INTERNET POLICY REVIEW
Journal on internet regulation

Volume 3 | Issue 2

Bitcoin: a regulatory nightmare to a libertarian dream

Primavera De Filippi
Research and Studies Center of Administrative Science (CERSA/CNRS), Université Paris II (Panthéon-Assas), France

Published on 23 May 2014 | DOI: 10.14763/2014.2.286

Abstract: This article provides an overview of national policies and current discussions on the regulation of bitcoin in Europe and beyond. After presenting the potential threat that cryptocurrencies pose to governmental and financial institutions worldwide, it discusses the regulatory challenges and the difficulty for national regulators to come up with a sound regulatory framework, which the author believes explains the current (lack of) regulatory responses in this field. The article concludes that regulation is needed, but that in order not to excessively stifle innovation in this nascent ecosystem, some of these challenges might better be addressed through self-regulation.

Keywords: Cryptocurrency, Bitcoin, Digital currency

Article information

Received: 27 Mar 2014 **Reviewed:** 16 May 2014 **Published:** 23 May 2014
Licence: Creative Commons Attribution 3.0 Germany
Funding: This work is supported by the ANR project ADAM - Architectures distribuées et applications multimédia and by the FP7 STREP project P2Pvalue - Techno-social platform for sustainable models and value generation in commons-based peer production in the Future Internet.
Competing interests: The author has declared that no competing interests exist that have influenced the text.

URL: http://policyreview.info/articles/analysis/bitcoin-regulatory-nightmare-libertarian-dream

Citation: De Filippi, P. (2014). Bitcoin: a regulatory nightmare to a libertarian dream. *Internet Policy Review*, *3*(2). https://doi.org/10.14763/2014.2.286

GENERAL OVERVIEW

Cryptocurrencies are digital currencies that rely on a cryptographic protocol to regulate the manner in which (and the extent to which) currency can be created and/or exchanged. As opposed to previous digital currencies (such as Second Life's Linden dollars, or World Of Warcraft's gold) which are both issued and regulated by a central server, bitcoin is a distributed, worldwide, decentralised cryptocurrency that is managed solely and exclusively by an open source cryptographic protocol: there is no government, company, or bank in charge of issuing or managing bitcoins.

Bitcoins are created through the process of 'mining' - a process which rewards users for contributing computing power to the network by awarding newly created bitcoins to every user who resolves a complicated mathematical problem (the so-called 'Proof of Work') whose difficulty increases with overall network strength[1]. The mining process ultimately serves to ensure the security and integrity of the overall system, by providing a means to verify transactions through a decentralised network of peers simultaneously processing transaction data (often in exchange of a fee) before they are recorded into a public ledger or 'blockchain'. Thus, instead of relying on a centralised bank or authority, bitcoin relies on cryptographic algorithms and peer-to-peer technologies to allow users to transfer money securely and pseudonymously, without passing through any given intermediary (Nakamoto, 2008).[2] It is important to note that - contrary to common belief - bitcoin transactions are not, strictly speaking, anonymous, to the extent that the bitcoin protocol makes it possible to trace all transactions to and from a pseudonymous bitcoin address, which can eventually be linked to a particular identity (Brito & Castillo, 2013). Yet, although the bitcoin protocol does not itself incorporate any specific feature for anonymity, the use of bitcoin in combination with anonymisation services (see e.g., DarkWallet or the various bitcoin mixing/laundry services, such as BitMixer, BitLaunder, CoinJoin, etc) could, as a matter of fact, provide the necessary degree of "unlikability" to preserve the anonymity of bitcoin users.

BITCOIN DEPLOYMENT AND GROWING ACCEPTABILITY

When bitcoin was released in 2009 by pseudonymous developer Satoshi Nakamoto, it was initially regarded as an interesting, yet unlikely attempt at creating an alternative currency (or cryptocurrency) that subsists independently from the traditional financial system (Grinberg, 2012).

