstract=2526736 or http://dx.doi.org/10.2139/ssrn.2526736

— the 91st academic paper published on Bitcoin in SSRN since it rose to prominence.

11. For the beginner interested in cryptocurrency, see, for example, D. Forrester and M. Solomon, 2013. *Bitcoin explained: Today's complete guide to tomorrow's currency* (Charleston, S.C.: CreateSpace); A.M. Antonopoulos, 2015. *Mastering Bitcoin: Unlocking digital cryptocurrencies* (Sebastopol, Calif.: O'Reilly); D. Wilcox, 2014. *Bitcoin beginner's guide: Everything you need to know to become rich with Bitcoins* (Clydebank Publishing); C. Barski and C. Wilmer, 2014. *Bitcoin for the befuddled* (San Francisco: No Starch Press).

12. Amongst libertarian texts are B. Kelly, 2015. *The Bitcoin big bang: How alternative currencies are about to change the world* (Hoboken, N.J.: Wiley); P. Vigna and M.J. Casey, 2015. *The age of cryptocurrency: How Bitcoin and digital money are challenging the global economic order* (New York: St. Martin's Press).

13. N. Popper, 2014. *Digital gold: Bitcoin and the inside story of the misfits and millionaires trying to reinvent money* (New York: Harper); D. Frisby, 2014. *Bitcoin: The future of money?* (London: Unbound); Y. Jenkins, 2015. Bitcoin: Millionaire maker or monopoly money? (Charleston, S.C.).

14. P. Anning, S. Hoegner and J. Brito, 2015. *The law of Bitcoin*. Bloomington, Ind.: iUniverse.

15. D.L.K. Cheun (editor), 2015. *Handbook of digital currency: Bitcoin, innovation, financial instruments, and big data*. Amsterdam : Elsevier/AP; P. Franco, 2015. *Understanding Bitcoin: Cryptography, engineering and economics*. Chichester, West Sussex: Wiley.

16. J. Robinson, 2014. *BitCon: The naked truth about Bitcoin*.

17. A useful introduction is M. Swan, 2015. *Blockchain: Blueprint for a new economy*. Sebastopol, Calif.: O'Reilly Media.

18. A. Guadamuz, "Virtual currency and virtual property revisited," *Technollama* (11 February 2013), at http://bit.ly/1MaeW4N. On regulation in virtual worlds see B.F. Fitzgerald, 1997. "Life in cyberspace: A simulating experience," *Computer and Telecommunications Law Review*, volume 3, number 3, pp. 136–138; R. Bond, 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*, volume 20, number 4, pp. 121–128; S. James, 2008. "Social networking sites: Regulating the online 'Wild West' of Web 2.0," *Entertainment Law Review*, volume 19, number 2, pp. 17–50; K.L. Petrasic, 2013. "DATA's self-regulatory quest to legitimise virtual currencies," *E-Finance & Payments Law & Policy*, volume 7, number 9, pp. 6–7; M. Taylor and M. Matteucci, 2009 "Virtual worlds," *Computer and Telecommunications Law Review*, volume 15, number 5, pp. 124–147; B. Regnard-Weinrabe, M. Taylor and R. Savary,

2013. “Virtual currencies, the risks and the regulatory radar,” *E-Finance & Payments Law & Policy*, volume 7, number 7, pp. 10–11.

19. See reviews of earlier literature in J.M. Balkin and B. Noveck (editors), 2006. *The state of play: Law and virtual worlds*. New York University Press; T. Davies and B. Noveck (editors), 2006. *Online deliberation: Design, research, and practice*. CSLI Publications/University of Chicago Press; B. Noveck, 2006. “A democracy of groups,” *First Monday*, volume 10, number 11, at http://firstmonday.org/article/view/1289/1209.

