BitCoin: General and Criminal Analysis of the Decentralized Virtual Currency

Daniel Eszteri
Budapest Police Headquarters, PhD student at University of Pécs

Keywords: *Bitcoin, virtual currency, decentralized payment system, anonymity, cybercrime*

Introduction

We can make money in many different ways. We can earn it, receive it as a present, steal it, counterfeit it, or find it on the street. These ways are traditional in our everyday world, whether legal or illegal, but what happens when a new type of money is invented?

There is a new virtual currency, Bitcoin, which exists only on the internet. It is an independent currency consisting only of bits and bytes, but not represented by bank notes or physical coins. There is no cover in terms of gold or stocks, for example – in fact, nothing but the thirty-one thousand lines of the software's source code.[1]

The life of this unique virtual currency started in November 2008, when a formerly unknown person, calling himself Satoshi Nakamoto posted his famous essay concerning the creation of a currency which exists only in virtual space on the internet.[2]

1 Davis, J., "The Crypto-Currency" (2011), <www.newyorker.com/reporting/2011/10/10/111010fa_fact_davis> (01.07.2013).

2 Nakamoto, S., "Bitcoin: A Peer-to-Peer Electronic Cash System" (2008), <bitcoin.org/bitcoin.pdf> (01.07.2013).

No-one had previously heard of this mysterious individual, and even the 'great old experts' of cryptography remained silent when they saw the name. The pseudonym Nakamoto was only an online profile of a mysterious, faceless hacker who claimed to be a software-engineer living in Japan.

The e-mail address used to publish the paper was registered by an anonymous German domain-registration company, and we can find no other information on the internet. Since then, this interesting person has disappeared into the endless depth of cyberspace for ever, even though in his thesis he gave an answer which had baffled the experts dealing with cryptography and digital currencies since the birth of the world-wide-web.[3] Bitcoin software was released in the beginning of 2009, and the first Bitcoin transactions were made using a network established according to Nakamoto's thesis. This works much as does a decentralised peer-to-peer network (as BitTorrent technology, used for file-sharing via the internet).

The Bitcoin phenomenon immediately raises questions. What is Bitcoin? How much is a Bitcoin worth? How can we pay with this new kind of money? What can we purchase in Bitcoin? How can we obtain, or earn Bitcoin? How does the network operate? Is it safe? What kind of legal framework is involved? Can the currency be used for illegal activities? The paper tries to answer these questions.

1. Brief history of virtual money

The history of money has heavily been influenced by virtualisation, and the first event in this was the introduction of credit cards, which reduced money-circulation by banks. After credit cards digital money, which holds its value in lines of digital code authenticated by the bank's digital signature, appeared. Digital money must be in accordance with the classical functions of money,[4] absorb new functions such as security, anonymity, acceptance, different denominations, offline working, different operating systems and hardware dependence.[5]

3 Wallace, B., "The Rise and Fall of Bitcoin" (2011), <www.wired.com/magazine/2011/11/mf_bitcoin/> (17.06.2012.)

4 The classic money functions are: medium of exchange, circulating medium, store of value, accounting function.

5 Infótér, "Bitcoin, a nonkonformista digitalis fizetőeszköz" (2012), <infoter.blog.hu/2012/06/11/bitcoin_a_nonkomformista_digitalis_fizetoeszkoz> (01.08.2012).

Before the coming of Bitcoin, many scientists had already taken up the question of an independent, anonymous and decentralized virtual form of money. The first of these, in the beginning of the 90s, was Timothy May and his cyberpunk-enthusiasts,[6] who tried to popularise his theories on the internet, thinking that privacy-protection would be the most important question in the following years. Members of this group shared their opinions via an electronic mailing list called 'Cyberpunks electronic mailing list' founded by May. These theories are summarised in the book 'Crypto Anarchy, Cyberstates, and Pirate Utopias', edited by Peter Ludlow.[7]

David Chaum also dealt with the problem in the 90s, and tried to issue totally virtual money – Ecash. His idea failed since both the government and the card issuer were crucial to the system.[8]

Wei Dai improved these thoughts and came up with the idea of B-money in 1998. He said that a virtual currency had to be built on work-mechanisms, and, further, subscribers had to deal with building the resources algorithmically.[9]

Nick Szabó conceived Bitgold in 1998, although it was made public only in 2005.[10] According to Szabó, Bitgold has to be stored in lines of computer code, must be impossible to counterfeit, safely stored, easily transferred and verifiable. The basic issue is that the parties have to minimise trust in a third party. The parties have to share their computers' calculating powers through a network to solve cryptographic equations.[11]

These theories advanced the birth of Bitcoin since its system already contains such factors. In the next chapters the Bitcoin system's working

6 Cyberpunk is a popular genre of contemporary mass culture, a sub-genre of science fiction which takes place in the near future. In cyberpunk stories people live in a huge, overcrowded metropolis, due to which their emotional life is bleak. The feeling to be part of a nation is overwhelmed by being part of a company. Typical characters are the cybercriminal and the IT-expert.

7 Ludlow, P. (ed), *Crypto Anarchy, Cyberstates, and Pirate Utopias* (A Bradford Book, 2001).

8 Zenner, E., „Ecash – Ein existierendes Zahlungssystem im WWW" (1996), <trumpf-3.rz.uni-mannheim.de/www/sem96s/webrum.uni-mannheim.de/bwl/zenner/seminar/ecash.htm> (01.08.2012).

9 Dai, W., "Bmoney" (1998), <www.weidai.com/bmoney.txt> (01.08.2012).

10 Szabó, N., "Bit gold" (2005), <unenumerated.blogspot.hu/2005/12/bit-gold.html> (01.08.2012).

11 Infótér, "Bitcoin", *supra nota* 5.

mechanisms will be explained, since this is the only decentralised money system in existence so far.

2. The essential characteristics of Bitcoin

Bitcoin (commonly abbreviated to BTC) is not a concrete, physically existing currency, but virtual money: an amount associated with a so-called virtual wallet. How can we have such a wallet? First, we have to download software, also called Bitcoin, from the internet. We can find this on the official homepage of the virtual currency.[12]

After installation this software functions as a digital wallet on our computer and it stores our virtual money. Our wallet is nothing but a file named 'wallet.dat' on our hard drive.[13] Therefore it can be stolen from us if some unauthorised person breaks into the system. In the interest of safety, it is advised to make a backup – or there are internet pages where we can upload our wallet and reach it only by using a password.[14] Bitcoin software is open-source, available for almost every operating system, updated regularly and it contains every necessary function for sending and receiving Bitcoin.[15]

After successfully installing the Bitcoin-client on our computer, we only need to start it and virtual transactions can begin. (How to obtain 'coins' will be explained later in the paper).

How can we send coins to each other with the wallet-software? We can generate so-called Bitcoin-addresses and these are used for financial transactions. Every user has at least one address. It works logically, similarly to an e-mail address, but we send not text messages and files to other users, but virtual coins.

