

Právnická fakulta Univerzity Karlovy
Katedra finančního práva a finanční vědy

Jiří Moravec

Právní aspekty Bitcoinu a jeho regulace



Diplomová práce

Datum uzavření rukopisu: 30. 07. 2016

Vedoucí: doc. JUDr. Michael Kohajda, Ph.D.

Faculty of Law Charles University
Department of Financial Law and Finances

Jiří Moravec

Bitcoin – Legal Aspects and Regulation



Master's Degree Thesis

Date: 30. 07. 2016

Thesis Supervisor: doc. JUDr. Michael Kohajda, Ph.D.

Prohlášení:

Prohlašuji, že jsem předkládanou diplomovou práci vypracoval samostatně, všechny použité prameny a literatura byly řádně citovány a práce nebyla využita k získání jiného nebo stejného titulu.

V Praze dne 8. srpna 2016

Jiří Moravec

Poděkování:

Na tomto místě bych rád poděkoval zejména vedoucímu práce doc. JUDr. Michaelovi Kohajdovi, že mi umožnil a podpořil mne v psaní této netradičně zaměřené diplomové práce. Rád bych mu také poděkoval za podmětné rady, přátelský přístup a trpělivost. Dík patří i mé rodině za výraznou pomoc a neutuchající podporu při studiu. V poslední řadě bych rád poděkoval svým přátelům. Na prvním místě Lukášovi Kutílkovi nejen za pomoc s anglickým textem a dále pak Chrisovi Müllerovi, Dominiku Maškovi a Martinu Žákovi za inspiraci, kterou mi poskytli po dobu studia.

Table of Contents

1	Introduction	1
1.1	Core Terms	4
1.1.1	Bitcoin Address.....	5
1.1.2	Private Key.....	6
1.1.3	Bitcoin Wallet.....	6
2	Monetary Aspects of Bitcoin	7
2.1	Virtual Currency	7
2.1.1	Virtually Created Currency.....	9
2.1.2	Virtual Currency Schemes.....	10
2.2	Bitcoin's Monetary Background	14
2.2.1	Icelandic Approach.....	14
2.2.2	The Court of Justice of the European Union.....	16
2.2.3	Electronic Money Directive.....	17
2.2.4	Bitcoin as a General Purpose Instrument.....	18
2.3	Bitcoin as a Money or a Currency?	19
2.3.1	Money Precursors?.....	20
2.3.2	Medium of Exchange.....	22
2.3.3	Unit of Account.....	23
2.3.4	Store of Value.....	24
2.4	Bitcoin as a Money Pursuant to the Czech Law	24
2.5	Summary	25
3	Legal Aspects of Bitcoin	27
3.1	Materialistic Conception	28
3.1.1	The Act no. 40/1964 Coll. the Civil Code.....	28
3.2	Idealistic Conception	30
3.2.1	The Act no. 89/2012 Coll. the Civil Code.....	30
3.3	Bitcoin as the Work of an Author	32
3.4	Bitcoin as a Computer Program and License	34
3.5	Bitcoin as a Right	38
3.6	Bitcoin as a Thing Without Absolute Proprietary Rights	40
3.7	Summary	44
4	Regulatory Aspects and Issues Regarding Bitcoin	46
4.1	The Need for Regulation	47
4.2	The Need for Systematic Regulation	48
4.3	Contemporary Problems	50
4.3.1	Decentralization.....	51
4.3.2	Anonymity.....	51
4.3.3	Solution to Contemporary Problems.....	53
4.4	Theoretical Problems	54
4.5	The Need for Regulation Dedicated Only to Bitcoin	56
4.6	Comparing BitLicense to the Czech Legislation	57
4.6.1	Virtual Currency Definition.....	58
4.6.2	Virtual Currency Business Activity.....	60
4.6.3	Cyber Security Program.....	62
4.6.4	Business Continuity and Disaster Recovery.....	64

4.6.5 Custody and Protection of Customer Assets.....	65
4.7 Summary.....	66
5 Conclusion	68
Sources	73
Abstract in English	84
Abstract v českém jazyce.....	85
Teze v českém jazyce	86

1 Introduction

Cypraea moneta is a small cowry shell found on the beaches of east Africa and Maldives islands with characteristic shiny look. This shell was once used by Indian and African tribes in the same sense as today's money.

During his Indian expedition, Englishman, Lovell Reeve documented a trade involving *Cypraea moneta*: “A gentleman residing some time since at Cuttack is said to have paid for the erection of his bungalow entirely in these cowries... ..he paid for it with above sixteen millions of these shells.”¹ Some 150 years after that trade in 2010, an American from Florida named Laszlo posted on an internet forum: “I'll pay 10,000 bitcoins² for a couple of pizzas...”³ Four days later Laszlo reported: “I just want to report that I successfully traded 10,000 bitcoins for pizza.”⁴ The pizzas for Laszlo were bought by Jeremy Sturdivan.⁵ This purchase is believed to be the first bitcoin material transaction among the Bitcoin users.⁶

The paradox between these two trades is that the the first trade that took place over 150 years ago was legally and economically speaking modern, as the cowries were used in the very same way as modern money. The bitcoin trade however, was a step back, because it was a mere barter. Jeremy first had to purchase the pizzas using a credit card, and subsequently exchange pizzas for Laszlo's bitcoins.

¹ REEVE, Lovell. *Conchologia Systematica* vol. 2. London: Longman, Brown, Green and Longmans, 1842, p. 262.

² In this thesis and generally Bitcoin with ‘B’ is used to refer to the whole network of computers processing transactions and thus developing the peer-to-peer environment and bitcoin with a ‘b’ is used to refer to the pieces of information that might be transacted among the users of such network.

³ LASZLO. Topic: Pizza for bitcoins? [entry in a discussion forum]. In: *Bitcoin Forum: Economy: Marketplace* [online]. 18.05.10, 12:35 [visited on 2016-05-27]. Available at: <https://bitcointalk.org/index.php?topic=137.0>

⁴ LASZLO. RE: Pizza for bitcoins? [entry in a discussion forum]. In: *Bitcoin Forum: Economy: Marketplace* [online]. 22. 05.10, 07:17 [visited on 2016-05-27]. Available at <https://bitcointalk.org/index.php?topic=137.0>

⁵ A Living Currency. *Bitcoinwhoswho.com* [online]. [visited on 2016-05-27]. Available at: <http://bitcoinwhoswho.com/index/jercosinterview>

⁶ Bitcoin Price Chart with Historic Events. *Bitcoinhelp.net* [online]. [visited on 2016-05-27]. Available at: <https://bitcoinhelp.net/know/more/price-chart-history>

The essence of money is that everybody accepts it, because everybody knows, that everybody accepts it.⁷ *Cypraea* was of this essence, but in the year of 2016 we still cannot assign the same attribute to Bitcoin even though over 100,000 shops world wide accept bitcoin as a means of payment.⁸ If the Bitcoin, at the moment, lacks the essence of money and yet is still used in the same way, what is it?

Bitcoin is a peer-to-peer⁹ network system. In a peer-to-peer network, all of its participants are equal, everyone acts as a server and a receiver at the same time. Such layout eliminates any need for central authority and server. Bitcoin network is therefore fully decentralized.¹⁰ Within the network participants might transfer encrypted lines of alphanumeric characters directly between each other. These alphanumeric characters are referred to as bitcoins.¹¹ Every single bitcoin is therefore just a line of text encrypted by secure hash algorithm 256¹².

Transfers of the encrypted lines of alphanumeric characters are referred to as spending bitcoins. What makes Bitcoin unique among all of other digital creations is that bitcoin cannot be spend more than once. The multiple usage of a single digital file in connection with a unit of exchange is being addressed as double spending.

Double spending is a long lasting problem in connection with digital files. Once a user obtains a digital file, what is here to stop him from creating a number of copies of that file? The author¹³ of Bitcoin came up with an unprecedented, yet apparent solution

⁷ HOLMAN, Robert. *Ekonomie*. 6th Edition. In Prague: C.H. Beck, 2016. Beckovy ekonomické učebnice. p. 446. ISBN 978-80-7400-278-6. In the Czech original: “*V tom tkví podstata peněz: Každý je přijímá, protože každý ví, že je každý přijímá.*”

⁸ Bitcoin now accepted by 100,000 merchants worldwide. *International Business Times* [online]. [visited on 2016-05-27]. Available at: <http://www.ibtimes.co.uk/bitcoin-now-accepted-by-100000-merchants-worldwide-1486613>.

⁹ SCHOLLMEIER, Rüdiger. *A Definition of Peer-to-Peer Networking for the Classification of Peer-to-Peer Architectures and Applications* [online]. Munchen, 2002 [Visited on 2016-05-28]. Available at: https://www.researchgate.net/publication/3940901_A_Definition_of_Peer-to-Peer_Networking_for_the_Classification_of_Peer-to-Peer_Architectures_and_Applications. Technische Universität München.

¹⁰ NAKAMOTO, Satoshi. *Bitcoin: A Peer-to-Peer Electronic Cash System: 1. Introduction* [online]. p. 1., 1-9 [Visited on 2016-02-16]. Available at: <https://bitcoin.org/bitcoin.pdf>.

¹¹ NAKAMOTO, Satoshi. *Bitcoin: A Peer-to-Peer Electronic Cash System: 2. Transaction* [online]. p. 2, 1-9 [Visited on 2016-02-16]. Available at: <https://bitcoin.org/bitcoin.pdf>.

¹² IWAR. *Descriptions of SHA-256, SHA-384, and SHA-512: SHA-256: Description of SHA-256* [online]. p. 2., 1-36 [Visited on 2016-02-16]. Available at: <http://www.iwar.org.uk/comsec/resources/cipher/sha256-384-512.pdf>.

¹³ The author of the Bitcoin remains, to the finalization of this work, unknown. The author of the first document that introduces Bitcoin is Satoshi Nakamoto, however it has been proven that it is not a real

- keep a public ledger of all bitcoin transactions; “*The only way to confirm the absence of a transaction is to be aware of all transactions.*”¹⁴ Using such system the Bitcoin network recognizes every unique bitcoin and never accepts any copy of it as it knows where exactly the original is. Some computers involved in the Bitcoin network therefore run a part of Bitcoin protocol that monitors ongoing transactions and keep the public ledger updated. Provided this solution the Bitcoin network does not need any central authority that would monitor the transactions as the users do so themselves.

Transactions are randomly hashed and subsequently organized into blocks, whichever computer is able to solve a mathematical problem first closes the block, confirms included transactions, and is rewarded with an incentive in form of bitcoins.¹⁵ Every block is subsequently locked into the previous block creating a chain, thus creating a blockchain.

Every transaction ever done is logged in the blockchain that makes the Bitcoin network very transparent as everyone is able to look up every transaction that ever took place and yet it keeps users relatively anonymous as the transactions are linked with bitcoin addresses only. Everyone can create multiple addresses and when following certain procedure¹⁶ it is impossible to link a person to an address. It is possible to give a simplified summarization that Bitcoin is a digital, decentralized, and partially anonymous network that enables its users to conduct transactions among each other.

Bitcoin protocol might have a great impact on the internet and payment services and change its format as we know it. The possibility to keep every digital file unique is very appealing and as such the blockchain technology might revolutionize not only the payment services, but it is also a key how to stop internet piracy.¹⁷

person. On April, 2016 Craig Wright claimed that he is the author of the Bitcoin, but failed to prove such statement.

¹⁴ NAKAMOTO, Satoshi. *Bitcoin: A Peer-to-Peer Electronic Cash System: 2. Transaction* [online]. p. 2, 1-9 [Visited on 2016-02-16]. Available at: <https://bitcoin.org/bitcoin.pdf>.

¹⁵ Id.

¹⁶ To maintain anonymity, users usually use a software that hides their IP address through many different virtual private networks (VPN). When someone creates bitcoin address using such software (for example TOR), this bitcoin address will be linked with a different IP address than of the computer, which the person operates at the moment and it will substantially lower the possibility of the person being recognized as an owner of such address and subsequently being linked to it.

¹⁷ How the Blockchain Can Help Authors Guild Fight Piracy. *Http://bitcoinist.net/* [online]. Brighton: Bitcoinist Ltd., 2015 [visited on 2016-02-29]. Available at: <http://bitcoinist.net/blockchain-help-authors-guild-fight-piracy/>.

Whereas the technical side of Bitcoin is thoroughly mapped, bitcoin in a legal sense remains open to interpretation. In this thesis we aim on the legal and economic aspects of bitcoin and questions concerning its regulation. We want to find an answer to the question of what bitcoin is, comparing bitcoin with money in economical and legal sense, and subsequently considering whether bitcoin might be looked upon as a thing in a legal sense. The reason behind such inquiries is that we are, at the beginning of writing this thesis, of the opinion that bitcoin as a medium of exchange cannot be considered a thing in a legal sense despite of the wide, idealistic approach to things in the civil law.

Another point of this thesis is to give our thoughts on the bitcoin's regulation. Especially, highlighting the need for systematic Bitcoin regulation, its contemporary and theoretical problems. Reasoning of this part of the thesis is that we are of the opinion that the partial anonymity and decentralization might be a future problem in choosing the right approach to bitcoin regulation. For this reason, we also present an American legal act, which was written strictly for the regulation of Bitcoin and similar protocols and we show a brief comparison to the Czech legislation. We also suggest that some parts of this act shall be incorporated to the Czech legislation regarding Bitcoin.

This thesis is divided into three main blocks. The first one (*Monetary Aspects of Bitcoin*) maps our road while we try to understand what is bitcoin from mostly economical point of view, but as those conceptions are closely connected there is also a legal insertion. Second block (*Legal Aspects of Bitcoin*) regards Bitcoin as an object of legal relations. Third block (*Regulatory Aspects and Issues Relating to Bitcoin*) holds bitcoin's regulation around the globe and in the Czech Republic, shows different approaches and talks about the problems in connection with the new technology.

1.1 Core Terms

As this thesis was being created we came to a conclusion that without further explanation of few core terms that are natural only to the Bitcoin, the following text would not be fully comprehensible.

We do not aim to provide a thorough technical definition of those terms. We rather want to explain its role in connection with the Bitcoin. For purpose of this thesis we consider crucial the following terms:

1. Bitcoin address;
2. Private key; and
3. Bitcoin wallet.

1.1.1 Bitcoin Address

Bitcoin address is a digital destination where a bitcoin transaction must be directed. Every transaction ever done will have as final destination a certain bitcoin address. Creating and maintain bitcoin address is free of charges. The number of them is, for human use, practically infinite.¹⁸

The address is only a receiving point. Bitcoins will never be send from an address but might be visualized in such way.¹⁹ Bitcoins are kept in the same place, in the blockchain, all the time. As abstract as it might be, bitcoins are technically never sent, but only received.²⁰

Bitcoin address also represents a combination of a public and private key. Those keys, essentially passwords, are crucial terms in connection with the Bitcoin network and will be explained later on. Bitcoin address is an encrypted public key that is paired with a specific private key, which when used allows bitcoins to be spent.

For this thesis it is important to know that to conduct a transaction, the sender must know the receiver's bitcoin address. When a sender initiates a transaction, it is at first broadcasted to the whole Bitcoin network and at the same time the transacted bitcoins receive a time-stamp to prevent double spending, but in real use the sender just copies the address in to the clipboard and chooses an amount of bitcoins he wishes to send and clicks "send".

That bitcoin address is a line of text in a specific format²¹ that works on similar basis as a regular bank account, and most importantly that the use of bitcoin address is only to receive bitcoins.

¹⁸ Bitcoin address is an encrypted number varying from 1 to 1,461,501,637,330,902,918,203,684,832,716,283,019,655,932,542,976 (2^{160}).

¹⁹ All bitcoin transactions are visualized in a sense that there is an address that initiated the transaction and a receiving address. Technical reality is different, but hardly comprehensible. To see the visualization of every bitcoin transaction that ever took place please see: <https://blockchain.info/>.

²⁰ For more information on this concept of missing "from address" please see: https://en.bitcoin.it/wiki/From_address

²¹ An example of bitcoin address: 1MJ9swVsNeSdX41p8jzHTMA77cmfyTTeB.

1.1.2 Private Key

Private key is essentially a password, a secret 256-bit number that must be used to initiate a bitcoin transaction.²² Every private key is mathematically and cryptographically tied to a bitcoin address to allow future transactions. Without the knowledge of the private key the transaction cannot be invoked and the bitcoins tied to such address cannot be handled. Therefore, everyone might know the public key, which is represented in its encrypted form as a bitcoin address, but no one but the “owner” shall know the private key.

It is advised that the private keys are stored in a safe place and used with precautions, because when the private key is compromised the loss of bitcoins could not be avoided, unless the righteous owner would have transferred the bitcoins first to a secure address.

1.1.3 Bitcoin Wallet

Bitcoin wallet is a secondary computer program that is written to help facilitate the work with the Bitcoin network. Bitcoin wallet software provides users with better interaction with the Bitcoin addresses and private keys. Bitcoin wallet stands, essentially, for a safe environment where the private keys are stored and through which it is possible to initiate bitcoin transactions.

Bitcoin wallets are created by private authors and are not directly connected with the Bitcoin network. Its use is usually free.

²² Bitcoin and its security is being developed over the time. In 2016 its now possible to use a 512-bit number as a private key.

2 Monetary Aspects of Bitcoin.

In this chapter we present a set of terminological, economic, and legal problems in connection with the Bitcoin. We came to a conclusion that the collocation “Virtual Currency²³” is used inaccurately, because this nomenclature creates an impression that bitcoin is something different than it really is. That bitcoin itself cannot be considered money and subsequently therefore a currency in the traditional conception. In our opinion, bitcoin shall be referred to as a “digital medium of exchange” instead of the nomenclature Virtual Currency.

We also provide a legal and economic background and development of the early years of bitcoin. We have chosen the country of Iceland, because it was one of the very first countries that made a legal decision in regard of bitcoin. We would like to address the slow but steady development and point out bitcoin’s characteristics that had been best shown thanks to those events.

Subsequently, we are comparing bitcoin evaluation from economic point of view to money in a general sense.

2.1 Virtual Currency

Over the time, for Bitcoin and similar data protocols²⁴ had established a nomenclature *Virtual Currency*. This thesis finds this nomenclature Virtual Currency and its subsequent definition unprecise, dated, and problematic.

European Central Bank had provided an early definition of Virtual Currency: “*A virtual currency is a type of unregulated, digital money, which is issued and usually*

²³ In spite of the above said, this thesis might still operate with the collocation “Virtual Currency” as well, but only because such term is used in laws or in future promised drafts. It should be also mentioned that the community around Bitcoin started to use a different denomination – cryptocurrency. This denomination is also wrong from a legal point of view, but at least compared to the virtual currency describes the defining factor of Bitcoin, which is cryptography.

²⁴ Some of those digital mediums of exchange shall be mentioned for its importance and for its contribution to the further development of decentralized payment systems. Ethereum as a digital medium of exchange with build in inflation and the possibility of smart contracts. For more information please see: <https://www.ethereum.org/>. Digibyte for its revolutionary approach to online gaming platforms. For more information please see: <https://digibyte.co//>. Dash for its absolute privacy. For more information please see: <https://www.dash.org/>. All the other similar data protocols might be found here: <https://coinmarketcap.com/>.

*controlled by its developers, and used and accepted among the members of specific virtual community.*²⁵

Another definition was provided by the Federal Bureau of Investigation: “*Virtual Currency is something used on the Internet that is in circulation as a medium of exchange but is not backed by a government.*”²⁶

At first it should be noted that Bitcoin not only had undergone a great technological development but also, in comparison with the year of 2012 (the year of both of the definitions above), it changed sociologically, economically, and most importantly legally. The nomenclature virtual currency, however, stays in general use, which is the root of the problems this thesis will address later on.

What was firstly meant by the connection of the two words currency and virtual cannot be found. Maybe the reason was that bitcoin is created virtually on the internet or that it is almost like a currency (virtually a currency), but most probably there was a terminological mistake at the beginning. We are of the opinion that bitcoins were considered of the same sort as artificial medium of exchange used in online games and so labeled Virtual Currency. This collocation might be and tends to be, wrongfully, conceived in a two different ways.

First way is to consider Bitcoin as some sort of virtually created currency. With the meaning that there is no actual issuer²⁷, but only a non-existent virtual one. Second unprecise approach to the explanation of Virtual Currency nomenclature would be to assert that Bitcoin operates within virtual boundaries and in between of a specific virtual community therefore in so called virtual economy. Virtual economy is a term often used in connection with a closed environment run by computer such as an online computer game.²⁸ Virtual economy might be described as; “*Social Virtual Words (SVW) typically*

²⁵ EUROPEAN CENTRAL BANK. *Virtual Currency Scheme* [online]. p.13., 1-53. [Visited on 2016-03-23]. ISBN 9789289908627. Available at: ECB.EUROPA.EU/PUB/PDF/other/virtualcurrencyschemes201210en.pdf.

²⁶ FBI DIRECTORATE OF INTELLIGENCE. (U) *Bitcoin Virtual Currency: Unique Features Present Distinct Challenges for Deterring Illicit Activity: Appendix A: Key Terms* [online]. 2012 [visited on 2016-03-23]. Available at: https://www.wired.com/images_blogs/threatlevel/2012/05/Bitcoin-FBI.pdf

²⁷ English language does not differ between the words ‘issuer’ and ‘emitter’. In the Czech language, however it is a substantial difference. Currency is always emitted and never issued. When we use the word ‘issue’ in connection with currency in the sense of a legal tender we have in mind the word ‘emit’ in the Czech legal sense.

²⁸ For example, compare with: THORPE, Christopher, Jessica HAMMER, Jean CAMP, Jon CALLAS a Mike BOND. *Virtual Economies: Threats and Risks* [online]. Harvard University, 2007 [visited on 2016-

have an economy-like system which simulates aspects of a real-world economy. This internal economic system of a SVW is called a virtual economy."²⁹

2.1.1 Virtually Created Currency

To assert that Bitcoin is a virtually created currency without an issuer is unprecise on three levels. First one is that bitcoin has an issuer³⁰. Second, that bitcoin is not created virtually, but digitally, and third that bitcoin is a currency, which will be regarded later on.

To address the first problem. Bitcoins are simply created by and within the Bitcoin network. The issuer exists even though it is decentralized over the world, but in its entirety it is the Bitcoin peer-to-peer network which represents the issuer. As such it illustrates the Bitcoin conception in sense of classic Bitcoin's saying; "*be your own bank*", everyone who participate is the issuer.

Second, bitcoin is not created virtually but digitally. It exists, in the literal sense of existence. The only perception that might be partially correct, would be to assume that bitcoin is created within the computer powered virtual space, but so is the electronic money, which are not addressed as virtual either.

Bitcoin is an electronically stored unit. There is even a physical representation in the form of electric energy that is stored within the hard drive of a computer.³¹

07-23]. Available at: <http://www.eecs.harvard.edu/~cat/papers/vetr.pdf>, or LEHDONVIRTA, Vili. VIRTUAL ECONOMICS: APPLYING ECONOMICS TO THE STUDY OF GAME WORLDS [online]. Helsinki Institute for Information Technology HIIT, 2005 [visited on 2016-07-23]. Available at: http://vili.lehdonvirta.com/wp-content/uploads/2015/08/Virtual_Economics_Applying_Economics_to_the_Study_of_Game_Worlds_Proceedings_of_the_2005.pdf.

²⁹ JUNG, Yoonhyuk. USERS' UNDERSTANDINGS OF THE VIRTUAL ECONOMY IN SOCIAL VIRTUAL WORLDS: CONSUMPTION AND ENTREPRENEURSHIP OF VIRTUAL GOODS [online]. Louisiana State University, 2010. p. 7 [visited on 2016-07-23]. Available at: http://etd.lsu.edu/docs/available/etd-04092010-154422/unrestricted/Jung_Diss.pdf.

³⁰ It has been said many times that the number of bitcoin that will be created is close to 21 million. All of those bitcoins has already been created, but the right to handle them was not assigned, yet. One of the possible interpretation of bitcoin is that bitcoin is a right, as explained in this work later on, and therefore we still work with the conception that bitcoins are issued, over the time.

³¹ This is a bit complicated statement, but recent studies show that data stored within electronically kept units presents certain, albeit minimal, mass. Please compare with: KISH, LASZLO a CLAES GRANQVIST. Does Information Have Mass? Proceedings of the IEEE [online]. 2013, **101**(9), 1895-1899 [visited on 2016-02-29]. Available at: <https://arxiv.org/pdf/1309.7889.pdf>, or for further information on this subject in relation to energy preservation compare with: HONG, J., B. LAMBSON, S. DHUEY a J. BOKOR. Experimental test of Landauers principle in single-bit operations on nanomagnetic memory bits. Science Advances [online]. 2016, **2**(3), e1501492-e1501492 [Visited on 2016-02-29]. DOI:

If this example sounds too abstract to imagine, a bitcoin can be printed on a piece of paper in the same manner as electronic money have a physical representation of a coin or a bank note.³² In this simplified sense, the difference between bitcoin and electronic money is that the issuer is not tied to any laws of a country or union, but that does not make anything virtual. The relationship of bitcoin and electronic money, in a legal sense, is addressed later on.

We are of the opinion that the defining attribute of virtual is the existence of something within artificial boundaries where the communication is limited into one-way stream. The right label to use in connection with bitcoin is therefore digital. Digital is an adjective that represents something that is; “*expressed as series of the digits 0 and 1, typically represented by values of a physical quantity such as voltage or magnetic polarization.*”³³

2.1.2 Virtual Currency Schemes

In the year of 2012, European Central Bank has issued a pamphlet regarding Bitcoin named Virtual Currency Schemes.³⁴ The virtual currency scheme itself is a phenomenon of a certain community that issues its own money or a currency for its limited use. This material differs in between three virtual currency schemes:

1. Closed virtual currency schemes;
2. Virtual currency schemes with unidirectional flow; and
3. Virtual currency schemes with bidirectional flow.

