Issues and Risks Associated with Cryptocurrencies such as Bitcoin

Félix Brezo and Pablo G. Bringas
Avenida de las Universidades 24, 48007
DeustoTech Computing (S3lab), Universidad de Deusto
Bilbao (Bizkaia), España
Email: {felix.brezo, pablo.garcia.bringas}@deusto.es

***Abstract*—Bitcoin is an electronic currency designed to use a public protocol that implements it in a totally decentralized manner, so as not to need the control of any central issuing organization that manages it. Though still in development, it has been proven to be a modern payment system referred to have been used in some procedures commonly associated to money laundering or trafficking of illegal substances of various kinds. Thus, in this article, we analyse those features which transform such a cryptocurrency in a useful tool to perform any kind of transactions far from the control of any kind of regulatory agency, as well as we pinpoint some of the fields in which their usage can derive in new illicit behaviours.**

Keywords-bitcoin; cryptoanarchism; cryptocurrency; fraud; speculation; virtual money.

I. Introduction

The phenomenon of virtual coins is neither new nor particularly recent. The inception of the concept is usually located in some distribution lists in the mid nineties [1]. Thus, nowadays, there are lots of virtual currencies being used with more or less success in the Internet: from Pecunix to e-gold, passing from all kind of virtual currencies associated to leisure applications such as Second Life's Linden Dollars, whose economy has also been studied by some authors [2], [3], and the well-known Facebook's Facebook Credits.

The novelty of Bitcoin —originally created by Satoshi Makamoto in 2009 [4]— is the fact of being a public protocol implementing a *peer-to-peer*-based cryptocurrency. Its definition as a distributed currency comes from the absence of an existing central entity in charge of regulating either the value or the amount of the total number of existing coins. It is the network itself, making use of the computational capacity of its own users, the one that manages and maintains it. This calculation capacity is used, amongst other things, to manage the transaction history —what is known as the *block chain*— and to confirm and validate each and every new transactions to be happening in the future.

The characteristics of its distribution protocol are providing Bitcoin with a strong boost in certain communities in the internet. In fact, the value of the total transactions performed annually has raised in 2011 to 150 million dollars as stated by the website blockchain.info while the protocol manages peaks of 25,000, 30,000 and even 47,000 daily transactions as displayed on Figure 1.

Thereby, the remainder of this paper is structured as follows. Section II states some of the key aspects that make Bitcoin special. Section III defines some scenarios in which the use of this cryptocurrency may lead to illegal behaviours. Section IV summarises and defines the main conclusions to be extracted about this new reality.

II. Bitcoin key features

Against this background, the appearance of a currency with such special characteristics leads to a new scenario which possibilities have never been explored before. In this section, we collect some of the aspects that make this cryptocurrency a differentiating factor.

A. Distribution protocol

Its specific characteristics stablish a particular method for allocating bitcoins amongst those nodes in the peer-to-peer network that share computing capacity for the distributed maintenance of the system. Notwithstanding, the coin assignation process effectiveness is inversely proportional to the total network's capacity. By protocol, the maximum number of total monetary units is set to the amount of 21 million bitcoins [4] —sometimes represented using the Thai baht (ISO 4217 code: THB) symbol ฿ or, in text format, as BTC—, being reached approximately by 2040. This definition of the protocol makes possible to predict the total number of coins in circulation in any moment of the history. For instance, by mid-2012, this figure rounds the 9 million of already distributed coins, with an estimated value in the markets of 52.99 million dollars.

By June 2012, the distribution process takes place approximately every 10 minutes. With that frequence, ฿50 are assigned randomly to one of the nodes that have contributed to solve a given mathematical problem: finding the result of a given *hash*. A hash function is a computable function that takes as an input a set of elements (usually strings) and maps them in a finite output range, typically fixed-length strings, being theoretically impossible to reverse it. Thus, the only way of finding the input of a given hash is to bruteforce the calculations. The complexity of this problem is adjusted every two weeks to maintain the rhythm of 6 handouts per hour. To illustrate this situation, in the current circumstances, the great amount of connected