As a digital cryptocurrency, bitcoin has no intrinsic value, per se. As opposed to gold - or other commodity-backed currencies, which can be redeemed for a certain amount of these commodities on demand, bitcoin is not backed by anything - i.e. it is not redeemable for any specific good or service. Bitcoin also distinguishes itself from most of the fiat[3] currencies currently in circulation (i.e. currency made legal tender by a fiat of the government, but not based on or convertible into gold or other commodities) to the extent that it is not recognised as 'money' by any state or government. Since the end of the gold standard, most national currencies are fiat currencies which are not redeemable for anything - yet, they benefit from the fact that they are legal tender, i.e. they are only currency with which taxes can be paid in their respective states. Hence, unlike traditional currencies (such as euros or dollars) whose value stems from and can be easily affected by government regulation, bitcoin's value is determined - solely and exclusively - by the law of supply and demand.

For many years, the ability for bitcoin to become a widely accepted cryptocurrency was considered very low, at least until 2012 when the currency started to receive significant media attention and its value began to rise (gaining over $200 in just a few months on most of the major exchanges). Today, bitcoin is accepted as a form of payment by major online retailers (such as overstock.com, tigerdirect.com, etc) and its value is fluctuating around an average of $500.

While it took many years for bitcoin to actually take off, its recent popularity spurred the deployment of a variety of alternative cryptocurrencies (such as Litecoin, Primecoin, Peercoin, and more recently Dogecoin) which implement similar, yet slightly modified protocols to

regulate the creation and transfer of currency.

Although the creation of bitcoin was tied to a utopian ideal of the future devoid of any centralised currencies, with Satoshi Nakamoto actively debating the perceived ills of nation-state control over money (Karlstrøm, 2014), none of these cryptocurrencies have thus gotten close to replacing any of the established currencies. Yet, they have nonetheless led to the establishment of a new ecosystem that coexists (more or less peacefully) alongside the traditional financial system. A variety of exchanges have emerged (such as MtGox, Bitstamp, BTC-e, etc) providing a simple and easy way for people to acquire and resell bitcoins. With the advent of intermediaries such as BitPay and Coinbase, or other merchant processors that immediately convert bitcoin into fiat currency at a very low fee, many more merchants are now accepting payments in bitcoins, without incurring the risks derived from the cryptocurrency's high rate of fluctuation. As a result, many internet users are nowadays given the choice to purchase more and more goods and services with bitcoin, in addition to national currencies.

From a consumer perspective, bitcoin transactions are, however, more risky to the extent that they cannot be reversed. As opposed to traditional payment systems, such as wire transfers, credit cards purchases, or even Paypal transactions (which can all be voided in case of errors, mistakes or anomalies), once performed, bitcoin transactions are irreversible and can only be refunded by the person who actually received the funds.

Yet, over the last few months, in spite of extensive value fluctuation and the lack of buyer protection, bitcoin and other decentralised cryptocurrencies have proven to be both technically and economically sound alternatives to established currencies whose creation and circulation is governed by a central authority (Wallace, 2011). Even though their use still represents only a small minority of monetary transactions, cryptocurrencies have nowadays reached an overall market capitalisation of over 7 billion dollars, and a number of bitcoin-ATMs are currently being deployed in Canada, the US, and more recently also Berlin.

LEGAL CHALLENGES RAISED BY CRYPTOCURRENCIES

If decentralised cryptocurrencies have generated a great deal of innovation and experimentation from both the inside and outside of the financial system, from a practical standpoint, alternative cryptocurrencies raise significant legal challenges that might require thorough scrutiny by regulators. In particular, while it is still far from being mainstream, bitcoin's growing rate of acceptance by both online and offline merchants could raise important issues in the context of cybercriminality and law enforcement, most of which have yet to be addressed by the law, or other normative systems.