The closed virtual schemes refer to a very limited virtual economy “... *that have almost no link to the real economy...*”³⁵ As an example we might look for an online

10.1126/sciadv.1501492. ISSN 2375-2548. Available at:
<http://advances.sciencemag.org/cgi/doi/10.1126/sciadv.1501492>

³² As an example we provide link to a webpage, where is possible to create so called paper wallets. Paper wallet represents a bitcoin address with a non-zero bitcoin balance and a concealed private key that is tied to the address. Paper wallets might be traded in hand or used as a fiat money. For more information, please see: <https://bitcoinpaperwallet.com/>.

³³ *Oxford Dictionaries: Language matters* [online]. [visited on 2016-03-23]. Available at:
<http://www.oxforddictionaries.com/definition/english/digital>

³⁴ EUROPEAN CENTRAL BANK. *Virtual Currency Scheme* [online]., 1-53. [Visited on 2016-03-23]. ISBN 9789289908627. Available at:
ECB.EUROPA.EU/PUB/PDF/other/virtualcurrencyschemes201210en.pdf.

³⁵ EUROPEAN CENTRAL BANK. *Virtual Currency Scheme* [online]. p.13., 1-53. [Visited on 2016-03-23]. ISBN 9789289908627. Available at:
ECB.EUROPA.EU/PUB/PDF/other/virtualcurrencyschemes201210en.pdf.

game where dealing with the in game money outside of the game is strictly prohibited by the terms and conditions of the game developer.

A classic example of a such virtual environment created within the computer powered virtual space might be an online gaming platform such as Tibia:³⁶ a game where a person's interaction are represented by virtual character that slain virtual monsters and acquire virtual money – gold pieces and virtual experience that might be used in game to kill more virtual monsters and gain more virtual money.

Bitcoin does not operate within a closed virtual currency scheme as bitcoins can be bought and sold on various places over the internet and in between persons using a legal tender. Also, Bitcoin lacks the central authority that would issue terms and conditions and limit its use. Bitcoin therefore might be freely linked to the real world economy. It cannot be, therefore, argued that Bitcoin presents the Closed virtual currency scheme.

Virtual currency schemes with unidirectional flow refer to a virtual currency that: “...can be purchased directly using real currency at a specific exchange rate, but it cannot be exchanged back to the original currency.”³⁷

Bitcoin again does not comply with this definition. No specific exchange rate can be given as bitcoins are purchased and sold under the influence of supply and demand and there is not and never could be any authority setting a specific exchange rate. All of the internet markets where it is possible to purchase bitcoin also have the option to sell it, and as such Bitcoin cannot be considered a scheme with unidirectional flow.

The third type, virtual currency scheme with bidirectional flow, is the closest one to Bitcoin. According to the European Central Bank this scheme is defined by the possibility to; “... buy and sell virtual money according to the exchange rates with their currency. The virtual currency is similar to any other convertible currency with regard to its interoperability with the real word.”³⁸ As an example European Central Bank gives the Linden Dollar, which is a virtual currency issued for the use in game Second Life. This virtual currency is created by the game developer but might be bought using United States Dollars and might be also sold for them. The material further argues that

³⁶ Tibia is an online gaming platform, where a person is represented by virtual character. For more information please see: www.tibia.com.

³⁷ EUROPEAN CENTRAL BANK. *Virtual Currency Scheme* [online]. p.14., 1-53. [Visited on 2016-03-23]. ISBN 9789289908627. Available at:

ECB.EUROPA.EU/PUB/PDF/other/virtualcurrencyschemes201210en.pdf

³⁸ Id.

Bitcoin is this third type of virtual currency scheme, but that it has certain innovations that; “... *make its use similar to conventional money.*”³⁹

We do not share the opinion with European Central Bank that Bitcoin is the bidirectional virtual currency scheme. First of all, the philosophy behind bitcoin is substantially different. Whoever is or was the author of Bitcoin, he did not want to create a bidirectional investment vehicle, but to reinvent money – general purpose instrument.

The main idea behind bitcoin comes from a mind of a libertarian. From someone to whom math is more than government and law. We are of the opinion that the creation was a sort of protest against the world, where; “...*banks create money, whenever when provide loan to other entities than banks.*”⁴⁰ “...*the loan expansion of bank is theoretically indefinite.*”⁴¹

As far as it is possible to assume what one’s intentions are, we believe that the author created the Bitcoin as a general trustless instrument that might be used without limitation by anyone.

Second and more importantly, bitcoin was not created as a specific purpose instrument for a single purpose or for a variety of purposes with a common denominator such as the virtual currency Linden Dollar. Linden Dollar has a specific purpose and that is to facilitate trades among the users of the game Second Life. Bitcoin never had any certain specific purpose it was more likely meant as a general purpose instrument from the very beginning. It was never intended to be used among specific group of people such as all three types of virtual currency schemes as presented by the European Central Bank. Bitcoin simply lacks a common denominator.

It might be argued that Bitcoin started as a bidirectional virtual currency scheme because Bitcoin was presented and firstly used in a group of cryptographers with common interests. However, even at that time bitcoin did not have a specific purpose or a specific society. The author presented his invention to the kind of people where he expected understatement and help. He was not looking for users but for developers. We

³⁹ Id.

⁴⁰ Tvorba peněz bankami. JÍLEK, Josef. *Peníze a měnová politika: Podstata tvorby peněz*. Prague: GRADA Publishing, a.s., 2004, p. 344. ISBN 8024707691. In the Czech original: “...banky vytvářejí peníze, kdykoliv poskytují úvěry jiným subjektům, než jsou banky.”

⁴¹ Id. In the Czech original: “...úvěrová expanze bank je teoreticky neomezená.”

therefore fail to understand why shall bitcoin be considered as a virtual currency scheme, when it is clearly very different from the Linden Dollars, with which it is being compared.

Let's continue further discussion with a question. Why is electronic money called electronic and not virtual? Is it not similar to the virtual currency scheme with the bidirectional flow? Could not we look on people using Euro, in the form of electronic money, as on specific group of people?

The answer would be that the electronic money is stored digitally, has an issuer and that the adjective 'virtual' is tied to a virtual economy used in online games, because such money simply does not exist in the real world. It exists in the game only.

Electronic money cannot be considered virtual, because it represents normal money that are just stored electronically. All the money - legal tender we deposit into electronic banking we might subsequently withdraw with the same nominal value and once we store money electronically we might still pay for pretty much everything using it. For electronic money and intangible values kept electronically and its subsequent use with the help of internet became accustomed term digital economy. Digital economy might be defined as; *“an economy that is based on digital technologies, although we increasingly perceive this as conducting business through markets based on the internet and the World Wide Web.”*⁴²

Bitcoin is not only based on digital technologies, but it also helps to facilitate trades over the internet. It acts very similarly to electronic money in the terms of usage. Once someone purchases bitcoins he might purchase various goods, services and things, where some of them might be virtual such as cloud data, but also might be real and tangible such as a real estate.⁴³ Bitcoin does not have a virtual borders that would limit its use, on the other hand it has a technological borders that do limit its use. Bitcoin is technologically tied to the internet, but might be theoretically used without it with the help of paper wallets.

⁴² THE BRITISH COMPUTER SOCIETY. The Digital Economy [online]. [visited on 2016-02-14]. Available at:

https://policy.bcs.org/sites/policy.bcs.org/files/digital%20economy%20Final%20version_0.pdf

⁴³ For more information please see: <http://bitcoin-realestate.com>, or: <https://www.bitpremier.com/5-real-estate>.

We conclude that bitcoin is not part of virtual economy or virtual currency schemes but a part of digital economy in the same sense of usage as electronic money. Taking in account the above stated reasons we do not see any sufficient reason why bitcoin shall be labeled virtual. Much more defining would be to mark Bitcoin digital.

2.2 Bitcoin's Monetary Background

We have expressed our disagreement with the collocation Virtual Currency, where we assert that the adjective 'virtual' shall be changed for digital. The other word 'currency' is also problematic.

We look upon currency as on a money under the shaping influence of laws of a particular country or union, which defines its format and enforces its acceptability as a general monetary instrument.⁴⁴ We might assume that all currencies are money, but not all money is currency. *“What makes money currency is not just the superior definiteness, fact that some object is considered money, but most importantly it is certain authority which stands behind the specification of the corresponding function of money, in qualified manner defines the form of money and sets forth the conditions of its existence and usage.”*⁴⁵ Therefore, for a bitcoin to be a currency, which is most probably not anyways, it must be money in the first place.

Whether bitcoin is or is not money had been a long lasting question. The core bitcoin community generally regards bitcoin as money or even a currency. The rest which is interested in bitcoin is rather temperate. In the development of economic and legal conception of Bitcoin, it was very soon clear that to mark bitcoin money is, at least, a difficult.

2.2.1 Icelandic Approach

One of the first countries which took actions against the Bitcoin was Iceland. Well, at least sort of took actions. Iceland was heavily affected by the world economic crisis in 2007 – 2008. Three of its largest privately owned banks were dealing with risky, but

⁴⁴ KOTÁB, Petr. *Finanční právo: Měna a peněžní oběh*. 6th Edition. Prague: C.H. Beck, 2012, p. 335. Beckovy právnické učebnice. ISBN 978-80-7400-440-7.

⁴⁵ Id. at 335-336. In the Czech original: *“Co však činí peníze měnou, není je vyšší míra konkrétnosti, skutečnost, že nějaký předmět je za peníze považován, ale především je to určitá autorita, která za konkretizaci příslušné funkce peněz stojí, kvalifikovaným způsobem formu peněz definuje a stanoví podmínky její existence a používání.”*

highly profitable short term financing of its both domestic, but mostly international clients. Subsequently, the investors found out that the probability of default increased every day and decided to sell off Krónur, which led to the default of the Icelandic banking sector and subsequently to the fall of Icelandic government.

*“The authorities responded with the unthinkable: they let the country’s three biggest banks collapse. It was the third largest bankruptcy in history. Then came the implementation of strict capital controls, austerity measures and a series of reforms; Iceland thus set out to reinvent itself. Skepticism was rife, but contrary to the qualms of critics, the controversial model actually seems to be working. Unemployment is down, interest rates have deflated and pre-crisis output levels are now being surpassed.”*⁴⁶

One of those implementations was the Icelandic Foreign Exchange Act.⁴⁷ This particular act, besides other things, prohibits residents of Iceland from purchasing bitcoin using the Icelandic Krónur as it might be used for cross-border capital movements; *“It should also be noted that the purchase and sale of virtual currency has been examined within the Central Bank in connection with enforcement of the Foreign Exchange Act, no. 87/1992 Coll. The Bank is of the opinion that there is no authorization to purchase foreign currency from financial institutions in Iceland or to transfer foreign currency across borders on the basis of transactions with virtual currency. For this reason alone, transactions conducted with virtual currency are subject to restrictions in Iceland.”*⁴⁸

The Foreign Exchange Act, involves a general exception for goods and services in the article 2: *“Foreign exchange transactions in connection with the import and export of goods and services shall be unrestricted, together with capital movements and foreign exchange transactions in connection with them, unless otherwise provided for by law.”*⁴⁹

⁴⁶ Failing banks, winning economy: the truth about Iceland’s recovery. World Finance [online]. 2015 [visited on 2016-07-25]. Available at: <http://www.worldfinance.com/infrastructure-investment/government-policy/failing-banks-winning-economy-the-truth-about-icelands-recovery>

⁴⁷ Act No. 87, 17 November 1992, as amended up to May 2013

⁴⁸ Significant risk attached to use of virtual currency. Cb.is [online]. 2014 [visited on 2016-04-13]. Available at: <http://www.cb.is/publications-news-and-speeches/news-and-speeches/news/2014/03/19/Significant-risk-attached-to-use-of-virtual-currency/>

⁴⁹ Foreign Exchange Act, Available at: [http://www.cb.is/library/Skraarsafn---EN/Capital-surveillance/Foreign%20Exchange%20Act%20-%20Copy%20\(1\).pdf](http://www.cb.is/library/Skraarsafn---EN/Capital-surveillance/Foreign%20Exchange%20Act%20-%20Copy%20(1).pdf)

According to the Icelandic National Bank, this exception, however, does not apply to bitcoin⁵⁰. Bitcoin itself is not illegal in Iceland. The possession of bitcoin is completely in accordance with Icelandic laws and so it is the process of generating bitcoins. Iceland, thanks to its cheap electric energy, is also very popular as a base for data centers generating bitcoin.⁵¹

The Icelandic interpretation of bitcoin does not see bitcoin as either a goods or service, but rather as some sort of an investment vehicle, which might be used to transfer funds. Even though Iceland did not directly specify what bitcoin is or is not, we might see an interpretation inclining for a bitcoin to be some sort of intangible monetary instrument but not money itself.

2.2.2 The Court of Justice of the European Union

On 22nd October, 2015 the Court of Justice of the European Union decided that bitcoin transactions are not subjected to value added tax.⁵² Reasoning behind this decision is that member states must exempt, pursuant to an article 135, section 1, letter e) of the council directive 2006/112/EC; *“transactions, including negotiation, concerning currency, bank notes and coins used as legal tender, with the exception of collectors' items, that is to say, gold, silver or other metal coins or bank notes which are not normally used as legal tender or coins of numismatic interest.”*

Even though bitcoin, in a legal sense, does not represent legal tender, the Court argues that; *“transactions to exchange traditional currencies for units of the ‘bitcoin’ virtual currency (and vice versa) constitute the supply of services for consideration within the meaning of the directive, since they consist of the exchange of different means of payment...”*⁵³ With this reasoning the Court had recognized, for tax purposes, bitcoin as a means of payment, rather than a good.

⁵⁰ Significant risk attached to use of virtual currency. Cb.is [online]. 2014 [visited on 2016-04-13]. Available at: <http://www.cb.is/publications-news-and-speeches/news-and-speeches/news/2014/03/19/Significant-risk-attached-to-use-of-virtual-currency>

⁵¹ For more information, please see: <http://www.ibtimes.co.uk/geothermal-gold-why-bitcoin-mines-are-moving-iceland-1468295>, or <http://uk.businessinsider.com/photos-iceland-bitcoin-mine-genesis-mining-cloud-2015-8>.

⁵² COURT OF JUSTICE OF THE EUROPEAN UNION. The exchange of traditional currencies for units of the ‘bitcoin’ virtual currency is exempt from VAT [online]. Luxembourg, 2015 [Visited on 2016-04-13]. Available at: <http://curia.europa.eu/jcms/upload/docs/application/pdf/2015-10/cp150128en.pdf>

⁵³ Id.

The Court of Justice of the European Union did resolve the issue regarding value added tax, but again did not bring much light to what bitcoin really is. Regarding this decision, bitcoin grew stronger to being recognized as an intangible monetary instrument, which could lead, under the European law, most probably to the electronic money.

2.2.3 Electronic Money Directive

In connection with the above meant decision, bitcoin could theoretically fall within the scope of Electronic Money Directive.⁵⁴

Important for bitcoin definition might be the preamble of Electric Money Directive, especially article 5 that sets forth that this directive shall be limited to payment services providers that issue electronic money, and should not apply to specific pre-paid instruments such as store card, public transport cards, meal vouchers, services vouchers etc. However, if such specific purpose instrument would develop into a general purpose instrument, then the regulation regarding electronic money should be applied. That said, bitcoin might be considered a general purpose instrument,⁵⁵ because it is accepted as a means of payment by undertakings other than the issuer and it is not linked to a specific service or good.

⁵⁴ Directive 2009/110/EC of the European Parliament and of the Council of 16 September 2009 on the taking up, pursuit and prudential supervision of the business of electronic money institutions amending Directives 2005/60/EC and 2006/48/EC and repealing Directive 2000/46/EC.

⁵⁵ Well mapped development from a specific purpose instrument to a general purpose instrument might be shown on in the history of a Q-coin, Chinese digital medium of exchange. Q-coin was created prior to bitcoin by one of the Chinese most significant telecom operator Tencent. It was developed as a virtual medium of exchange for services provided specifically within the Tencent network. Q-coin could be obtained by user spending his remaining balance on pre-paid telephone card. Q-coin had developed a popularity among young users who started to pay and tip each other with Q-coins. Seeing the popularity Q-coin gained among the youngsters, several online games started to award its players with Q-coins. Subsequently some stores and merchants started to accept Q-coins as a means of payment, which led to a wide spread of Q-coin and subsequently to the interest from a Chinese government. As the popularity of Q-coin grew stronger and the possibility of purchase was very limited, the Q-coin caught interest of a black market and the facilitating the purchase of Q-coins using Renminbi appeared. Q-coin market grew each year about 20% to several billion Renminbi a year, which gave reason to the Chinese government to ban the alternative medium of exchange.

2.2.4 Bitcoin as a General Purpose Instrument

Could we consider bitcoin to be electronic money pursuant to the Electronic Money Directive? Electronic money is defined in article 2, section 2 of this directive under following criteria:

1. Electronic money shall be electronically stored monetary value;
2. Electronic money shall represent a claim on receipt of funds of an amount not less in value than the monetary value issued; and
3. Electronic money shall be accepted as a means of payment by natural and legal person other than the issuer.

As per compliance with criterion one. Bitcoin is digitally stored in a decentralized public ledger, which is kept updated by various computers around the world. The data in the ledger are decentralized within the network and stored on those computers. It is safe to say that bitcoin is stored electronically and therefore, at least partially, complies with the first criterion.

According to criterion number two, electronic money shall be interpreted as an obligation against authority that issues the electronic money, while maintaining the value of the transaction at par. The easiest example of such process is a deposit of legal tender through ATM on a bank account.

A person inserts bank notes into the ATM and the exact value appears on display of the ATM that very value is subsequently transferred to that person's bank account linked with credit or debit card. The balance on the bank account linked with the card represents electronic money issued by the administrator of the bank account.

Electronic Money Directive sets forth in article 11 section 1 that; "*Member States shall ensure that electronic money issuers issue electronic money at par value on the receipt of funds.*" and in section 2 that; "*Member States shall ensure that, upon request by the electronic money holder, electronic money issuers redeem, at any moment and at par value, the monetary value of the electronic money held.*"

Within the Bitcoin network there is no authority that could issue bitcoin in exchange for monetary value, therefore there is no place for any kind of obligation. Bitcoins are generated in accordance with the algorithm written in the bitcoin source code. The issuance of bitcoins depends on the computing power invested within the network. As there is no entity that would issue bitcoins in a way similar to a bank can issue

electronic money, the process of generating bitcoins using the computing power is clearly out of scope of the Electronic Money Directive, because these bitcoins are generated without any link to an authority, and thus the Member States cannot ensure that the bitcoin user could redeem the legal tender invested in the purchase of bitcoin at par value.

Purchase of bitcoins using legal tender also does not constitute an obligation for a seller of bitcoins to redeem the sold bitcoins for the exact same amount of monetary value invested in the purchase by the buyer.

Section 1 and 2 of the Electronic Money Directive cannot be satisfied within the Bitcoin network, as bitcoins are not issued at the first place and as there is no authority that might be held responsible for redeeming the price. Also it is worthy to note that electronic money is reflecting the value of its physical equivalent, but bitcoin's price is decided in matters of supply and demand only. Bitcoin thus, does not satisfy the second criterion pursuant to article 2, section 2 of Electronic Money Directive.

As for the third criterion stating that electronic money shall be accepted by others than the issuer. Bitcoin is accepted at various places and the issuer is decentralized over the world. It is safe to say, that bitcoin is accepted by others than its issuer and so Bitcoin complies with the last criterion.

Summarizing, Bitcoin satisfies, partially, the first defining criterion of electronic money and fully the third. Bitcoin, however is contradictory to the second criterion. For bitcoin to be electronic money it would have to meet all of those requirements. Bitcoin therefore cannot be considered electronic money.

2.3 Bitcoin as a Money or a Currency?

So far if we look upon the Icelandic interpretation and the decision of European Court of Justice and compare it to our analysis above, bitcoin inclines to be some sort of medium of exchange but not electronic money.

Electronic money is just a specific legal term referring to a digitally stored legal tender. We therefore, still should work with an assumption that bitcoin might be money. After all even the author presents his invention as an electronic cash system.⁵⁶ The label

⁵⁶ NAKAMOTO, Satoshi. *Bitcoin: A Peer-to-Peer Electronic Cash System*: [online]., 1-9 [Visited on 2016-02-16]. Available at: <https://bitcoin.org/bitcoin.pdf>

“electronic cash” is very suitable for bitcoin. It works exactly the same way as if someone had taken out the corporeal substrate out of bank notes and coins but left everything else as is.

2.3.1 Money Precursors?

What is money, is surprisingly a hard question to answer. The issue is that money is an economical term, which is represented, in today’s world, by currency or more accurately by a legal tender. So naturally, when someone thinks of and refers to money, they refer to currency.

The design, form or shape of money is important only to some extent. Money is an essence. Theoretically, every object might become money. Yet the predispositions of the object that will become money in future, is unknowingly taken into account much sooner. Usually, only the objects with the right characteristics are chosen to become money. The object shall satisfy the following criteria:

1. Value common assets,
2. Common and accessible,
3. Constant utility,
4. Low cost of preservation,
5. Transportability,
6. Divisibility,
7. Durability,
8. High market value in relation to volume and weight,
9. Recognisability, and
10. Resistance to counterfeiting.

We cannot say that bitcoin satisfies all of the above meant criteria but neither we can say that bitcoin would fail them. Bitcoin is exceptionally good in satisfying some of them and exceptionally fails the others.

Bitcoin takes the resistance to counterfeiting to a whole new level. There is literally no way to counterfeit bitcoin. It is just not possible. Bitcoin always stays part of the Bitcoin network and therefore adding a counterfeited one would be recognized and refused.

High market value in relation to volume and weight is also something where bitcoin excels. Bitcoin is a string of a coded message saved on a Bitcoin network; the only weight and volume will be the medium where the private keys to bitcoin are stored.

Divisibility is also satisfied to the highest level as bitcoin is divisible to eight decimal places and so is transferability as it is possible to transfer bitcoin over the internet or in hand. It is also much easier to transport a million Czech Korunas in bitcoin than in Korunas.

With other characteristics it is a different story. For instance, recognisability. Bitcoin, being the best known artificial digital medium of exchange, is still known very little. We are unable to say how many people use bitcoin and even if we were, we would not know how many of them use bitcoin on a daily basis.

The low cost of preservation is also hard to answer for the sole purpose that keeping the Bitcoin as a network running is extremely costly. On the other hand, for a normal user who does not want to generate bitcoins, storing bitcoin is extremely cheap, because he only needs to load his hard drive with certain data and keep the hard drive safe or print the private key on paper and keep the paper safe. Without keeping the network alive the bitcoin would be unusable and keeping the network counting transactions needs thousands or millions of top tier computers working nonstop. We have to take into account that the costs are decentralized and that the network itself pays to those who keep it alive in incentive of bitcoins. Therefore we might say that the cost of preservation is somewhat low⁵⁷.

Truly problematic might be the constant utility and accessibility. Over the time, bitcoin shall grow in value, because of its deflationary nature. Theoretically speaking what could happen is that the people who now hold bitcoin would have no reason to sell it as it will grow in value forever, which could limit bitcoin's usability maximally to some sort of settlement layer. The constant utility remains in question and so does the accessibility.

We should bear in mind that bitcoin is a developing technology and that some of these characteristics might change from worse to better and vice versa. We are of the

⁵⁷ In our experience, it is safe to conclude that just holding the bitcoins does not cost anything. The authors hold bitcoins for over a year and there were no additional costs to the operating cost of the computer.

opinion that bitcoin still represents a unique corpus where the positives outweigh the negatives and uncertainties at least when it comes to the characteristics. Thus, bitcoin has the corpus to be money, but does it satisfy the economic conception of Money?

The universal definition of money considers three basic criteria:

1. Medium of exchange;
2. Unit of Account; and
3. Store of Value.⁵⁸

2.3.2 Medium of Exchange

*“Money can only serve its required function if it is intended to serve as the universal means of exchange in the State of issue.”*⁵⁹ Contrary to this statement, could bitcoin still be considered a medium of exchange if there is no state of issue? Definition of medium of exchange is surprisingly hard to find. A very general definition might be found in Hubbard: *“[A]nything that is generally accepted as payment for goods and services or in the settlement of debts.”*⁶⁰ Other sources do not even distinguish in between the conception of medium of exchange and means of payment.⁶¹ We see medium of exchange as anything that acts as an intermediary instrument that helps to facilitate trade among two or multiple parties.

Bitcoin was designed to facilitate trade among two or multiple parties. It has a perfect attributes of an intermediary instrument. It is durable, divisible, easily storable and transferable. Bitcoin is also used as a medium of exchange. We might therefore easily conclude that bitcoin is a medium of exchange.

⁵⁸ Definice peněz, JÍLEK, Josef. *Peníze a měnová politika: Podstata tvorby peněz*. Prague: GRADA Publishing, a.s., 2004, p. 26. ISBN 8024707691. In the Czech original: *“Peníze obecně slouží třem účelům: jako účetní jednotka kupní síly, tj cen zboží a služeb, jako platební prostředek mezi spotřebiteli, podniky a vládou, jako prostředek uchování hodnoty.”*

⁵⁹ The Concept of Money. PROCTOR, Charles. *MANN ON THE LEGALS ASPECT OF MONEY: Universal Means of Exchange*. Sixth edition. New York: Oxford university press, 2005, p. 28. ISBN 9780198260554.