 ISBN: 978-1-61208-228-8

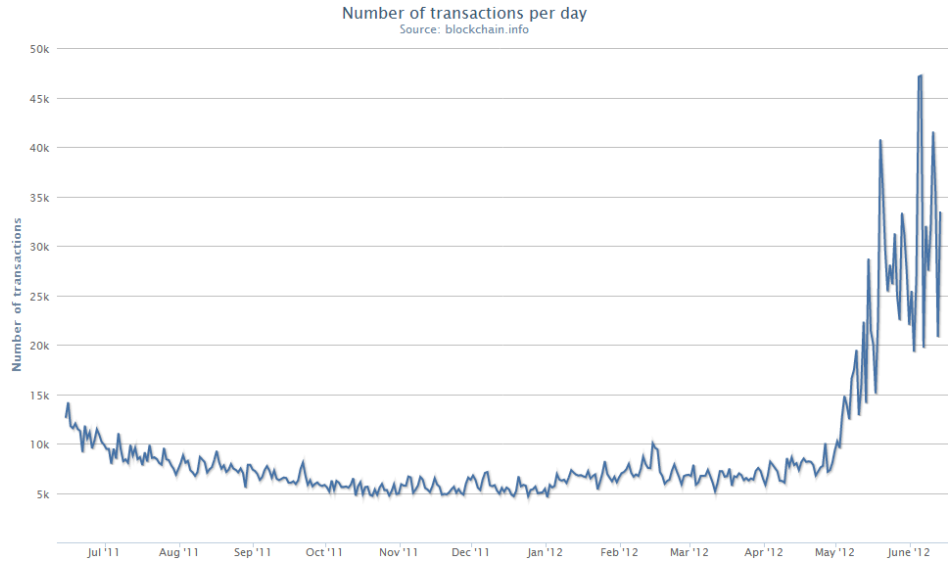

Figure 1. Total daily Bitcoin transactions as stored by Blockchain website.

Table I
ESTIMATED TIME NEEDED TO OBTAIN ฿50 DEPENDING ON THE COMPUTING CAPACITY DEPLOYED BY A GIVEN USER, MEASURED IN MILLIONS OF HASHES PER SECOND.

Computing capacity	Average time needed	Daily generation
5 *MHashes*/s	43 years, 45 days	฿0.0032
20 *MHashes*/s	10 years, 285 days	฿0.0127
100 *MHashes*/s	2 years, 57 days	฿0.0635
500 *MHashes*/s	157 days, 9 hours	฿0.3177
2,000 *MHashes*/s	39 days, 8 hours	฿1.2706
10,000 *MHashes*/s	7 days, 20 hours	฿6.3532
50,000 *MHashes*/s	1 days, 13 hours	฿31.7661

devices and the increasing capabilities of the network to work out this hashes will let a standard user exploiting not optimized hardware —i3 processor, 4 cores, NVIDIA GT240 graphic card— and contributing without any kind of affiliation to the development of the network —practice known as *solo mining*— to develop a computing capacity of 20 million hashes solved per second. In other words, this standard user would receive the mentioned ฿50 per block approximately every 11 years. Although we could also use the processors computing capacity, this chance is deprecated as it is estimated to be between 30 and 50 times slower that the one produced by modern graphic cards designed for GPU computing —8 Intel ® Core™ i7 processors are hardly capable of reaching the figure of 2 million hashes/second—. In the table I, we show some estimations of the needed time for the obtention of the ฿50 depending on the computing capacity deployed by the user.

This reality has led to the concept of *pool mining* versus the already described of *solo mining*. The philosophy of the former lies in the grouping of isolated users computer power under one unique operator with the final goal of hoarding a much greater power to receive the bitcoins assignations more continuously and relying less on luck. Thus, pool operators retain a fixed amount —between the 2 and the 10 per cent depending on the mining pool and its distribution method— in concept of management and maintenance of the website, resharing the remaining amount proportionally to the computer power provided by all the users who have trusted on that operator. Usually, the corresponding traffic runs on port 8,332, but, as a side note, it is true that there exist some pools that encapsulate Bitcoin traffic through port 80 to avoid the blocking of certain firewalls.