Given the inherent difficulty of tracking the identity of anonymous users (Reid & Harrigan, 2011), cryptocurrencies are often used as a means to obfuscate the source and the destination of financial transactions. Bitcoin has been used, in many instances, to support the operations of online gambling websites and black market operations, as was recently illustrated by the Silkroad case, where users were relying on the anonymity provided by Tor and bitcoin in order to reduce the likelihood of being incriminated for performing criminal activities such as the purchase or sale of drugs and weapons. Following the arrest of a US citizen for the sale of a gun to a Dutch policeman through SilkRoad, the issue was raised as to whether the use of bitcoin should be banned in The Netherlands. The Dutch Minister of Justice and Security, Ivo Opstelten, dismissed the claim, arguing that, while it is true that bitcoin has been used in

connection with criminal practices, “financial transactions for criminal activities are not reserved for cryptographic payment forms.” (Rank, 2014)

Cryptocurrencies could, more generally, also be employed for executing a variety of illegal transactions, such as fraud or money laundering (Stokes, 2012) - even though the transparent character of every transaction might actually make them less appealing in this regard (Androulaki & al., 2013). Indeed, according to Rob Wainwright (head of the EU law enforcement agency for criminal intelligence, Europol), “virtual currencies are being used as an instrument to facilitate crime, particularly in regard to the laundering of illicit profits.” (Wainwright, 2014 as cited in Reuters, 2014). Given the potential anonymity (or pseudonymity) provided by cryptocurrencies such as bitcoin, it has become increasingly difficult for law enforcement agencies to identify criminals operating in the ‘darkweb’. Europol is thus urging legislators to introduce improved mechanisms for the police to fight criminal activities online, at the European level (Wainwright, 2014 as cited in McCallion, 2014).

Beyond the potential for criminal activities, alternative cryptocurrencies also constitute a potential threat to national sovereignty to the extent that they escape the scope of many governmental policies. While some scholars have argued against the regulation of bitcoin (see, in particular, Kaplanov, 2012; and, more generally, Hughes & Middlebrook, 2014) on the grounds that governments should not have any control over the money supply (Hayek, 1976) unless necessary to ensure the security of financial institutions (Stiglitz, 1993) or to facilitate market exchanges in the global economy (Kapstein, 1994), the decentralised and unregulated character of bitcoin might nevertheless jeopardise most of the economic and financial policies established by the nation-states (Kleiman, 2013; Twomey, 2013). Taxation is probably the most relevant issue in this regard. Given that cryptocurrencies’ transactions are independent from any financial intermediary, it is virtually impossible for anyone to monitor or control how the currency is being used. Even if all transactions are transparent to the public, the anonymity inherent to their network makes cryptocurrencies the best candidate to qualify as a new tax haven (Gruber, 2013). Besides, as opposed to state-regulated currencies whose overall market capitalisation is determined by a central bank in charge of issuing the money, in the case of most alternative cryptocurrencies, the overall amount of money available on the market is determined in advance, according to the specificities of the underlying protocol. As such, no central authority can intervene to increase or decrease their inflation rate, as their value depends solely and exclusively on market demand.

Finally, by virtue of their distributed character, there is no single entity in charge of establishing the overall interest rate for any one of these currencies. If the currencies were to be widely adopted, nation states might eventually lose their ability to regulate the economy by means of traditional monetary policies. Of course, while this might (perhaps) be conceivable in a country with bad monetary policy and high inflation - like Zimbabwe, historically - in the case of most (generally stable) fiat currencies, it is highly unlikely that a cryptocurrency like bitcoin will ever sufficiently supplant the official currency to seriously affect macroeconomic policy (Luther, 2013)

CURRENCY OR COMMODITY? THE AMBIGUOUS LEGAL STATUS OF BITCOIN

Despite the uncertainty surrounding the regulatory framework in which they operate, the

popularity of cryptocurrencies has grown significantly in the past few years. Yet, in order to become mainstream, cryptocurrencies need more stability and regulatory oversight. The viability and long-term sustainability of these alternative currencies or payment systems ultimately depends on the way in which they will be regulated by the law - which will determine whether they can effectively (and reasonably) secure public trust.