20. The vast recent literature on Bitcoin and its legal challenges includes M.G. Munck, 2011. “Future payments in a disruptive digital world,” *E-Finance & Payments Law & Policy*, volume 5, number 4, pp. 12–13; A. Alleyne, 2010. “Virtual currencies: Can they classify as property?” *E-Finance & Payments Law & Policy*, volume 4, number 5, pp. 14–15; D. Tavan, 2013. “A brave new Bitcoin world?” *Banker* (August), pp. 74–76; M. Taylor, R. Savary, and B. Regnard-Weinrabe, 2013. “Virtual currencies,” *Computers & Law*, volume 24, number 3, pp. 31–34; T.A. Anderson, 2014. “Bitcoin — Is it just a fad? History, current status and future of the cyber-currency revolution,” *Journal of International Banking Law and Regulation*, volume 29, number 7, pp. 428–435; R. Courtneidge, 2014. “Crypto currencies and the regulators: Friends after all?” *E-Finance & Payments Law & Policy*, volume 8, number 2, pp. 8–9; J. Dixon, 2013. “The importance of an effective Bitcoin exchange market,” *E-Finance & Payments Law & Policy*, volume 7, number 6, pp. 6–7; E. Jankelewitz, D. Nemirovsky, B.I. Reyhani, and A. Vaziri, 2014. “Regulators respond to the big questions posed by Bitcoin,” *E-Finance & Payments Law & Policy*, volume 8, number 4, pp. 6–8; J. Meek, 2014. “Banks ‘killing’ bitcoin industry, expert warns,” *Operational Risk & Regulation*, volume 15, number 5, p. 10; J. Meek, 2014 “Funny money,” *Operational Risk & Regulation*, volume 15, number 2, pp. 23–25.

21. 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.

22. See the review by Second Life’s co-founder C. Ondrejka, 2004. “Aviators, moguls, fashionistas and barons: Economics and ownership in Second Life,” at http://ssrn.com/abstract=614663.

23. On gaming and virtual currencies see N.J. Gervassis, 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*, volume 3; S. Anil, A.K.W. Jie, J.S.H. Min, and Q.C.W, Xiu, 2012. “Virtual property — A theoretical and empirical analysis,” *European Intellectual Property Review*, volume 34, number 3, pp. 188–202; R. Courtneidge and V. Lloyd, 2013. “Accepting Bitcoin as payment for online gambling services,” *World Online Gambling Law Report*, volume 12, number 2, 3–4; D. Margaritov, 2014. “Bitcoin: On the frontier of online gambling

innovation," *World Online Gambling Law Report*, volume 13, number 3, pp. 8–9.

24. On the role of social network gatekeepers, see K. Barzilai-Nahon, 2006. "Gatekeepers, virtual communities and the gated: Multidimensional tensions in cyberspace," *International Journal of Communications Law & Policy*, volume 11; D.B. Garrie and R. Wong, 2010. "Social networking: opening the floodgates to 'personal data'," *Computer and Telecommunications Law Review* volume 16, number 6, pp. 167–175; L.H. Gonzalez, 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*, volume 24, number 3, pp. 83–87; T. Gray, T. Zeggane, and W. Maxwell, 2008. "US and EU authorities review privacy threats on social networking sites," *Entertainment Law Review*, volume 19, number 4, pp. 69–74; L. Hicks, 2010. "Through the privacy wall," *European Lawyer*, volume 98, p. 51.

25. The existence of these exchanges is one of the premises of N. Stephenson, 2011. *Reamde*. HarperCollins.

26. G. Davies and J.H. Bank 2002. *A history of money: From ancient times to the present day*. Third edition. Cardiff: University of Wales Press, p. 36.

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

28. English King John's more infamous mistake than even signing Magna Carta was to lose his gold reserve and jewels in a flood in The Wash a week prior to his death.

29. 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/.

30. From the Latin "let it be done".

31. See D. Flint, 2014. "Computers and Internet: Are all modern currencies not virtual? — The Bitcoin phenomenon," *Business Law Review*, volume 35, number 2, pp. 60–62; R. Folsom and M. Cashman, 2014. "Digital currency: A primer," *Computers & Law*, volume 24, number 6, pp. 27–30.

32. S. Nakamoto, 2008. "Bitcoin: A peer-to-peer electronic cash system," at https://bitcoin.org/bitcoin.pdf.

33. "History of Bitcoin" (2015), http://historyofbitcoin.org/.

34. Bitcoin and the Silk Road became prominent with this article: A. Chen, "The underground Website where you can buy any drug imaginable," *Gawker* (1 June 2011), http://bit.ly/1My9klz.

35. See, for example, https://bitcointalk.org/.

36. S. Lui, 2013. "The demographics of Bitcoin," *Simulacrum*, at http://bit.ly/1FUXFru.

37. A. Yelowitz and M. Wilson, 2015. "Characteristics of Bitcoin users: An analysis of Google search data," *Applied Economics Letters*, volume 22, number 13, pp. 1,030–1,036.