B. Currency exchange markets

There are numerous ways of buying or selling bitcoins. In fact, in Bitcoincharts [5], more than 50 active markets were already listed in June 2012, with very different available currencies as shown in Figure 2, but the options are unlimited: from accessing to exchange websites in which perform Paypal, Liberty Reserve, WebMoney or OKPay transferences or executing directly bank transfers depending on the site (some of the most well-known are MTGox, Bitcoinmarket or BTC-e); till the acquisition of the gift vouchers to be used in sites such as eBay, Amazon or Steam; passing by buying directly any kind of goods and services in E-Commerce platforms supporting Bitcoin such as osCommerce, which counts with a plugin that permits the transferences using Bitcoin since May 2011 [6].

C. Off-line payments and transactions acceptance period

One of the main problems of using a cryptocurrency is the need to verify that the coin has not already been previously used by its owner to perform another transaction. Bitcoin

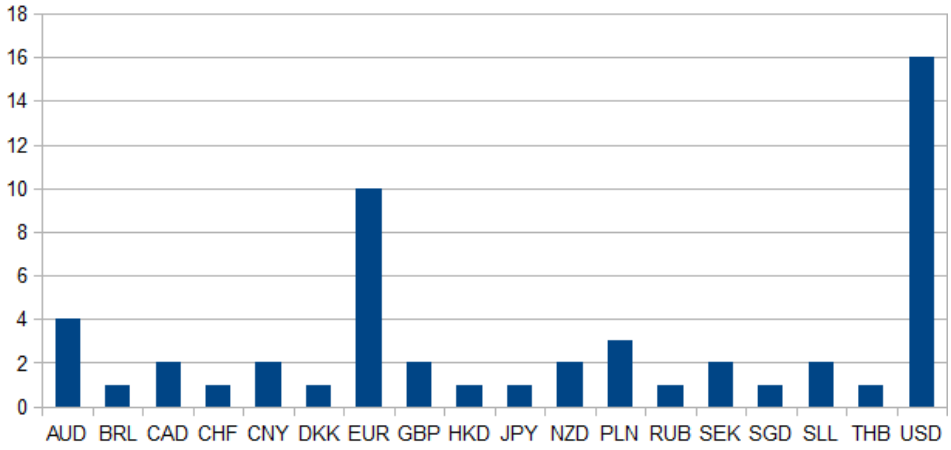

Figure 2. Number of available markets depending on the exchange currency.

choose a distributed checking model instead of checking the legitimacy of its use against a single point.

Thus, this verification process requires the disclosure of the transfer to the rest of the network nodes, which are responsible for verifying that the given coin has not been used in more than one occasion by introducing duplication. To achieve this objective, it is necessary that the charging platforms were connected, being impossible to confirm whether a transfer is valid or not if this were not so. This process often lasts an undefined period of time ranging from 10 to 60 minutes [4]. However, this period is potentially reducible if it includes the payment of a small commission to be assigned to that node in the network that is able to verify the transfer. This fact introduces a new motivation component for user sharing their computing power whenever the total amount of bitcoins have been handed out.

D. Transactions tracking

Anyway, the anonymity of the transactions is not guaranteed by the protocol itself since this is not its ultimate goal [4]. In fact, the need for open verification requires the disclosure and publication of every transfer. Recent studies have used traffic analysis tools so as to identify the called *egocentric networks*, showing that anonymity is not a standard pattern in the majority of the transactions [7]:

- In the analysis conducted by Reid et al. [7], a collection of transactions were monitored from an *self-incriminated* thief, to whom the authors assume the interest of remaining anonymous so as not to be tracked. The point is that the authors were capable of identify relationships of up to $n = 1, 2, 3$ hops between the victim and the alleged cybercriminal.
- Another case brought by the authors referred to the announcement of Wikileaks to accept *anonymous donations via Bitcoin* using a single public key per transaction. The authors call into question the real anonymity of the donor.

In short, it is assumed that the strength of Bitcoin does not rely on boostening the anonimity: in fact, the transactions will be only as anonymous as impossible it were to uniquely identify the connection of the user that runs them.

III. Prospective on criminal behaviour

The aforementioned characteristics can be exploited in a healthy and reliable way, but also agglutinate features that may be exploited in the shadow. In this section, we will cover some of them.