⁶⁰ HUBBARD, R. Glenn. *Money, the financial system, and the economy*. 5th ed. Boston: Pearson/Addison-Wesley, 2005, p. 14. ISBN 0321237854.

⁶¹ THOMAS, Lloyd Brewster. *Money, banking, and financial markets*. 5th ed. Mason, Ohio: Thomson/South-Western, 2006, p. 21. ISBN 0324176732.

2.3.3 Unit of Account

*“The unit of account provides a standard of value against which the value of commodities can be measured.”*⁶² Bitcoin is currently being used in above one hundred thousand shops around the world as a medium of exchange, but all of these shops have one similarity. The price of a service or a goods (commodity) is never measured against bitcoins.

The price is always determined in a legal tender and the amount of bitcoins is interconnected with the price expressed in legal tender. Therefore, the standardized measure used to reckon the price is a legal tender, such as Euro.

It is often argued that bitcoin resembles gold to some extent. Such arguments are best shown on its limited amount and deflationary nature. We argue that if bitcoin is similar to gold in those terms, it cannot be a unit of account.

*“Despite their history within national monetary systems, neither gold nor silver can be regarded as “money” for their value may fluctuate in terms of money and is determined according to market demand; neither commodity is denominated by reference to a unit of account.”*⁶³

Bitcoin follows the exact path stated above. At the moment it cannot be used as a unit of account as it often changes its value very quickly. In contrary, we further argue that Bitcoin might be considered as a unit of account in future. As such it depends on whether the value of bitcoin will be able to stabilize itself enough. Most of the spikes in value of bitcoin are because of various cyber security related events and bitcoin halving. Both of those might be eliminated in future or substantially lowered.

The bitcoin halving is every four years and each of the halving shall both increase and stabilize the value. Much more problematic for the bitcoin value are various security problems that might affect the places where bitcoin is sold or traded. If the amount of those businesses will grow in the future, the occasional security breach should not influence the overall value that much.

⁶² The Concept of Money. PROCTOR, Charles. *MANN ON THE LEGALS ASPECT OF MONEY: Universal Means of Exchange*. Sixth edition. New York: Oxford university press, 2005, p. 27. ISBN 9780198260554.

⁶³ Id. at p. 28.

2.3.4 Store of Value

Is bitcoin able to hold value? As long as the value can be retrieved over time, the form in which the value was invested in the first place, acts as a store of value. We might look upon this function in two ways; value and purchasing power.

*“In modern times, the value of money in terms of its purchasing power is prescribed by law and is wholly unrelated to the cost of materials involved in its production.”*⁶⁴

Bitcoin’s purchasing power and therefore subsequently its value is not prescribed and cannot be prescribed by any law. What is thus the value of bitcoin?

Considering bitcoin exchange rate to the United States Dollar development, we might illustrate its ability to hold value. During the year of 2009, bitcoin had practically zero value, spiking 1000% in just 5 days in July, 2010 from \$0.008 to \$0.08. On 12th of February, 2011 bitcoin parities with USD and on 8th of July falls from \$31 to \$2. At the end of 2012 bitcoin price climbs back to \$13. On November 27th, 2013 the price reaches over 1000\$ and slowly falls ever since, with occasional spikes, to \$200 in early 2015 stabilizing around \$400 and slowly growing in the first three months of 2016, just to spike again on June 17th, 2016 to \$748.

From the above shown example it is clear that the value of bitcoin is very volatile, which is directly in contrary to the price stability. The purchasing power of bitcoin is thus very dependable on the supply and demand. Much like a commodity.

Bitcoin presents in this case a very similar problem as in the previous case of the unit of account. In future, bitcoin might be stable enough to satisfy the characteristics of store of value, but at the moment it cannot. We conclude that at the moment bitcoin is unable to store value to the extent that it would satisfy the third criterion – store of value. Pursuant to our analysis, bitcoin does not satisfy two out of three criteria and therefore cannot be considered money in economic sense.

2.4 Bitcoin as a Money Pursuant to the Czech Law

When the majority of people think of bitcoin, they unknowingly ascribe the attributes of money to bitcoin and therefore subsequently think of bitcoin as money. It

⁶⁴ Id. at p. 31.

would be unfair to blame them; after all it does have many similarities. The word “bitcoin” even involves the coin inside of it.

Money, however, is rather an economical term. The law of the Czech Republic regards money in the sense of legal tender. The closest definition of money is possible to find in the act no. 284/2009 Coll. On Payment System in section 2 paragraph 1 letter c); “*For the means of this act money shall be; bank notes, coins, non-cash money and electronic money.*”⁶⁵ Pursuant to this definition and in connection with the analysis above, bitcoin cannot be considered money in legal sense under the Czech laws. We determined that bitcoin is not electronic money, it is also not a bank note or a coin. The only remaining category is non-cash money, but we have proved that bitcoin does not satisfy the economic conception of money.

We can conclude that bitcoin, as of now, is a medium of exchange but not money. To the extent we assume that, because bitcoin is not money it is hardly a currency. Even if we would assume that bitcoin is money in the economic and legal sense, it still could not be considered currency for various reasons.

Probably the most comprehensive reason is that there is no country, where bitcoin would be a recognized as a legal medium of exchange and the acceptance of such medium could be enforced by authorities. Bitcoin is a stand alone project that is not pegged to any legal tender nor commodity and yet is unable to be a unit of account as stated above. Therefore, bitcoin is not a legal tender and thus it cannot be a currency. The nomenclature Virtual Currency is therefore absolutely wrong. As bitcoin is neither virtual not a currency.

2.5 Summary

The nomenclature Virtual Currency is faultily used. It is so, not only because of the wrong adjective ‘virtual’, but also because bitcoin cannot be considered currency. Virtual Currency is connected to a virtual economy that might be found in online games, whereas bitcoin is connected to the digital economy in the form of general

⁶⁵ In the Czech original: “pro účely tohoto zákona peněžními prostředky jsou bankovky, mince, bezhotovostní peněžní prostředky a elektronické peníze.”

instrument. Bitcoin is, therefore, not limited by any virtual boundaries or a specific purpose such as a classic virtual currency.

Further, bitcoin does not satisfy the legal definition of electronic money pursuant to the Electronic Money Directive. As there is no central issuer, who would be obliged to retrieve invested customer's funds of an amount not less in value than the monetary value issued in the first place. Nevertheless, as electronic money is just a legal type of money, might be bitcoin considered money in general economic sense?

Bitcoin cannot be considered money as it does not comply with its definition. We must agree with Papp's statement that "*[b]itcoin shows great potential as a medium of exchange for e-commerce, but its weaknesses as a unit of account and store of value hinder its ability to permanently replace the dollar.*"⁶⁶ As all of the characteristics must be satisfied, bitcoin is at the moment just a medium of exchange. Despite of the above said, if in the future bitcoin becomes widely accepted the price of bitcoin will necessarily stabilize enough to hold value for a longer periods of time and then bitcoin will probably satisfy all of the criterions of economic money definition.

It is further argued that currency is legal term for specific money under the influence of law, and because bitcoin is not money, it cannot be currency. We are of the opinion that at the moment bitcoin is a digital medium of exchange, which is of capability to become money in economic sense in the future.

⁶⁶ PAPP, Jeremy. A Medium of Exchange for an Internet Age: How to Regulate Bitcoin for the Growth of E-Commerce. *Pittsburgh Journal of Technology Law and Policy* [online]. 2015, **15**(1), 39 [visited on 2016-07-24]. DOI: 10.5195/tlp.2014.155. ISSN 2164-800x. Available at: <http://tlp.law.pitt.edu/ojs/index.php/tlp/article/view/155>

3 Legal Aspects of Bitcoin

To determine what bitcoin is, under the Czech law, we have to start with the very basic diversification. We might either look at bitcoin as a subject of legal relations or as on an object of legal relations.

Knapp provides a definition of the subject of legal relations: “*The recipient, the one to whose will and consciousness is related a legal norm, respectively to whose will and consciousness is applied, is a man and might not be no one else than man.*”⁶⁷

Bitcoin essentially has never been alive and under no circumstances might be considered a man. As a man is able to maintain a free will⁶⁸ and decide on his own. We cannot look on bitcoin as on a recipient, therefore we have to consider bitcoin as an object of legal relations.

Object of legal relations is defined by Gerloch: “*Objects of legal relations are in particular things, values of human personality, results of human creativity, legally relevant human actions etc.*”⁶⁹

This work is based on the assumption that bitcoin, thanks to its unique characteristics, might fall outside the scope of the objects that have to be legally considered a thing in a legal sense pursuant to the act no. 89/2012 Coll. the Civil Code.

Legal theory supports dualistic approach to the conception of a thing. It is being differentiated between materialistic and idealistic conception of a thing.⁷⁰ In another words, law either views tangible items as things in a factual sense or everything that is different from a person as things in a legal sense.

⁶⁷KNAPP, V. Teorie práva. Prague: C.H. Beck, 1995, p. 70. Beckovy právnické učebnice. ISBN 80-7179-028-1. In Czech original: “*Jeho recipientem, tj. tím, k jehož vůli a vědomí se právní norma obrací, resp. na jehož vůli a vědomí působí, je člověk a nemůže jím být nikdo jiný než člověk.*”

⁶⁸In general use of the collocation free will not in the sense as for example Kutílek. Even though we would like to point out that from philosophical point of view Blockchain technology is the first real expression of determinism. More on determinism might be find here: KUTÍLEK, Lukáš. Právněfilozofické aspekty svobodné vůle. Právnická Fakulta Univerzity Karlovy, 2015. Diplomová práce.

⁶⁹GERLOCH, A. Teorie práva. 6th edition. Pilsen: Vydavatelství a nakladatelství Aleš Čeněk, 2013, p. 141. Beckovy právnické učebnice. ISBN 978-80-7380-454-1. In the Czech original: “*Objekty právních vztahů jsou zejména věci, hodnoty lidské osobnosti, výsledky tvůrčí lidské činnosti, právně relevantní chování lidí apod.*”

⁷⁰SEDLÁČEK, J. Vlastnické právo: všeobecné nauky. Prague: Wolters Kluwer Česká republika, 2012, p. XVI. Klasická právnická díla (Wolters Kluwer ČR). ISBN 978-80-7357-758-2.

3.1 Materialistic Conception

Materialistic conception considers things as an actually existing objects with corporeal basis that are controllable and serves the needs of people.⁷¹ Until the year of 2014, the law of the Czech Republic has followed the materialistic conception, even though it was criticized.⁷² Eliáš even made a remark that the materialistic approach to things is a “*crude materialism*”⁷³

Most notably, the problem with a factual or materialistic conception of a thing is that some objects which are things factually are not legally under this concept and some which are legally, are not factually. Not to mention that this conception could have hardly anticipated the digital World of today.

3.1.1 The Act no. 40/1964 Coll. the Civil Code

The act no. 40/1964 Coll. Civil Code was based on the materialistic approach of the conception of things, however, the legislator decided not to define what a thing was at all. The reason behind the lack of such a fundamental definition is simple: “*The Civil Code does not include a definition of a thing, because thing is a natural fact, which cannot be defined.*”⁷⁴

Not defining the thing, the act no. 40/1964 Coll. Civil Code at least sets forth, in section 118 paragraph 1, what the object of legal relations is. “*Things and, if their nature admits so, rights or other property values can be subject to civil legal relationships.*”⁷⁵ Legal doctrine then deduced that thing is a corporeal object if it is controllable and serves the needs of people.⁷⁶

This definition is the root of the previous statement that some things are not things and some that are, are not. For example, a cadaver – a corpse of a person is factually a

⁷¹ ELIÁŠ, Karel. Věc jako pojem soukromého práva. Právní Rozhledy [online]. 2007, **2007**(4), 119 [visited on 2016-04-08]. Available at: beck-online.cz

⁷² ELIÁŠ, Karel. Vlastnické právo. Paradigmata českého pojetí pod zkušebním kamenem kontinentální právní kultury. Právní Rozhledy [online]. 2005, **2005**(22), 807 [visited on 2016-04-08]. Available at: beck-online.cz

⁷³ Id. para 70, At p. 119. In the Czech original: “*surový materialismus.*”

⁷⁴ Kratochvíl, Z. and col. Nové občanské právo. Prague: Orbi s, 1965, p. 186. In the Czech original: “*Definici věci občanský zákoník neobsahuje, neboť věc je přírodní fakt, který nepřísluší právu definovat.*”

⁷⁵ In the Czech original: “*Předmětem občanskoprávních vztahů jsou věci, a pokud to jejich povaha připouští, práva nebo jiné majetkové hodnoty.*”

⁷⁶ Please compare with: KNAPP, V., KNAPPOVÁ, M. IN KNAPPOVÁ, M., ŠVESTKA, J., DVOŘÁK, J. A KOL. Občanské právo hmotné. 4th Edition. Prague: ASPI, 2006, p. 272. ISBN 9788073571313

thing but legally is not. Eliáš further provides another example where a cup and saucer are two different things, but legally just one.

Even though this conception might look hardly logical at a first glance, for a legally non-educated person it seems to be much more understandable. Thing is everything that exists in the real world, is possible to be controlled and serves the needs of people. Anything that lacks a physical representation in the world, but might be of control or value was identified as another property value. *“The object of civil relations might be, if its nature admits so, also other property value than a thing or right, that is monetary expressible values...”*⁷⁷ It is much easier to explain that a stone is a thing and that right is a right and that computer program is another property value, than explain that everything except a person is a thing.

As we have indicated, according to the discontinued approach bitcoin could be considered, among others, another property value. Bitcoin is after all a computer program. Computer program was generally considered to be an other property value as it is not a thing nor right.⁷⁸ As bitcoin is not corporeal, and under certain circumstances might be object of civil legal relations, bitcoin must have been another property value.

Such conception, that software, generally, is another property value has been a root of several problems and has shown the weaknesses of the materialistic conception in the modern age. For instance, if someone had ordered a construction of a table and the table was faultily constructed, the act no. 40/1964 Coll. Civil Code involved a section 499: *“A person who leaves a thing to someone else for payment shall be liable for that at the moment of the performance, the thing has explicitly stipulated or usual qualities, that it can be used according to the nature and purpose of the agreement or according to what was agreed by the parties and that the thing has no legal defects.”*⁷⁹ In accordance with the above mentioned, the person was liable for the defects of the thing. Software, however, was not considered a thing and therefore if someone had ordered a specific

⁷⁷ ŠVESTKA, J., SPÁČIL, J., ŠKÁROVÁ, M., and HULMÁK, M., *Občanský zákoník: komentář*. 2nd Edition. Prague: C.H. Beck, 2009, p. 442. Velké komentáře. ISBN 978-80-7400-108-6. In the Czech original: *“Předmětem občanskoprávních vztahů mohou být, připouští-li to jejich povaha, i jiné majetkové hodnoty, než je věc či právo, neboli hodnoty vyjádřitelné v penězích...”*

⁷⁸ Further explanation regarding this approach might be found in the points 1-3 in: TELEEC, I., TŮMA, P., *Autorský zákon, Komentář*, C. H. Beck, 2007, pp. 37-38 ISBN 9788071796084.

⁷⁹ In Czech original: *“Kdo přenechá jinému věc za úplatu, odpovídá za to, že věc v době plnění má vlastnosti výslovně vymíněné nebo obvyklé, že je ji možno použít podle povahy a účelu smlouvy nebo podle toho, co účastníci ujednali, a že věc nemá právní vady.”*

software and the software was faultily written, the author of the software was not legally liable.

The answer to the above stated problems is the idealistic approach. Under the idealistic approach, software is considered a thing, which helps to solve the day to day legal issues that might arise for example from a contractual dispute.

3.2 Idealistic Conception

The idealistic conception is best explained by the definition of a thing itself as presented in the act no. 89/2012 Coll. the Civil Code, where thing in a legal sense is defined in section 489 as “ *everything that is different from a person and serves the needs of people.*”⁸⁰

The definition of a thing in a legal sense presented in contemporary Civil Code is comprehensive and so various sources argue that bitcoin is a thing in a legal sense pursuant to section 489 of Civil Code.⁸¹

None of the resources we found derive the explanation from anything else than the Civil Code definition of a thing in a legal sense. What is being left out completely, but not only in the very little of the Czech resources that might be found on Bitcoin, but also in the foreign resources is that Bitcoin and bitcoin is primarily a software and subsequently, therefore, also a creation of the author.

We are of the opinion that Bitcoin, and therefore also bitcoin, is so substantially different from anything else that it deserves a deeper analysis.

3.2.1 The Act no. 89/2012 Coll. the Civil Code

Pursuant to the definition of a thing in a legal sense at first glance it appears that bitcoin cannot be anything else but a thing in legal sense. However, the definition of a thing in a legal sense has another aspect, which is not written in the act, but is specified

⁸⁰ In the Czech original: “*vše, co je rozdílné od osoby a slouží potřebě lidí.*”

⁸¹ Bitcoin: právní náladu u nás i ve světě. Zakonyvkapse.cz [online]. 2013 [visited on 2016-05-16]. Available at: <http://zakonyvkapse.cz/bitcoiny-z-pohledu-prava-ceske-urady-a-instituce-stale-mlci/>. Further see: PRADUBICKÝ, Jan. Právní rámec a praktické aspekty jeho používání v platebním styku. Prague, 2014. p. 21, Magister thesis. Charles University, Faculty of Law.

in the explanatory memorandum. “... *the thing in a legal sense is, what might be subjected to subjective property rights, especially the proprietary right.*”⁸²

If we would proceed solely pursuant to the text of the section 489 of the Civil Code, we could establish following premises:

1. Everything that serves the needs of people is a thing.
2. Person is never a thing.
3. Sun serves the needs of people and is not a person, therefore Sun is a thing.

“Generally, *for a thing in a legal sense is typical that it can be usurped. Such attribute expresses that particular item is a thing in a legal sense if is controllable. Not everything that is beneficial for man (air, rain, Sun, the glowing Earth’s core) might be connected with the term thing. Thing in a legal sense is shaped by its controllability.*”⁸³

As of now, the mankind cannot control Sun in a sense that someone could usurp it for himself. Sun is therefore not a thing in a legal sense as it lacks the possibility to be owned - controlled.

The thing in a legal sense must be of such nature that allows to be subject of absolute proprietary rights. We therefore concur that: “*The term of a thing in a legal sense is built upon three fundamental characteristics:*

1. *The difference from a person;*
2. *The ability to serve the needs of people, utility;* and
3. *Controllability.*”⁸⁴

Bitcoin is a problematic case when it comes to applying the above mentioned criteria. The complications arise not only from the different possible angles we might look at Bitcoin, but also from the factual interconnection of them.

⁸² DŮVODOVÁ ZPRÁVA: Zvláštní část. In: Justice.cz [online]. 2011, p. 115., [visited on 2016-03-09]. Available at: http://obcanskyzakonik.justice.cz/images/pdf/Duvodova_zprava_leden_2011_.pdf In the Czech original: “*věcí v právním smyslu je to, čeho se mohou týkat subjektivní majetková práva, především právo vlastnické.*”

⁸³ DŮVODOVÁ ZPRÁVA: Zvláštní část. In: Justice.cz [online]. 2011, p. 115., [visited on 2016-03-09]. Available at: http://obcanskyzakonik.justice.cz/images/pdf/Duvodova_zprava_leden_2011_.pdf, In the Czech original: “*Obecně je pro věc v právním smyslu typické, že si ji lze přivlastnit. V tom je vyjádřeno, že určitý předmět je věcí v právním smyslu, je-li ovladatelný. Ne vše, co je pro člověka užitečné (vzduch, déšť, slunce, žhavé zemské jádro) lze spojit s pojmem věci. Věc v právním smyslu profiluje její ovladatelnost.*”

⁸⁴ THONDEL, ZUKLÍNOVÁ in DVORÁK, J., ŠVESTKA, I, ZUKLÍNOVÁ, M. a kol. Občanské právo hmotné. Svazek 1. Díl první: Obecná část. Prague: Wolters Kluwer ČR, 2013, 432 p. 372. In the Czech original; Pojem věci v právním smyslu je vystaven na třech základních znacích: a) rozdílnost od osoby, b) schopnost sloužit potřebě osob, tj. užitečnost, c) ovladatelnost.

Bitcoin is not only the work of an author, decentralized peer-to-peer network, software, but also an “open to public” group of indefinite number of people. Subsequently, we might consider bitcoin as the medium of exchange, a right, or a license.

Bitcoin as a social phenomenon cannot be controlled but only spectated. Bitcoin as a medium of exchange, however, must be controlled, otherwise it cannot be used. The work of an author consists of copyrights and cannot be transferred to any other person, but might be licensed to facilitate its further use, and the peer-to-peer network is designed to be futile to any outside controllability.

To find a solution, on the following pages, we are going to diversify the different approaches to Bitcoin under the condition of compliance and non compliance with the 3 defining characteristics of a thing in a legal sense.

Those different layers of meaning, according to our findings, are:

1. Bitcoin as the work of an author;
2. Bitcoin as a computer program and license;
3. Bitcoin as a right; and
4. Bitcoin as a thing in a legal sense without the absolute proprietary rights.

3.3 Bitcoin as the Work of an Author

Bitcoin was created by the author who never came forward. It is not usual that in connection with creation of something so monetary potent as Bitcoin the author remains unknown. Nevertheless, logic asserts that there must have been an author, even though we do not know who it was, unless we believe that the nickname Satoshi Nakamoto is a real person. Bitcoin is therefore still the work of an author, even though the author is unsung.

The work in a form of a computer program and as such is internationally protected under the Berne Convention for the Protection of Literary and Artistic Works in connection with the WIPO Copyright Treaty.

“Computer programs are protected as literary works within the meaning of Article 2 of the Berne Convention. Such protection applies to computer programs, whatever may be the mode or form of their expression.”⁸⁵

The article 2 of the Berne Convention, among other, stipulates that “[t]he expression “literary and artistic works” shall include every production in the literary, scientific and artistic domain, whatever may be the mode or form of its expression, such as books, pamphlets and other writings; ...”⁸⁶

We want to determine whether the work of an author might be considered a thing in legal sense pursuant to the act 89/2012 Coll. As such we shall compare the work to the three criterions of a thing in a legal sense.

The first question therefore is, does Bitcoin in the form of the work serves the needs of people? The answer here is yes, Bitcoin in the form of the work serves the needs of people, because bitcoins might be used to facilitate trades and has other functions.

The second question is whether Bitcoin in the form of the work is different from a person. This question might be answered in a classic two-way answer: “Yes, and no.” Bitcoin is a technological solution, a data protocol, and as such we cannot render it as a subject of legal relations as we have pointed out earlier, because the subject of legal relations might be only a person. For the reason that Bitcoin is not a person then it must be something different from a person and therefore it satisfies this criterion.

As for the answer “no”, we shall also look at a Bitcoin as at the work of an author in the sense of copyright law.

“The creation of an author – the work, cannot be assign within the scope of intangible things, because regarding its character of unique consequences of the creative activity of a man, it represents entities inerasably connected with its authors. This, always present, personal element, which forms the essence of the work, prevents the consideration of the work as a thing in a legal sense. In consequence of that the exclusive moral rights of the author are not transferrable and the proprietary rights of

⁸⁵ Article 4 of the WIPO Copyright Treaty (1996)

⁸⁶ Article 2 of the Berne Convention for the Protection of Literary and Artistic Works (1971)

*the author are untradeable, which contradicts one of the imperative characteristic of the definition of a thing, which is the objective controllability by a man.*⁸⁷

Even though we cannot consider Bitcoin to be a real human being or an artificial legal person, we must take into account the inseparable aspects of a man that have been invested in the Bitcoins code. We are of the same opinion as Sýkora that the work always carries the inseparable essence of the author, and therefore it cannot be differentiated from the author's person, thus the difference from the person is not satisfied.

The last question is, whether the Bitcoin in the form of the work is controllable. The work of an author is a representation of copyright, which according to the section 10 of the act no. 121/2000 Coll. on Copyright, Right Related to Copyright and on the Amendment on Certain Laws is (Copyright Act): "*Copyright shall include exclusive moral rights and exclusive economic rights.*"⁸⁸

The exclusive economic rights will be addressed in the part 3.4 of this work. The exclusive moral rights are not transferrable and are inseparably tied to the author, as such, those rights cannot be controlled in the sense of the defining characteristic of a thing in a legal sense. The answer to the question stated above is that Bitcoin in the form of the work is not controllable, unless licensed.

We can conclude that, because the Bitcoin in the form of the work does not satisfy two out of three criteria of the definition of a thing in a legal sense, it cannot be considered a thing in a legal sense, but only the work of an author.

3.4 Bitcoin as a Computer Program and License

As the section 10 of the Copyright Act states, there are two different types of rights involved. We have addressed the moral rights tied to Bitcoin in sense of the work, but

⁸⁷ SÝKORA, Matěj. Autorské dílo ve světle právního pojetí věci v novém občanském zákoníku. In: Fairart.cz [online]. Praha, 2014 [visited on 2016-03-12]. Available at: <http://www.fairart.cz/blog/autorske-dilo-ve-svetle-pravniho-pojeti-veci-v-novem-obcanskem-zakoniku/>. In the Czech original: "*Autorská díla do skupiny nehmotných věcí opravdu přiřadit nelze, neboť s ohledem na svůj charakter jedinečných důsledků tvůrčí činnosti člověka představují entity nesmazatelně spojené se svými autory. Tento vždy přítomný osobnostní prvek, jenž formuje samu podstatu autorského díla, znemožňuje zacházet s autorským dílem jako s věcí v právním smyslu. V důsledku toho jsou osobnostní práva autora nepřevoditelná a majetková práva autora nezczitelná, což odporuje jedné z nutných podmínek definice věci, již je objektivní ovladatelnost věci člověkem.*"

⁸⁸ In the Czech original: "*Právo autorské zahrnuje výlučná práva osobnostní a výlučná práva majetková.*"

we should also address the exclusive economic rights. As the work in this case is a software, we shall speak about a computer program and subsequently a license.