38. G. Coleman, 2014. *Hacker, hoaxer, whistleblower, spy: The many faces of Anonymous*. London: Verso.

39. C. Soghoian, 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.

40. This problem set of ideology and currency is discussed in depth in the EC FP7 grant agreement no. 610349 D-Cent project: http://dcentproject.eu/. See Denis Roio, Marco Sachy, Stefano Lucarelli, Bernard Lietaer and Francesca Bria, 2015. "D4.4 design of social digital currency" (31 March 2015), D-cent Project, at http://dcentproject.eu/wp-content/uploads/2015/05/D4.4-final_v4.pdf, describing the D-Cent Freecoin Toolchain.

41. 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).

42. See https://en.bitcoin.it/wiki/Genesis_block.

43. See: L. Luu, R. Saha, I. Parameshwaran, P. Saxena and A. Hobor, 2015. "On power splitting games in distributed computation: The case of bitcoin pooled mining," *Cryptology ePrint Archive, Report* 2015/155, http://eprint.iacr.org; Y. Lewenberg, Y. Bachrach, Y. Sompolinsky, A. Zohar and J.S. Rosenschein, 2015. "Bitcoin mining pools: A cooperative game theoretic analysis," *Proceedings of the 2015 International Conference on Autonomous Agents and Multiagent Systems*, pp. 919–927.

44. T. Moore and N. Christin, 2013. "Beware the middleman: Empirical analysis of bitcoin-exchange risk," In: *Financial cryptography and data security*. Berlin: Springer, pp. 25–33.

45. R. Reynolds, "A bit too far?" *Terranova* (10 June 2011), at http://bit.ly/1mJtwFj. D. Ron and A. Shamir, 2012. "Quantitative analysis of

the full Bitcoin transaction graph," *Cryptology ePrint Archive, Report* 2012/584, at http://eprint.iacr.org/2012/584.

46. M. Vasek, M. Thornton, and T. Moore, 2014. "Empirical analysis of denial-of-service attacks in the Bitcoin ecosystem," In: *Financial cryptography and data security*. Berlin: Springer, pp. 57–71.

47. Released under the MIT License, the code is found at https://github.com/bitcoin/bitcoin.

48. A. Hayes, 2015. "The decision to produce altcoins: Miners' arbitrage in cryptocurrency markets," *SSRN paper* 2579448, http://bit.ly/1MybbXF.

49. http://www.ixcoin.co/.

50. http://namecoin.info/.

51. https://litecoin.info/.

52. https://ripple.com/.

53. http://dogecoin.com/.

54. Market capitalization is obtained by multiplying the current value of a currency with the number of available coins.

55. http://knowyourmeme.com/memes/doge.

56. https://github.com/bitcoinxt/bitcoinxt.

57. http://coinmarketcap.com/currencies/bitcoin/. This figure may be an exaggeration, as many coins have been lost.

58. For comparison, the market capitalisation of Apple at the time of writing was US$741.16 billion, and that of Google was US$369.9 billion.

59. J. Bouoiyour, R. Selmi, and A. Tiwari, 2014. "Is Bitcoin business income or speculative bubble? Unconditional vs. conditional frequency domain analysis," *Research Papers in Economics (RePEc) working paper*, at http://bit.ly/1G3YHVq.

60. http://blockchain.info/.

61. "How does Bitcoin work" (2011), at https://bitcoin.org/en/how-it-works.

62. "Transaction fees explained" (2015), at https://en.bitcoin.it/wiki/Transaction_fees.

63. "Bitcoin transaction fees explained" (2014), http://bitcoinfees.com/.

64. R. Wu, 2014. “Why we accept Bitcoin,” *Forbes* (12 February), at http://onforb.es/1JEHaao.

65. K. Kaskaloglu, 2014. “Near zero Bitcoin transaction fees Cannot last forever,” *International Conference on Digital Security and Forensics (DigitalSec2014)*, at http://bit.ly/1SffTwJ.

66. N. Christin, 2013. “Traveling the Silk Road: A measurement analysis of a large anonymous online marketplace,” *Proceedings of the 22nd International Conference on World Wide Web*, pp. 213–224.