In the case of bitcoin, while it already has acquired a critical mass of users, and is now being accepted by a growing number of online and offline merchants, it is, at the same time, struggling to get regulatory approval at the national level. Indeed, thus far, only a few countries have enacted specific regulations, which are for the most part unsupportive of bitcoin.

Brazil is perhaps the exception, with the enactment in October 2013 of a law regulating the creation and exchange of 'electronic currencies' defined as "resources stored on a device or electronic system that allow the end user to perform a payment transaction" (see: Lei nº 12.865, de 9 de outubro de 2013; Article 6-VI). Aimed at the normalisation of mobile payment systems, the law introduces the possibility for Brazil to regulate bitcoin and every other (current or future) cryptocurrencies - which shall be subject to the same rules as any other currency. The recognition of bitcoin as an actual currency in Brazil had a significant impact on its credibility, and probably contributed to the strong peak of bitcoin trading on the online broker Mercado bitcoin (the Brazilian national exchange), whose trading volume went up to almost $4.5 million in December 2013. More recently, the Brazilian tax authority (Receita Federal) announced that - as a financial asset - bitcoin transactions are subject to 15% taxation on capital gains, but only if these gains actually exceed 35,000 real (or $16,000). Such exemption allows for taxes to be collected from bitcoin investors, without hindering the activities of normal bitcoin users and consumers. In the wake of the recent inflation of the Brazilian real, such a regulatory framework might actually encourage the use of bitcoin as a realistic alternative to the dollar or euro, for all these people trying to avoid transactions in the national currency.

But other countries seem to have taken a different direction. In December 2013, China's national bank declared that bitcoin is a 'virtual commodity' and financial institutions have since then been precluded from exchanging bitcoin on the market, although individuals remain free to buy or sell bitcoins amongst themselves. According to Jeremy Bonney (Product manager at Coindesk, a news operation aiming at becoming the "Reuters of bitcoin"), this reaction is not too alarming: "China has a history of wanting to control anything it sees as disruptive to the status quo (much like the internet in the 1990s) – so the very fact that it has taken notice of bitcoin, and is trying to exert some control over it, is a positive sign for its disruptive potential" (Bonney, 2014 as cited in Osborne, 2014).

And yet, China is not alone in the fight against bitcoin. Earlier this year, Russia's central bank stipulated that any institution providing services for the exchange of 'virtual currencies' will be regarded as being involved in 'potentially suspicious' activities, thereby discouraging many financial institutions from dealing with bitcoins. The Reserve Bank of India, as well as the Bank of Indonesia recently raised some concerns as regards the validity of bitcoin as a currency; yet they did not take any practical action to advocate against its use. Thailand's approach is, to a large extent, confusing. The Bank of Thailand initially ruled that bitcoin is not a currency, and made it forbidden for anyone to buy, sell, or exchange bitcoins in the country. The Bank subsequently changed its mind, declaring that bitcoins can legitimately be traded in Thailand as long as they are only converted to or from the national Thai baht. The bitcoin exchange has since then been allowed to resume its operations.

Hence, while the global regulatory environment might seem - at the outset - largely hostile to

bitcoin, it is actually much more positive than not[4]. China and Russia have thus far been the most hostile, but these governments are - like Thailand - especially concerned about capital flight.

In fact, Iceland's reaction to bitcoin is just as hostile as Russia's, and that also stems from a desire to protect the capital controls implemented by the Icelandic Foreign Exchange Act, i.e. to stop money flight on the Icelandic króna. Indeed, according to the Icelandic Central Bank, "it is prohibited to engage in foreign exchange trading with the electronic currency bitcoin." (mbi.is, 2013)

In most other countries, where the legal status of bitcoin has yet to be determined, governments have generally taken a wait-and-see approach. Many countries - such as Singapore, Malaysia, Germany, Finland, and even Canada (the first country to introduce bitcoin ATMs) - consider bitcoin to be no legal tender: the cryptocurrency is not regarded as a currency, but merely as a commodity that can be used for barter or exchange. This means that the purchase, sale or exchange of bitcoins can be done freely, without previous supervisory licensing.