A. Speculative movements sensitivity

As most economic elements, bitcoins are also sensitive to radical changes linked to speculation. The exchange of bitcoins for euros, dollars, pounds or any other cryptocurrency is particularly sensitive to speculative movements and the subjective perception of its value. Figure 3 shows the evolution of the exchange markets since the birth of the cryptocurrency till the actual situation. As can be seen, the perception of their value has markedly fluctuated to reach the astonishing levels of 25 dollars/bitcoin, figures far removed from the far more stabilized 5.3 dollars/bitcoin in June 2012; identifying around June 2011, what some authors have defined as the *Bitcoin Bubble* [8].

Speculation is also present in the long run. Considering a constantly growing user population over time and knowing that the total amount of bitcoins ends up being a finite number, the value of ฿1 will tend to represent goods with increasing value: that is to say, Bitcoin will move towards becoming an economy with hints of finally evolving into a potentially deflationary system. The main operational problem that entails the divisibility of money, is already tackled by Bitcoin as each coin is divisible up to 10^{-8} parts. Or what would be the same, each coin could be divided in parts equivalent to μ฿10 (10 *nanobitcoins*), placing the total amount of independent coins in 2,100 trillion units.

 ISBN: 978-1-61208-228-8

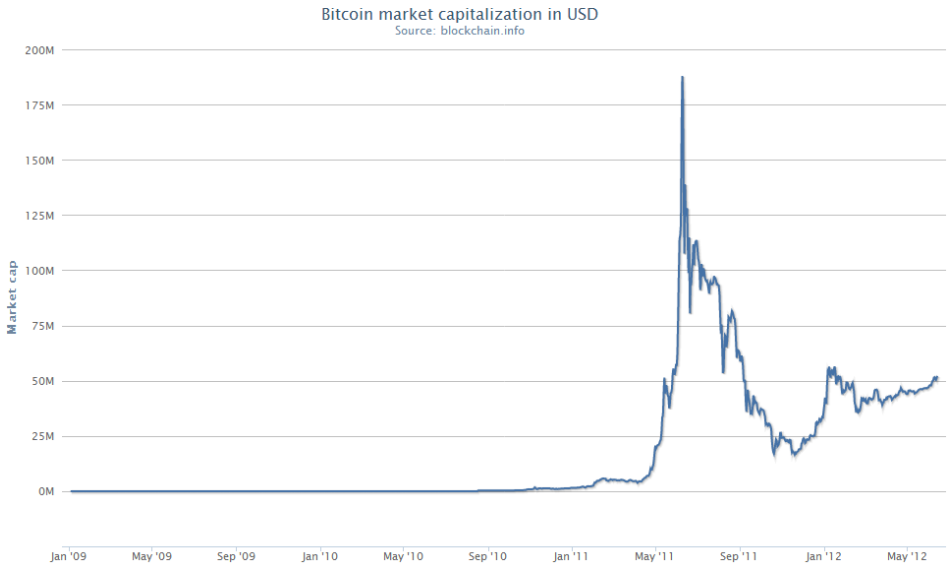

Figure 3. Evolution of the Bitcoin market capitalization in USD since the inception of the cryptocurrency.

However, the actual circulation of all coins is an utopia. The reason for this is the existence of hundreds of coins which are assigned daily to users who lost or will lose the control over them for reasons that do not need to be associated with fraudulent practices:

- It could happen that bitcoins get either lost or forgotten somewhere inside a legitimate computer.
- This hardware, can also be affected by any kind of technical issues that may make impossible the recovery of the cyberwallets.
- It could also happen that the legitimate users would forget the password that unlocks them.

B. Money laundering and illegal traffic

Using online entertainment platforms that somewhat simulate an internal monetary system to hide certain cyberdelictive behaviours is not a recent issue. Mallada [9] described how certain criminals have started to exploit the possibilities offered by some *Role-Playing Games* (RPG) such as *World of Warcraft* or the virtual world of *Second Life*. For instance, in the case of the latter, the author estimates its Gross Domestic Product in $500 million.