67. E. Ploshay, 2013. “First Iranian Website open to Iranians to buy and sell Bitcoin,” *Bitcoin Magazine* (18 July), at http://bit.ly/1QL2IRu.

68. S. Feld, M. Schönfeld and M. Werner, 2014. “Analyzing the deployment of Bitcoin’s P2P Network under an AS-level perspective,” *Procedia Computer Science*, volume 32, pp. 1,121–1,126.

69. J. Britto and A. Castillo, 2013. *Bitcoin: A primer for policymakers*. Arlington Va.: George Mason University, p. 14, at http://mercatus.org/publication/bitcoin-primer-policymakers.

70. J. Lukasiewicz, 2013. “Bitcoin ‘market manipulators’ strike on the weekend,” *Coinsetter Blog* (3 June), at http://bit.ly/1MLy4XE.

71. J. Southurst, 2014. “A bot named Willy: Did Mt. Gox’s automated trading pump Bitcoin’s price?” *CoinDesk* (26 May), at http://bit.ly/1IJB1cH.

72. A. Madrigal, 2011. “Libertarian dream? A site where you buy drugs with digital dollars,” *Atlantic* (1 June), at http://theatln.tc/1pvw0IK.

73. F. Reid and M. Harrigan, 2013. “An analysis of anonymity in the bitcoin system,” In: Y. Altshuler, Y. Elovici, A.B. Cremers, N. Aharony and A. Pentland (editors). *Security and privacy in social networks*. New York: Springer, pp. 197–223; doi: http://dx.doi.org/10.1007/978-1-4614-4139-7_10. 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.

74. M. Netter, S. Herbst and G. Pernul, 2013. “Interdisciplinary impact analysis of privacy in social networks,” In: Y. Altshuler, Y. Elovici, A.B. Cremers, N. Aharony and A. Pentland (editors). *Security and privacy in social networks*. New York: Springer, p. 13; doi: http://dx.doi.org/10.1007/978-1-4614-4139-7_2.

75. *Ibid.*, p. 22.

76. M. Ober, S. Katzenbeisser and K. Hamacher, 2013. "Structure and anonymity of the bitcoin transaction graph," *Future Internet*, volume 5, number 2, pp. 237–250.

77. *Ibid.*, p. 245.

78. M. Möser, 2013. "Anonymity of Bitcoin transactions," *Münster Bitcoin Conference*, at http://bit.ly/1B8YJwb.

79. *Ibid.*, p. 9.

80. A. Guadamuz, 2015. "The Silk Road trial: Lessons for Internet regulation," *Technollama* (15 June), at http://bit.ly/1KZEKQI.

81. One BTC was worth US$9.57 on 1 June 2011, and US$223.31 on 1 June 2015. For more historical data, see http://www.coindesk.com/price/.

82. N.T. Courtois, M. Grajek and R. Naik, 2013. "The unreasonable fundamental incertitudes behind Bitcoin mining, *arXiv*, at http://arxiv.org/abs/1310.7935.

83. M. Yglesias, 2013. "Bitcoin will spiral up and down forever," *Slate* (10 April), at http://slate.me/1tZI4ni.

84. M. Ferdinando, 2014. "Hayek Money: The cryptocurrency price stability solution," *SSRN Research Papers*, at http://ssrn.com/abstract=2425270.

85. Anecdotally, one of the authors lost 0.01 BTC when he mistakenly deleted the wallet file, the address is still there, it just cannot be accessed, see http://bit.ly/1G592gB.

86. D. Ron and A. Shamir, 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 at http://bit.ly/1BbT0Gk.

87. J.W. Ratcliff, 2014. "Rise of the zombie Coins," *LTB Blog* (22 June), at http://bit.ly/1BbSWGt.

88. 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. See I. Fisher, 1933. "The debt-deflation theory of great depressions," *Econometrica*, volume 1, number 4, pp. 337–357.

89. B.P. Hanley, 2013. "The false premises and promises of Bitcoin," *arXiv*, at http://arxiv.org/abs/1312.2048.

90. D. Ron and A. Shamir, 2012. "Quantitative analysis of the full Bitcoin transaction graph," *Cryptology ePrint Archive*, Report 2012/584, at http://eprint.iacr.org/2012/584.