However, even if it does not qualify as a currency, various countries have already issued - or are planning to issue - a series of guidelines to regulate the taxation of bitcoin (see e.g., Israel and Singapore). In this regard, Vitalik Buterin (editor at Bitcoin Magazine and co-founder of Ethereum) believes that, by the end of this year, "we will see over half of the world's governments take a formal position on bitcoin." "We will likely see substantial reforms" he says, with the emergence of "specific licensing category for bitcoin businesses" - and "we will continue to see more tax clarification," he adds (Buterin, 2014 as cited in Osborne, 2014).

Already in Canada it is considered that whenever bitcoins are used to pay for goods or services, the rules for barter transactions apply - i.e. the value of the purchased goods or services must be included in the seller's income for tax purpose. On February 2014, Jim Flaherty (Canada's former Finance Minister) presented the Canadian Federal Budget for 2014-2015, which includes, *inter alia*, the plan to introduce financing regulations against money laundering and tax evasion for cryptocurrencies such as bitcoin. Likewise, the Australian Tax Office promised earlier this year to issue a set of guidelines on how the profits derived from bitcoin transactions should be dealt with through taxation.

In the US, the Internal Revenue Service recently issued a notice indicating that digital currencies should be treated as property (rather than currency) for the purposes of taxation. This means that any profit or loss resulting from the sale of digital currencies must be reported and are subject to taxation on capital gains.

Yet, regulatory powers delegated to individual states are such as to allow for different approaches to be implemented at the state level. In the past, for instance, several US states - such as Texas, Louisiana, and Utah - have already enacted legislation designating gold or silver as legal tender (in accordance with Article 1, section 10 of the US Constitution). Texas Congressman Steve Stockman even went a step further, claiming that bitcoin should be treated as currency, rather than property, thus suggesting to enact legislation officially recognising bitcoin as legal tender (although the Bill is unlikely to succeed to the extent that it might go counter the provisions of the US Constitution).[5]

NO SPECIFIC POSITION AT THE EUROPEAN UNION LEVEL

At the European level, the situation is far from clear. In October 2012, the European Central Bank's 2012 report on Virtual Currency Schemes briefly analysed the legal status of bitcoin under EU legislation. The report highlighted that, out of the three criteria that must be fulfilled to qualify as 'electronic money' according to the Electronic Money Directive (ECB) of 2009 (electronic storage; issuance upon receipt of funds; and acceptance as a means of payment by a legal or natural person other than the issuer), bitcoin does not satisfy the second criteria (ECB, 2012, p. 43). The report also situates bitcoin outside of the scope of the Payment Services Directive of 2007 which precludes payment institutions from issuing electronic money (ECB, 2012, p. 43). The issue has been raised within the European Commission's Payments Committee, and, on December 2013, the European Banking Authority (EBA) issued a warning on the risks that can be derived from the trade in bitcoin. Yet, no specific position has been taken at the European level as regards the legal status of bitcoin. Member states are thus free to decide whether (and how) to regulate the trading of bitcoin by financial institutions and/or individuals, and whether to impose a tax over the added-value generated from bitcoin transactions. The Danish government has taken the lead on the matter, with the Danish Tax Board declaring that gains or losses resulting from casual bitcoin transactions are exempt from taxation. This means that profits derived from bitcoin trading are not subject to taxation, but also that the resulting losses are not deductible. Beyond Denmark however, no specific legislation has thus far been passed, at the national level, concerning the status and use of bitcoin as a virtual currency.