*“In a very simplified way, it is possible to define software as everything, that is not hardware, but is included within.”*⁸⁹ It is a very well know fact that the Czech legislator decided not to provide a legal definition of software. It is probably so, because the Czech legislator works with the term computer program as might be found in the Copyright act.⁹⁰

The terminological difference between software and computer program is given by the different fields where these terms, which are identical as to the content, are used. The specific set of 1's and 0's that governs the actions of a processor in connection with is subsequent user interference is being referred as software by the people who *“... are associated with the practical field of the informative technology.”*⁹¹

Legal practice rather uses the term computer program. The definition of a computer program might be found in the preamble under the point 7 of the European Union's directive 2009/24/ES: *“...the term ‘computer program’ shall include programs in any form, including those which are incorporated into hardware. This term also includes preparatory design work leading to the development of a computer program provided that the nature of the preparatory work is such that a computer program can result from it at a later stage.”*

Looking at the definitions above, it is quite clear that the Bitcoin is a computer program - software. Computer program is being generally addressed⁹² as an intangible thing in a legal sense and we do not have a problem with such categorization. The only difference we think is important to highlight once again is that the computer program is also the work of an author and as such it is not a thing in a legal sense as argued in the previous part of this thesis. Therefore, computer program represents both a thing in

⁸⁹ JANSÁ, Lukáš and Petr OTEVŘEL. Softwarové právo: Definice softwaru, práva k softwaru a jeho ochrana, databáze.2nd. Edition. Brno: Computer Press, 2014, p. 31. ISBN 978-80-251-4201-1. In the Czech original: *“Velmi zjednodušeně lze software definovat jako vše co není hardware, ale je v něm obsaženo.”*

⁹⁰ Section 65 and following of the act 121/2000 Coll. on Copyright, Right Related to Copyright and on the Amendment on Certain Laws.

⁹¹ JANSÁ, Lukáš and Petr OTEVŘEL. Softwarové právo: Definice softwaru, práva k softwaru a jeho ochrana, databáze.2nd. Edition. Brno: Computer Press, 2014, p. 32. ISBN 978-80-251-4201-1. In the Czech original: *“... osob pohybujících se v praktické oblasti informačních technologií.”*

⁹² Id.

legal sense and the work of an author, which is not a thing in legal sense. The part of a computer program that is considered a thing is the exclusive economic right that might be transferred in a form of a license.

License (in the sense of license agreement) is defined within the act no 89/2012 Coll. Civil Code, in the section 2358 as follows: *“By a license agreement, a licensor grants to a licensee an authorization to exercise intellectual property rights (a license) within the stipulated limited or unlimited extent, and a licensee undertakes to pay remuneration to the licensor, unless otherwise stipulated.”*⁹³

Bitcoin as a computer program is licensed under the MIT license, which stands for: *“Permission is hereby granted, free of charge, to any person obtaining a copy of this software and associated documentation files (the “Software”), to deal in the Software without restriction, including without limitation the rights to use, copy, modify, merge, publish, distribute, sublicense, and/or sell copies of the Software, and to permit persons to whom the Software is furnished to do so, subject to the following conditions: The above copyright notice and this permission notice shall be included in all copies or substantial portions of the Software.”* The other condition stated by the MIT license is that the software is provided “as is”.⁹⁴

License is essentially a right to use the copy of the authors work. Such right is under the idealistic conception considered a thing and once again we do not see a problem here, that needs to be specifically addressed.

The particularly interesting topic here is rather complicated. Every other software or a computer program is licensed for the purpose of use of its copies. A classic example is the copy of Microsoft Windows operation system. Bitcoin’s computer program is licensed as well for the same purpose - the use of the copies of the original work of the author. That being said the interesting part here is that the Bitcoin that is being used by everyone is the very first code. That is the work, the creation.

⁹³ In the Czech original: *“Licenční smlouvou poskytuje poskytovatel nabyvateli oprávnění k výkonu práva duševního vlastnictví (licenci) v ujednaném omezeném nebo neomezeném rozsahu a nabyvatel se zavazuje, není-li ujednáno jinak, poskytnout poskytovateli odměnu.”*

⁹⁴ Open Source Initiative. Opensource.org: The MIT License [online]. [visited on 2016-03-11]. Available at: <https://opensource.org/licenses/MIT>.

*“Computer program (the work); i.e. such computer program, which is statistically unique (unrepeatable) outcome of the author’s production (creative activity). Is statistically unique piece of work that is effusion of personality of its originator.”*⁹⁵

Bitcoin, even though licensed, is licensed only for the use of its copies. Therefore, all of the creations the peer-to-peer network and Bitcoin’s blockchain that are actually the very first work of the author, have never been licensed. Both of those phenomena never have had to be copied, because the source code keeps itself unique. Thus, every copy of the blockchain or peer-to-peer network leads to creation of a completely new digital medium of exchange. Such new digital medium of exchange is for example Litecoin. Litecoin is an alternated clone of Bitcoin, which is licensed under the MIT license. Bitcoin itself is, however, not. We therefore can argue both of those creations are subjected to the copyrights laws and as such should not be considered things in a legal sense.

We have already stipulated that Bitcoin is the work, but what about bitcoin as a medium of exchange? Shall the bitcoin, as a medium of exchange, be considered the same as the two above stated phenomena?

We might argue that the bitcoin was the intentional creation of the author that was implemented in to the source code and therefore bitcoin is the same code. Or we might argue that the bitcoin is creation of the code itself without the authors effort.

This difference is important as the Copyright Act sets forth the following condition for the work. The work of an author must be a “...*unique outcome of the creative activity of the author...*”⁹⁶ and must be “...*expressed in any objectively perceivable manner including electronic form...*”⁹⁷ According to the author, bitcoin is the “*pur[e] peer-to-peer version of electronic cash*”⁹⁸. It is hardly imaginable that the author did not want to create the bitcoins. That it was some sort of a by-product lacking a direct intent of the author.

⁹⁵TELEC, Ivo a Pavel Tůma.: *Autorský zákon. Komentář*, 1st Edition, Prague: C.H.Beck, 2007. p. 40
In the Czech original: “*Počítačový program (dílo); tzn. takový program, který je statisticky jedinečným (neopakovatelným) výsledkem autorovy tvorby (tvůrčí činnosti). Je statisticky jedinečným výtvorem autora neboli výronem osobnosti svého tvůrce.*”

⁹⁶ Section 2 of the act 121/2000 Coll. on Copyright, Right Related to Copyright and on the Amendment on Certain Laws.

⁹⁷ Id.

⁹⁸ NAKAMOTO, Satoshi. *Bitcoin: A Peer-to-Peer Electronic Cash System*: [online]., 1. [visited on 2016-02-16]. Available at: <https://bitcoin.org/bitcoin.pdf>

Nakamoto probably never intended for bitcoins to be considered anything different than the code that created Bitcoin. Actually, bitcoins might be stored only within the blockchain and thus, inside of the Bitcoin code. The consequence of relocation of bitcoins outside of the Bitcoin protocol, if it is even possible, would lead either to different digital units or to destruction of the code. We argue that Bitcoin and bitcoin together stand for a single code and thus a single entity. This entity is protected under the original moral rights of the author and thus the work.

We therefore might conclude that bitcoin is also creation of an author, and because the license applies only to Bitcoin's copies, it is not licensed and therefore not a thing in legal sense. We are aware that this conception might give rise to many different problems that will be natural only to Bitcoin. Nevertheless, we think that it is important to highlight this approach as Bitcoin is the first digital creation that keeps itself unique and as such there might be a basis for it being something different.

3.5 Bitcoin as a Right

To illustrate this approach let's think about the way how bitcoins are obtained. Generally, as we have said earlier, there are two possibilities how to obtain bitcoin – via the use of computing power and through juridical acts such as a gift or purchase.

The first option through computing power is quite simple to understand. It is often regarded as mining. *“Bitcoin mining—termed from the software used to create a block called Bitcoin miner—is designed to mimic the extraction of minerals. Anyone is able to obtain bitcoins without purchasing them from other users by downloading and running bitcoin's mining program.”*⁹⁹ Computer using a special software directs its power on a mathematical problems provided by the Bitcoin data protocol and if the computer will be the first one to solve it, it is rewarded in the form of bitcoins.¹⁰⁰

The reality is a little different. If this would be true, the person behind a computer in question would now have 12.5 bitcoins stored in his computer. The person would have owned them. The difference that is not being stressed is that the person in this

⁹⁹ KAPLANOV, Nikolei. NERDY MONEY: BITCOIN, THE PRIVATE DIGITAL CURRENCY, AND THE CASE AGAINST ITS REGULATION [online]. Philadelphia, 2012. p. 119, [visited on 2016-05-17]. Available at: <http://www.luc.edu/media/lucedu/law/students/publications/clar/pdfs/kaplanov.pdf>. Temple University Beasley School of Law.

¹⁰⁰ Id. p. 120.

example only has only the possibility to spent 12.5 bitcoins. To put it in another words, those 12.5 bitcoins never moved. It never changed position and it never will.

We might even say that all of the bitcoins, 21 million of them, had been already created, but the option to transfer them was not yet assigned. Thus, the person in our example never generated anything else than the possibility to do a single operation and that is to transfer the option to transfer the option.

The above stated “option to transfer the option” might be hard to understand at first. It might be illustrated on the second option, the possibility to obtain bitcoin through a juridical act. A person might purchase, sell, or even donate a bitcoin to somebody or from someone. The right question here is, what exactly is being transferred to the other person if the bitcoin always stays confine in the decentralized ledger?

It is possible to think about bitcoin in the same way as of something really located in a shop window. Say there is an expensive ring in a shop window. The owner of the store approaches someone and says that he is going to sell him the possibility to assert that the ring is his and that he will be always able to sell such possibility to someone else, but that he is not selling the ring and the ring will never change place. That person agrees under a condition that the owner will keep a book, where everyone would be able to find who has the possibility to assert that he owns the ring.

Now, everyone can see the ring through the window and ask the owner of the store, whether it is for sale. The owner would say that it is not, but that someone has the possibility to assert that the ring is his and such right is for sale. If the person who might rightfully assert that he owns the ring wants to sell this option, what is he selling? He is selling an option to transfer this option. It is therefore the very same situation as with bitcoin.

The bitcoins never change position. Thus, the only transferable ‘thing’ is, again the option to transfer the option. This possibility of course depends on the disposition with the corresponding private key, which is however activated by the transaction. Apart from the owner of the shop, in the example above, in connection with Bitcoin, such option is governed by the computer program itself. It is again a part of the code. Part of the decentralized peer-to-peer network.

We are of the opinion that we could look at this option to transfer bitcoin as at a right. The right to transfer bitcoins. Thus, the possession of the private key shall be

considered a right. Unsurprisingly, right under the idealistic conception is considered a thing in legal sense.

The question here is whether we can think of such disposition as of ownership. Is this control over the bitcoin enough to satisfy the criterion of controllability? Is there any control at all?

Bitcoin cannot be usurped in the classic sense such as for example a lemon or an apple. The only option that this disposition provides is to spend bitcoin or spend it later on. We are of the opinion that the bitcoin might be more likely possessed than owned. Not only because of the limited control, but also because in the same sense as the ring in our example is owned by the owner of the store, there is also a possibility that the bitcoins are owned by the author of the network as it has never been licensed to anyone or that the bitcoin are not owned by anyone at all. The next chapter further develops the question of control.

3.6 Bitcoin as a Thing Without Absolute Proprietary Rights

The new civil code might give rise to an interesting hybrid. To something that satisfies the characteristic of thing in legal sense, such as bitcoin, however still lacks the most important theoretical characteristic, which is the absolute proprietary right. In another words it is a thing that simply cannot be controlled to the extent it could be owned, theoretically like bitcoin.

Such construction is described by professor Telec in his article named the Possession of Information.¹⁰¹ As an example he presents analysis of a recipe for a fish soup:

“Under the jus in rem it is considered a property, a thing in a legal sense, which might even have economic value, although it does not have to be necessarily connected with a specific restaurant (company). Recipe for a fish soup, whether a Christmas or common one, satisfies legal characteristics of a thing in a legal sense as specified in the Civil Code, but also a thing that is possess-able in the same civil meaning. Not a single act assigns to such recipe (nor similar recipes) absolute proprietary rights (right in rem

¹⁰¹TELEC, Ivo. Držba informací. Právní rozhledy [online]. 2014, **2014**(2), 115 [Visited on 2016-04-12]. Available at: <http://www.beck-online.cz/bo/document-view.seam?documentId=nrptembrpxa4s7grpxg5dsl4ytcni&groupIndex=8&rowIndex=0>.

and the hereditary right). Terminologically it is a possession of a thing and as such intangible thing without the absolute proprietary rights.”¹⁰²

We are of the opinion that it is possible to look at bitcoin in a similar way as bitcoin shares many similarities with the example stated above, regarding the recipe for a fish soup. Recipe for a fish soup is an information and after all bitcoin is just a string of text, and might considered an information as well. “Since, bitcoin is essentially composition of the records in a public ledger of transaction and encrypted keys, which’s nature is a complex number, it is possible to infer that it is an information – a thing without tangible basis, which might be saved on a tangible substrate.”¹⁰³ The private key that is used to handle bitcoin is essentially just a piece of information, which when shared cannot be protected in the same very sense as a recipe for a fish soup.

“Apparently, materially it is diverse examples of various intangible things (economic and another property values), which comply with the legal conceptual (definitional) characteristic of a thing in a legal sense, the characteristics of an intangible thing, without legally ascribed absolute proprietary rights. We might therefore say that materially (and generally in an absolute proprietary sense) it is out of the nature *res nullius* (understand a thing without anyone’s proprietary right etc.)”¹⁰⁴

The idealistic conception of a thing gives enough space to consider bitcoin a thing in a legal sense. From the three criteria, however, the only non-problematic is the criterion of usefulness. The criteria of difference from a person and controllability are

¹⁰² Id. in the Czech original: “Věcněprávně se jedná o majetek, o věc v právním smyslu, která může mít dokonce hospodářskou hodnotu, ačkoli nemusí být nutně spjata s určitou restaurací (obchodním závodem). Recept na rybí polévku, ať již vánoční nebo všední, splňuje legální pojmové znaky nejen věci v právním smyslu občanského zákoníku, ale i věci držitelné ve stejném soukromoprávním významu. Žádný zákon k němu (ani jiným podobným receptům) ovšem nepřiznává absolutní majetková práva (věcná práva a právo dědické). Pojmově se ale jedná o držbu věci, a to nehmotné věci bez absolutních majetkových práv.”

¹⁰³ PARDUBICKÝ, Jan. Právní rámec a praktické aspekty jeho používání v platebním styku. Prague, 2014. p. 21-22, Magister thesis. Charles University, Faculty of Law. In the Czech original: “Vzhledem k tomu, že bitcoin je vlastně složen ze zápisu ve veřejném záznamu transakcí a šifrovacích klíčů, které mají podstatu několikamístného čísla, dá se dovodit, že jde o informaci - věc bez hmotné podstaty, kterou lze uchovávat zachycenou na hmotném nosiči.”

¹⁰⁴ Id. In the Czech original: “Jak je již patrné, věcně se jedná o rozmanité případy různých nehmotných předmětů (hospodářských a jiných majetkových hodnot), které splňují zákonné pojmové (definiční) znaky věci v právním smyslu, a to znaky věci nehmotné, aniž však jsou k těmto nehmotným věcem zákonem přiznána absolutní majetková práva. Můžeme proto říci, že věcněprávně (a vůbec absolutně právně) se povahově jedná o věci ničí (rozuměno o věci bez něčího vlastnického apod. práva k nim).”

problematic. At this point we should address the controllability as the difference from a person was already addressed.

Telec, in connection with the possession of information, presents two important criterions, which take its part while deciding whether an object might be fully controlled and thus whether we can link the absolute proprietary right with the object in question. The object in question must satisfy these criterions in order to be considered a thing in a legal sense:

1. the limitation of the right in rem and;
2. the hereditary right.

Bitcoin certainly presents a factual limitation to both of them. Starting with the hereditary right we should point out that the main difference that renders the right of heritage is the *succession* of rights that are subjected to the heritage.

In a normal trade, for example a purchase of a lemon, the rights in connection with the lemon are *transferred* by the juridical act carried out by the seller and by the buyer. From a theoretical point of view, there is a substantial difference when we talk about the right of heritage. Heritage is defined by universal *succession* of rights.

Succession right is created upon the decedent's death.¹⁰⁵ That said, there is no direct juridical act on behalf of the decedent. The main difference therefore is that in a classical trade the rights are transferred and in case of death the rights are advanced on the basis of legal event.

Bitcoin cannot be advanced; it can be only transferred. The unique conception of bitcoin simply does not allow it. The only possible utilization of bitcoin is to transfer the option to transfer it. Such option is protected by the knowledge of the private key linked with the amount of bitcoin the holder can transfer the right to transfer them. Anyone who knows the private key might handle the bitcoins right away and cannot be stopped from doing so. If someone wanted to advance bitcoin to another person, he would have to provide the private key linked with the bitcoin to a third person and at that moment he would be transferring it, because he would give full disposition not only to the addressee, but also to the intermediary.

¹⁰⁵ Section 1479 of the act 89/2012 Coll. the Civil Code.

There is no factual way how to advance bitcoin, because of the private key protection. It is the very same case as if a person shares secret with someone else, the information is shared at the exact point it gets to the other person and that moment it cannot be taken back.

Professor Telec also talks about the limitation of rights in rem. He argues that a specific range of things in legal sense cannot be owned but can be only possessed, because of the legal setting, in connection with the factual character of such thing.¹⁰⁶ We are of the opinion that bitcoin, even though not specifically mentioned by Telec, is one of those things.

All bitcoins stay as integral part in the Bitcoin network logged in the blockchain. As we have said earlier, it is impossible to take one bitcoin and move it away from the blockchain. It is not possible to do anything else with bitcoin then to transfer the option to transfer the option.

At this point it might be argued that there is a documented case of someone losing bitcoins.¹⁰⁷ The case of James Howells losing 7,500 bitcoin has been covered by many news sites on the internet and we came over many similar yet smaller cases of people losing access to bitcoins while gathering the resources for this work. Truth is that James Howells never lost a single bitcoin. He simply does not have access to handle them anymore. The bitcoins are still theoretically findable on the internet via the site blockchain.info. Most probably James Howells is able to look them up as he knows the bitcoin's address the private key is associated with. He is simply missing the private key, which renders the possibility to transfer them. Again, theoretically, he might be able to recover the private key and obtain the right again.

Theoretically. Practically, it is not possible.¹⁰⁸ One of the best arguments against recovering private keys or hacking bitcoin at all will never be as much profitable as using the necessary power recover or hack it as to use it to generate new bitcoins.

¹⁰⁶ See para.98.

¹⁰⁷ Missing: hard drive containing Bitcoins worth £4m in Newport landfill site. *Theguardian.com* [online]. Alex Hern, 2013 [Visited on 2016-04-11]. Available at: <https://www.theguardian.com/technology/2013/nov/27/hard-drive-bitcoin-landfill-site>

¹⁰⁸ The only possibility would be a hard hacking, which means trying to guess the password (private key) by trying every possible combination of numbers and text. Various sources prove various times depending on the computer that would be in use. As of the year of 2016 it seems it would take about 0.61 billion years in 2070, however it might be only 1 year and few months, if the encryption used on bitcoin would not change. Additional information might be found here:

By this example we want to prove that bitcoins are always accessible, it is always possible to look them up, but to transfer them it is necessary to have a password in the form of a private key. Bitcoin therefore cannot be lost. Bitcoin also cannot be destroyed. Bitcoin might be just inaccessible.

We are therefore of the opinion that bitcoin cannot be owned but can be only possessed, because of its factual characteristics bitcoin cannot be inherited and the control over bitcoin is limited to a single option. Thus, bitcoin resembles the recipe for a fish soup as presented by Telec.

It might be further argued that bitcoin is *res nullius* or that bitcoin is something that might satisfy the definition of a thing in a legal sense and yet factually it cannot be usurped and controlled. A thing in a legal sense without an absolute proprietary rights.

3.7 Summary

Bitcoin presents particular factual and legal characteristics that make it stand out. There are four main ways, how to approach bitcoin. None of those conceptions, however, did yield an outcome that would solve the question whether bitcoin is a thing in a legal sense irretrievably.

The main problem is in compliance with two out of three characteristics of a thing in a legal sense. That is the difference from a person and controllability. Bitcoin as the work, the creation of an author, is not different from a person, as it carries inseparable essence of the author and thus cannot be considered a thing in legal sense. Bitcoin as a computer program is similarly problematic, because neither Bitcoin nor bitcoin were ever licensed and are surprisingly the very first work of the author and as such it is protected under the copyright law, which does not make them a thing in a legal sense either. The situation is complicated as Bitcoin is actually licensed, but only for purpose of its copies, which are, however, irrelevant for the use of bitcoin.

Another approach is to consider bitcoin a right. A right to transfer this right to transfer this (that) right to another person. Bitcoin's code allows to users just one kind of operation, which makes the possibility of control questionable. Nevertheless, bitcoin

<https://bitcointalk.org/index.php?topic=1289433.0>,
<http://bitcoin.stackexchange.com/questions/2847/how-long-would-it-take-a-large-computer-to-crack-a-private-key>,

in the sense of right is probably the most practical solution to the question of what bitcoin is, as right is considered a thing under the idealistic approach.

Last approach is comparison of bitcoin and a conception of possession of information as presented by Telec. Telec argues that under the idealistic conception of a thing in a legal sense, information satisfies the legal definition of a thing in a legal sense, but lacks absolute proprietary rights. Bitcoin is substantially similar to the examples provided by Telec. Bitcoin also lacks absolute proprietary rights, as it cannot be inherited and also cannot be fully controlled, for example cannot be destroyed.

Even though we have shown possible copyright related issues of bitcoin and even though when bitcoin is examined more deeply, the concept of a thing in a legal sense does not fit bitcoin flawlessly. At the moment it is the easiest and most practical approach to consider bitcoin a thing in legal sense. It is probably also, at least for state and law enforcement, the most economical solution, as various laws might be applied to bitcoin.

In the end we must say that we still do not feel about bitcoin to be a thing in legal sense. It might legally be a right or a thing, but according to our opinion, bitcoin shall have its own category. It shall be rather considered, at least for future use, some sort of non-cash monetary instrument. We incline to the monetary conception, even though we have proven in the previous chapter that bitcoin is not money nor a currency.

Nevertheless, we came to the conclusion that for practical and regulatory use bitcoin shall be considered a right, which is subsequently a thing in legal sense.

4 Regulatory Aspects and Issues Regarding Bitcoin

The negative impacts of bitcoin had been pointed out many times. Apparently, every serious or an even an academic work regarding the Bitcoin has found numerous issues in connection with bitcoin. For example “*In the context of criminal law, Bitcoins are often used as a method of payment to disguise the origin of money illegally obtained.*”¹⁰⁹ Or another example: “*Due to the difficulty in classifying Bitcoin, opportunistic individuals may engage in activities that swindle unsuspecting people of their bitcoins while skirting the law.*”¹¹⁰ Our experience is not any different, when we read an article relating Bitcoin on a normal media, such as Czech newspaper or see something in television it always has the same denominator and that is its criminal aspect.

Bitcoin is being used in connection with child pornography.¹¹¹ Bitcoins are being stolen and used for facilitating a drug trades.¹¹² All the suspicious activities that happen on the internet or more specifically on the dark web¹¹³ are somehow connected to Bitcoin.¹¹⁴

Why is that so? The usual answer is that Bitcoin provides a partial anonymity or even a complete anonymity to its users and thus it is best tool to facilitate monetary

¹⁰⁹ BOEHM, Franziska a Paulina PESCH. *Bitcoin: A First Legal Analysis: with reference to German and US-American law*[online]. University of Münster, 2014. p. 4. [visited on 2016-05-06]. Available at: http://fc14.ifca.ai/bitcoin/papers/bitcoin14_submission_7.pdf

¹¹⁰ COINING BITCOIN’S “LEGAL-BITS”: EXAMINING THE REGULATORY FRAMEWORK FOR BITCOIN AND VIRTUAL CURRENCIES. *Harvard Journal of Law & Technology* [online]. 2014, 27(2), p. 596 [visited on 2016-07-27]. Available at:

<http://jolt.law.harvard.edu/articles/pdf/v27/27HarvJLTech587.pdf>

¹¹¹ see: Bitcoinový pomáhají šířit dětské porno. Nový projekt si na zločince posvítí. *Idnes.cz:*

ekonomika [online]. Prague: Mafra a.s., 2016 [visited on 2016-05-29]. Available at:

http://ekonomika.idnes.cz/londynsky-startup-pomuze-vyresit-zneuzivani-bitcoinu-v-byznysu-s-detskou-pornografi-g67/-eko-zahranicni.aspx?c=A160708_094912_eko-zahranicni_nio

¹¹² see: Drogovým dealerům zmizely dvě miliardy korun v bitcoinech. Čech vinu odmítá. *Idnes.cz:*

technet [online]. Prague: Mafra a.s., 2016 [visited on 2016-05-29]. Available at:

<http://technet.idnes.cz/bitcoin-sheep-marketplace-kradez-d4q->

[/sw_internet.aspx?c=A131202_194657_sw_internet_pka](http://sw_internet.aspx?c=A131202_194657_sw_internet_pka)

¹¹³ Dark web is a collocation that is used to refer to a place within the internet, which is accessible via some special browsers. The inaccessibility through normal internet browsers and anonymity of web pages creates a very good environment for illicit activities. For more information and the difference between dark web and deep web, please see: <https://brightplanet.com/2014/03/clearing-confusion-deep-web-vs-dark-web/>, and <http://whatis.techtarget.com/definition/deep-Web>.