Our Bitcoin address is generated automatically by the software. The computer program creates a new address for every single transaction, making the system theoretically fully anonymous and safe. When we publish one of our

12 Bitcoin homepage, <bitcoin.org/> (16.10.2011).
13 Wikipedia, "Bitcoin", <en.bitcoin.it/wiki/Wallet> (26.10.2011).
14 Wiki, "Securing your wallet", <en.bitcoin.it/wiki/Securing_your_wallet> (18.10.2011).
15 Gedda, R., "Google releases open-source Bitcoin client" (2011), <www.techworld.com.au/article/380396/google_releases_open_source_bitcoin_client/> (26.10.2011)

addresses on a public forum, the software will use it for more transactions; this happens when we publish it in the hope of donations, or use it for regular, rather than single, transactions. We cannot delete our once-created Bitcoin addresses, but we can navigate among them and see how much we have received or sent.

Every single Bitcoin-address consists of two parts. One is the so-called 'public key'; the other is the 'private key'. Our public key can be seen in the application on the 'Your Bitcoin Address' line, but the private key stays hidden. The readable form of the public key has 33 characters, starting with number 1 – e.g., *1HCA3fcadYRQk5Sm3WGD2CPxsZqhdRXTY9*. If we wish to send money through the network to others, we must give them this *public key*.[16]

The software uses the private key to authenticate transactions. This key also belongs to the randomly generated Bitcoin-addresses but is invisible to other users; it functions as a specific digital signature. The software uses private keys as digital signatures to authenticate every single transaction with the virtual coins. The public and private key pairs are stored in the 'wallet.dat' file on the hard drive of the user's computer. We can only see the private keys in this file, and, if we want our Bitcoin not to be stolen, we do not tell them to anybody. In contrast to this, the public key must always be given to others for a successful transaction.[17] How do these transactions work, and what are the functions of these public and private key pairs?

Every single transaction made through the Bitcoin-network is published on the internet. The traditional financial institutions such as banks protect their customers' privacy as they hide the transactions from unauthorised persons. In the Bitcoin system privacy protection is solved so that users' personal data are totally unknown, but the money transaction is made public.[18] For example, when the software generates a new address, we do not have to give any personal data. We do not have to register on the network, but simply start the application, and using the various addresses, the digital 'coins' are received and saved on the computer in our electronic wallet. Let us see an example of how the system works.

16 Bitcoin, <bitcoins.hu/bitcoin_faq.htm> (26.10.2011).
17 The Economist, "Virtual Currency – Bits and Bob" (2011), <www.economist.com/blogs/babbage/2011/06/virtual-currency> (17.10.2011).
18 Bitcoin, <bitcoins.hu/bitcoin_geekeknek.htm> (26.10.2011).

Let us assume that Alice wants to send Ben 10 Bitcoin. Ben gives Alice his Bitcoin-address – that is, the public key belonging to the address. This is the 33 character code which the software displays. If Ben has more than one address for his wallet, he could give Alice any of them, or he could simply generate a new one for this transaction. Ben will receive the money and the software saves the amount in his virtual wallet, without reference to the address used. After Ben has told Alice his address, Alice simply clicks on the 'Send coins' button. In the next window she enters Ben's Bitcoin-address and the amount to be sent. Then Alice clicks on the 'Send' button, and the human part of the transaction is over. In fact the process has not ended; the software uses Alice's private key to confirm the transaction, as in signing a contract. The application sends the transaction (visible to all) to the network. This information is that 10 Bitcoin were sent from '*172Xdzb99rsmwVyZ8HSHgoScmTuEtU3Kgr*' public key address to '*12HnGCwvS4ES1tRC3JXeEYHuFLs9mzMjF7*' public key address. The software can be used perfectly anonymously since the private keys function as digital signatures; they are not visible on the network, and we can generate a new address for each transaction (hence the public and private key pair).

Later, when Ben wants to send this amount to Charles, he does so in the same way. Charles gives Ben one of his public keys, and then Ben sends the amount to this address. The software signs the transaction also, but now uses Ben's private key. This transaction is also visible to everyone browsing the network, as mentioned above.

If Diana wants to steal Ben's Bitcoin, she could not do so by copying Ben's public key to her digital wallet, since the transaction was signed on the network with Alice's private key, and this signature certifies that the amount belongs to Ben. For transactions we need both the public and private keys, and Diana does not know Alice's private key in this case.[19] The following illustrates how transactions work.[20]

19 Wiki, Bitcoin, <en.bitcoin.it/wiki/Introduction#Transferring_a_coin> (17.10.2011).
20 Nakamoto, "Bitcoin", *supra nota* 2, p 2.

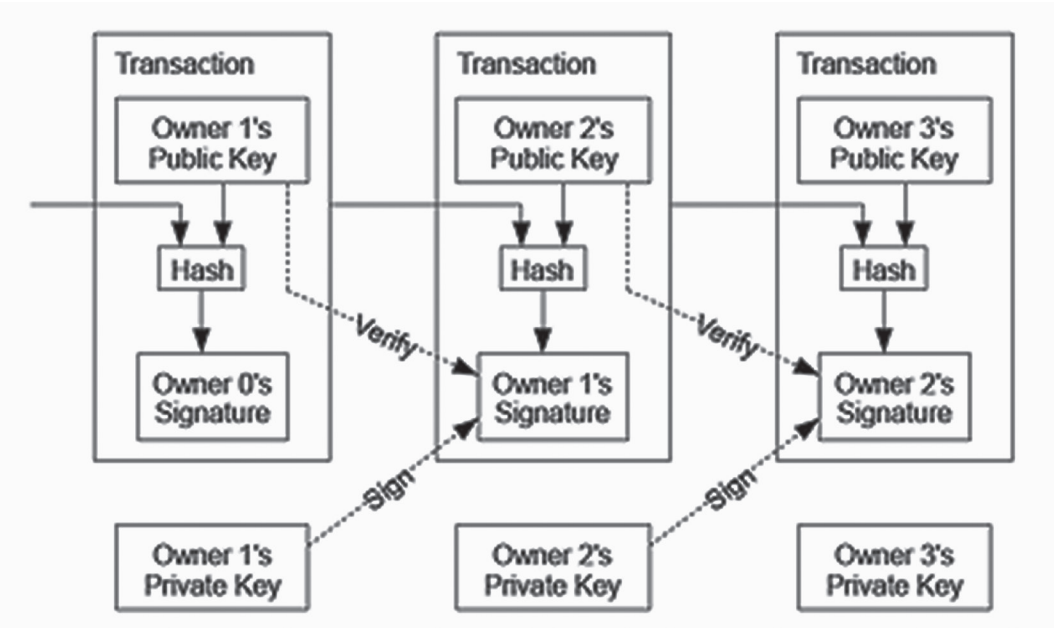


Table 1

3. The decentralised network

According to the table above, the Bitcoin network can be used quite safely, since stealing by changing addresses is technically impossible. Those who use the system cleverly can hide in perfect anonymity, and so the personal data protection problem is also solved, but there is no guarantee that we can spend the same amount twice – which would be a virtual form of counterfeiting. The Bitcoin system makes double spending impossible, as will be shown.