Nevertheless, the situation is likely to change soon, as there seems to be a growing need for clear and consistent regulation around the globe. As Elizabeth Ploshay (manager at Bitcoin Magazine) puts it, "as bitcoin continues to become more mainstream and as larger and more prominent companies also start utilizing the currency, [...] we will see a larger group of companies requesting further regulatory clarity."

Yves Mersch, member of the Executive Board of the European Central Bank, considers that although cryptocurrencies do not (yet) constitute a threat to financial stability in Europe, they do, however, pose significant threats to consumers. Thus, in the same way as banks and financial institutions are heavily regulated to protect users from the improper management of their funds, online platforms and exchange dealing with bitcoin also need to be subject to a more comprehensive scrutiny from regulators.

This is especially true in the wake of the recent attacks to bitcoin platforms and exchanges, which resulted in the overall loss of over $350 million worth of bitcoins.

On 13 February 2014, the administrator of Silk Road 2.0 (the second incarnation of Silk Road) reported that the platform had been hacked: a bug in the bitcoin protocol (known as 'transaction malleability') had been exploited in order to steal more than 4,400 bitcoins (about $2 million at today's rate) from the platform.

The same bug had allegedly been exploited to steal from the former largest bitcoin exchange MtGox, which was recently shut down on 25 February 2014, following a claim for bankruptcy. The hack - which had been carried on over the course of two years - had gone unnoticed by the company, which eventually went insolvent after having been drained of 850,000 bitcoins (worth about $375 million at today's rate).

These hacks clearly illustrate the risks that bitcoin trading entails (Moore & Christin, 2013). Yet, these risks are not specific to bitcoin, they are the result of improper security configurations, negligence and, perhaps, dishonesty on the part of the platforms or exchanges in charge of executing bitcoin transactions. While transaction malleability is, indeed, a problem (to the extent that it is not properly understood by the designer of a bitcoin wallet), it can be avoided through secure wallet management schemes and high security measures - which both Silk Road 2.0 and MtGox had obviously failed to implement. Following these hacks, a coalition of bitcoin business issued a statement underlining that "This tragic violation of the trust of users of Mt. Gox was the result of one company's abhorrent actions and does not reflect the resilience or value of bitcoin and the digital currency industry [...] There are hundreds of trustworthy and responsible companies involved in bitcoin." (Ehrsam et al., 2014)

And yet, problems keep coming. On 2 March 2014, the Canadian-based exchange Flexcoin was forced to shut down after suffering a theft of 896 bitcoins (almost $400,000 at today's rate) due to a flow in the server's front-end[6]. On 4 March, it was the turn of the Polish exchange Poloniex, which lost 12.3% of its bitcoin assets (slightly under $50,000 at today's rate) as a result of a flaw in the server's withdrawal code[7].

These events clearly illustrate the various risks that are emerging following the recent growth in popularity of bitcoin (Kleiman, 2013; Trautman, 2014). This, in addition to the other problems characteristic of this nascent ecosystem - especially concerning trust, security and volatility - might push people to request the introduction of formal, regulatory solutions to those problems. Hence, while the mere subsistence of these risks does not - in and of itself - indicate that regulation is needed, governments might well decide to pursue a regulatory response to reduce the likelihood, or at least lessen the impact of these risks.

But regulation could also come from the private sector. Indeed, despite the distributed and to a large extent anonymous (or pseudonymous) character of the bitcoin network, and in spite of the libertarian values expressed by many bitcoin advocates, the whole bitcoin ecosystem nonetheless operates within an entrenched institutional framework, composed of important stakeholders - including, but not limited to, financial institutions, exchanges, mining pools, online merchants, etc.

The Bitcoin Foundation is a non-profit organisation created to "standardise, protect and promote the use of bitcoin cryptographic money for the benefit of users worldwide." In addition to establishing an interface for dialogue with regulators, legislators and the general public, the Foundation acts as a private regulatory body, in charge of coordinating and guiding the development of the bitcoin protocol (and clients). Although its influence is limited, it decides on the implementation changes made to the bitcoin protocol - which can have potentially large implications for bitcoin users, private actors and policymakers worldwide.