91. *Ibid.*

92. On criminal law issues in using Bitcoin, see D. Birch, 2007. "Money laundering in virtual worlds: Risk and reality," *E-Commerce Law & Policy*, volume 9, number 5, pp. 12–13; A.S.M. Irwin, J. Slay, K.–K.R. Choo and L. Lui, 2014. "Money laundering and terrorism financing in virtual environments: A feasibility study," *Journal of Money Laundering Control*, volume 17, number 1, pp. 50–75; doi: http://dx.doi.org/10.1108/JMLC-06-2013-0019; F. Mok and K. Tiah, 2014. "Singapore: money laundering — Virtual currencies," *Journal of International Banking Law & Regulation*, volume 29, number 7, p. N–69; S. Ramage, 2014. "Bit coins — Kiss of death to us all in the developed world," *Criminal Lawyers*, volume 220, pp. 1–2; M. Rees and R. Willis, 2014. "Virtual currencies — Virtual frauds?" *Fraud Intelligence*, pp. 17–19, at http://www.counter-fraud.com/fraud-types-n-z/online-fraud/virtual-currencies--virtual-frauds-96389.htm; E. Southall and M. Taylor, 2013. "Bitcoins," *Computer and Telecommunications Law Review*, volume 19, number 6, pp. 177–178; B. Stoeckert and T. O'Brien, 2014. "Impossible to ignore — Virtual currencies, the next challenge," *Money Laundering Bulletin*, volume 214, pp. 4–7; R. Stokes, 2012. "Virtual money laundering: The case of Bitcoin and the Linden dollar," *Information & Communications Technology Law*, volume 21, number 3, pp. 221–236;doi: http://dx.doi.org/10.1080/13600834.2012.744225; R.J. Straus, 2013. "The FinCEN virtual currency guidance: Neutering Bitcoin?" *E-Finance & Payments Law & Policy*, volume 7, number 4, p. 9; W. Stuber, 2014. "Brazil: virtual currencies — Pyramid financial schemes," *Journal of International Banking Law and Regulation*, volume 29, 7, pp. N–66–N–67; G. Varriale, 2013. "Bitcoin: Regulating the wild west," *International Financial Law Review* volume 30, number 28, p. 17.

93. See the famous xkcd comic about security failure at https://xkcd.com/538/.

94. See the famous 25k BTC theft from June 2011 at http://bit.ly/1BbV94N.

95. For a list of exchanges and individual heists, see http://bit.ly/1BbVggM.

96. M. Kiran and M. Stanett, 2015. "Bitcoin risk analysis," *NEMODE Policy Paper*, at http://bit.ly/1Kv0lnK.

97. In the U.K., see, for example, sections 83, 84 and 75 of the Consumer Credit Act 1974 (at http://www.legislation.gov.uk/ukpga/1974/39/contents), which provide consumers with wide-ranging protection for misuse of credit cards, and gives users recourse in case of breach of contract.

98. I. Eyal and E. Sirer, 2014. "It's time for a hard Bitcoin fork," *Hacking, Distributed* (13 June), at http://bit.ly/1nZezSx.

99. I. Eyal and E.G. Sirer, 2014. “Majority is not enough: Bitcoin mining is vulnerable,” In: N. Christin and N. Safavi-Naini (editors). *Financial cryptography and data security*. *Lecture Notes in Computer Science*, volume 8437. Berlin: Springer, pp. 436–454; doi: http://dx.doi.org/10.1007/978-3-662-45472-5_28

100. See https://ghash.io/ghashio_press_release.pdf.

101. See https://blockchain.info/pools.

102. E. Faggart, 2014. “Bitcoin mining centralization: The market is fixing itself,” *Coin Brief*, at http://bit.ly/1nZia3a.

103. See https://blog.ethereum.org/2014/06/19/mining/.

104. K.J. O’Dwyer and D. Malone, 2014. “Bitcoin mining and its energy footprint,” p. 5, at https://karlodwyer.github.io/publications/pdf/bitcoin_KJOD_2014.pdf.

105. *Ibid.*, p. 4.

106. See https://blockchain.info/charts/blocks-size.

107. https://blockchain.info/charts/avg-confirmation-time.

108. A. Wagner, 2014. “Ensuring network scalibility: How to fight blockchain bloat,” *Bitcoin Magazine* (6 November), at http://bit.ly/1SKI6Kb.