A centralised system (e.g. the classic bank-system) prevents double spending in that all transactions go through a central database which stores them and blocks 'short' transactions. The system prevents such an action if a user wants to spend unavailable funds.

The Bitcoin-system is decentralised and there is no central database, server or any organisation to verify transactions. Many decentralised virtual money ideas failed since they could avoid double spending only by using a central verification system. In this way virtual money resembled real-world

currencies, as normal banking systems did such checking. It was, therefore, necessary to find a blocking mechanism to prevent Bitcoin users signing a contract with their private key before making the transaction and 'selling' the amount twice.

Solving this problem is a very simple regulation which says that only the first transaction matters; others which include the same virtual money are invalid. The operation of this rule was checked in centralised systems by an independent organ, as in a bank. The decentralised Bitcoin system, however, solves the problem by every transaction being public and visible to anyone.[21] The system solves this problem technically in the following way.

Firstly, the system runs a hash algorithm on every transaction. Hash algorithms are unidirectional coding methods and are used to encrypt digital information. The algorithm converts the digital data to numbers, called hash-value. If this number is long enough, it makes unique data totally identifiable. The hash value identifies certain data, but we cannot decrypt the original – useful, since, using the number, we can easily identify the data needed.[22]

The sender digitally signs (with his private key) a pack consisting of the transaction's hash-value and the receiver's public key. It verifies that the sender wanted to send this particular sum of virtual money to the receiver.[23] There is a register of the hashes, addresses and the digital signatures on the Bitcoin-network in the so-called blocks. We can browse these blocks on the blockexplorer.com website. These blocks are small databases, and every single Bitcoin transaction's information can be found in them. Differently from the traditional banking system, in the Bitcoin network it is not the accountholder's data which are public, but those of the transaction. The Bitcoin client downloads every single block from the network to the user's computer, and later the new ones also. The safest bank data-system does not have such a level of redundancy.[24] The database consists of every single successful Bitcoin-transaction to be found on every single Bitcoin-

21 *Ibid*, p 6.
22 Programozas Wiki, <wiki.prog.hu/wiki/Hash> (26.10.2011).
23 Bitcoins homepage, <bitcoins.hu/bitcoin_geekeknek.htm> (26.10.2011).
24 *Ibid*.

user's computer, and it is permanently updated through the network. At least six other computers have to legitimise a transaction on the network to be successful.[25]

In time this method will not be able to be maintained, since the growth of blocks means that the size of the transaction register will also grow.[26] This, however, is a future concern. There will be more about the role of the blocks in the later chapters of the study.

The receivers of the amount transferred can only identify themselves (and use their virtual money) if they have the private key belonging to the public key in the packet. The public and private key pairs are stored in the virtual wallet (wallet.dat file) on the hard-drive of our computer. These files store the most important information in the world of Bitcoin, and so it is advisable to create a backup frequently. The information stored in the virtual wallet is compared with that in the blocks, and this is how the software counts how many Bitcoin we have. According to Nakamoto, a Bitcoin is nothing more than *a chain of digital signatures*.[27] We can compare Bitcoin to registered securities in this way, since their holder is listed in their registers – together with when they were transferred to someone else.

4. Bitcoin mining

If Bitcoin has no central issuer, then how can we obtain some? We can buy from other users or we can begin to produce them ourselves.

How can we produce? The virtual coins are generated on the nodes of the Bitcoin network, when computers find the solution to a mathematic problem.[28] If we want to be part of Bitcoin creation, then, first of all, we have to download software which uses the computing power of our computer's processor or video-card to solve such algorithmic problems on the network. These applications are called "mining-software" and work completely

25 Szedlák, Á., "Kábítószerterjesztők is érdeklődnek az új internetes pénz" után (2011), <www.origo.hu/techbazis/internet/20110615-bitcoin-a-torrentrol-mintaztak-az-internetes-penzt.html> (18.10.2011)
26 Bitcoin Wiki, <en.bitcoin.it/wiki/Blocks> (17.10.2011)
27 Bitcoin homepage, <bitcoin.hu/?page_id=316> (27.10.2011)
28 Bitcoins homepage, <bitcoins.hu/index.html> (16.10.2011)

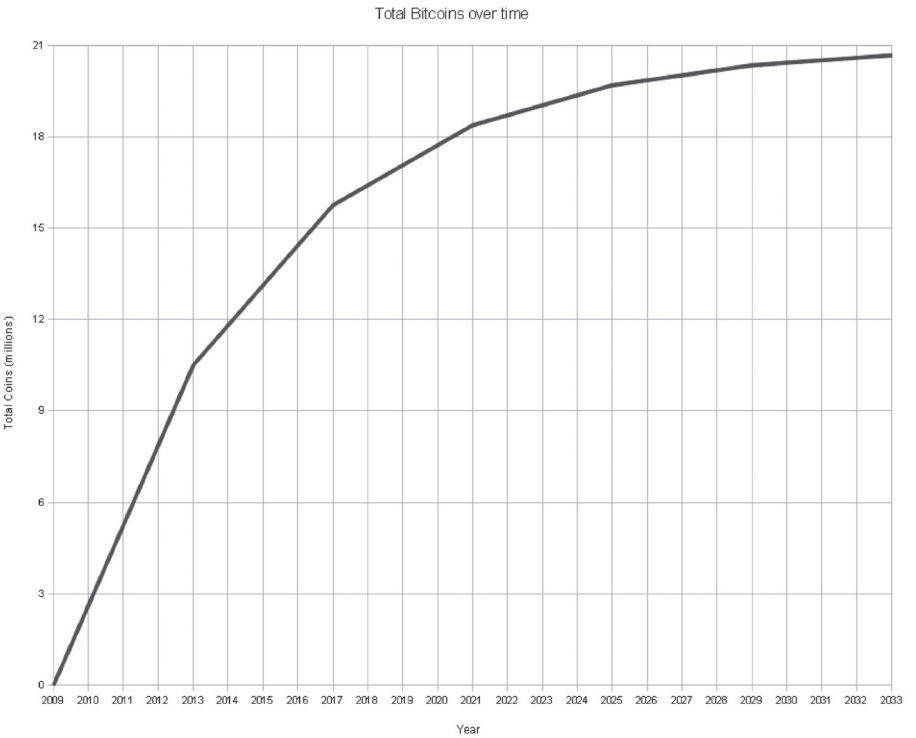
independent of the 'wallet' software.[29] When we manage to solve an algorithm, a block which stores virtual coins and contains every single transaction carried out with them is created. If we find such a block today (February 2014) worth 25 Bitcoin, it appears in the virtual wallet after 10 minutes (the lead-time of the system). We can then spend it or change it freely. We can solve such algorithms alone ('solo-mining') or join a mining community known as a 'mining pool'. More than one user joins a mining pool, and they have their computers work together to create Bitcoin on the network. The difficulty in solving an algorithm depends on how many computers are joined to the network at the same time. It is more difficult to solve a problem if more computers join and easier with fewer.