¹¹⁴ See: Podsvětí nejhlubšího internetu. DeepWeb & Bitcoin 3. díl. *Kurzy.cz* [online]. Prague: AliaWeb, spol. s r.o., 2016 [visited on 2016-05-30]. Available at: <http://www.kurzy.cz/zpravy/397613-podsveti-nejhlubsiho-internetu-deepweb--bitcoin-3-dil/>

operations connected with the illicit activities. That is a true statement, however we see one more important reason.

4.1 The Need for Regulation

On August, 2015 redactor of the web page e-republika.cz asked a question to Miroslav Singer at that time the governor of the Czech Nation Bank: “*What is your opinion on Bitcoin like currencies?*”¹¹⁵ To which he answered: “*Low volume, not interesting. The whole existing emission of Bitcoin does not represent even a one tenth of our reserves.*”¹¹⁶

So, on the one side of the coin, Bitcoin is not interesting enough for the authorities and on the other side, Bitcoin presents a great tool for all the criminals smart enough to use it. How dangerous can Bitcoin be? Bitcoin is generated by various unknown entities without any applicable regulation. As of today (July 27, 2016), every day is created roughly 1300 – 2000 bitcoins.¹¹⁷ With bitcoin being offered for around \$650 that equals circa \$1,150,000.00 of tradable, potentially untraceable, value every day. It might be argued that \$1.15 million of is not a particularly great amount compared to what is being dealt with on the worlds markets, and yet pursuant to the section 4 of the act 254/2004 Coll. on the Restriction on Cash Payments. It is prohibited to pay and accept amount higher than 270,000.00 Czech Koruna (circa 10,000.00 Euro) in cash. The reason of such prohibition, to put it in a very simple way, is that the cash is partially anonymous and therefore might be used to launder illegal money, but that amount equals just about 18 bitcoins¹¹⁸ Therefore every 20 minutes is created an amount in bitcoins that would be otherwise prohibited to be spent in cash. How is that not interesting enough?

¹¹⁵ DOTAZNÍK PRO Miroslava Singera: ČNB. *E-republika.cz* [online]. České Budějovice: spolek eRepublika, 2015 [visited on 2016-06-02]. Available at: <http://e-republika.cz/article3255-DOTAZNÍK-PRO-Miroslava-Singera-ČNB>. In the Czech original: “*Jaký máte názor na měny typu Bitcoin?*”

¹¹⁶ Id. In the Czech original: “*Malý objem, nezajímavé. Celková stávající emise Bitcoinu není ani desetina našich rezerv.*”

¹¹⁷ On average, the Bitcoin network closes one block of transactions every 10 minutes, which equals 144 blocks (1800 bitcoins) a day. However, the number of people interested in generating bitcoin constantly increases, which raises the difficulty of the mathematical problems that are needed to be solved in order to obtain bitcoin. The difficulty adjusts around every two weeks, therefore the actual number of bitcoins might be slightly higher.

¹¹⁸ Counting with bitcoin around 650 United States Dollars.

As pointed out in by the example above, this approach to Bitcoin is nothing but wrong. Even though Bitcoin is incomparably smaller in the volume to the other financial markets, it should not be left unattended in this spirit. What the state should do is the exact opposite and that is to consider Bitcoin to be interesting. Come up with solutions to the challenges it puts upon the legislator. Countries should prepare its own Bitcoin only systematic legislation, and so should the Czech Republic. The world should have as much control over the Bitcoin as possible, not just simply stay next to it and say we are not interested.

4.2 The Need for Systematic Regulation

As we have pointed out earlier in this work, Iceland took the first systematic steps against Bitcoin right a way, but that was mostly because of the Foreign Exchange Act, which was not written specifically to regulate Bitcoin, but rather happened to have influence over it.

Why we assert that the regulation shall be systematic? It so because some other countries have taken a rather interesting steps against the Bitcoin. Take for instance the Kingdom of Thailand. At first the Bank of Thailand issued a statement that because of the lack of laws its is prohibited to purchase and sell bitcoins, to purchase or sell any goods using bitcoin, and to send and receive bitcoins outside of Thailand.¹¹⁹

Little over a year later the Bank of Thailand informed that trading and conducting business with bitcoin does not require a specific license.¹²⁰ Just to inform, few days into the bitcoin trading, that their intentions were misinterpreted and that trading bitcoins and generally any Bitcoin related business might be once again illegal.¹²¹ To the extent, recent development shows that there has been a smartphone application launched for the Thailand and Philippines, which would suggest that even though there are still active

¹¹⁹ Trading suspended due to Bank of Thailand advisement. *Bitcoin.co.th* [online]. Bitcoin Co. Ltd, 2013 [visited on 2016-06-29]. Available at: <https://bitcoin.co.th/trading-suspended-due-to-bank-of-thailand-advisement>.

¹²⁰ Bitcoins back in the Thai marketplace. *Bangkokpost.com* [online]. The Post Publishing PLC, 2014 [visited on 2016-06-29]. Available at: <http://www.bangkokpost.com/archive/bitcoins-back-in-the-thai-marketplace/395952>.

¹²¹ Bitcoin firm licensed to trade in baht. *Bangkokpost.com* [online]. The Post Publishing PLC, 2014 [visited on 2016-06-29]. Available at: <http://www.bangkokpost.com/archive/second-bitcoin-company-licensed-to-trade-in-baht/427339>.

instruction that dealing with bitcoin is illegal, it is in fact not.¹²² It should be noted that Thailand is being labeled as a country where Bitcoin is illegal, but the situation is slowly getting cleared off, probably because it has come to the general attention that the Bank of Thailand does not have authorization to issue such prohibitions. The case of Thailand proves that it is necessary to approach Bitcoin systematically. Otherwise, such legal situation works only in favor of criminals and substantially limits normal business owners who cannot provide their services.

Similarly, wrong is the approach of other countries, which decided to ban Bitcoin completely. For instance, Bolivia. The Central Bank of Bolivia (El Banco Central de Bolivia) had issued a statement: “*As of today, it is prohibited to use any currency, not issued or regulated by states, countries or economical unions as well as the electronic payment orders on currency and money denominations not authorized by the central bank of Bolivia in the field of its national payment system.*”¹²³

Banning the Bitcoin is systematic only to some extent. There is a very simple rule that bitcoin shall not be used. As such it does not cause any trouble for the people to understand what is allowed and what is not. However, the realization of such regulation might be of issue. We must differ between regulating the technology itself, and the bitcoin such as the medium of exchange. It is hardly possible to regulate the technology behind Bitcoin as the access to the network cannot be limited. Banning the bitcoin as the medium of exchange is somewhat possible. But it is not without problems.

If someone already holds bitcoins, in Bolivia, there is literally no way to stop him from transferring it to someone else. Will the authorities shut down the electricity or will they limit the use of the Internet? Would not such actions be a little too much to stop a few bitcoin transactions?

¹²² Coins.ph Launches Peer-to-Peer Bitcoin App for Southeast Asia. *Coindesk.com* [online]. The Post Publishing PLC, 2015 [visited on 2016-06-29]. Available at: <http://www.coindesk.com/coins-ph-abra-style-bitcoin-app-southeast-asia/>.

¹²³ BOLIVIA. *ERENCIA DE ENTIDADES FINANCIERAS — PROHIBICION DEL USO DE MONEDAS Y DENOMINACIONES MONETARIAS NO REGULADAS EN EL AMBITO DEL SISTEMA DE PAGOS NACIONAL*. In: La Paz, 2014, Year 2014, No. 44. Available at: https://www.bcb.gob.bo/webdocs/01_resoluciones/044%202014.PDF. In the Spanish original: “*A partir de la fecha queda prohibido el uso de monedas no emitidas o reguladas por estado, países o zonas económicas y de órdenes de pago electronicas en monedas y denominaciones monetarias no autorizadas por el BCB en el ambito del sistema de pagos nacional.*”

Authorities will be confronted with the decentralization and anonymity of Bitcoin. That means locating the person behind a bitcoin transaction will be very hard. If the authorities against all the odds actually find the computer that initiated the transaction will they be able to prove, who was at that computer at the time of the transaction? All of those questions above illustrate just the tip of the iceberg of problems connected with Bitcoin. There will be much more issues in connection with enforcing such crude regulation such as complete ban.

Thus, we opine that banning Bitcoin is a wrong approach. This step is taken usually by countries with a left wing oriented government. Vietnam, Bolivia, and Russia all of those countries struggle with its own currency, and therefore bitcoin is not a welcome technology.

Society and business are evolving. Instead of hotels, it is now possible to reserve someone's apartment via Airbnb.¹²⁴ Instead of taking a taxi, it is now possible to share a car with a stranger via Uber.¹²⁵ So why instead of legal tender we cannot have Bitcoin that is based on similar principle as Airbnb and Uber. A principle where people are in charge instead of a global authority. A government shall support what is better for the people. The ban on bitcoin however, is just a suppress of technology, and suppress of technology is usually in contrary with greater good. The bitcoin shall be properly regulated, it should have its own legislation, but such legislation presents a unique challenge.

The legal problems that relate to Bitcoin's regulation and to Bitcoin generally could be differentiated as contemporary and theoretical. The contemporary problems are such problems that are already in effect. The theoretical problems take into account the future development of Bitcoin and its impact on the possible regulation and legal framework.

4.3 Contemporary Problems

The contemporary problems are caused by two key characteristics of Bitcoin and that is the decentralization and partial anonymity.

¹²⁴ For more information, please see: <https://www.airbnb.com/about/about-us>.

¹²⁵ For more information, please see: <https://www.uber.com/our-story/>.

4.3.1 Decentralization

The author who created bitcoin must have been aware that his creation will fall outside of the scope of the law. We might only speculate to what extent Nakamoto wanted to disturb today's monetary system and to what extent he wanted to create something new and innovative. We might find a clue as to his intentions in one of his rare statements.

In one email discussion, Nakamoto answers a statement that he would not find a political solution in cryptography: "Yes, but we can win a major battle in the arms race and gain a new territory of freedom for several years. Governments are good at cutting off the heads of a centrally controlled networks like Napster, but pure P2P networks like Gnutella and Tor seem to be holding their own."¹²⁶ Basically, Nakamoto says that he was aware that decentralized networks cannot be controlled.

Why is decentralization so problematic? There is no entity to target, no servers to shut down. The technology itself does not rely on any government. Even though states have power to regulate the internet, in peer-to-peer networks there is, technically, no one to be regulated. Since Bitcoin does not have a centralized authority, detecting suspicious activity, identifying users, and obtaining transaction record is problematic for law enforcement.¹²⁷

In practice we can show the problems of decentralization on the example of Bolivia and its ban on Bitcoin. Any dealings with Bitcoin are illegal in Bolivia, but in reality it is still possible to buy or sell bitcoins in La-Paz, the largest city in Bolivia.¹²⁸

4.3.2 Anonymity

Another issue in connection with the Bitcoin is the partial anonymity that Bitcoin provide to its users. If in the year of 1999, Smejkal said that the use of computer technology gives the offenders wings¹²⁹. Then bitcoin in the year of 2008, had learned

¹²⁶ Satoshi Nakamoto Institute. Satoshi Nakamoto Institute [online]. [visited on 2016-03-06]. Available at: <http://satoshi.nakamotoinstitute.org/emails/cryptography/4/#selection-29.0-39.18>

¹²⁷ FBI DIRECTORATE OF INTELLIGENCE. (U) *Bitcoin Virtual Currency: Unique Features Present Distinct Challenges for Deterring Illicit Activity*: [online]. 2012 [visited on 2016-06-23]. Available at: https://www.wired.com/images_blogs/threatlevel/2012/05/Bitcoin-FBI.pdf

¹²⁸ Trade bitcoins in La Paz, BO. *Localbitcoins.com* [online]. Helsinki, 2015 [Visited on 2016-06-01]. Available at: <https://localbitcoins.com/places/608956/la-paz-bo/>

¹²⁹ SMEJKAL, Vladimír. Počítačová a internetová kriminalita v České republice. *Právní rozhledy* [online]. 1999, **1999**(12), 1 [see 2016-05-23]. Available at: <http://www.beck->

them how to fly. Bitcoin came up with something very appealing, with unregulated environment that allows anonymous transfers of value everywhere, where is internet connection. The anonymity rests in the use of bitcoin addresses that does not require any personal data to be created.

Bitcoin technology does not reveal the user, but reveals the amount of bitcoins that is being transferred: *“Certain financial transactions are private but not anonymous; for example, the donor wall at the local art museum, which identifies the names of donors but not the amounts donated. Bitcoin, by contrast, is anonymous but not private: identities are nowhere recorded in the Bitcoin protocol itself, but every transaction performed with Bitcoin is visible on the distributed electronic public ledger known as the blockchain.”*¹³⁰ Thus, everyone can see how much is being transferred but not who stands behind the amount transferred and so bitcoin partially anonymous.

For a future legislator a good news is that Bitcoin’s anonymity is not everlasting, at least in most cases. It is possible to locate a user using various techniques that are based on monitoring all the addresses in the ledger.¹³¹ However, there are other – easier ways how to find who had initiated a transaction.

It is very common that someone, in the expectation of bitcoins, publishes his Bitcoin address and his name or his internet nickname together on a webpage. Such person then might be very well spectated. Another way is to wait until someone purchase something using bitcoins. Not every business requires customers to provide their name and address when they buy the product or service, but large part of the businesses does. To the extend if the product shall be shipped to the customer he must provide name and address regardless.

online.cz/bo/document-view.seam?documentId=nrptcojzhfpxa4s7gez643uojptcyi&groupIndex=5&rowIndex=0

¹³⁰ KOSHY, Philip, Diana KOSHY a Patrick MCDANIEL. An Analysis of Anonymity in Bitcoin Using P2P Network Traffic [online]. Pennsylvania State University, 2013 [visited on 2016-06-29]. Available at: http://fc14.ifca.ai/papers/fc14_submission_71.pdf. Further see: How Anonymous is Bitcoin? *Coincenter.org* [online]. Washington, D.C., 2015 [visited on 2016-06-29]. Available at: <https://coincenter.org/entry/how-anonymous-is-bitcoin>

¹³¹ Id.

That being said, there are still operations that might stay 100% anonymous. Such as the bitcoin to bitcoin transaction. Sponsorship of illicit groups such as WikiLeaks or so called Islamic State.¹³² Probably also Bitcoin generating.

Decentralization and anonymity are the root of many issues and challenges. The decentralization alone is a basis for a question: “Who exactly shall be responsible for the regulation?” Shall it be international authority or is it better to impose legislation on national level? Or others questions; How to confiscate the bitcoins of an individual? How to freeze assets in the form of bitcoin? How to stop possible tax evasion? How to deal with money laundering? For many of the contemporary problems there is an existing solution.

4.3.3 Solution to Contemporary Problems

This solution is based upon an assumption that bitcoin must be obtained, somehow. Out of the two ways by which it is possible to obtain bitcoin the harder, slower and more expensive one is generating bitcoins. For that reason, bitcoins are usually bought. Every person who wants to purchase bitcoin or to sell it needs an intermediary. By purchasing or selling bitcoin everyone discloses certain amount of personal information relating to them. The 100% anonymity we spoke of above, might be maintained only within the Bitcoin network.

The contemporary problems are, therefore, solvable with legal duties that would require businesses to identify the customer and to conduct an anti-money laundering check of the transaction. Those legal duties shall be aimed on intermediaries who facilitate the bitcoin trades, on business that accept bitcoin as a medium of exchange, and on other business where their general scope of business is in connection with Bitcoin. This solution shall be able to bypass all of the challenges that are natural to decentralized peer-to-peer networks.

There are currently three comprehensive legal acts that are regarding solely Bitcoin and similar protocols and that operate this way. The best of them is the “Regulations of

¹³² It has not been proven that terrorist would use Bitcoin so far, but the possibility is still here. See: Isis: Bitcoin not used by Daesh terrorists, but dark web, Facebook and Twitter still common. *Ibtimes.co.uk* [online]. IBTimes Co., Ltd., 2016 [visited on 2016-06-29]. Available at: <http://www.ibtimes.co.uk/isis-bitcoin-not-used-by-daesh-terrorists-dark-web-facebook-twitter-still-common-1540319>

the Superintendent of Financial Services Part 200. Virtual Currencies”, which among the people in connection with Bitcoin is being referred as the BitLicense. We will regard the BitLicense in the chapter 4.6.

4.4 Theoretical Problems

Another set of problems we would like to address is labeled theoretical. It is so, for the reason that such problems might or might not occur. It will all depend on the future development of the Bitcoin.

We have pointed out that the contemporary problems are solvable by imposing the regulation on businesses which scope of business is closely in connection with Bitcoin. The future development of Bitcoin might change such approach and a different solution might be needed.

In the future, there is a certain possibility that bitcoin becomes capable of satisfying the two remaining criterions of money. Bitcoin might become stable enough to become a unit of account and store of value and if that happens, there might not be a sufficient reason why customers shall sell bitcoins for a legal tender. In such case the need for subsidiaries would be substantially lower and the imposed regulation on them would not provide enough of control.

One more of the future aspects, which depends more likely on the technical development of the Bitcoin is a further decentralization. At the moment the intermediaries such as a Bitcoin “exchanges”¹³³ are based centrally in sense that there is a central server and an owner. Problem is that all of those intermediaries might be completely decentralized as well. Those intermediaries might look exactly like Bitcoin today, as a peer-to-peer network without central authority, without a central server. Some of those already exists and some are in development.

In reaction to FBI shutting down the famous virtual drug marketplace Silk Road¹³⁴, there is a new working project called the OpenBazaar.

¹³³ Bitcoin exchange cannot be considered exchange in the legal meaning of exchange. It is rather a place where is possible to purchase and sell bitcoins.

¹³⁴ Silk Road was a marketplace located within the dark web offering various controlled substances for sale. The only possible way of payment was Bitcoin. The owner was located, prosecuted and given a life sentence. Another similar marketplace was created in reaction such as Silk Road 2.0., but subsequently been shut down as well.

“OpenBazaar is a different way to do online commerce. Instead of visiting a website, you download and install a program on your computer that directly connects you to other people looking to buy and sell goods and services with you. This peer to peer network isn't controlled by any company or organization - it's a community of people who want to engage in trade directly with each other.”¹³⁵

As much as its description might sound poetic, the reality is slightly different. It took only hours after launch of the OpenBazaar to facilitate the trade of first illicit goods - drugs.¹³⁶

Even though the author behind OpenBazaar rejects¹³⁷ any similarities to the Silk Road, it is used in the very same sense. The sale of illicit goods might be unwanted, but it is not the biggest problem. The problem is that OpenBazaar sets precedent on how to successfully create such programs that allow decentralization of standardly centralized entities.

Similar example is the B&C Exchange.¹³⁸ The developer promises creating a decentralized exchange that will facilitate the exchange of various types of “virtual currencies”, including bitcoin, without the need for a central authority. If such solution gets widely accepted and bitcoin’s price range will stabilize, it might be a serious problem for the regulators. As there will be a substantially lesser need for purchasing and selling bitcoin.

We do not think that the theoretical problems have a legal solution. The further decentralization cannot be solved legally. The regulators, first needs technology that would allow them to compete with the proceeding decentralization. At the moment it is possible to say that the law is one step behind.

¹³⁵ How does OpenBazaar work. *Zendesk.com* [online]. 2016 [visited on 2016-06-29]. Available at: <https://openbazaar.zendesk.com/hc/en-us/articles/207982443-How-does-OpenBazaar-work->

¹³⁶ Hours After Launch, OpenBazaar Sees First Drug Listings. *Coindesk.com*[online]., 2016 [visited on 2016-06-13]. Available at: <http://www.coindesk.com/drugs-contraband-openbazaar/>

¹³⁷ OpenBazaar founder: We aren't the next Silk Road. *Fortune.com* [online]. 2015 [visited on 2016-06-13]. Available at: <http://fortune.com/2015/06/25/openbazaar-not-silk-road/>

¹³⁸ BCExchange. Topic: ****MANDATORY UPGRADE REQUIRED**** [ANN] B&C Exchange - All users must upgrade [entry in a discussion forum]. In: *Bitcoin Forum: Bitcoin: Project Development* [online]. 21.05.04, 14:15 [visited on 2016-06-9]. Available at: <https://bitcointalk.org/index.php?topic=1033773.0>

4.5 The Need for Regulation Dedicated Only to Bitcoin

Comparing the Czech Republic to other countries in the world, the legal situation regarding bitcoin is above average. For instance, Croatia have not taken any measures regarding Bitcoin what so ever. In contrary to the other states of European Union, Croatia did not even issue a statement warning in regard to the possible threads of the use of Bitcoin. The only thing that Croatia acknowledges, is that bitcoin is not a currency, legal tender and electronic money. Further, we can mention Russia, which is drafting legislation that should ban the use of various “money surrogates” including bitcoin.¹³⁹ Russia seeks a criminal penalization for anyone who would use Bitcoin in very similar way such as Bolivia. We have shown our concerns that banning bitcoin is not the right approach.

The Czech Republic has slow, but steady approach. In 2013 Ministry of Finance, more specifically the Financial Analytic Unit, published instruction regarding the anti money laundering and Bitcoin.¹⁴⁰ The Czech National Bank at the start of the year 2014, has prepared a pamphlet stating what bitcoin is not.¹⁴¹ There is also upcoming novelization of the law no. 253/2008 Coll. on Selected Measures Against Legitimization of Proceeds of Crime and Financing Terrorism. This novelization will be covered in the subsequent chapter.

Nevertheless, we are of the opinion that the Czech Republic, shall take into account the need for a special – Bitcoin only regulation. Specific act on Bitcoin, or on virtual currencies, might help to solve tax issues by defining bitcoin. To the extent, the act might require specific license that would be needed in order to conduct a Bitcoin related business and various duties of the licensee such as a cyber security program, identification of customers, anti-money laundering precautions specific to virtual

¹³⁹ Bitcoin Users Would Face Jail Under Russian Cryptocurrencies Law. Bloomberg.com [online]. New York: BLOOMBERG L.P., 2016 [visited on 2016-04-12]. Available at: <http://www.bloomberg.com/news/articles/2016-04-28/russian-law-would-send-bitcoin-users-to-jail-as-cybercriminals>

¹⁴⁰ MINISTERSTVO FINANCÍ ČESKÉ REPUBLIKY. *METODICKÝ POKYN č. 2 Finančního analytického útvaru Ministerstva financí ze dne 16. září 2013 určený povinným osobám O PŘÍSTUPU POVINNÝCH OSOB K DIGITÁLNÍM MĚNÁM*[online]. Praha, 2013 [visited on 2016-07-09]. Available at: <http://www.mfcr.cz/cs/zahranicni-sektor/ochrana-financnich-zajmu/boj-proti-prani-penez-a-financovani-tero/novinky-fau/2013/digitalni-meny-14568>

¹⁴¹ ČNB. *Obchodování s bitcoiny: a Je k obchodování s bitcoiny nebo k jejich směně potřebné povolení ČNB?* [online]. Praha, 2014 [visited on 2016-07-29]. Available at: https://www.cnb.cz/cs/faq/obchodovani_s_bitcoiny.pdf

currencies, protection of customer assets, an amount of the registered capital of the company, type of liability of the operator, etc. Such step has taken the New York State of the United States of America.

The superintendent of New York State has issued an act labeled; Regulations of the Superintendent of Financial Services Part 200. Virtual Currencies. It is also being referred in a shorter collocation as BitLicense.

BitLicense is a vast legal material issued by the New York State Department of Financial Services that came into existence in August, 2015. It aims on any individual and or a company that conducts business relating to Bitcoin and similar protocols.

Even though some of the bitcoin firms located in New York decided to cease operating business relating Bitcoin in the state of New York,¹⁴² we are of the opinion that such approach is the only correct and possible as of now.

It should be noted that the BitLicense is often a target of criticism. The criticism highlights its principal cost, which is \$5,000¹⁴³, but realistically \$40,000¹⁴⁴ and the costs required to be in compliance with the BitLicense. It is therefore being argued that as such the BitLicense is only for large companies that have enough money to operate in conformity with BitLicense, as it requires a specific and expensive education of the licensees' employees, thorough background checks and expensive cybersecurity programs.

4.6 Comparing BitLicense to the Czech Legislation

At the very beginning we would like to say that we are aware that BitLicense is not ideal, that there are certain problems, but it is still the most comprehensive legal material regarding Bitcoin. It was the very first Bitcoin's only legal act and as such it

¹⁴² The 'Great Bitcoin Exodus' has totally changed New York's bitcoin ecosystem. Bizjournals.com [online]. New York, 2015 [visited on 2016-07-30]. Available at: <http://www.bizjournals.com/newyork/news/2015/08/12/the-great-bitcoin-exodus-has-totally-changed-new.htm>, or see: Bitcoin company ditches New York, blaming new regulations. Fortune.com [online]. New York: Time Inc., 2015 [visited on 2016-07-30]. Available at: <http://fortune.com/2015/06/11/bitcoin-shapeshift-new-york-bitlicense>

¹⁴³ see: section 200.5 Applications fees in DEPARTMENT OF FINANCIAL SERVICES CHAPTER I. REGULATIONS OF THE SUPERINTENDENT OF FINANCIAL SERVICES PART 200. VIRTUAL CURRENCIES.