Taking into account that Bitcoin develops a payment system which final objective is no longer to simulate but to substitute traditional currencies, the implications and chances of the aforementioned potential applications are even bigger. Even more, despite the characteristics in the previous subsection which do not make the payment method intrinsically anonymous, it is true that the performance of transfers could end being untraceable if some appropriate preventive measures were taken [10]:

- The performance of transferences behind a *proxy* or other anonymisation systems such as networks like Tor. This is the case of the *Silk Road* online merchant [11]: to access to the offered services it is compulsory to be using the Tor browser so as to preserver the anonymity of both, buyers and sellers. Already referenced by some authors as the *Amazon of illegal drugs* [12], [13], in some countries such as the USA some policy initiatives have been carried out to close similar platforms to prevent the illegal drug trafficking [14].
- The execution of n transferences at a time towards an account that, later and as part of a *batch* or *offline* self-controlled, redistributed the received money in m different accounts. Given a great number of transactions from a great number of users, it would be virtually impossible to track the coins from their real owner lost in a woods of relations. This process, as defined in Nakamoto's original description of the system [4], can take place under the following circumstances: either by means of individuals offering the chance of voluntarily increase the anonymity, or by means of organized networks offering this and other similar services in a sort of *dark-market* operating with cyberwallets in the cloud, also kwnown as eWallets. These eWallets are Bitcoin accounts created and managed by third parties which offer to their users an easier way of keeping in touch with their bitcoins. However, given the irreversibility of the transactions, there is no real guarantee that those transferences performed to or from an eWallet will be run, apart from the confidence that the user has on the service itself. A possible scenario may be the following:
  1) A big amount of bitcoins is to be sent to a new eWallet anonymously created using, for example, tools like Tor, described above.
  2) Small transfers are made from such wallet in the

 ISBN: 978-1-61208-228-8

cloud to a set of similar eWallets —inside or outside the original service— before receiving in a collection of new Bitcoin accounts the money to operate with them again.

This approach raises points that are likely to require an automated account management, suggesting a greater knowledge and better use of the computer tools already available.

C. Virtual pickpocketing

System features make the *coins* being stored as .dat files in the computers of their owners. Those may make backup copies to be stored in alternative computers or devices —or even in the *cloud*— in order to maintain access to them whatever kind of failure takes place as this would imply the automatic loss of the control on the coins as there would be no way to recover them.

Nonetheless, any user or program with logical access to the .dat file could execute transactions on his/her/its own if this file has not been adequately protected. Although the use of the so called *military* encryption standards —as, for example, AES-256, the Advanced Encryption Standard specification for encrypting electronic data adopted by the U.S. government [15], widely considered as a *de facto* cryptographic standard— is accessible by any user since the protocols are public and implemented in numerous libraries and open-source platforms; it is a standard pattern coming across with unprotected files, resulting in a stream of malware threats uniquely dedicated to stealing these files.

In this line, Laboratories such as Kaspersky Labs, deactivated in late March the Command & Control channel (simplifying, the C&C channel is the tool for managing and controlling a network of kidnapped computers or *botnets*, used in a bunch of different criminal ways) of Hlux/Kelihos. In this case, *Hlux* was a botnet specialised in stealing Bitcoin wallets [16], proving that even cybercriminals have found a new battlefield from which obtain illegal benefits easy to monetize. Meanwhile, the Sections on ÇyberIntelligence and Criminal Intelligence of the Federal Bureau of Investigation (FBI) stated in a recently filtered intelligence report [17] that there exist Zeus samples —a Zbot trojan version specialised in the recruitment of machines as part of a botnet— specially designed to operate in the shadow using the victim's resources in the dark.

D. Unauthorized use of computing power

However, the use of similar networks may also have other purposes. Similarly to what happens with the distributed computing projects, could be used downtime CPU or GPU of infected machines for the generation process of exchange without the user's knowledge. Currently, mining of bitcoins is not considered a profitable business if it is not performed using the appropriate hardware. In many cases, the revenues produced in the mining process are not able to cover the energy costs of the generation.

An important aspect to avoid the detection of any unauthorized process is to give the user the fewer indicator as possible. This also occurs when hiding illegal mining processes. In this sense, the use of *applets* which make use of processor idle time —for example, assigning the mining processes the lowest possible priority as the *Bitcoinplus* miner does— or not exploiting all the capabilities of the graphics card —avoiding overloading and warming— would become essential. This may be enough to avoid the end inexpert user of the machine noticing the symptoms of a machine being remotely used, unless he/she manually checks the use percentage of the processor.