Bitcoin, however, cannot be created in unlimited quantities, since they would become valueless at the same time. The system solves this problem by predetermining the maximum quantity of Bitcoin which can be created. Moreover, the amount of Bitcoin created when finding the solution to an algorithm depends on the current number of blocks on the network. One block is worth 50 Bitcoin for the first 210,000 block findings. This means that, when a miner finds the solution to a mathematical problem, he receives 50 Bitcoin in return, or this amount will be divided among the miners in a pool. According to the system, one block finding will be worth 25 Bitcoin for the next 210.000 blocks, after which 12.5 coins, then 6.25 and so on. In the first four years of the Bitcoin-network 10,500,000 virtual coins will be created (210,000 blocks multiplied by 50 Bitcoin).

The amount halves every fourth year, and so in the second four-year period 5.250.000 coins will be found (210.000 blocks multiplied by 25 BTC), in the third period 2.625.000 and so on.

With time fewer Bitcoin are mined and it takes longer to mine them. The final number of Bitcoin will be 21,000,000 and the last block to produce them will do so in 2140, after which the number in circulation will be constant.[30] This process is illustrated in the following graph.

29 We Use Coins, <www.weusecoins.com/mining-guide.php> (26.10.2011).
30 Bitcoin Wiki, <en.bitcoin.it/wiki/Introduction#Creation_of_coins> (16.10.2011).



Graph 1

5. How much is a Bitcoin worth

Our money can be changed on some special exchange web-pages, where we can change our funds to Bitcoin using a bank wire transfer. It is accepted as a paying option by various online suppliers, and it can be used to donate to organisations. Bitcoin can be used as a totally decentralised, digitalised and anonymous virtual currency, which is backed by no specific legal entity, as it is transferred via a peer-to-peer network directly between users and involving no central authority.[31]

There are more and more web-pages to be found on the internet which accept Bitcoin as a paying option. The most popular Bitcoin-USD exchange operates under the domain mtgox.com. It is a little difficult to give the exact

31 Grinberg, R., "Bitcoin: An Innovative Alternative Digital Currency", <ssrn.com/abstract=1817857>, p 3 (26.10.2011).

value of a Bitcoin, due to the constant and sometimes drastic exchange rate fluctuations. In 2009, soon after the Bitcoin system was created, a single unit was worth no more than a few cents. Then it was easy to earn coins: with a normal PC one could even mine 1,000 Bitcoin. The solving of mathematic algorithms was much easier for computers, as fewer were connected to the net. After a while people began to discover the new currency and the possibilities in the network. As a result more and more users started to mine coins, and the demand rose rapidly. In December 2010 a Bitcoin was worth about 25 US cents, but three months later exchange rates had the two currencies at the same price. Thanks to media hype, in June 2011, 1 BTC was worth about US$ 30[32]. But this attention had also its dark side, since the underworld began to pay attention to Bitcoin, too. At the end of June 2011 a hacker group attacked the Bitcoin exchange site mtgox.com, and managed to steal more than 60.000 user's uploaded virtual wallets. The exchange rate fell steeply and the fall lasted until the end of 2011.[33] In 2012 the rate began to rise again.

The second big media hype in the history of the currency was in the first three months of 2013 and caused a so-called 'Bitcoin-bubble' in April, when the rate ran too high. After a exchange rate was around 266$/1BTC trading suddenly stopped and the rate fell steeply back again to 77$.[34] In October and November 2013 traders gave more than 1200$ for a single BTC, but the rates fell back to 600$, when the Chinese central bank prohibited the handling of Bitcoin transactions by financial organizations. They also said that private persons could continue to trade it on their own risk.[35] This market behaviour shows us that Bitcoin is such a new phenomenon, that it is hard to predict anything about its future, since stable behavioural norms have not yet emerged.

32 Bitcoin homepage, <bitcoin.hu/?p=74> (26.10.2011).

33 Mick, J., "Inside the Mega-Hack of Bitcoin: the Full Story" (2011), <www.dailytech.com/Inside+the+MegaHack+of+Bitcoin+the+Full+Story/article21942.htm> (26.10.2011).

34 Isidore, C., „Bitcoin bubble may have burst" (2013), <money.cnn.com/2013/04/12/investing/bitcoin-bubble/index.html> (02.06.2013).

35 Bloomber News 5. December, 2013. <www.bloomberg.com/news/2013-12-05/china-s-pboc-bans-financial-companies-from-bitcoin-transactions.html> (02.01.2014).

6. Rivals of the new currency

Bitcoin has at least three competitors on the market. The traditional internet payment options which make online commerce easier belong to the first group, the currencies of social networks and online games to the second, and official national currencies to the third.

6.1. Traditional online paying options

The most common option for online payment is PayPal, with which we can transfer our real-world money to a virtual PayPal-account, and buy, quickly and easily, goods in various online stores. It is similar to Bitcoin but lacks the decentralised and anonymous features. However, it is unlikely that Bitcoin can be a serious rival to traditional methods of payment, as most customers do not care about such features. They like to see prices in EUR or USD instead of BTC, and most people will accept a brand new, unknown currency only reluctantly.[36]

The only advantage of Bitcoin is that there are no transaction costs. An article mentions that employees working abroad regularly send money home to their families. A proportion of the amount transferred is taken by banks as transaction costs, but the use of Bitcoin would remove this problem.[37]

6.2. Currencies of virtual worlds

Another interesting area of online commerce is trading in online games, or in the so-called virtual worlds. Most online role-playing games have their own currencies and we can buy virtual goods for our avatars in the game world. Even such games exist where we can change virtual money to real-world currencies, as in Second Life.[38] Facebook recently introduced Facebook's credit system, with which we can change our money to credits. With these credits we can buy virtual goods (e.g. virtual potatoes) in the network's applications such as Farmville.

36 Grinberg, „Bitcoin", *supra nota* 31, p 13.

37 Bitcoin homepage, <bitcoin.hu/?p=1007> (20.10.2011).

38 Second Life is an interactive virtual reality, which is playable on the internet since 2003. Developer: Linden Lab. Homepage: <secondlife.com/> (01.07.2013).

Developing such virtual economies takes much time and knowledge, and it also requires constant attention from the developers, who tend to charge for costs for transactions and changes. In Diablo III[39] we can even buy (for US$ in the game's real-money auction house) a magic sword for our character, but we must also pay a transaction fee.[40] Bitcoin-based commerce can be accepted more easily by online 'gamers' since it is not strange for them to trade with the virtual currencies of fantasy worlds and then exchange these for real-world money. It is true that the developing companies are behind these virtual markets and pay close attention to them, but they also mean security, since users can apply to them in the case of misuse.

Bitcoin itself could be an excellent option for introducing a common virtual currency in game worlds. Software developers would save time and money were they to fix prices in a common virtual currency, whilst transfers would also be simpler. For this Bitcoin would be perfect.