¹⁴⁴ The Good, the Bad and the Ugly of the New York BitLicense. Paxful.com [online]. Paxful Inc., 2015 [visited on 2016-07-30]. Available at: <http://blog.paxful.com/the-good-the-bad-and-the-ugly-of-the-new-york-bitlicense/>

cannot be flawless. There is also a strong emphasis on the anti-terrorist financing and anti-terrorism in general, which in this scale is sort of special for the United States.

4.6.1 Virtual Currency Definition

BitLicense provides comprehensive legal definitions of crucial terms such as Virtual Currency Business Activity or Virtual Currency.

The Virtual Currency is defined both in positive sense and negative sense. In the positive sense it is defined as:

“Virtual Currency means any type of digital unit that is used as a medium of exchange or a form of digitally stored value. Virtual Currency shall be broadly construed to include digital units of exchange that

- (i) have a centralized repository or administrator;*
- (ii) are decentralized and have no centralized repository or administrator; or*
- (iii) may be created or obtained by computing or manufacturing effort.”¹⁴⁵*

In the negative sense the Virtual Currency is defined as:

“Virtual Currency shall not be construed to include any of the following:

(1) digital units that:

- (i) are used solely within online gaming platforms,*
- (ii) have no market or application outside of those gaming platforms,*
- (iii) cannot be converted into, or redeemed for, Fiat Currency or Virtual Currency, and*
- (iv) may or may not be redeemable for real-world goods, services, discounts, or purchases.*

(2) digital units that can be redeemed for goods, services, discounts, or purchases as part of a customer affinity or rewards program with the issuer and/or other designated merchants or can be redeemed for digital units in another customer affinity or rewards program, but cannot be converted into, or redeemed for, Fiat Currency or Virtual Currency; or

(3) digital units used as part of Prepaid Cards.”¹⁴⁶

¹⁴⁵ 200.2 Definitions letter p) Virtual Currency in Department of Financial Services Chapter I. Regulations of the Superintendent of Financial Services Part 200. Virtual Currencies.

¹⁴⁶ Id.

The Czech legislator is also coming up with its own definition of the Virtual Currency. It might be found in the draft of amendment to the law 253/2008 Coll. on Selected Measures Against Legitimization of Proceeds of Crime and Financing of Terrorism.

Under the draft of amendment, the Virtual Currency is defined as: “...*electronically stored unit disregard of its issuer, which is not a monetary unit pursuant to the act on Payment Systems, but is accepted as a payment for goods or services by other person than its issuer*¹⁴⁷.”

The Czech legislator was able to write a substantially shorter definition with very similar meaning. In our opinion, Czech definition is describing a general purpose instrument without issuer. Whereas the American approach describes thorough fully the difference between specific and general purpose instrument, landing bitcoin somewhere in the middle.

One of the differences between the two definitions is just verbal and that is the distinction between digital and electrical in the BitLicense Virtual Currency is stored digitally where as under the Czech definition is stored electronically, but that is essentially the very same type of storage.

Probably the most legally concrete difference we see, is that the Czech definition explicitly states that it does not see Virtual Currencies as money, whereas in the BitLicense the legislator does not draw such distinction.

At the moment it is maybe better to define that Virtual Currencies does not represent money, however as we have pointed out in the chapter 4.4 (*Theoretical Problems*), in future it might be a reason for a new definition, because the Virtual Currencies are in constant development and might theoretically satisfy the economic definition of money.

We would say that the Czech legislator had made it clear what the Virtual Currency is and what is not. In the BitLicense the approach is much wider, but the BitLicense takes into account the future development of Bitcoin and similar data protocols.

¹⁴⁷ Section 2 letter i) of the future draft of an Act no. 253/2008 Coll. o Selected Measures Against Legitimization of Proceeds of Crime and Financing Terrorism. In: ASPI [Legal information system]. Praha: Wolters Kluwer ČR [visited on 2016-03-26], also available at: <https://apps.odok.cz/veklep-detail?pid=KORN9XSEVDCD>. In the Czech original: “...*elektronicky uchovávaná jednotka bez ohledu na to, zda má nebo nemá emitenta, a která není peněžním prostředkem podle zákona o platebním styku, ale je přijímána jako platba za zboží nebo služby i jinou osobou odlišnou od jejího emitenta.*”

Where both of the definitions are, in our opinion, wrong, is the use of the nomenclature Virtual Currency. We have expressed our opinion regarding such nomenclature earlier in this work.

4.6.2 Virtual Currency Business Activity

Both of the acts also define the range of activities that are under the influence of such legislation. BitLicense once again has a wide approach, defining the Virtual Currency Business Activity as:

“Virtual Currency Business Activity means the conduct of any one of the following types of activities involving New York or a New York Resident:

- (1) receiving Virtual Currency for Transmission or Transmitting Virtual Currency, except where the transaction is undertaken for non-financial purposes and does not involve the transfer of more than a nominal amount of Virtual Currency;*
- (2) storing, holding, or maintaining custody or control of Virtual Currency on behalf of others;*
- (3) buying and selling Virtual Currency as a customer business;*
- (4) performing Exchange Services as a customer business; or*
- (5) controlling, administering, or issuing a Virtual Currency.*

*The development and dissemination of software in and of itself does not constitute Virtual Currency Business Activity.”*¹⁴⁸

The Czech legislator has specified the activities in question as the activities of a person, where: *“... the scope of business is to purchase, sell, store, administer or arrange on behalf of others the purchase and sale of Virtual Currency, alternatively provides other services in connection with Virtual Currency.”*¹⁴⁹

The BitLicense is logically connected to the New York residents, however in connection with the Bitcoin characteristics it might be a basis for illogical connections. If a New York resident would purchase bitcoins from say a Czech Bitcoin company

¹⁴⁸ Section 200.2 letter q) Virtual Currency Business Activity in Department of Financial Services Chapter I. Regulations of the Superintendent of Financial Services Part 200. Virtual Currencies.

¹⁴⁹ Section 4 paragraph 8 of the future amendment of an Act no. 253/2008 Coll. o Selected Measures Against Legitimization of Proceeds of Crime and Financing Terrorism. In: ASPI [Legal information system]. Praha: Wolters Kluwer ČR [visited on 2016-03-26], also available at: <https://apps.odok.cz/veklep-detail?pid=KORN9XSEVCDC>. In the Czech original: *“Jako předmět své podnikatelské činnosti kupuje, prodává, uchovává, pro jiného spravuje nebo zprostředkovává nákup nebo prodej virtuální měny, případně poskytuje další služby spojené s virtuální měnou.”*

should the Czech Bitcoin company be subjected to the BitLicense?

Pursuant to the section 200.3 letter (a) of the BitLicense that sets forth: “*No Person shall, without a license obtained from the superintendent as provided in this Part, engage in any Virtual Currency Business Activity.*”, the Czech Bitcoin company shall have, against all the logic in the world, a BitLicense for such trades.

How is the Czech Company supposed to know that it deals with the New York citizen, unless the customer says so? This construction will lead to a situation that no non-New York Bitcoin company will provide service to the New York residents.

We are of the opinion that such wide range is unreasonable. It would be enough to impose those limitations only on Bitcoin related businesses located in the New York State. We simply cannot imagine that some European company will obtain the license for the sole reason to be able to carry on with business with New York citizens.

Another flaw we have to address is the use of the word ‘nominal’ as used in the point (1) in the Virtual Currency Business Activity. The legislator clearly wanted to extract some non-financial transactions (in example transporting a physical bitcoin wallet¹⁵⁰) but failed to provide a clear border. In connection with Bitcoin, where bitcoin transmission as defined in BitLicense: “*Transmission means the transfer, by or through a third party, of Virtual Currency from a Person to a Person, including the transfer from the account or storage repository of a Person to the account or storage repository of a Person.*”¹⁵¹, it is especially necessary to define what the nominal means.

Does the BitLicense apply on company that acts as a transporter in case if a New York resident decides to sell his old physical bitcoin wallet, but in the wallet there is an amount of 0.2 bitcoin? Would it be any different that with an amount say 0.02 bitcoin? Maybe the word ‘nominal’ should have been defined as “in denomination not exceeding the amount of 1000 United States Dollars”. In this connection we also have to address the fact that the BitLicense does not state any amount that does not have to be subjected to the anti-money laundering requirements.

The Czech approach does have an exemption for trades not exceeding the amount of 1000 Euro: “*Obligated person performs the identification of a customer no later*

¹⁵⁰ For more information, please see: <https://bitcointrezor.com>

¹⁵¹ Section 200.2 letter o) Virtual Currency Business Activity in Department of Financial Services Chapter I. Regulations of the Superintendent of Financial Services Part 200. Virtual Currencies.

*then, when is apparent that the value of trade exceeds the amount of 1000 Euro, unless this act stipulate otherwise.*¹⁵² The relevant exemptions are stipulated in section 7, paragraph 2 of the law 253/2008 Coll.¹⁵³

This limit is for a practical - day to day use absolutely crucial. The operational costs that are imposed by the absence of such provision are often the source of the criticism of the BitLicense.

The Czech legal definition of Virtual Currency Business Activity is in our eyes better. The law shall be simple, effective and most importantly easily understandable. Those criterions are better satisfied by the Czech conception.

In the following subchapters we would like to introduce a few legal institutes that are stipulated in the BitLicense and the Czech law does not involve them. We believe that those institutes might help regulation Bitcoin in the Czech Republic, as such we would suggest, that if the Czech Republic would draft a Bitcoin specific act, this act should involve those following institutes.

4.6.3 Cyber Security Program

What we consider as a very good implementation and possible future inspiration for the Czech legislation is the BitLicense's Cyber Security Program. Under the BitLicense all of the licensees are required to develop and maintain a program that protects customers and licensees' data. The importance of the mandatory cyber security program is best illustrated on the multiple cases of a security breach followed by a subsequent theft of bitcoins.¹⁵⁴ Any licensee's cyber security program must, in accordance with the BitLicense, satisfy a five core functions.

¹⁵² Section 7 paragraph 1 of the future draft of an Act no. 253/2008 Coll. o Selected Measures Against Legitimization of Proceeds of Crime and Financing Terrorism. In: ASPI [Legal information system]. Praha: Wolters Kluwer ČR [visited on 2016-03-26], also available at: <https://apps.odok.cz/veklep-detail?pid=KORN9XSEV CDC>. In the Czech original: "*Povinná osoba provede identifikaci klienta nejpozději tehdy, kdy je zřejmé, že hodnota obchodu překročí částku 1 000 EUR, pokud tento zákon dále nestanoví jinak.*"

¹⁵³ Where probably the most relevant of them is the "suspicious trade". In the Czech original: "*podezřelý obchod*".

¹⁵⁴ Hackers Steal \$2 Million from Bitcoin Exchange In Hong Kong, Bounty Offered To Recover Funds. Forbes.com [online]. Southfield: Forbes Cohen Properties, 2016 [visited on 2016-05-30]. Available at: <http://www.forbes.com/sites/robertolsen/2016/05/24/hackers-steal-2-million-from-bitcoin-exchange-in-hong-kong-bounty-offered-to-recover-funds/#c597af011c72>, or see: Cryptsy Hacked: Bitcoin Worth \$USD 6 Million Stolen. Databreaches.net [online]. 2016 [visited on 2016-05-30]. Available at: <https://www.databreaches.net/cryptsy-hacked-bitcoin-worth-usd-6-million-stolen/>

First function is to identify. Licensee's security program must be able to locate internal and external risk, which requires a knowledge of the information stored within the licensee's data center. BitLicense highlights the knowledge of accessibility of such information.¹⁵⁵ To be legally obligated to know who might access what information is an important step to a greater transparency and liability, because many of the thefts of bitcoin that had happened in the past does not have a specific party at fault as no one knows, whether it was a breach from outside or inside.

Following core function are necessary, but very common so we just mention them for completeness. Second function is a protection of the information stored within the data systems. Third is a detection of breaches and intrusions and fourth is a respond to the detected threads. What is interesting is the fifth function.

The fifth function is to “*recover from Cyber Security Events and restore normal operations and services.*”¹⁵⁶ We have to again say that the legislator here did a very thorough work, because in history many of the businesses in connection with Bitcoin has been decimated by a security breaches and subsequently the customers had lost their investment. Under the BitLicense the licensee must expect such problems to occur and be able to carry on business afterwards, which might potentially save customers a lot of money.

The BitLicense further requires an existence of a written policy and procedures regarding a cyber security and also specific employee, who will oversee the implementation and enforcement of such policy. That is however, not the only personal requirement set forth in the BitLicense. Licensee must also employ a specific personnel to manage the core functions of the cyber security program.

The main problem in connection with the cyber security is its high cost. It is often argued that the BitLicense discriminates the starting companies and that obtaining and maintaining the license is extremely costly.¹⁵⁷ That might be true, but the problem is that those companies are willing to operate with people's funds.

¹⁵⁵ Section 200.16 letter a) part 1 in Department of Financial Services Chapter I. Regulations of the Superintendent of Financial Services Part 200. Virtual Currencies.

¹⁵⁶ Id. Section 200.16 letter a) par 5.

¹⁵⁷ The Real Cost of Applying for a New York BitLicense. Coindesk.com [online]. 2015 [visited on 2016-07-30]. Available at: <http://www.coindesk.com/real-cost-applying-new-york-bitlicense/>

Any company that operates with people's money is under very thorough legislation. Take for instance the bank license that must be satisfied under the Czech law.¹⁵⁸ Where just the registered capital must be at least 500,000,000 Czech Koruna that is over \$20 millions. Therefore, we honestly disagree with the opinions regarding the BitLicense as limiting in this sense. Those are the minimal standards that have to be met, to be able to create a satisfactory environment for other's people funds.

This kind of business is very profitable but also very risky, we therefore argue that, because of the high risks in connection with Bitcoin, only the well funded entities shall be able to conduct them.

4.6.4 Business Continuity and Disaster Recovery

Another particularly important requirement imposed by the BitLicense that we think the Czech legislation should involve in the future Bitcoin regulation is a recovery plan. Under the BitLicense the licensee must develop a plan: “...*reasonably designed to ensure the availability and functionality of the Licensee's services in the event of an emergency or other disruption to the Licensee's normal business activities.*”¹⁵⁹

Subsequently, BitLicense sets forth minimal requirements of such plan. The plan must involve both essential personnel and equipment, including documents, data and infrastructure. To the extent, the plan should involve alternate personnel for events of disaster, identify third parties and authorities that shall be contacted in case of the event of an emergency and of course a written process of a relevant training of all employees, where their role and responsibilities will be stipulated.

BitLicense provides minimum requirements for a business to cope up with an unexpected situation. As we have said in the previous chapter, this is crucial for any Bitcoin business. Bitcoin is still an early stage technology and as such relating businesses are vulnerable to many security risks. It is therefore, very important that such businesses are prepared for those events and sets forth plans that might be reviewed by authorities to ensure that such business is competent enough to handle other people's funds.

¹⁵⁸ Section 4 of an act no. 21/1992 Coll., the Banking Act.

¹⁵⁹ Section 200.17 letter a) in Department of Financial Services Chapter I. Regulations of the Superintendent of Financial Services Part 200. Virtual Currencies.

Here also applies the same as in the previous subchapter, it is necessary to know, who is liable in the event of an emergency. Most of the times the threat comes from outside of the business and the perpetrator will not be easily findable, if even findable. If, however, the business owner neglects the compliance with his own business continuity and disaster recovery plan he shall be liable as well so the customers have at least some chance to reclaim damages.

4.6.5 Custody and Protection of Customer Assets

Lastly, we would like to present the custody and protection of customer assets as described in BitLicense. BitLicense sets forth three core principles that must be followed by the licensee.

First rule is to maintain a trust account denominated in the United States Dollars maintained by a qualified custodian. As bitcoin at the moment cannot be considered a unit of account and store of value it is necessary for the protection of customers to make sure that the business operators have a certain amount of fiat currency. The designated amount, under the BitLicense depends on the decision of the superintendent.¹⁶⁰

We are of the opinion that the Czech legislator shall accept a similar concept where a business operating with bitcoins, shall have a surety bond in the Czech Koruna or Euro, in amount either proportional to the amount of Virtual Currency or an amount specifically stipulated by the corresponding Czech authority.

Second rule states that the licensee shall always held the same kind and same amount of Virtual Currency which is owned or obligated to the customer. This rule is beneficial for the customers as it prevents the licensee to use the Virtual Currency for his own satisfaction. In contrary to banks in Eurozone which have to held only 2% of its initial non-banking (customers) deposits or in United States of America, where the minimal reserve requirement is 10%. The Virtual Currency businesses shall hold 100% of the customer's deposits. Customers, therefore, might be sure that the Virtual Currency they deposit, will remain be retrievable in the same type and amount.

The third rule is closely connected to the second one. License is prohibited from from; *“selling, transferring, assigning, lending, hypothecating, pledging, or otherwise*

¹⁶⁰ Section 200.9 Custody and protection of customer assets, letter a, in Department of Financial Services Chapter I. Regulations of the Superintendent of Financial Services Part 200. Virtual Currencies.

using or encumbering assets, including Virtual Currency, stored, held, or maintained by, or under the custody or control of, such Licensee on behalf of another Person...”.¹⁶¹

The licensee might sell, transfer, or assign the Virtual Currency only if the rightful owner directs the licensee to do so. In other words, the licensee cannot manipulate with the entrusted assets, unless specifically asked to do so.

4.7 Summary

Bitcoin is a phenomenon that needs to be regulated. Bitcoin requires a systematic regulation, where an ideal approach is to develop a Bitcoin specific act. Partial regulation of Bitcoin might lead to a chaotic environment such as in case of Thailand. Banning Bitcoin might lead to development of black market such as in case of Bolivia.

The anonymity and decentralized character of Bitcoin presents two kinds of issues. We address them as contemporary and theoretical problems. The contemporary problems are, according to us, solvable by imposing specific regulatory requirements on the Bitcoin intermediaries and similar businesses. However, we do not see a legal solution to the theoretical problems as we think that it is more a question of technology development than of a legal regulation.

First Bitcoin act, which we refer to as the BitLicense, was issued by the New York State Department of Financial Services in the year of 2015. Even though this act is not flawless, there are certain conceptions and legal institutes that might be of an inspiration to the Czech legislator.

By comparison of the comparable parts of the BitLicense and the Czech upcoming legislation regarding Bitcoin and we conclude that BitLicense provides a slightly better definition of the Virtual Currency, but an unreasonably wide approach to the virtual currency business activity definition which results in an illogical number of recipients of such legislation.

BitLicense involves some further requirements that we think that should be among other, applied in the Czech Bitcoin legislation. Those requirements are; a potent cyber security plan that shall eliminate the threats of data breaches, business continuity and disaster recovery plan that shall handle the eventual crisis, and Bitcoin specific custody and protection of customers' assets such as a surety bond denominated in legal tender,

¹⁶¹ Id. letter c.

obligation to always keep the initial amount of the very same Virtual Currency, and prohibition from handling customers' assets otherwise than at their direction.

5 Conclusion

At the beginning, we have asked a simple question, what is Bitcoin? As this question itself is quite broad we have decided to compare bitcoin with money in economical and legal sense. In the second part of this thesis, we then address the regulatory issues in connection with Bitcoin.

Bitcoin is commonly referred to as a Virtual Currency. This nomenclature is incorrect. Bitcoin is not used within any virtual borders, but in digital economy in the very same sense as electronic money. Bitcoin, also cannot be considered currency for two reasons. First is that bitcoins are not considered to be a legal tender and second is that bitcoin does not satisfy the defining characteristics of money. Bitcoin is, therefore, neither virtual but digital and nor shall be considered a currency, but rather just a medium of exchange. Correct nomenclature for Bitcoin is a digital medium of exchange.

This work further inquiries, whether Bitcoin can be considered money. Money is defined by three core criterions. Medium of exchange, unit of account, and store of value. Bitcoin satisfies only one of those criterions and that is the medium of exchange. Bitcoin complies with the interpretation of medium of exchange as it is possible to transfer value using it. On the other hand, bitcoin is does not satisfy the interpretation of unit of account and store of value. Both of those criterions are not satisfied, because of the highly volatile character of Bitcoin. Bitcoin therefore, cannot be used as a measurement to express price nor as a store of value. Bitcoin thus cannot be considered money. Nevertheless, future less volatile Bitcoin might satisfy those criterions, and become money in economic sense. In connection with the monetary characteristics of Bitcoin, legally under the Czech law, bitcoin cannot be considered money as it does not comply with relevant legislations.

Thus, after the first chapter, to the question what is Bitcoin, we present an answer that Bitcoin is a digital medium of exchange that does not satisfy neither the economical definition of money nor the legal definition of money and currency.

Second part of this thesis takes into regard a fact that Bitcoin is being commonly referred to as a thing in a legal sense, but works on an assumption that Bitcoin is so unique that it might be legally something else than a thing in legal sense.

Legal theory takes into account either materialistic approach or idealistic approach to things. Materialistic conception sees thing as a corporeal object that is different from a person. Under the materialistic conception which was followed by the act 40/1964 Coll. the Civil Code until the year of 2014, Bitcoin would be considered another property value. As Bitcoin is a computer program it is intangible and it could not be considered a thing, as thing was always material.

Under the idealistic conception a thing in a legal sense is everything that is different from a person and serves the needs of people. We present four different angles at which it is possible to view at Bitcoin. Bitcoin might be considered the work of an author, a computer program, a right, and a thing without absolute proprietary right.

Bitcoin was created by an unknown author, but known or not the author inserted his personality into the Bitcoin's code. Every artwork, music or a painting, but also a computer program, resembles in its entirety its author character. The work carries inseparable essence of its author. The work therefore is not different from a person and cannot be considered a thing in a legal sense.

Usually computer program and its license are both considered an intangible thing in legal sense. Computer program legally consists of exclusive moral right and exclusive economic rights. The exclusive economic rights might be traded in the form of a license agreement. The situation regarding Bitcoin is different. Its MIT license regards only its copies, but Bitcoin itself has never been copied. Bitcoin is the very first implementation of an author that keeps itself unique, the primary code, cannot be duplicated, because any copy of the code would create a completely new Bitcoin. It would be a Bitcoin number two. It is therefore the work of an author. Bitcoin as the medium of exchange shall be considered as a part of the primary code as well because the intention of the author was to create a decentralized payment network, where the value would be transferred by bitcoin and as such it might be also considered the work, which was never licensed and therefore is not a thing.

Bitcoin as a medium of exchange has only one use and that is to transfer value. The only operation a person can conduct with bitcoin is to spent it, and therefore transfer it to a different bitcoin address. This option we denote as the opinion to transfer the opinion, because the bitcoins are never transferred the only thing that is transferred is the option to spent bitcoin. This construction might be considered a right, right to spent

bitcoin. Right is under the idealistic conception a thing in a legal sense. However, we express our concerns, whether we can such disposition, the option to transfer the option, consider control in the sense of usurpation as is required under the legal theory. We are of the opinion that the lack of control reminds more likely a possession than ownership.

As to the fourth case, Bitcoin might be considered a thing in a legal sense without the absolute proprietary rights. In an article "*Possession of information*" professor Telec argues that we might look at information as at a thing in legal sense without absolute proprietary rights. Further argues that the information might be of economic value, but cannot be inherited or owned, but might be possessed. Bitcoin could be considered an information. Bitcoin factually cannot be inherited, for the reason that bitcoin can be only transferred not advanced. It is hard to have absolute control over bitcoin as it is incorporated in a decentralized ledger which is located somewhere in cyberspace. The ledger either belongs to nobody or is the work of an author. In both cases the bitcoin cannot be owned but only possessed.

Nevertheless, the easiest and most practical approach for law is to consider Bitcoin and bitcoin a thing, even though in our mind bitcoin is not. We see as an another option to pronounce bitcoin money which would fit bitcoin much more. The Czech law also knows the term non-cash money, which might fit Bitcoin perfectly in future.

In the third part of this thesis we describe the need for systematic regulation and problems that the specific character of Bitcoin imposes on the regulator.

Bitcoin is a phenomenon that deserves to be regulated. Best option would be to set aside a specific act regarding only Bitcoin and similar data protocols. Currently, countries have different approaches. The worst approach might be shown on an example of Thailand where as of today no one still really knows whether Bitcoin is legal or illegal. Similarly, bad approach is in Bolivia where Bitcoin is banned, but still sold on black market.

The unique character of Bitcoin might present two kind of problems. Contemporary problems and theoretical problems. Contemporary problems arise out of the anonymous and decentralized character of bitcoin, but are solvable by specific regulation. The theoretical problems might happen in future and are at the moment unsolvable. It is possible that the decentralization and anonymity will progress. Intermediaries which

now might be regulated, because of their centralized character might be decentralized as well. The further decentralization shall not be regulated by law, but by technology.

In the United States of America in the state of New York there is already a first specific Bitcoin act. To the extent, Czech Republic has prepared its own definition of the Virtual Currency and Virtual Currency Business Activity.

In these two comparable parts of the BitLicense and the Czech upcoming legislation regarding Bitcoin, BitLicense provides thorough full definition of the Virtual Currency. The Czech definition sets forth that Virtual Currency is not money and that makes it for future use a little worse than the American equivalent.

On the other hand, the Czech regulation provides much better definition of the Virtual Currency Business Activity as the conception of an American equivalent is unreasonably wide.

The BitLicense further involves three requirements, which we think that should be part of the Czech Bitcoin legislation. First is cyber security program, a plan for protecting systems and data of the business owner and therefore subsequently the data and funds of customers.

The second requirement, which is the business continuity and disaster recovery, requires its licensees to develop a plan for an event of an emergency and a method for rebuilding the business and serving its customers after a disastrous event.