109. J.B. Konvisser, 1997. “Coins, notes, and bits: The case for legal tender on the Internet,” *Harvard Journal of Law & Technology*, volume 10, number 2, pp. 321–352, at http://jolt.law.harvard.edu/articles/pdf/v10/10HarvJLTech321.pdf.

110. S. Lotz and G. Rocheteau, 2002. “On the launching of a new currency,” *Journal of Money, Credit, and Banking*, volume 34, number 3, part 1, pp. 563–588; doi: http://dx.doi.org/10.1353/mcb.2002.0003.

111. L.D. Solomon, 1995. “Local currency: A legal and policy analysis,” *Kansas Journal of Law & Public Policy*, volume 5, p. 59.

112. See http://www.acbi.org.uk/media/sni_notes_factsheet_nov12_copy1.pdf.

113. 31 U.S.C. § 5103, at https://www.gpo.gov/fdsys/granule/USCODE-2010-title31/USCODE-2010-title31-subtitleIV-chap51-subchapI-sec5103.

114. U.S. F.B.I., 2011. “Defendant convicted of minting his own currency” (18 February), at http://1.usa.gov/1Lan5ZT.

115. See D.A. Dion, 2013. “I’ll gladly trade you two bits on Tuesday for a byte today: Bitcoin, regulating fraud in the e-conomy of hacker-cash,”

University of Illinois Journal of Law, Technology & Policy, volume 2013, pp. 165–201, at http://illinoisjltp.com/journal/wp-content/uploads/2013/05/Dion.pdf; and C.K. Elwell, M.M. Murphy and M.V. Seitzinger, 2015. Bitcoin: questions, answers, and analysis of legal issues. Congressional Research Service Paper, http://bit.ly/1HJXFQK. .

116. J.J. Doguet, 2012. "Nature of the form: Legal and regulatory issues surrounding the Bitcoin digital currency system," *Louisiana Law Review*, volume 73, number 4, pp. 1,119–1,153, at http://digitalcommons.law.lsu.edu/lalrev/vol73/iss4/9/.

117. J. Bartlett, 2014. *The dark net: Inside the digital underworld*. London: William Heinemann.

118. R. Yang, 2013. "When is Bitcoin a security under US securities law?" *Journal of Technology Law & Policy*, volume 18, number 2, p. 99.

119. *Ibid.*, p. 109.

120. In *SEC v. WJ. Howey Co.* 328 U.S. 293, 301 (1946); version at https://www.law.cornell.edu/supremecourt/text/328/293.

121. R. Yang, 2013. "When is Bitcoin a security under US securities law?" p. 109.

122. 7 U.S.C. §1a(9), at https://www.gpo.gov/fdsys/granule/USCODE-2011-title7/USCODE-2011-title7-chap1-sec1a.

123. M. Naqvi and J. Southgate, 2013. "Banknotes, local currencies and central bank objectives," *Bank of England Quarterly Bulletin*, pp. 317–325, at http://bit.ly/1Lb4OZu.

124. R. Ali, J. Barrdear, R. Clews and J. Southgate, 2014. "Innovations in payment technologies and the emergence of digital currencies," *Bank of England Quarterly Bulletin*, pp. 262–275, at http://bit.ly/1HK2k5d.

125. Directive 2009/110/EC of the European Parliament and of the Council of 16 September 2009 on the taking up, pursuit and prudential supervision of the business of electronic money institutions amending Directives 2005/60/EC and 2006/48/EC and repealing Directive 2000/46/EC.

126. European Banking Authority (EBA), 2014. "EBA Opinion on 'virtual currencies'," EBA/Op/2014/08 (4 July), at http://bit.ly/1HOuUT5.

127. For more on the subject of regulation, see P. De Filippi, 2014. "Bitcoin: A regulatory nightmare to a libertarian dream," *Internet Policy Review*, volume 3, number 2, at http://bit.ly/1teQq8l; doi: http://dx.doi.org/10.14763/2014.2.286; and A. Mallard, C. Méadel and F. Musiani 2014. "The paradoxes of distributed trust: Peer-to-peer architecture and user confidence in Bitcoin," *Journal of Peer Production*, number 4, at

http://peerproduction.net/issues/issue-4-value-and-currency/peer-reviewed-articles/the-paradoxes-of-distributed-trust/.