6.3. Official national currencies

Could Bitcoin be a rival to official real-world banknotes and coins, the banking system behind them and the legal guarantees? In this, as in online transactions, Bitcoin has both advantages and disadvantages. Minimising transaction costs is important, but online payment can be difficult in some situations. Nevertheless, there are already restaurants and shops around the world where we can pay with Bitcoin.[41] The biggest disadvantage of virtual money is at the same time its greatest advantage – that is, there is no legal entity behind it, and it lacks central control. The value of a Bitcoin was 2,000 times more in June 2011 than in the beginning of 2009, but it then shrank to 1/30 following the news of hacker attacks against the exchange site. This is possible as the value of a virtual currency is based only on supply and demand. Deflation being calibrated into the system and becoming better known among internet users suggests that, before long, rates will be more stable.

39 Diablo III is a hack and slash type online role-playing game, playable since May 2012. Developer: Blizzard Entertainment. Homepage: <eu.battle.net/d3/en/?-> (31.07.2012).

40 Diablo3.hu: "Tisztázzuk a hallottakat: Real-Money Auction House" (2011) <diablo3.hu/2011/08/02/tisztazzuk-a-hallottakat-real-money-auction-house/> (20.10.2011).

41 Roberty, D., "The clock is ticking on Bitcoin" (2011), <tech.fortune.cnn.com/2011/06/17/the-clock-is-ticking-on-bitcoin/> (20.10.2011).

7. The future of Bitcoin

Behind national currencies lie government guarantees, but Bitcoin is backed by no legal entity. Facts, however, do show that there is demand for the new virtual currency and its users trust the system. The case below illustrates that such currencies do have a reason to exist.

In 2011 Reuben Grinberg compared Bitcoin in one of his essays to the 'Iraqi Swiss dinar', as that was the only currency in history not backed by any state guarantee, by a valuable raw material such as gold or commodities, despite which it stayed on the market for over 10 years.

An interesting monetary situation evolved in Iraq after the Gulf War of 1991. Before the war Iraqi bank-notes were printed with Swiss platens in England, but after the war, because of the embargo, this was no longer possible and so new notes were printed locally in Iraq and in China. The quality of the new notes was bad and counterfeiting began to increase. Sometimes the forged notes were of better quality than the original ones. Due to the war, the autonomous territory of Kurdistan became *de facto* independent, although it never declared itself as such *de jure*. The new, poor quality banknotes were not accepted in Kurdistan, but people continued to use the old dinars which had already been withdrawn in other parts of the country. The exchange rates of the two currencies soon started to diverge and a new currency came into being called the 'Iraqi Swiss dinar'. There was no central bank, or official exchange rate – and even no guarantee of value. However, in Kurdistan new notes were not printed and so Swiss dinars did not lose value, even if, with wear and tear, a little deflation was seen.[42]

After the 2003 US occupation of Iraq, the interim government issued new currency and allowed people to change it for Swiss dinars. The central bank gave 150 New Dinars for every Swiss Dinar. This shows that a currency can remain in use, even if not backed by government guarantee when the market accepts it as money and trusts it.[43]

42 Wikipedia, <hu.wikipedia.org/wiki/Iraki_din%C3%A1r> (26.10.2011).
43 Grinberg, „Bitcoin", *supra nota* 31, pp 18-19.

8. The legal status of Bitcoin

The only certain thing that we can say about the legal status of Bitcoin, is that it is legally regulated nowhere in the world. Due to its economic behaviour, the uncontrollable, independent virtual currency bypasses every law made so far, and it is located in a so-called 'legal grey area'. In this chapter I shall examine Bitcoin's status in Hungarian law.

8.1. Bitcoin as money

A basic question must be about whether countries will ban Bitcoin as money. In most of the world the exclusive right to issue money belongs to the central bank of the state. The period in the USA between 1837 and 1866 is called the 'Free Banking Era' since at that time almost anyone could issue their own money and more than 8,000 types of currency were traded on the market. If an issuer went bankrupt, closed, moved or suspended activity, the issued money simply became worthless. The National Bank Act ended this practice in 1863 as it banned issuing private money.[44] Many countries use such regulations to limit competition between the private sector and the government. For example, in Hungary the exclusive right to issue money belongs to the Hungarian National Bank.[45] Bitcoin has no central issuer, but the coins are generated in the nodes of the network by the users' computers. Anyone who runs a mining software or is a member of a mining pool, counts as a Bitcoin issuer. As Bitcoin is generated by various users around the world, it would be impossible for a state to ban them in the absence of international action against mining.

At least one private currency; the Liberty Dollar, was a victim of such banning action. It was developed and issued by Bernard von NotHaus in the USA between 1998 and 2011. He created it to avoid USD inflation.[46] Many people used the currency, and, after some time, the government paid attention and finally banned it as a 'false currency'. Unlike Bitcoin, Liberty Dollars were backed by gold, silver and other commodities, and it appeared

44 Wikipedia, <hu.wikipedia.org/wiki/P%C3%A9nz#Mag.C3.A1np.C3.A9nz> (24.10.2011).
45 Act LVIII of 2001 about the Hungarian National Bank, in force 01.07.2013, section 4 paragraph (2).
46 Wikipedia, <en.wikipedia.org/wiki/Liberty_Dollar> (26.10.2011).

on the market in banknote and coin form.[47] According to the justification of the judgment, the action was not to be interpreted as an attack on private currencies, but to prevent fraud and counterfeiting.[48]

Due to these problems Bitcoin cannot be classified as a traditional currency, since legal regulations cannot be applied. Could it be interpreted otherwise, as a security, a right- representing asset, an intellectual product or commodity?

8.2. Bitcoin as intangible property

We can divide a legal entity's property into active and passive parts. Active property embraces assets such as objects, intangible properties and demands.[49] Intangible properties are rights which have an expressed value in money, such as the right of land use, the right of beneficial ownership, the right of intellectual property use or the right to manage the assets of another person.

If we look at the value of Bitcoin owned by a certain user and attempt to interpret it in some way, we have intangible rights. Can we interpret this as someone's intellectual property and a related right of use?

We cannot regard a certain Bitcoin amount created on the internet as an intellectual creation, since blocks are created by the user's computer solving mathematical algorithms. According to Hungarian copyright law and international norms, the solution to a mathematical problem is not protected by copyright.[50] After its creation the right to use a unit belongs to the user whose computer solved the algorithm. Due to the nature of the system, a Bitcoin does not have an owner and cannot be deemed as intellectual property, as it is merely data created by mathematical algorithms on a computer's hard drive in the virtual wallet file. The user of a unit is the person who has the wallet file on his computer.

47 Morrison, C., "Liberty Dollar creator convicted in Federal Court" (2011), <www.citizen-times.com/article/99999999/NEWS01/110319006/Liberty-Dollar-creator-convicted-federal-court> (18.03.2013).

48 Lipsky, S., "When Private Money Becomes a Felony Offense" (2011), <online.wsj.com/article/SB10001424052748704425804576220383673608952.html?mod=googlenews_wsj> (24.10.2011).