In the scenario of a middle-size-botnet compounded by 10,000 usable computers, and considering a computing power of an average of the 0.005 bitcoins/day and machine, the derivated exploitation would round the 50 bitcoins/day—about 200 euros/day in the most common exchange markets—. Taking into consideration the dismantling in 2010 of the botnet Butterfly, on a combined action of Panda Labs along with the Spanish Guardia Civil, and which size stood at 13,000,000 infected machines, the numbers speak for themselves about the potential benefit in which may incur the administrator of such a network. Being able to exploit these characteristics would make any botmaster leverage from a seemingly innocuous part of the computing power of the infected machines obtaining a direct benefit and increasing artificially the electric bill of the legitimate user.

E. A likely jump to the real world

For the writing of this report, the authors have independently contacted with certain European business that publicly state that accept Bitcoin as a payment and which actually use this cryptocurrency as bait to attract Bitcoin new customers. In the public list available online in Bitcoin's official Wiki [18], where the reader can mainly find local hotels and restaurants among other businesses, it becomes clear that the use of this currency, which in principle might seem limited to Internet shopping, has surpassed, although still timidly, the barriers to real world.

Its presence introduces an additional component of complexity in the control of buying and selling process as there is no official entity to recognize its use and, therefore, there is a full absence of any kind of official change in the different central banks. What is more, this may lead to problems associated to tax evasion and fraud because of the impossibility of calculating the official value of the transaction in what can be considered, technically, a barter economy: that is to say, exchanging goods or services for bitcoins, which may be defined under certain circumstances as *other cryptographic goods with some subjective value*.

 ISBN: 978-1-61208-228-8

F. Alternative cryptocurrencies based on Bitcoin

Bitcoin's source code can be widely studied since it is distributed under the MIT License. This, almost naturally, has led to various *sister* cryptocurrencies which implement specific characteristics that differentiate them from the original:

- IXcoin (IXC). This is a cryptocurrency with a parallel development to Bitcoin but scheduled to have a shorter maturity period, as the maximum number of coins (also 21 million) will have been generated by 2015. This suggests that speculative movements in the maturation period of the currency are potentially more violent and less predictable.
- Devcoin. This is a currency that allocates the 90% of the resources generated to developers participating in open source programs so as to fund their work, reserving only the remaining 10% to the miners.
- Namecoin (NMC). Also based on the architecture of Bitcoin, the namecoins constitute a currency which target is creating a domain name system (DNS) using the .bit TLD. The objective is to provide resources and tools to protect the community against a censorship to be potentially applied by a central entity (like ICANN in the case of domain names). Thus, the .bit domains are maintained entirely by a Bitcoin-like peer-to-peer network.

In another development, the philosophy Bitcoin uses to prevent double spending and limit the proliferation of fraudulent currency has been studied by some authors as Becker et al. [19] for a generalization and export to other areas that share similar needs, even beyond the domains management Namecoin tries to implement.

IV. Conclusion

Though yet in an underground development phase and, mostly, pretty unknown for the general public, the proliferation of these new payment alternatives brings many uncertainties. What is more, the intrinsic complexity of the protocol and the necessity of having some relatively advanced knowledge on cryptography and computer studies to understand its real behaviour, make these cryptocurrencies the perfect place for speculation and misinformation. For instance, as already stated, there is a widespread belief of the mere fact of using it is sufficient guarantee to perform anonymous transactions, when this is not true by definition.

At the same time, the absence of a regulatory central organism and the chance of not being able to fix the prizes in a explicit way as it happens with the traditional cryptocurrencies, defines a new scenario on an economy strictly ruled by the market movements with all the consequences that this fact leads to in terms of control of massive speculative efforts. At this point, amongst the possible failure scenarios the most urgent for Bitcoin, excepting a dramatical reduction of users which may devaluate the currency once mature, is, precisely, a global governmental campaign against its use.