128. V. Mayer-Schönberger and J. Crowley, 2006. "Napster's Second Life? The regulatory challenges of virtual worlds," *Northwestern University Law Review*, volume 100, number 4, pp. 1,775–1,826. See also M. Gillen, 2007. "Managing virtual communities: Time to turn the whetstone?" *International Review of Law, Computers & Technology*, volume 21, number 3, pp. 211–220; doi: http://dx.doi.org/10.1080/13600860701701371.

129. See further C. Marsden, 2011. *Internet co-regulation:: European law, regulatory governance and legitimacy in cyberspace*. Cambridge: Cambridge University Press, at pp. 71–100 for virtual world regulation.

130. L.P. Nian and D.L.K. Chuen, 2015. "A light touch of regulation for virtual currencies," In: D.L.K. Chuen (editor). Handbook of digital currency: Bitcoin, innovation, financial instruments, and big data. Amsterdam: Elsevier, pp. 309–326.

131. D. Sonderegger, 2015. "A regulatory and economic perplexity: Bitcoin needs just a bit of regulation," *Washington University Journal of Law & Policy*, volume 47, pp. 175–217, at http://openscholarship.wustl.edu/law_journal_law_policy/vol47/iss1/14/.

132. K. Dotson, 2011. "Mt. Gox warns Bitcoin popularity attracting increased phishing attacks," *Silicon Angle* (30 August), at http://bit.ly/1nZes9A.

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

134. B. Weber, 2014. "Can Bitcoin compete with money?" *Journal of Peer Production*, number 4, at http://bit.ly/1gvL6Ng.

135. Bitcoin Co. Ltd., 2013. "Trading suspended due to Bank of Thailand advisement" (13 July), at http://bit.ly/1R3IZMV.

136. Bitcoin Co. Ltd., 2014. "Bitcoin trading re-opened" (31 January), at http://bit.ly/1J1aA2w.

137. A. Ostroukh, 2014. "Russia softens stance on Bitcoin: Central bank will allow use of virtual currency," *Wall Street Journal* (2 July), at http://on.wsj.com/1J1baNE.

138. People's Bank of China, 2013. "Notice on preventing Bitcoin risk" (5 December), at http://bit.ly/1J1cJLD; translation into English from this site, at http://bit.ly/1R3MjYz.

139. L.P. Nian and D.L.K. Chuen, 2015. "A light touch of regulation for virtual currencies," p. 315.

140. Particularly after it has stopped being used by electronic commerce outlets, see L.Y. Chen, 2014. "Bitcoin banned by Alibaba's Taobao after China tightens rules," *Bloomberg Business* (8 January), at http://bloom.bg/1J1fsVf.

141. http://bitcoincharts.com/markets/.

142. J.I. Wong, 2014. "China's market dominance poses questions about global Bitcoin trading flows," *CoinDesk* (27 September), at http://bit.ly/1R3Pqj9.

143. *Ibid.*

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

145. U.S. Department of he Treasury. Financial Crimes Enforcement Network, 2013. "Application of FinCEN's regulations to persons administering, exchanging, or using virtual currencies," FIN-2013-G001 (18 March), at http://1.usa.gov/1kWrsK7.

146. Her Majesty's Revenue and Customs, 2014. "Bitcoin and other similar cryptocurrencies," *Revenue and Customs Brief* 9, at http://bit.ly/1kWrBgE.

147. U.S. Securities Exchange Commission, 2014. "SEC sanctions operator of Bitcoin-related stock exchange for registration violations" (8 December), at http://1.usa.gov/1HOr4ti.

148. U.S. Securities Exchange Commission. Office of Investor Education and Advocacy, 2012. "Exchange-traded funds (ETFs)," *Investor Bulletin* (August), at http://1.usa.gov/1IiogAq.

149. US Securities Exchange Commission, 2014. "Investor alert: Bitcoin and other virtual currency-related investments" (7 May), at http://1.usa.gov/1HOtkRl.

150. European Banking Authority (EBA), 2014. "EBA Opinion on 'virtual currencies'," p. 25.

151. http://japandailypress.com/japan-to-monitor-illegal-bitcoin-activity-stops-short-of-regulation-1548441/.

152. http://www.bankofcanada.ca/wp-content/uploads/2014/05/boc-review-spring14-fung.pdf.