49 Lábady, T., *A magyar magánjog (polgári jog) általános része* (General part of the Hungarian private law, civil law) (Dialóg Campus Kiadó, Budapest-Pécs, 2002), pp 291-292.

50 Act LXXVI of 1999 on Copyright, in force 08.02.2014, section 1, paragraph 6.

8.3. Bitcoin as intellectual property

There could, however, be an alternative view if we look at the file which contains Bitcoin and try to analyse it legally. Wallet.dat can be found on the hard drives of computers. Its function is to hold public and private key pairs for Bitcoin. Every user has a unique file. It is possible to make a copy, but this will not double the available amount. When someone uses coins to make a transaction, the contents of the file change. Despite this, we cannot treat wallet.dat as someone's intellectual creation, since copyright law does not treat money transactions in this way. So, wallet.dat is not protected by copyright law and does not belong to a user's intellectual property; it is merely a file on the computer which can be owned, used, copied and altered in content, but only by Bitcoin client software.

8.4. Bitcoin as a commodity

Given the use of electricity and the computer's computing capabilities, Bitcoin emerges as a special commodity which can be traded as goods or services on the virtual market.

According to Hungarian legal regulation of stock exchanges Bitcoin could be treated as a special digital commodity if it is traded at a stock exchange.[51] But in other situations Bitcoin behaves more like money on the market and not as a special commodity, for example when persons do not trade Bitcoin using exchange sites, but buying goods on it in web shops. The problem is that legislation has not dealt with legal issues of decentralized virtual currencies so far.

In my former essay about Bitcoin I classified it as special decentralized money.[52] New behaviours on the market of crypto currencies show that traders buy Bitcoins not to spend them in web shops, but to invest to it as a special treasure-forming device like gold, silver or platinum. Many Bitcoin-investors speculate on the rise and fall of exchange rates to make profit.[53]

51 Act CXX of 2011 on capital market, in force 01.01.2014, section 5, paragraph 1, point 7.

52 Eszteri, D., "Bitcoin – Anarchist money or Currency of the Future" — *Studia Iuridica Auctoritate Universitatis Pécs Publicata* (Hungary 2013).

53 Lee, T. B., „Bitcoin startup raises a record of $ 25 million. Is this a Bitcoin investment bubble?", *The Washington Post*, 12.12.2013 <www.washingtonpost.com/blogs/the-switch/wp/2013/12/12/bitcoin-startup-raises-a-record-25-million-is-this-a-bitcoin-investment-bubble/> (02.01.2014).

We cannot classify this new virtual currency by using the existing law, but, due to its nature, Bitcoin is more akin to a special digital commodity in most situations.

But it is all the same that we treat it as commodity or money, because these are considered as assets and are capable of appropriation according to civil law.[54] Since users treat Bitcoin so, we can regard it as a 'virtual thing' or 'virtual asset'. Custom and practice also shaped the behaviour with which users treat Bitcoin and use it as a valid medium of exchange on the market. The law was not prepared for such an invention, and so Bitcoin's egal status has not been clearly regulated yet. Fortunately the debate about the legal status of the crypto currency is evolving rapidly around the world with some countries such as Thailand[55] banning Bitcoins outright, some countries such as Germany[56] stating Bitcoin entirely legal, and other countries such as China[57] limiting some uses of Bitcoin while stating others are legal. The ideal solution would be an international regulation of virtual assets and crypto currencies.

9. Bitcoin as a possible criminal tool

As mentioned earlier, the anonymous currency can be a perfect tool in the hands of criminals for reaching their goals. Such law enforcement authorities such as the FBI have dealt with the question recently in a major report which has already been leaked to the internet.[58] It may be interesting to examine the 'Bitcoin-problem' from this point of view also, since the anonymous transfer of money seems, at first sight, to be the basis for money laundering. Is Bitcoin's appearance really so great a problem for the jurisdiction as it seems? What is the danger to the system and how can damage be prevented? In this chapter I try to answer these questions.

54 Act V of 2013 on the Civil Code of Hungary, in force 15.03.2014, section 5:14.

55 The Telegraph, "Bitcoins banned in Thailand", <www.telegraph.co.uk/finance/currency/10210022/Bitcoins-banned-in-Thailand.html> (08.02.2014).

56 CNBC, "Bitcoin recognized by Germany as 'private money'", <www.cnbc.com/id/100971898> (08.02.2014).

57 BBC News, "Bitcoin sinks after China restricts yuan exchanges", <www.bbc.co.uk/news/technology-25428866> (08.02.2014).

58 Federal Bureau of Investigation, Intelligence Assessment: "Bitcoin Virtual Currency: Unique Features Present Distinct Challenges for Deterring Illicit Activity", 24.04.2012, Online: <cryptome.org/2012/05/fbi-bitcoin.pdf> (31.07.2012).

9.1. Advantages and dangers of the lack of central control

Due to the Bitcoin network features that users give no personal information about themselves and that there is no central control authority behind the system, the identification of suspect transactions and users or obtaining transaction logs seem impossible at first sight. Nevertheless the network has features which can help us track transactions and link them to someone. First, every transfer is public and can be seen on www.blockexplorer.com or http://blockchain.infowebsites.[59] We do not have to request transaction records from authorities or financial institutions, since they can be browsed freely on the internet. Every single transfer made by a suspect Bitcoin address can be followed along the chain.

However, it is not guaranteed that the person behind a transfer can be identified since the information includes no personal data – especially not the sender's or receiver's IP address – but merely the amount transferred between two public keys.

We have to keep in mind that most people use Bitcoin as a simple, anonymous, online payment tool and not as a currency to replace real world money. Most users buy Bitcoin for a certain purpose (for example to buy something from a web shop), but sooner or later they change back to real world currencies.

It was mentioned earlier that official currencies can be changed to Bitcoin and back on some special exchange websites, such as the Japan-based Mt-Gox (http://mtgox.com). To use services offered by the website, users have to register an account and give it an account name, password and e-mail address. This information is not too serious, but it can be a good starting point for further identification. The operators of the website could confirm whether or not someone is the user of a certain Bitcoin-address registered on their website. If the answer is yes, they could provide further information such as the registered account name, e-mail address or IP-addresses used during logins.[60] Also such exchange sites exist which asks for the bank account numbers of users, and so the service providers can transfer the amount changed in real world money. A bank account's

59 Nakamoto, "Bitcoin", *supra nota* 2, p 6.
60 Federal Bureau of Investigation, *supra nota* 58, p 10.

transactions and documents concerning the owner of the account mostly provide enough information to identify a person.

According to the FBI, it is good to keep in mind that some users publish their Bitcoin addresses on online forums in their comments.

9.2. Money laundering with virtual currencies

It seems that Bitcoin could be an ideal tool for hiding money made by committing crime – money laundering – because of the anonymous paying opportunity and the absence of transaction costs. According to the FBI's analysis, this is possible since such attempts have happened recently with other virtual currencies. These can be simple electronic payment tools such as WebMoney, or virtual currencies of online role-playing games such as gold in the World of Warcraft.