BITCOIN IN A REGULATED FRAMEWORK

Overall, whether or not bitcoin will actually succeed in becoming an alternative currency that peacefully coexists alongside a variety of established national currencies does not actually depend on the technical and/or economic viability of the cryptocurrency - which has already proven to be sustainable in the long run (Barber & al., 2012). It will be, rather, depend on the ability of the bitcoin ecosystem to operate in a more regulated framework, either as a result of self-regulation (i.e. through market-based mechanisms, or with the support of a private

regulatory body like the Bitcoin Foundation) or by means of state regulation. While the former can be implemented - informally - by the community through a dynamic process of trials and errors, the latter will require legislators to come up with a proper way to regulate an inherently decentralised currency, in such a way as to preclude it from being used as a support for criminal activities and/or to escape from the financial regulations and economic policies of nation states.

In this regard, it is important to note that bitcoin only really took off in the last couple of years and is still a very new phenomenon and nascent industry. It creates a space for permissionless innovation (in the realm of finance) just as the internet did in the realm of communications. While it has great potential, its effects on the global economy are currently minimal. There is, therefore, currently little pressing for governmental intervention, especially as such intervention - if implemented by means of harsh regulations based on speculation about worst case scenarios - might forestall the potential benefits of such an open space for experimentation, including low-cost remittances and new services for the unbanked. Ultimately, regulation of the protocol will most probably arise "organically" as bitcoin adoption increases (Karlstrøm, 2014). Accordingly, before turning to regulation, it might be wise to first look at whether the solutions forthcoming from the market could actually provide a satisfactory answer to these aforementioned problems.

FOOTNOTES

1. The reward for solving a block is automatically adjusted so that, ideally, every four years of operation of the bitcoin network, half the amount of bitcoins created in the prior 4 years are created.Thus the total number of bitcoins in existence can never exceed 21,000,000.

2. More information on the technical features of bitcoin can be found here: https://bitcoin.org/bitcoin.pdf

3. Fiat money is money which derives its value from government regulation or law. The term derives from the Latin fiat ("let it be done", "it shall be").

4. See http://bitlegal.net/ for a country-by-country analyses of bitcoin regulation.

5. Article I, section 10 of the US Constitution specifically states that "No state shall enter into any treaty, alliance, or confederation; grant letters of marque and reprisal; coin money; emit bills of credit; *make anything but gold and silver coin a tender in payment of debts*; pass any bill of attainder, ex post facto law, or law impairing the obligation of contracts, or grant any title of nobility." (emphasis added)

6. Flexcoin's hack was not due to a flaw in the bitcoin protocol (the so-called 'transaction malleability') but rather to a bug in the implementation of the exchange's front-end allowing transfers between flexcoin users. By sending thousands of simultaneous requests, the attacker was able to "move" coins from one user account to another until the sending account was overdrawn, before balances were updated.

7. The theft was due to a flow in Poloniex's withdrawal system, which allowed for bitcoin transactions to be processed simultaneously (rather than sequentially) thereby resulting in possible

REFERENCES

Androulaki, E., Karame, G. O., Roeschlin, M., Scherer, T., & Capkun, S. (2013). Evaluating user privacy in bitcoin. In Financial Cryptography and Data Security (pp. 34-51). Springer Berlin Heidelberg.

Barber, S., Boyen, X., Shi, E., & Uzun, E. (2012). Bitter to better—how to make bitcoin a better currency. In Financial Cryptography and Data Security (pp. 399-414). Springer Berlin Heidelberg.

Brito, J. & Castillo, A. (2013). Bitcoin: a Primer for Policymakers. Mercatus Center, George Mason University.

Ehrsam, F., Powell, J., Kodric, J., Lee, B., Cary, N., & Allaire, J. (2014, February 25). Joint statement regarding mtgox. Blockchain [Web page]. Retrieved from https://blog.blockchain.com/2014/02/25/joint-statement

European Central Bank (2012). Virtual Currency Schemes, October 2012.