Just before the end, we can conclude that there is a real risk of a recurrent illegal use of the cryptocurrency. The great number of existing markets and the possibility of exchanging easily bitcoins by euros, pounds or dollars, make this new method the perfect vehicle to perform every kind of transactions related to money laundering or illegal traffic of substances, with all the legal implications associated to the jurisdictional limitation of the criminal acts performed in the cyberspace.

Acknowledgments

The authors would like to thank the Spanish Guardia Civil from their interest and support to this research and, personally, to the person of José María Blanco.

References

[1] D. Barok, Bitcoin: censorship–resistant currency and domain system for the people, in *Networked Media*, Piet Zwart Institute, 2011.

[2] P. Ernstberger, Linden dollar and virtual monetary policy, in *Macroeconomics*, p. 20, Department of Economics, Economics I, Bayreuth University, 2009.

[3] B. Mennecke, W. D. Terando, D. Janvrin, and W. Dilla, It's just a game, or is it? Real money, real income, and real taxes in virtual worlds, in *Communications of the Association for Information Systems*, volume 20, pp. 134–141, 2007.

[4] S. Nakamoto, Bitcoin: A Peer-to-Peer Electronic Cash System, http://www.bitcoin.org, 2009.

[5] B. Charts, *All Markets*, 2012, available online http://bitcoincharts.com/markets/list/ [retrieved: August, 2012)].

[6] *Bitcoin payment module*, 2011, available online http://addons.oscommerce.com/info/8007/ [retrieved: August, 2012)].

[7] F. Reid and M. Harrigan, 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 Confernece on Social Computing (SocialCom)*, pp. 1318–1326, IEEE, 2011.

[8] B. M. Maurer, Money nutters, in *Economic Sociology - The European Electronic Newsletter*, p. 5, 2011.

[9] C. Mallada, Las nuevas tecnologías y el blanqueo de Capitales: Second Life, entretenimiento online y el método delictivo, in *Challenges and Opportunities of Online Entertainment. Proceedings of the 8th International Conference on Internet, Law and Politics*, pp. 199–209, Universitat Obverta de Catalunya and HUYGENS Editorial, 2012.

[10] S. Martins and Y. Yang, Introduction to bitcoins: a pseudo-anonymous electronic currency system, in *Proceedings of the 2011 Conference of the Center for Advanced Studies on Collaborative Research*, pp. 349–350, IBM Corp., 2011.

 ISBN: 978-1-61208-228-8

[11] N. Christin, Traveling the Silk Road: A measurement analysis of a large anonymous online marketplace, CMU-CyLab-12-018, 2012, Id: paper.tex 1286 2012-07-30 21:29:14Z nicolasc.

[12] E. Jacobs, Bitcoin: A Bit Too Far?, in *Internet Banking and Commerce Vol.*, volume 12, 2011.

[13] M. J. Barrat, SilkRoad: Ebay for drugs, in *Addiction*, volume 107, pp. 683–683, Wiley Online Library, 2012.

[14] J. Manchin, *Manchin Urges Federal Law Enforcement to Shut Down Online Black Market for Illegal Drugs*, 2011, Press Release http://manchin.senate.gov/public/index.cfm/2011/6/manchin-urges-federal-law-enforcement-to-shut-down-online-black-market-for-illegal-drugs [retrieved: August, 2012].

[15] Biryukov, A. and Khovratovich, D. and Nikolić, I., *Advances in Cryptology-CRYPTO 2009* , 231 (2009).

[16] Kaspersky Lab, How Kaspersky Lab and CrowdStrike Dismantled the Second Hlux/Kelihos Botnet: Success Story, 2012.

[17] Directorate of Intelligence: Cyber Intelligence Section and Criminal Intelligence Section, Bitcoin Virtual Currency: Unique Features Present Distinct Challenges for Deterring Illicit Activity, in *FBI Intellligence Assesment*.

[18] *Real world shops*, 2012, available online https://en.bitcoin.it/wiki/Real_world_shops [retrieved: August, 2012)].

[19] J. Becker, D. Breuker, T. Heide, J. Holler, H. Rauer, and R. Böhme, Can We Afford Integrity by Proof-of-Work? Scenarios Inspired by the Bitcoin Currency, in *Workshop on the Economics of Information Security WEIS 2012*, 2012, JEL Classification: E42, Q30.

 ISBN: 978-1-61208-228-8