A good example is of when an online, organised crime group changed their crime-related money to an online game's virtual currency on a special exchange website. Later they bought several virtual items using the virtual world's in-game market and sold them to other players for real-world 'clean money'.[61] Popular in-game currencies can be changed to real world money on several websites. There are also such online games where the developers have made it possible to exchange virtual money for real currencies via the game client itself (for example in life-simulator Second Life or in the fantasy role-playing game Diablo III).

To revert to our original topic, it is possible (criminally) to commit money laundering when someone uses Bitcoin-exchange as a *modus operandi*. He changes criminally acquired money to Bitcoin and then forwards this to various addresses. On the other hand, it is possible to track the transactions because they are public and can be accessed by everyone on the internet. Information could also be made available in the log files of exchange websites where people can change their Bitcoin to real-world currencies.

It could be difficult, however, to reach a specific exchange-website's ad-

61 *Ibid*, p 7.

ministrators, when the HQ of the law enforcement authorities and of the company which operates the website are not in the same country. Let us take a Hungarian authority which wants information on a Bitcoin public key user from the exchange site mtgox.com as an example. The web page is maintained by Tibanne Co. Ltd. a company registered in Japan and operating the site from there.[62] From Japanese (and from almost all other foreign) authorities it is possible to obtain such data in criminal procedure via a formal legal request. The procedure can last for many months due to assessment and translation. Under Hungarian law this procedure is regulated by Act XXXVIII of 1996 on International Legal Assistance. It can also happen that, by the time this official legal assistance reaches the foreign authority, the company has already deleted the logs from the database (for example, the IP addresses using a certain profile). It could be expedient for Bitcoin exchange sites to maintain an online request service for law enforcement authorities, where they can ask for logs or other information rapidly. Sadly this is not the case with any website to date.

More difficulties can surface when exchange companies register themselves in countries which are not obliged by international agreement to share data and information. It is not yet the case that companies convert their homes into offshore centres, but the possibility should not be ignored.

Tracking is more difficult when the exchange is not done on the internet, but in real life, from hand to hand, or when Bitcoin from different addresses is accumulated or distributed etc.

We can find special websites tailor-made for Bitcoin laundering to maintain user anonymity. One is http://bitcoinlaundry.com/, a central Bitcoin-address where users can send their Bitcoin which the operator then forwards to another given address for a small fee.[63]

62 Informations about the company on the webpage of the Tokyo Chamber of Commerce: <www.tokyo-cci.or.jp/english/ibo/2353440.htm> (31.07.2012).

63 Bitcoin, Wiki, <en.bitcoin.it/wiki/Bitcoin_Laundry> (31.07.2012).

9.3. Bitcoin theft

Bitcoin represents a certain value on the internet, and so we should keep in mind that they could be a possible target for thieves, as is real-world money. Despite money-laundering Bitcoin-thefts are already documented in the literature and in the media, and more such incidents can be expected in the future.

The most important factor in these abuses is the virtual wallet file (wallet.dat) which contains the actual amount of a user's Bitcoin. If someone deletes this file – and has not made a backup – he or she could lose access to the Bitcoin forever. Bitcoin will not be deleted from the system, but the user loses the public and private key pairs which are crucial for access and transactions. As already mentioned, Bitcoin is located in a 'legal grey area', but it behaves in the virtual space in most situations as digital commodity, in fewer situations as money, and so it is advised to treat it so in legal practice. According to Hungarian civil law, money is treated as 'things', and since, under Act C of 2012 on the Hungarian Criminal Code, Section 370, the subjects of theft should be only alien things, we should treat property abuses with Bitcoin as theft, at least in Hungarian relations. This classification could cause many problems due to Bitcoin's dubious legal status. Sometimes a Bitcoin-related abuse should be classified as *'traditional' fraud* (section 373 of the Hungarian Criminal Code), *information technology system fraud* (section 375), *breaching information technology system or data* (section 423), or *compromising or defrauding the integrity of information technology system or device* (section 424), or possibly an accumulation of these. We have to take every circumstance of the case in consideration to choose the correct classification. Because of its nature the computer environment is essential for Bitcoin-related abuses, and so it could be better to classify such crimes as computer crimes (sections 375, 423 or 424 of the Hungarian Criminal Code) than thefts. Even so, due to its nature Bitcoin behaves more like 'things' (e.g. money) than data. This forced classification stems from the outdated law. It would be useful in the future to update the (non-existent) regulation of virtual 'things'.

To look at some examples, the most cited event was the ominous hacking attack against exchange site MtGox, when the virtual wallets of many users were stolen. If we would like to classify this crime in relation to Hungarian law, the right interpretation would be *information technology system fraud*

(section 423) and not *theft*. According to text of the code, this type of crime is committed when a person overrides or infringes the user privileges, modifies the data stored in the computer system and causes certain amount of damage in this context. In the case referred to the hackers monitored and used the security gaps of the Bitcoin exchange site to break into the system and steal the virtual wallets.

Another case arose when, in June 2011, a Trojan virus began to spread on the internet and tried – using the default access path for wallet.dat – to send the virtual wallet file to a Polish server for the cybercriminal.[64] The virus – called Infostealer.coinbit – was not a significant danger for Bitcoin users, because it only knew the default access path for wallet.dat, and even a simple firewall could block it when it tried to send the file through the web. In Hungarian law we should classify the virus programmer's behaviour as a crime regulated in section 424 of the Hungarian Criminal Code. This crime is committed by the person who, to commit the criminal activities defined in Section 375, or 423 creates, obtains, distributes or trades, or otherwise makes available computer software, passwords, entry codes, or other data with which to gain access to a computer system or network. If the virus had managed to send the virtual wallet to the cybercriminal, than he must be responsible for committing the crime regulated in section 375, too.

It is more sophisticated criminal behaviour when somebody steals virtual money not directly, but tries to impact other computers to mine Bitcoin, creating a Bitcoin-miner zombie network without the permission and knowledge of the owners of participating computers.[65] Computer networks created with such illegal intent are called botnets.[66] At first the cybercriminal needs to install – somehow – a virus on the target computer that uses its video card's or CPU's computing power to mine Bitcoin. This could be achieved most easily by spams (unsolicited bulk messages) or phishing websites. If the victim opens a link in an unsolicited advertisement message, or visits such harmful webpages where he has to give out personal information (e.g. e-mail address, Facebook-profile and passwords related to them) the virus could be easily downloaded to the computer.

64 Information about the virus: <www.symantec.com/security_response/writeup.jsp?docid=2011-061615-3651-99> (08.07.2012).
65 Federal Bureau of Investigation, *supra nota* 58, p 8.
66 Wikispam webpage, <hu.spam.wikia.com/wiki/Botnet> (31.07.2012).