The third requirement is specific custody and protection of customer assets. Where the licensee is required to operate a surety bond denominated in legal tender for the protection of the customers' assets. Further, the licensee shall have the same amount of the same Virtual Currency that was entrusted to him by a customer, and shall never operate with customers unless specifically directed by the customer.

In the very end of this thesis, we would also like to shortly express our opinion on Bitcoin. We do not see Bitcoin only as a technology, digital medium of exchange or a thing in a legal sense. We see Bitcoin also as a philosophy, as a something that connects people who are not content with the contemporary financial world. We see bitcoins as a unique answer to the statement and concept; *"there is never enough money"*. Contemporary world economy is based on unlimited growth which is impossible in the long run. *"In the year of 1971 was the amount of private and public debts in US 1700 billions of United States Dollars. In the 2013 those debts were 58 000 billions of United*

*States Dollars.*¹⁶² The answer that Bitcoin gives is the revelation that there is too much money in the world which periodically causes crises. That the bank loans might not be necessary. That there is a different way.

We would like to end this thesis with a question. If the current financial world is about unlimited growth, why the unsung author of Bitcoin had never spent a single bitcoin if he supposedly has 1,148,800.00 of them, worth about 749,017,600.00 United States Dollars?¹⁶³

¹⁶² CERVENKA, Andreas. *Peníze: jakou mají cenu?: a čemu věřit v současném světě?*. Prague: Práh, 2014. p. 122-123 ISBN 978-80-7252-504-1. *In the Czech original: "V roce 1971 byla výše soukromých a veřejných dluhů v Americe 1700 miliard dolarů. V roce 2013 činily dluhy 58 000 miliard dolarů."*

¹⁶³ That is about 18.1 billions of Czech Korunas, see: The Well Deserved Fortune of Satoshi Nakamoto, Bitcoin creator, Visionary and Genius. *Bitslog.wordpress.com*[online]. San Francisco: Automattic, Inc., 2012 [visited on 2016-06-29]. Available at: <https://bitslog.wordpress.com/2013/04/17/the-well-deserved-fortune-of-satoshi-nakamoto/>

Sources

Books

CERVENKA, Andreas. *Peníze: jakou mají cenu?: a čemu věřit v současném světě?*. Prague: Práh, 2014. p. 122-123 ISBN 978-80-7252-504-1.

GERLOCH, A. *Teorie práva*. 6th edition. Pilsen: Vydavatelství a nakladatelství Aleš Čeněk, 2013, p. 141. Beckovy právnické učebnice. ISBN 978-80-7380-454-1.

HOLMAN, Robert. *Ekonomie*. 6th Edition. In Prague: C.H. Beck, 2016. Beckovy ekonomické učebnice. p. 446. ISBN 978-80-7400-278-6.

JANSA, Lukáš and Petr OTEVŘEL. *Softwarové právo: Definice softwaru, práva k softwaru a jeho ochrana, databáze*. 2nd. Edition. Brno: Computer Press, 2014, p. 31. ISBN 978-80-251-4201-1.

JÍLEK, Josef. *Peníze a měnová politika: Podstata tvorby peněz*. Prague: GRADA Publishing, a.s., 2004, p. 344. ISBN 8024707691.

KNAPP, V. *Teorie práva*. Prague: C.H. Beck, 1995, p. 70. Beckovy právnické učebnice. ISBN 80-7179-028-1.

KNAPP, V., KNAPPOVÁ, M. IN KNAPPOVÁ, M., ŠVESTKA, J., DVOŘÁK, J. A KOL. *Občanské právo hmotné*. 4th Edition. Prague: ASPI, 2006, p. 272 ISBN 9788073571313.

KOTÁB, Petr. *Finanční právo: Měna a peněžní oběh*. 6th Edition. Prague: C.H. Beck, 2012, p. 335. Beckovy právnické učebnice. ISBN 978-80-7400-440-7.

Kratochvíl, Z. and col. *Nové občanské právo*. Prague: Orbi s, 1965, p. 186

THOMAS, Lloyd Brewster. *Money, banking, and financial markets*. 5th ed. Mason, Ohio: Thomson/South-Western, 2006, p. 21. ISBN 0324176732.

HUBBARD, R. Glenn. *Money, the financial system, and the economy*. 5th ed. Boston: Pearson/Addison-Wesley, 2005, p. 14. ISBN 0321237854.

REEVE, Lovell. *Conchologia Systematica* vol. 2. London: Longman, Brown, Green and Longmans, 1842.

SEDLÁČEK, J. *Vlastnické právo: všeobecné nauky*. Prague: Wolters Kluwer Česká republika, 2012, p. XVI. Klasická právnícká díla (Wolters Kluwer ČR). ISBN 978-80-7357-758-2.

ŠVESTKA, J., SPÁČIL, J., ŠKÁROVÁ, M., and HULMÁK, M., *Občanský zákoník: komentář*. 2nd Edition. Prague: C.H. Beck, 2009, p. 442. Velké komentáře. ISBN 978-80-7400-108-6.

TELEC, I., TŮMA, P., *Autorský zákon, Komentář*, C. H. Beck, 2007, pp. 37-38.

The Concept of Money. PROCTOR, Charles. *MANN ON THE LEGALS ASPECT OF MONEY: Universal Means of Exchange*. Sixth edition. New York: Oxford university press, 2005, p. 28. ISBN 9780198260554.

THONDEL, ZUKLÍNOVÁ in DVOŘÁK, J., ŠVESTKA, J., ZUKLÍNOVÁ, M. a kol. *Občanské právo hmotné. Svazek 1. Díl první: Obecná část*. Prague: Wolters Kluwer ČR, 2013, 432 p. 372

Articles

COINING BITCOIN'S "LEGAL-BITS": EXAMINING THE REGULATORY FRAMEWORK FOR BITCOIN AND VIRTUAL CURRENCIES. *Harvard Journal of Law & Technology* [online]. 2014, 27(2), p. 596 [visited on 2016-07-27]. Available at: <http://jolt.law.harvard.edu/articles/pdf/v27/27HarvJLTech587.pdf>

ELIÁŠ, Karel. Věc jako pojem soukromého práva. *Právní Rozhledy* [online]. 2007, **2007**(4), 119 [visited on 2016-04-08]. Available at: beck-online.cz

ELIÁŠ, Karel. Vlastnické právo. Paradigmata českého pojetí pod zkušebním kamenem kontinentální právní kultury. *Právní Rozhledy* [online]. 2005, **2005**(22), 807 [visited on 2016-04-08]. Available at: beck-online.cz

HONG, J., B. LAMBSON, S. DHUEY a J. BOKOR. Experimental test of Landauers principle in single-bit operations on nanomagnetic memory bits. *Science Advances* [online]. 2016, **2**(3), e1501492-e1501492 [Visited on 2016-02-29]. DOI: 10.1126/sciadv.1501492. ISSN 2375-2548. Available at: <http://advances.sciencemag.org/cgi/doi/10.1126/sciadv.1501492>

KISH, LASZLO a CLAES GRANQVIST. Does Information Have Mass? *Proceedings of the IEEE* [online]. 2013, **101**(9), 1895-1899 [visited on 2016-02-29]. Available at: <https://arxiv.org/pdf/1309.7889.pdf>

PAPP, Jeremy. A Medium of Exchange for an Internet Age: How to Regulate Bitcoin for the Growth of E-Commerce. *Pittsburgh Journal of Technology Law and Policy* [online]. 2015, **15**(1), 39 [visited on 2016-07-24]. DOI: 10.5195/tlp.2014.155. ISSN 2164-800x. Available at: <http://tlp.law.pitt.edu/ojs/index.php/tlp/article/view/155>

SMEJKAL, Vladimír. Počítačová a internetová kriminalita v České republice. *Právní rozhledy* [online]. 1999, **1999**(12), 1 [see 2016-05-23]. Available at: <http://www.beck-online.cz/bo/document-view.seam?documentId=nrptcojzhfpxa4s7gezf643uojptcyi&groupIndex=5&rowIndex=0>

TELEC, Ivo. Držba informací. *Právní rozhledy* [online]. 2014, **2014**(2), 115 [Visited on 2016-04-12]. Available at: <http://www.beck-online.cz/bo/document-view.seam?documentId=nrptembrgrpxa4s7grpxg5dsl4ytcni&groupIndex=8&rowIndex=0>.

Research papers

BOEHM, Franziska a Paulina PESCH. *Bitcoin: A First Legal Analysis: with reference to German and US-American law*[online]. University of Münster, 2014. p. 4. [visited on 2016-05-06]. Available at: http://fc14.ifca.ai/bitcoin/papers/bitcoin14_submission_7.pdf

FBI DIRECTORATE OF INTELLIGENCE. *(U) Bitcoin Virtual Currency: Unique Features Present Distinct Challenges for Deterring Illicit Activity: Appendix A: Key Terms* [online]. 2012 [visited on 2016-03-23]. Available at: https://www.wired.com/images_blogs/threatlevel/2012/05/Bitcoin-FBI.pdf

IWAR. *Descriptions of SHA-256, SHA-384, and SHA-512: SHA-256: Description of SHA-256* [online]. p. 2., 1-36 [Visited on 2016-02-16]. Available at: <http://www.iwar.org.uk/comsec/resources/cipher/sha256-384-512.pdf>

JUNG, Yoonhyuk. *USERS' UNDERSTANDINGS OF THE VIRTUAL ECONOMY IN SOCIAL VIRTUAL WORLDS: CONSUMPTION AND ENTREPRENEURSHIP OF VIRTUAL GOODS* [online]. Louisiana State University, 2010. p. 7 [visited on 2016-07-23]. Available at: http://etd.lsu.edu/docs/available/etd-04092010-154422/unrestricted/Jung_Diss.pdf

KAPLANOV, Nikolei. *NERDY MONEY: BITCOIN, THE PRIVATE DIGITAL CURRENCY, AND THE CASE AGAINST ITS REGULATION* [online]. Philadelphia, 2012. p. 119, [visited on 2016-05-17]. Available at: <http://www.luc.edu/media/lucedu/law/students/publications/clr/pdfs/kaplanov.pdf>.
Temple University Beasley School of Law.

KOSHY, Philip, Diana KOSHY a Patrick MCDANIEL. *An Analysis of Anonymity in Bitcoin Using P2P Network Traffic* [online]. Pennsylvania State University, 2013 [visited on 2016-06-29]. Available at: http://fc14.ifca.ai/papers/fc14_submission_71.pdf.

KUTÍLEK, Lukáš. Právněfilozofické aspekty svobodné vůle. Právnická Fakulta Univerzity Karlovy, 2015. Diplomová práce.

LEHDONVIRTA, Vili. VIRTUAL ECONOMICS: APPLYING ECONOMICS TO THE STUDY OF GAME WORLDS [online]. Helsinki Institute for Information Technology HIIT, 2005 [visited on 2016-07-23]. Available at: http://vili.lehdonvirta.com/wp-content/uploads/2015/08/Virtual_Economics_Applying_Economics_to_the_Study_of_Game_Worlds_Proceedings_of_the_2005.pdf

NAKAMOTO, Satoshi. *Bitcoin: A Peer-to-Peer Electronic Cash System: 1. Introduction* [online]. p. 1., 1-9 [Visited on 2016-02-16]. Available at: <https://bitcoin.org/bitcoin.pdf>

SCHOLLMEIER, Rüdiger. *A Definition of Peer-to-Peer Networking for the Classification of Peer-to-Peer Architectures and Applications* [online]. Munchen, 2002 [Visited on 2016-05-28]. Available at: https://www.researchgate.net/publication/3940901_A_Definition_of_Peer-to-Peer_Networking_for_the_Classification_of_Peer-to-Peer_Architectures_and_Applications.

THORPE, Christopher, Jessica HAMMER, Jean CAMP, Jon CALLAS a Mike BOND. Virtual Economies: Threats and Risks [online]. Harvard University, 2007 [visited on 2016-07-23]. Available at: <http://www.eecs.harvard.edu/~cat/papers/vetr.pdf>

Legal sources

Act no. 121/2000 Coll. on Copyright, Right Related to Copyright and on the Amendment on Certain Laws.

Act no. 21/1992 Coll. the Banking Act

Act no. 253/2008 Coll. on Selected Measures Against Legitimization of Proceeds of Crime and Financing Terrorism

Act no. 284/2009 Coll. On Payment System

Act no. 40/1964 Coll. the Civil Code

Act no. 89/2012 Coll. the Civil Code.

BOLIVA. ERENCIA DE ENTIDADES FINANCIERAS — PROHIBICION DEL USO DE MONEDAS Y DENOMINACIONES MONETARIAS NO REGULADAS EN EL AMBITO DEL SISTEMA DE PAGOS NACIONAL. In: La Paz, 2014, Year 2014, No. 44. Available at: https://www.bcb.gob.bo/webdocs/01_resoluciones/044%202014.PDF.

ČNB. *Obchodování s bitcoiny: a Je k obchodování s bitcoiny nebo k jejich směně potřebné povolení ČNB?* [online]. Praha, 2014 [visited on 2016-07-29]. Available at: https://www.cnb.cz/cs/faq/obchodovani_s_bitcoiny.pdf

DEPARTMENT OF FINANCIAL SERVICES CHAPTER I. REGULATIONS OF THE SUPERINTENDENT OF FINANCIAL SERVICES PART 200. VIRTUAL CURRENCIES.

DŮVODOVÁ ZPRÁVA: Zvláštní část. In: Justice.cz [online]. 2011, p. 115., [visited on 2016-03-09]. Available at: http://obcanskyzakonik.justice.cz/images/pdf/Duvodova_zprava__leden_2011_.pdf,

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

Foreign Exchange Act, Available at: [http://www.cb.is/library/Skraarsafn---EN/Capital-surveillance/Foreign%20Exchange%20Act%20-%20Copy%20\(1\).pdf](http://www.cb.is/library/Skraarsafn---EN/Capital-surveillance/Foreign%20Exchange%20Act%20-%20Copy%20(1).pdf)

MINISTERSTVO FINANCÍ ČESKÉ REPUBLIKY. *METODICKÝ POKYN č. 2 Finančního analytického útvaru Ministerstva financí ze dne 16. září 2013 určený povinným osobám O PŘÍSTUPU POVINNÝCH OSOB K DIGITÁLNÍM MĚNÁM*[online]. Praha, 2013 [visited on 2016-07-09]. Available at: <http://www.mfcr.cz/cs/zahranicni-sektor/ochrana-financnich-zajmu/boj-proti-prani-penez-a-financovani-tero/novinky-fau/2013/digitalni-meny-14568>
the Berne Convention for the Protection of Literary and Artistic Works (1971)

WIPO Copyright Treaty (1996)

Online sources

A Living Currency. *Bitcoinwhoswho.com* [online]. [visited on 2016-05-27]. Available at: <http://bitcoinwhoswho.com/index/jercosinterview>

BCEXCHANGE. Topic: ****MANDATORY UPGRADE REQUIRED**** [ANN] B&C Exchange - All users must upgrade [entry in a discussion forum]. In: *Bitcoin Forum: Bitcoin: Project Development* [online]. 21.05.04, 14:15 [visited on 2016-06-9]. Available at: <https://bitcointalk.org/index.php?topic=1033773.0>

Bitcoin company ditches New York, blaming new regulations. Fortune.com [online]. New York: Time Inc., 2015 [visited on 2016-07-30]. Available at: <http://fortune.com/2015/06/11/bitcoin-shapeshift-new-york-bitlicense>

Bitcoin firm licensed to trade in baht. *Bangkokpost.com* [online]. The Post Publishing PLC, 2014 [visited on 2016-06-29]. Available at: <http://www.bangkokpost.com/archive/second-bitcoin-company-licensed-to-trade-in-baht/427339>.

Bitcoin now accepted by 100,000 merchants worldwide. *International Business Times* [online]. [visited on 2016-05-27]. Available at: <http://www.ibtimes.co.uk/bitcoin-now-accepted-by-100000-merchants-worldwide-1486613>

Bitcoin Price Chart with Historic Events. *Bitcoinhelp.net* [online]. [visited on 2016-05-27]. Available at: <https://bitcoinhelp.net/know/more/price-chart-history>

Bitcoin Users Would Face Jail Under Russian Cryptocurrencies Law. *Bloomberg.com* [online]. New York: BLOOMBERG L.P., 2016 [visited on 2016-04-12]. Available at: <http://www.bloomberg.com/news/articles/2016-04-28/russian-law-would-send-bitcoin-users-to-jail-as-cybercriminals>

Bitcoins back in the Thai marketplace. *Bangkokpost.com* [online]. The Post Publishing PLC, 2014 [visited on 2016-06-29]. Available at: <http://www.bangkokpost.com/archive/bitcoins-back-in-the-thai-marketplace/395952>.

Bitcoiny pomáhají šířit dětské porno. Nový projekt si na zločince posvítí. *Idnes.cz: ekonomika* [online]. Prague: Mafra a.s., 2016 [visited on 2016-05-29]. Available at: http://ekonomika.idnes.cz/londynsky-startup-pomuze-vyresit-zneuzivani-bitcoinu-v-byznysu-s-detskou-pornografi-g67-/eko-zahranicni.aspx?c=A160708_094912_eko-zahranicni_nio

Coins.ph Launches Peer-to-Peer Bitcoin App for Southeast Asia. *Coindesk.com* [online]. The Post Publishing PLC, 2015 [visited on 2016-06-29]. Available at: <http://www.coindesk.com/coins-ph-abra-style-bitcoin-app-southeast-asia/>.

Cryptsy Hacked: Bitcoin Worth \$USD 6 Million Stolen. *Databreaches.net* [online]. 2016 [visited on 2016-05-30]. Available at: <https://www.databreaches.net/cryptsy-hacked-bitcoin-worth-usd-6-million-stolen/>

DOTAZNÍK PRO Miroslava Singera: ČNB. *E-republika.cz* [online]. České Budějovice: spolek eRepublika, 2015 [visited on 2016-06-02]. Available at: <http://e-republika.cz/article3255-DOTAZNIK-PRO-Miroslava-Singera-ČNB>.

Drogovým dealerům zmizely dvě miliardy korun v bitcoinech. Čech vinu odmítá. *Idnes.cz: technet* [online]. Prague: Mafra a.s., 2016 [visited on 2016-05-29]. Available at: http://technet.idnes.cz/bitcoin-sheep-marketplace-kradez-d4q-/sw_internet.aspx?c=A131202_194657_sw_internet_pka

Failing banks, winning economy: the truth about Iceland's recovery. World Finance [online]. 2015 [visited on 2016-07-25]. Available at: <http://www.worldfinance.com/infrastructure-investment/government-policy/failing-banks-winning-economy-the-truth-about-icelands-recovery>

Hackers Steal \$2 Million From Bitcoin Exchange In Hong Kong, Bounty Offered To Recover Funds. Forbes.com [online]. Southfield: Forbes Cohen Properties, 2016 [visited on 2016-05-30]. Available at: <http://www.forbes.com/sites/robertolsen/2016/05/24/hackers-steal-2-million-from-bitcoin-exchange-in-hong-kong-bounty-offered-to-recover-funds/#c597af011c72>

Hours After Launch, OpenBazaar Sees First Drug Listings. *Coindesk.com* [online]., 2016 [visited on 2016-06-13]. Available at: <http://www.coindesk.com/drugs-contraband-openbazaar/>

How does OpenBazaar work. *Zendesk.com* [online]. 2016 [visited on 2016-06-29]. Available at: <https://openbazaar.zendesk.com/hc/en-us/articles/207982443-How-does-OpenBazaar-work->

How the Blockchain Can Help Authors Guild Fight Piracy. *Http://bitcoinist.net/* [online]. Brighton: Bitcoinist Ltd., 2015 [visited on 2016-02-29]. Available at: <http://bitcoinist.net/blockchain-help-authors-guild-fight-piracy/>

Isis: Bitcoin not used by Daesh terrorists, but dark web, Facebook and Twitter still common. *Ibtimes.co.uk* [online]. IBTimes Co., Ltd., 2016 [visited on 2016-06-29]. Available at: <http://www.ibtimes.co.uk/isis-bitcoin-not-used-by-daesh-terrorists-dark-web-facebook-twitter-still-common-1540319>

LASZLO. RE: Pizza for bitcoins? [entry in a discussion forum]. In: *Bitcoin Forum: Economy: Marketplace* [online]. 22. 05.10, 07:17 [visited on 2016-05-27]. Available at <https://bitcointalk.org/index.php?topic=137.0>

LASZLO. Topic: Pizza for bitcoins? [entry in a discussion forum]. In: *Bitcoin Forum: Economy: Marketplace* [online]. 18.05.10, 12:35 [visited on 2016-05-27]. Available at: <https://bitcointalk.org/index.php?topic=137.0>

Missing: hard drive containing Bitcoins worth £4m in Newport landfill site. *Theguardian.com* [online]. Alex Hern, 2013 [Visited on 2016-04-11]. Available at: <https://www.theguardian.com/technology/2013/nov/27/hard-drive-bitcoin-landfill-site>

Open Source Initiative. Opensource.org: The MIT License [online]. [visited on 2016-03-11]. Available at: <https://opensource.org/licenses/MIT>.

OpenBazaar founder: We aren't the next Silk Road. *Fortune.com* [online]. 2015 [visited on 2016-06-13]. Available at: <http://fortune.com/2015/06/25/openbazaar-not-silk-road/>

Podsvětí nejhlubšího internetu. DeepWeb & Bitcoin 3. díl. *Kurzy.cz* [online]. Prague: AliaWeb, spol. s r.o., 2016 [visited on 2016-05-30]. Available at: <http://www.kurzy.cz/zpravy/397613-podsveti-nejhlubsiho-internetu-deepweb--bitcoin-3-dil/>

Significant risk attached to use of virtual currency. Cb.is [online]. 2014 [visited on 2016-04-13]. Available at: <http://www.cb.is/publications-news-and-speeches/news-and-speeches/news/2014/03/19/Significant-risk-attached-to-use-of-virtual-currency/>

SÝKORA, Matěj. Autorské dílo ve světle právního pojetí věci v novém občanském zákoníku. In: Fairart.cz [online]. Praha, 2014 [visited on 2016-03-12]. Available at: <http://www.fairart.cz/blog/autorske-dilo-ve-svetle-pravniho-pojeti-veci-v-novem-obcanskem-zakoniku/>.

The 'Great Bitcoin Exodus' has totally changed New York's bitcoin ecosystem. Bizjournals.com [online]. New York, 2015 [visited on 2016-07-30]. Available at: <http://www.bizjournals.com/newyork/news/2015/08/12/the-great-bitcoin-exodus-has-totally-changed-new.htm>

THE BRITISH COMPUTER SOCIETY. The Digital Economy [online]. [visited on 2016-02-14]. Available at: https://policy.bcs.org/sites/policy.bcs.org/files/digital%20economy%20Final%20version_0.pdf

The Good, the Bad and the Ugly of the New York BitLicense. Paxful.com [online]. Paxful Inc., 2015 [visited on 2016-07-30]. Available at: <http://blog.paxful.com/the-good-the-bad-and-the-ugly-of-the-new-york-bitlicense/>

The Real Cost of Applying for a New York BitLicense. Coindesk.com [online]. 2015 [visited on 2016-07-30]. Available at: <http://www.coindesk.com/real-cost-applying-new-york-bitlicense/>

The Well Deserved Fortune of Satoshi Nakamoto, Bitcoin creator, Visionary and Genius. *Bitslog.wordpress.com*[online]. San Francisco: Automattic, Inc., 2012 [visited on 2016-06-29]. Available at: <https://bitslog.wordpress.com/2013/04/17/the-well-deserved-fortune-of-satoshi-nakamoto/>

Trading suspended due to Bank of Thailand advisement. *Bitcoin.co.th* [online]. Bitcoin Co. Ltd, 2013 [visited on 2016-06-29]. Available at: <https://bitcoin.co.th/trading-suspended-due-to-bank-of-thailand-advisement>.

Abstract in English

The motivation for this thesis is to analyze Bitcoin as Bitcoin is still a new phenomenon and requires an economical, legal, and legislative evaluation. In this thesis we seek an answer to the question what is Bitcoin.

This thesis is divided into three main blocks, within them we use analytical, descriptive, and comparative methods. In the first part, we aim mostly on the economic side of Bitcoin, comparing Bitcoin to money in general sense. In the second part, we argue whether Bitcoin shall be considered a thing in a legal sense under the Czech law. In the third part, we describe the current Bitcoin's regulatory situation and suggest a drafting of Bitcoin specific regulation.

The conclusion of this thesis is that Bitcoin is a digital medium of exchange that cannot be considered money or currency. To the extent, Bitcoin might be interpreted in ways where it does not satisfy the legal definition of a thing in legal sense, but for regulatory purposes it shall be, at least for now, considered a thing in legal sense. We also suggest that Bitcoin shall be systematically regulated by imposing various duties on persons who's scope of business is relating to the Bitcoin.

Abstract v českém jazyce

Motivací pro tuto diplomovou práci je analýza Bitcoinu, neboť Bitcoin je stále ještě nový fenomén a vyžaduje ekonomické, právní a legislativní zhodnocení. V této práci hledáme odpověď na otázku co je to Bitcoin.

Tato práce je rozdělena do tří bloků, v jejich rámci používáme analytické, popisné a komparativní metody. V první části se zejména zaměříme na ekonomickou stránku Bitcoinu porovnáním Bitcoinu a generální pojetí peněz. V druhé části diskutujeme, zda by v rámci českého práva měl být Bitcoin věcí v právním smyslu. Ve třetí části popisujeme současnou situaci právní úpravy Bitcoinu a navrhuje, aby byl vytvořen zákon o Bitcoinu.