153. European Banking Authority (EBA), 2014. "EBA Opinion on 'virtual currencies'," p. 36.

154. California Legislature, 2015. "Virtual currency," Assembly Bill 1326 (27 February), at http://bit.ly/1GbM9s4.

155. Ministére des Finances et des Comptes Publics, 2014. "Remise du rapport sur les monnaies virtuelles," at http://bit.ly/1HOzG2V.

156. European Banking Authority (EBA), 2014. "EBA Opinion on 'virtual currencies'," pp. 39–43. For more about the proposal, see N. Vandezande, 2014. "Between Bitcoins and mobile payments: Will the European Commission's new proposal provide more legal certainty?" *International Journal of Law and Information Technology*, volume 22, number 3, pp. 295–310; doi: http://dx.doi.org/10.1093/ijlit/eau003.

157. J. Britto and A. Castillo, 2013. *Bitcoin: A primer for policymakers*, p. 3.

158. R. Ali, J. Barrdear, R. Clews and J. Southgate, 2014. "Innovations in payment technologies and the emergence of digital currencies," p. 267.

159. D. Roio, M. Scachy, S. Lucarelli, B. Lietaer and F. Bria, 2015. "Design of social digital currency," FP7 — CAPS EU Project, http://bit.ly/1Ioz0wP, p. 16.

160. *Ibid.*, p. 17.

161. *Ibid.*, p. 18.

162. R. Ali, J. Barrdear, R. Clews and J. Southgate, 2014. "Innovations in payment technologies and the emergence of digital currencies," p. 271.

163. A. Wright and P. de Filippi, 2015. "Decentralized blockchain technology and the rise of lex cryptographia," at http://ssrn.com/abstract=2580664.

164. P. Van Valkenburgh, J. Dietz, P. de Filippi, H. Shadab, G. Xethalis and D. Bollier, 2015. "Distributed collaborative organisations: Distributed networks & regulatory frameworks," at http://bit.ly/1LeE2PJ.

165. *Ibid.*, p. 7.

166. D. Bollier, 2015. "The blockchain: A promising new infrastructure for online commons," *David Bollier Blog* (4 March), at http://bit.ly/1LeDSIj.

167. https://www.ethereum.org/.

168. J.M. Leflet 2014. “A next-generation smart contract and decentralized application platform,” at http://bit.ly/1TqTldO.

169.Bria, *et al.*, 2015. “Design of social digital currency”, p. 28.

170. https://chain.com/.

171. http://bit.ly/1LeHUjR.

172. A. Hern, 2015. “Nasdaq bets on bitcoin’s blockchain as the future of finance,” *Guardian* (13 May), at http://gu.com/p/48pfp/stw.

173. The authors do not claim to be immune from this.

174. The inimitable Jon Bing was already writing about legal decision-making by automated systems in 1977, see J. Bing and T. Harvold, 1977. *Legal decisions and information systems*. *Publications of the Norwegian Research Center for Computers and Law*, number 5. Oslo: Universitetsforlaget.

175. P. Leith, 2010. “The rise and fall of the legal expert system,” *European Journal of Law and Technology*, volume 1, number 1, at http://ejlt.org/article/view/14, reviews many such claims. Earlier, see R.E. Susskind, 1986. “Expert systems in law: A jurisprudential approach to artificial intelligence and legal reasoning,” *Modern Law Review*, volume 49, number 2, pp. 168–194; doi: http://dx.doi.org/10.1111/j.1468-2230.1986.tb01683.x.

176. https://www.apple.com/apple-pay/.

177. P. Dini, 2012. “Community currencies and the quantification of social value in the digital economy,” *London School of Economics and Political Science*, at http://eprints.lse.ac.uk/47349/.

178. Y. Benkler, 2011. *The penguin and the leviathan: How cooperation triumphs over self-interest*. New York: Crown Business.

Editorial history

Received 22 October 2015; accepted 7 December 2015.

Blockchains and Bitcoin: Regulatory responses to cryptocurrencies
by Andres Guadamuz and Chris Marsden.
First Monday, Volume 20, Number 12 - 7 December 2015
http://firstmonday.org/ojs/index.php/fm/article/view/6198/5163
doi: http://dx.doi.org/10.5210/fm.v20i12.