An example of this phenomenon was the malware named ZeUs, which used the computer's resources to illegally mine Bitcoin. This harmful software spread through deceptive advertisements posted to various websites in the first half of 2011.[67]

Other sources mention that larger computer networks would be ideal for cybercriminals to target for joint Bitcoin-mining (e.g. a company's or a university's local network). This technique is more expedient, because effective mining typically requires excessively high calculating power.[68] Sections 423 and 424 are normative for legal classification of this behaviour also, in that harmful software prevents the normal functioning of a computer, in addition to which virus-distribution is also independent criminal behaviour.

The European Commission's Recommendation No. C7-0293/10 deals with such problems, and draws up good suggestions for the harmonisation of the legal framework of member states for attacks against informatics systems. *Inter alia* that creating botnets for committing cybercrime should be an aggravating circumstance in the criminal codes of member states.[69]

9.4. Buying illegal goods with Bitcoin

There are several pages on the internet where Bitcoin can be used as a paying option. We can browse clothes, books, trinkets or computer parts.[70] These are quite innocent everyday goods, but Bitcoin, due to its anonymous, decentralised system, can be a good tool in criminal hands.

According to an article published on gawker.com on June 1, 2011, there was a webpage where any drug imaginable could be bought.[71] The page was called SilkRoad and could be visited only through a special anonymous browser

67 Segura, J., "Zeus, Bitcoin and the Ub3erhackers" (2012), <blog.sparktrust.com/?p=572> (10.07.2012).
68 Bitcointalk webpage, <bitcointalk.org/index.php?topic=11506.0> (10.07.2012).
69 Proposal for a Directive of the European Parliament and of the Council on attacks against information systems and repealing Council Framework Decision 2005/222/JHA.
70 Bitcoin, Wiki, <en.bitcoin.it/wiki/Trade> (02.06.2013).
71 Chen, A., "The Underground Website Where You Can Buy Any Drug Imaginable" (2011), <gawker.com/5805928/the-underground-website-where-you-can-buy-any-drug-imaginable> (18.10.2011).

called Tor (The Onion Router).[72] After some search and registration effort one could look at the world's largest drug market, where anything from marijuana to heroin or LSD could have been ordered. However, drugs are not everything: we could find tools for growing or producing drugs, or even order ammunition, registration codes for websites, licences etc. We could pay only with one type of currency: Bitcoin.[73] The anonymous marketplace was shut down by FBI on 2. October 2013.[74]

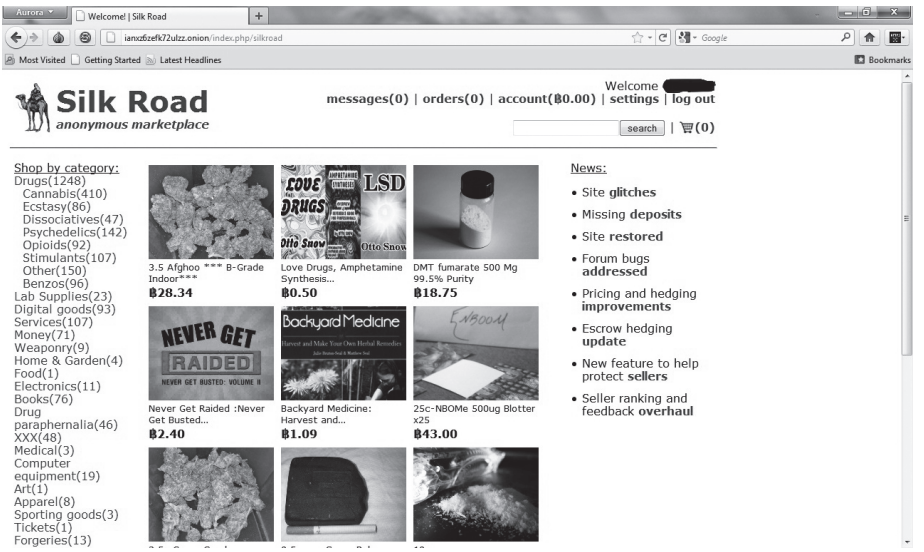


Figure 1

Sadly, virtual money can be an excellent tool for criminal activities, because it is nearly impossible to trace who sent what amount to whom. However, in my opinion, the virtual currency will not become the prime currency of crime, as it is more likely that they are only a small group among the Bitcoin using community. Anonymous payment and money laundering were present in the crime world before Bitcoin surfaced.

72 The Tor Project homepage, <www.torproject.org/> (18.10.2011).

73 Fischermann, T., „Anarcho-Geld" (2011), <www.zeit.de/2011/27/Internet-Bitcoins> (19.10.2011).

74 Index.hu, "Az FBI lecsapott a web sötét oldalára", <index.hu/tech/2013/10/03/az_fbi_lecsapott_a_web_sotet_oldalara/> (27.01.2014).

10. Conclusion

Governments of the Industrial World, you weary giants of flesh and steel, I come from Cyberspace, the new home of Mind. On behalf of the future, I ask you of the past to leave us alone. You are not welcome among us. You have no sovereignty where we gather. We have no elected government, nor are we likely to have one, so I address you with no greater authority than that with which liberty itself always speaks. I declare the global social space we are building to be naturally independent of the tyrannies you seek to impose on us. You have no moral right to rule us nor do you possess any methods of enforcement we have true reason to fear.[75]

The Declaration of the Independence of Cyberspace was written by John Perry Barlow on 8th February 1996 and its starting lines reflected whenever the regulation of the internet is in question. With its technical development, the web will always stretch the law, and so it is impossible to regulate it effectively in every detail, as there will always be zones and loopholes uncovered. The Declaration states that governments simply do not have power over this field of human activity. The Bitcoin phenomenon is also a good example, since it raises unprecedented questions - due to its modernity.

The technology behind the virtual currency is a novelty, which means a paradigm shift without parallel among financial systems, and it is still unclear what may become of it, since the tools necessary for its greater evolution are still under development.

Even such views exist which say that it is pointless to look at Bitcoin as money, but more as a protocol with which we can send money to everyone in the world through the internet. It is irrelevant how much a virtual unit is worth since, sooner or later, we will exchange it for real world currencies or buy different products with it.[76]

This exemplifies that it is now very difficult to form an opinion of this virtual phenomenon since it is too new to interpret it clearly. At first everyone on the market has to understand Bitcoin, and then the right view can be

75 Barlow, J. P., "A Declaration of the Independence of Cyberspace", <projects.eff.org/~barlow/Declaration-Final.html> (26.10.2011).

76 Bitcoin homepage, <bitcoin.hu/?p=1280> (26.10.2011).

formed which should judge the new currency's possible evolution and spread. It is, therefore, better to regard Bitcoin as digital commodity and medium of exchange – because it was so designed and it so behaves – and to interpret it as such in the market and in legislation. In addition, law enforcement authorities should train their officers about special investigating techniques about virtual economies and payment systems.

In my opinion the optimal final goal should be a concrete legal regulation on international – at least European – level dealing with issues about virtual items and decentralized payment systems.

Daniel Eszteri
Budapest Police Cybercrime Unit
1027 Budapest, Gyorskocsi utca 31, Hungary
E-mail: eszterid@budapest.police.hu