Grinberg, R. (2012). Bitcoin: An Innovative Alternative Digital Currency. Hastings Science & Technology Law Journal, 4, 1.

Gruber, S. (2013). Trust, Identity, and Disclosure: Are Bitcoin Exchanges the Next Virtual Havens for Money Laundering and Tax Evasion?. Quinnipiac Law Review, 32, 1.

Hayek, F. A. (1976). Denationalisation of money: an analysis of the theory and practice of concurrent currencies. London: Institute of economic affairs.

Hughes, S. J., & Middlebrook, S. T. (2014). Regulating Cryptocurrencies in the United States: Current Issues and Future Directions. William Mitchell Law Review, 40(813)

Kaplanov, N. (2012). Nerdy money: bitcoin, the private digital currency, and the case against its regulation.

Kapstein, E. B. (1994). Governing the global economy: international finance and the state. Harvard University Press.

Karlstrøm, H. (2014). Do libertarians dream of electronic coins? The material embedness of bitcoin. Scandinavian Journal of Social Theory, Vol. 15, No. 1, 23-36.

Kleiman, J. A. (2013). Beyond the Silk Road: Unregulated Decentralized Virtual Currencies Continue to Endanger US National Security and Welfare. American University National Security Law Brief, 4(1), 5.

Luther, W. J. (2013). Cryptocurrencies, network effects and switching costs. Working paper No. 13-17, September 2013. Mercatus Center, George Mason University.

mbi.is (2013, December 19). Höftin stöðva viðskipti með bitcoin. Mbl.Is [Web page]. Retrieved from http://www.mbl.is/vidskipti/frettir/2013/12/19/hoftin_stodva_vidskipti_med_bitcoin

McCallion J. (2014). Europol calls for greater bitcoin policing powers. ITPro, March 25th. Retrieved from http://www.itpro.co.uk/public-sector/21903/europol-calls-for-greater-bitcoin-policing-powers

Moore, T., & Christin, N. (2013). Beware the middleman: Empirical analysis of bitcoin-exchange risk. In Financial Cryptography and Data Security (pp. 25-33). Springer Berlin Heidelberg.

Nakamoto, S. (2008). Bitcoin: A peer-to-peer electronic cash system. Available at https://bitcointalk.org/bitcoin.pdf

Osborne, C. (2014, January 23). 50+ Bitcoin Experts Share Their Thoughts On What The Future Holds For bitcoin [Part One: Regulation] [Web log post]. Retrieved from http://foundersgrid.com/bitcoin-regulation

Rank, A. (2014, Mar 20). Dutch minister of justice stands for bitcoin. Good investors online [Web page]. Retrieved from http://good-investors-online.com/hyip/news/3120-dutch-minister-of-justice-stands-for-bitcoin.htm

Reid, F., & Harrigan, M. (2011, October). An analysis of anonymity in the bitcoin system. In Privacy, security, risk and trust (passat), 2011 ieee third international conference on and 2011 ieee third international conference on social computing (socialcom) (pp. 1318-1326). IEEE.

Reuters (2014, March 24). Police need powers to tackle virtual money laundering: Europol. Retrieved from http://ca.reuters.com/article/technologyNews/idCABREA2N1A420140324

Stiglitz, J. E. (1993). The role of the state in financial markets (No. 21). Institute of Economics, Academia Sinica.

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

Twomey, P. (2013). Halting a Shift in the Paradigm: The Need for bitcoin Regulation.

Trautman, L. J. (2014). Virtual currencies: bitcoin & what now after Liberty Reserve, Silk Road, and Mt. Gox? Working Paper

Wallace, B. (2011). The rise and fall of bitcoin. Wired Magazine. Available at http://fromm.robertkeahey.com/wp-content/uploads/2013/07/Session-7-The-Rise-and-Fall-of-bitcoin.pdf