Závěrem této práce je, že Bitcoin je digitální prostředek směny, který nemůže být považován ani za peníze ani za měnu. Bitcoin může být právně interpretován i způsoby, kdy nebude moci být považován za věc v právním smyslu, ale pro účely regulace by měl být, alespoň v současné době, považován za věc v právním smyslu. Navrhujeme, aby Bitcoin byl systematicky regulován tím, že na osoby jejichž předmětem podnikání je Bitcoin, budou uvaleny odpovídající povinnosti.

Teze v českém jazyce

Bitcoin – Právní Aspekty a Regulace

Úvod

Když v roce 2010 došlo k první materiální transakci za pomoci bitcoinu, nejednalo se o platbu. Uživatel Laszlo sice na populárním Bitcoinovém¹⁶⁴ fóru napsal, že zaplatí 10 000 bitcoinů za dvě pizzy a po úspěšné transakci dokonce informoval, že koupil 2 pizzy, ale z ekonomického a právního pohledu se jednalo o směnný obchod. V té době nebylo možné považovat bitcoin za peníze, neboť nebyl běžně přijímán jako platidlo. Otázka tedy je, co je to Bitcoin?

Z technického hlediska lze Bitcoin považovat za decentralizovanou peer-to-peer síť, jejímž prostřednictvím lze posílat hodnotu. Tato síť postrádá centrální autoritu, která by síť řídila a ověřovala správnost jednotlivých transakcí. Naopak jsou si všichni účastníci této sítě rovni a jednotlivé transakce ověřují společně. Každá transakce představuje zprávu, jejíž obsahem je zašifrovaný alfanumerický text, jenž se označuje jako bitcoin. Bitcoin je jedinečný svým přístupem k zamezení vícenásobného utracení jednotlivého platidla - bitcoinu. Již tradičním problémem digitálních dat je totiž možnost jejich neomezeného kopírování.

Autor Bitcoinu tento problém vyřešil. Napsal zdrojový kód Bitcoinu tak, že Bitcoinová síť zaznamenává v paměti počítače všechny transakce, které se kdy staly a stanou. Takto je možné zamezit, aby jeden účastník utratil ten samý bitcoin více než jednou. Pokud by se o to pokusil, Bitcoinová síť by kontrolou zjistila, že takový bitcoin už utracen byl a znovu by jej nepřijala. Technické řešení spočívá v tom, že každá transakce je nejprve oznámena celé Bitcoinové síti a ve stejném okamžiku je nesmazatelně datována. Celá Bitcoinová síť tedy dostává informaci, že konkrétní IP adresa a v konkrétním čase vyvolala transakci. Počítače následně ověří, zda transakci se stejným datem a IP adresou již jednou nezaznamenaly a pokud ne, zařadí ji do bloku transakcí čekajících ke zpracování. Každých 10 minut počítače uzavřou jeden blok a transakce, které jsou uvnitř zahrnuty, se potvrdí. Počítač, který svou výpočetní silou uzavře blok jako první, je sítí odměněn ve formě bitcoinů. Každý jednotlivý blok má

¹⁶⁴ Rozlišujeme mezi Bitcoinem s velkým B a bitcoinem s malým b. Bitcoin je souhrnné označení pro technologii, síť a celý projekt, zatímco bitcoin je označení pouze pro prostředek směny.

specifické označení, které navazuje na předchozí blok. Bitcoinová síť označení porovná s předcházejícím blokem, a pokud dojde k závěru, že je všechno v pořádku, zamkne bloky ve správném pořadí do sebe a vytvoří řetěz. Od tohoto principu je odvozen anglický název pro tento postup - Blockchain.

Technická stránka Bitcoinu je dnes již velmi dobře známa, ale otázkou zůstává, jak je to s ekonomickou, právní a legislativní stránkou Bitcoinu. Tato práce si klade za cíl odpovědět na otázku: Co je to Bitcoin? V této souvislosti je v práci kladen důraz na porovnání bitcoinu s penězi, dále pak na posouzení, zda je možné bitcoin považovat za věc v právním smyslu. Z legislativního pohledu se práce věnuje potřebě systematické regulace Bitcoinu. Představuje problémy, které nová technologie přináší a navrhuje převzetí několika institutů z americké právní úpravy.

1. Peněžní aspekty bitcoinu

Bitcoin bývá označován jako virtuální měna. Toto označení je však přinejmenším nepřesné. Přídavné jméno virtuální je dlouhodobě spojováno s počítačovými hrami, kde v umělém – virtuálním prostředí, existuje kvazirealita, do které vstupuje hráč prostřednictvím simulovaného charakteru. Pro peněžní prostředí počítačových her se dokonce vžilo spojení virtuální ekonomika.

Také Evropská Centrální Banka označuje Bitcoin a jemu podobné protokoly za virtuální měny. Dokonce shodně argumentuje i americká FBI. Nejhlubší analýzu virtuální měny provádí v pamfletu „Schémata virtuálních měn“ právě Evropská Centrální Banka. Tato banka dělí virtuální měny pomocí tří různých schémat. Uzavřené virtuální schéma, které není nijak spojeno s reálnou ekonomikou. Jako příklad lze uvést počítačovou hru, kde hráč vydělává peníze hraním a utrácí je pouze v rámci hry. Druhým typem je takzvané jednosměrné schéma, kdy uživatel může nakoupit virtuální měnu za zákonné platidlo, ale použít virtuální měnu může pouze ve hře. Třetím typem pak je dvousměrné schéma, které se vyznačuje tím, že uživatel může nakoupit i prodat virtuální měnu za zákonné platidlo. Jako příklad třetího typu je uváděn Linden Dolar. Linden Dolar je označení pro virtuální peníze ze online počítačové hry Druhý Život.

Evropská Centrální Banka nahlíží na Bitcoin jako na dvousměrné schéma tedy jako třetí typ. S tímto pojetím nelze souhlasit. Bitcoin je především velmi odlišný od uvedených virtuálních Linden Dolarů. Bitcoin není centralizovaně vydáván a má předem omezený počet bitcoinů. Bitcoin také nemůže být centrálně řízen. Hlavním

rozdílem je, že bitcoin nikdy neměl specifický účel. Linden Dolary mají být užity především v rámci hry. Bitcoin může být užíván velmi podobně jako elektronické peníze. Bitcoin tedy již od svého počátku byl všeobecným prostředkem směny, neomezen žádnými virtuálními hranicemi, ba naopak byl vždy součástí globální digitální ekonomiky.

Máme za to, že bitcoin by neměl být označován jako virtuální, neboť je elektronicky uchovávan a představuje existující stopu na datovém úložišti. Data označujeme vždy jako digitální, správné označení pro Bitcoin je tedy digitální. Podobně nesprávná je i druhá část označení a sice „měna“. Bitcoin není vydáván žádnou státní autoritou nebo měnovou unií. Nelze ho považovat za konkrétní peněžní prostředky, jejichž přijímání by bylo možno vynutit zákonem. Na bitcoin proto nelze nahlížet jako na měnu. Správné označení bitcoinu je digitální prostředek směny.

Do právního a ekonomického pohledu na Bitcoin vnesl z počátku nejvíce světla svým přístupem Island. Island vymezil bitcoin jako cosi, co je odlišné od zboží a služeb. Islandské pojetí přibližuje bitcoin investičnímu nástroji, který je schopen přenosu hodnoty. Podobný názor měl i soud Evropské unie, když uzavřel, že bitcoin by měl být pro daňové účely považován za prostředek směny ve smyslu směrnice Evropské unie 2006/112/EC.

Nejběžnějším prostředkem směny jsou peníze. Bitcoin svým nehmotným charakterem připomíná elektronické peníze. Porovnáme-li zákonného vymezení elektrických peněz a Bitcoin, docházíme k názoru, že Bitcoin za elektrické peníze považován být nemůže. Bitcoin je sice uchovávan elektronicky a přijímán osobami odlišnými od vydavatele, ale ostatní definiční znaky již nenaplnuje. Bitcoin není centrálně vydáván a tudíž nemůže představovat obligaci vůči jeho vydavateli tak jako elektronické peníze. Stejně tak členské státy nejsou schopny zajistit, aby decentralizovaný vydavatel bitcoinů přijímal bitcoiny zpět za cenu, za kterou byly primárně nakoupeny. Minimálně už proto, že bitcoiny jsou přidělovány za odvedenou práci, nákup či prodej bitcoinů je až prostředek redistribuce.

Elektronické peníze jsou nicméně pouze jedním typem peněz. Na peníze je potřeba nahlížet jako na esenci, tedy peníze mohou být vše, co lidé přijímají, protože jsou si vědomi, že je všichni lidé přijímají.

Peníze mají tři definiční znaky. Prvním znakem je, že peníze jsou schopny plnit funkci prostředku směny. Tento požadavek bitcoin splňuje, neboť jeho užitím lze převést hodnotu. Druhým definičním znakem peněz je, že jsou schopny sloužit jako účetní jednotka, tedy že jimi lze vyjádřit cenu jiného objektu. Bitcoin tento definiční znak nesplňuje, neboť přestože je používán jako prostředek směny, ceny jednotlivých služeb či zboží, které si lze za bitcoin koupit, jsou vyjádřeny zákonným platidlem a pouze ve velmi malém procentu případů je cena vyjádřena v bitcoinech. Bitcoin funkci účetní jednotky tedy neplní. Posledním definičním znakem peněz je schopnost udržet hodnotu v čase. Ani zde bitcoin požadavky definičního znaku není schopen naplnit. Bitcoin je charakteristický vysokou volatilitou, jeho cena se v závislosti na nabídce a poptávce mění velmi rychle, nelze tedy říci, že by byl z dlouhodobého hlediska schopen udržovat konstantní hodnotu. Bitcoin nenaplnuje dva ze tří definičních znaků peněz, není možné ho tedy za peníze považovat.

O bitcoinu nelze uvažovat jako o penězích ani podle právního vymezení, neboť není uveden v §2 zákona č. 284/2009 Sb. zákon o platebním styku. Nabízí se sice úvaha, že by bitcoin mohl představovat bezhotovostní peníze, ale vzhledem k tomu, že bitcoin neplní definiční znaky základního ekonomického vymezení peněz, není tato úvaha v současné době přijatelná.

Bitcoin tedy není penězi a proto nemůže být ani měnou, neboť měna jsou zákonem uznané, konkrétní a konkretizované peníze, jejichž přijímání je vynutitelné zákonem. Na druhou stranu ale máme za to, že nelze vyloučit, že v budoucnu bitcoin dva zbývající znaky peněz naplní a tím se stane penězi v ekonomickém smyslu. Označení Bitcoinu ve smyslu virtuální měny je nepřesné a Bitcoin by takto označován být neměl. Na Bitcoin lze nahlížet jako na digitální prostředek směny.

2. Právní aspekty Bitcoinu

Bitcoin je v České Republice obecně považován za věc v právním smyslu. Jedním z důvodů vzniku diplomové práce však byl náš názor, že Bitcoin a tedy i bitcoin je natolik jedinečný, že by mohl být něčím jiným.

Na bitcoin jako na věc je třeba nahlížet jako na objekt právních vztahů. Pojetí věci v právu lze rozdělit z pohledu materialistického a idealistického přístupu. Materialistický přístup byl charakteristický pro zákon č. 40/1964 Sb. Občanský Zákoník. Podle tohoto zákona bitcoin skutečně věcí nebyl, neboť materialistický přístup

považuje za věci pouze ty objekty, které mají hmotnou podstatu, což Bitcoinu nelze přiznat. Protože je Bitcoin počítačový program bez hmotné podstaty, uzavíráme, že se podle zákona 40/1964 Sb. Občanský Zákoník, jednalo o takzvanou jinou majetkovou hodnotu, což je v souladu se soudobým právním pojetím softwaru.

Účinností zákona č. 89/2012 Sb. Občanský Zákoník, vstupuje do českého práva idealistické pojetí věci. Ve světle idealistického pojetí věci je možné nahlížet na Bitcoin pod více úhly. Idealistický přístup vidí věc jako vše, co je rozdílné od osoby, slouží k potřebě lidí a je objektivně kontrolovatelné.

V rámci idealistického pojetí lze nahlížet na Bitcoin čtyřmi způsoby. První možností je posuzovat Bitcoin jako autorské dílo, chráněné autorským zákonem č. 121/2000 Sb. Autorské dílo nespĺňuje pojetí věci v právním smyslu, neboť nelze říci, že je odlišné od osoby. Každý autor zanechává ve své tvorbě neoddělitelnou součást sebe sama. Tak jako malíř má své specifické tahy štětcem, kterými se stane známým a jeho díla jedinečná, tak i programátor má svůj specifický styl psaní programového kódu. Bitcoin může být považován za autorské dílo, byť jeho autor není znám.

Druhá možnost dle našeho názoru je pohlížet na Bitcoin jako na specifický počítačový program. Počítačový program bývá v praxi považován za věc. Autorský zákon sice v §65 chrání počítačový program jako literární dílo, ale zároveň tento zákon stanovuje, že se autorské dílo skládá ze dvou druhů práv a sice z výlučných osobnostních práv a z výlučných majetkových práv. Vzhledem k tomu, že výlučná osobnostní práva jsou nepřevoditelná, lze za věc v právním smyslu považovat pouze tu část práv, kterou lze kontrolovat a tedy i převést, což jsou výlučná majetková práva. Počítačový program tak může být jak autorským dílem tak i věcí v právním smyslu. Aby mohlo být s autorským dílem ekonomicky a po právu nakládáno, výlučná majetková práva se převádí licenční smlouvou.

Bitcoin byl licencován pod MIT licenci, která dovoluje bez větších omezení, užívat kopie programu bezplatně. Specifikem Bitcoinu ovšem je, že ten kód, který tvoří Bitcoinovou síť, tedy Bitcoin jako celek, nemůže být kopírován. Pokud by byl kopírován, vytvořil by novou síť, vytvořil by druhý Bitcoin. Jedná se tak o stále první verzi programu o autorské dílo, které licencované nikdy nebylo. Na Bitcoin lze znovu nahlížet jako na autorské dílo, jehož výlučná majetková práva nabyla nikdy delegována.

Je bitcoin jako prostředek směny je také autorským dílem, ač nebyl vytvořen přímo autorem, ale až působením programu? Záměrem autora bylo vytvořit platební síť, v rámci této sítě je bitcoin prostředkem směny. Lze si jen těžko představit, že za takových okolností autor nechtěl stvořit bitcoin. Je jasné, že autor vznik bitcoinů předpokládal a jeho cílem bylo, aby je program vytvořil. Je tedy možné nahlížet na i bitcoin jako na předmět autorského práva, čili jako na autorské dílo. Pod tímto úhlem pohledu bitcoin není věcí v právním smyslu.

Třetí způsobem jak lze pohlížet na bitcoin, je oprávnění. Bitcoin nedává uživateli mnoho možností jak s ním nakládat, je možné ho pouze převádět. Z tohoto pohledu bitcoin představuje pouze možnost převést na někoho tuto možnost převodu. Vzhledem k tomu, že Bitcoin v podstatě dovoluje tento typ převodu, lze tuto možnost považovat za oprávnění. Oprávnění je v rámci idealistického pojetí věci považováno za věc v právním smyslu.

Problematická může být otázka ovladatelnosti tedy kritérium kontroly. Limitující oprávnění užití bitcoinu má totiž spíše znaky držby než vlastnictví. Je otázkou zda bitcoiny, které jsou součástí prvotního počítačového kódu, mohou tak jako běžná věc, být usurpovány jeho uživateli. S bitcoiny lze nakládat pouze v rámci Bitcoinové sítě, nelze si je přivlastnit, neboť je z této sítě nelze odebrat. Bitcoin lze držet a převádět, ale v této koncepci mu chybí absolutní majetková práva. Bitcoin ve smyslu oprávnění lze považovat za věc v právním smyslu, ale lze ho pouze držet, nikoliv vlastnit, což pro věcné vymezení ovšem nemá význam.

Poslední způsob pohledu je koncepce pana profesora Telce, který tvrdí, že ve světle idealistického pojetí věci v právu, lze nahlížet na informace jako na věci v právním smyslu které postrádají absolutní majetková práva. Telec uvádí příkladem recept na rybí polévku a tvrdí, že takový recept sice splňuje zákonné znaky věci, ale zároveň není možné s ním stejným způsobem nakládat. Neboť takové věci nepožívají dědické a vlastnické právo. Uzavírá, že takové ekonomické hodnoty lze pojmově považovat za věci, věci ničí, které nelze vlastnit, ale pouze oprávněně držet.

Stejným způsobem lze nahlížet i na bitcoin. Bitcoin je velmi podobný uvedenému příkladu receptu na rybí polévku. Bitcoin nelze zdědit, neboť povaha bitcoinu nedovoluje aby byl postoupen. Právo vyžaduje, aby dědictví bylo postoupeno na základě právní události - smrti. Bitcoin však může být převeden pouze na základě

právního jednání, neboť jakmile někomu sdělíme privátní klíč, který slouží k převodu bitcoinu, dáváme mu tím plnou kontrolu nad bitcoinem. Takovým to jednáním dochází k plnému předání dispozice s bitcoinem a tedy k převodu. Na druhou stranu, pokud nesdělíme privátní klíč nikomu a zemřeme, pak je bitcoin neovladatelný a dispozice s ním je navždy ztracena, nedochází tedy k automatickému postoupení. Postoupení není fakticky možné.

Jak již bylo zmíněno, bitcoin není ovladatelný ve smyslu, že by ho mohl někdo usurpovat pro sebe tak jako běžnou věc. Vzhledem k tomu, že bitcoiny jsou vždy uloženy na decentralizované síti, která buď nepatří nikomu nebo je autorským dílem, lze je jen těžko vlastnit. Je možné se domnívat, že je-li bitcoin věc ničí, pak ho lze v rámci práva držet.

Co je tedy Bitcoin? Pro účely regulace a současného pojetí by na bitcoin mělo být nahlíženo jako na právo. Právo převést toto právo na další osobu. Takovéto právo je idealistickou koncepcí považováno za věc v právním smyslu. Vedle toho bitcoin nemůže být v současné době považován za peníze v ekonomickém ani právním smyslu.

Máme však k pojetí bitcoinu jako věci v právním smyslu výhrady. Do tohoto pojetí zasahuje zejména autorské právo a také zde prakticky chybí možnost absolutní kontroly nad bitcoinem. Bitcoin by si zřejmě zasloužil vlastní právní kategorii. Máme za to, že v budoucnu by bitcoin mohl splňovat pojetí bezhotovostních peněz.

3. Aspekty regulace Bitcoinu a související problémy

Bitcoin je velmi často spojován s kriminální činností. Zatímco významné autority shledávají Bitcoin mnohdy jako nezajímavý či nedůležitý, různí kriminální činitelé považují Bitcoin za revoluci v legalizaci peněz pocházejících z trestné činnosti.

Na Bitcoin je potřeba pohlížet jako na revoluční technologii, přelomový vynález a novou filosofii. Je zároveň potřeba k němu i tak přistupovat. Především by si Bitcoin zasloužil vlastní zákonnou úpravu.

Jednotlivé státy ovšem pohlíží na Bitcoin různě. Jako špatný příklad lze uvést Bolívii, která se rozhodla celkově Bitcoin zakázat. Takový zákaz se ale jen velmi těžko vynucuje. Na internetu lze i dnes, několik let po zákazu, najít několik zdrojů, kde lze bitcoin koupit přímo v La Pazu největším městě Bolívie. Dalším a možná ještě horším případem je regulace v Thajsku, kde dodnes nikdo přesně neví, zda je či není Bitcoin

zakázaný. Bitcoin byl nejdříve dovozen, pak zakázán pak znovu povolen, ale během pár dnů byla thajská veřejnost informována, že Bitcoin by stále mohl být nelegální.

Pravdou je, že Bitcoin sám o sobě představuje pro regulaci nejen jeden problém. Tato diplomová práce rozděluje tyto problémy na současné a teoretické. Současné problémy jsou ty problémy, se kterými se již regulace potýká, zatímco teoretické problémy se odvíjejí od budoucího vývoje Bitcoinu.

Za současnými problémy Bitcoinu stojí jeho klíčové vlastnosti, kterými jsou decentralizace a anonymita. Bitcoin je decentralizován po celém světě, chybí mu centrální autorita, na kterou by se daly uvalit sankce nebo přímá regulace. V Bitcoinové síti chybí centrální server, který by v případě nutnosti mohl být vypnut.

Bitcoin je zároveň částečně anonymní, neboť uživatele v síti reprezentují pouze jednotlivé adresy, ze kterých jsou posílány transakce. Transakce nevyžaduje, aby uživatel uváděl o sobě cokoli jiného než IP adresu. Bylo ovšem prokázáno, že za určitých okolností lze pomocí statistických metod dohledat, kdo používá jakou Bitcoinovou adresu. Bitcoinovou adresu lze dohledat a spojit s konkrétním uživatelem i pomocí internetového vyhledávače, protože je celkem časté, že uživatelé v očekávání bitcoinů svou adresu zveřejní i se svým jménem.

Na druhou stranu je potřeba říci, že v rámci Bitcoinové sítě lze zůstat absolutně anonymní. Bitcoinových adres lze vytvořit pro lidskou potřebu v podstatě nekonečné množství a za použití speciálního softwaru lze vystupovat pod jinou IP adresu, než kterou počítač doopravdy má. Je tedy možné absolutně anonymně poslat bitcoiny na jinou adresu či podpořit organizace jako jsou Wikileaks nebo takzvaný islámský stát.

Pozitivní je, že současné problémy jsou celkem dobře řešitelné. Jak již jsme uváděli, bitcoin nelze považovat za peníze. Bitcoin je díky tomu předmětem koupě a prodeje na mnoha internetových stránkách. V okamžiku, kdy se kdokoliv rozhodne koupit nebo prodat bitcoin, musí o sobě zveřejnit alespoň nějaké údaje. Tím okamžik, už není uživatel pouze anonymní adresou v rámci Bitcoinové sítě, ale existující osobou. O takové osobě lze potom již vést údaje, neboť každá její transakce je automaticky zaznamenávána v rámci sítě. Jakmile se osoba rozhodne bitcoiny použít ke koupi zboží či služby, přestává být chráněná anonymitou sítě.

Řešením decentralizace a anonymity Bitcoinu je tedy regulace těch osob, jejichž předmět podnikání je navázán Bitcoin. Jedná se kupříkladu o osoby, které prodávají či

kupují bitcoiny, ale i osoby, které za bitcoiny prodávají zboží a služby. Tímto způsobem je možné získat dostatek informací o jednotlivých uživateli sítě, ale i zamezit legalizaci výnosu z trestné činnosti.

Výrazně větší výzvu regulaci představují teoretické problémy. Teoretické problémy spočívají v tom, že decentralizace se nadále vyvíjí a již dnes je možné decentralizovat jak obchody tak jednotlivá prodejní místa bitcoinu. V okamžiku, kdy dojde k celkové decentralizaci jak obchodů tak míst, kde lze koupit či prodat bitcoin, výše zmíněný způsob regulace bude neefektivní.

Dalším budoucím problémem může být samostatný vývoj Bitcoinu, pokud by se bitcoin stabilizoval natolik, že by byl schopen dlouhodobě držet hodnotu, zřejmě by došlo k větší míře jeho používání a tím pádem by se mohl stát penězi v ekonomickém smyslu. Takovýto vývoj by měl za následek, že bitcoiny by již nemusely být prodávány či nakupovány tak často jako je tomu nyní.

Tyto budoucí problémy nejsou řešitelné ani tak na základě regulace, ale vyžadují řešení spíše technického řádu, které by bylo schopné s postupující decentralizací bojovat.

V Americe vznikl první zákon, který se zabývá pouze úpravou Bitcoinu a podobných digitálních prostředků směny. Tento zákon je původem ze státu New York ze Spojených Států Amerických a postupuje způsobem, o kterém jsme mluvili v rámci řešení současných problémů.

Ze strany Bitcoinové komunity se nesetkal s kladným přijetím, dokonce většina závodů, které figurovaly ve státě New York, se přesunula jinam. My naopak považujeme toto řešení za jediné možné. Tento zákon vyžaduje, aby každý, kdo chce vykonávat podnikatelskou činnost v souvislosti s Bitcoinem, měl k této činnosti licenci udělenou od státní autority.

I v České Republice se postupně objevuje první zákonná zmínka o Bitcoinu. Novelou zákona č. 253/2008 Sb.¹⁶⁵ bude Bitcoin definován a zároveň bude vymezen okruh aktivit a povinné osoby, které se musí řídit danými povinnostmi v souvislosti s Bitcoinem.

¹⁶⁵ Takzvaný zákon proti praní špinavých peněz.

Krátkým porovnáním definic virtuální měny a vymezení povinných osob respektive předmětu podnikání v souvislosti s Bitcoinem, lze dojít k názoru, že americká definice virtuální měny je pro budoucí užití lepší, neboť vysloveně nestanovuje, že Bitcoin nejsou peníze. Česká úprava naopak Bitcoin za peníze nepovažuje. Z budoucího hlediska je přesnější úprava americká, která bere v potaz možnost vývoje pojetí Bitcoinu, zatímco česká úprava lépe reflektuje současné pojetí Bitcoinu jako všeobecného prostředku směny, který ale není penězi.

V případě vymezení povinných osob a aktivit (tedy okruh osob a aktivit), na které se legislativa vztahuje, je jistě lépe pojata úprava česká. Americká právní úprava se dopouští nelogicky širokého pojetí, když veškeré požadavky, které vztahuje na společnosti, jejichž předmět činnosti je spojen s Bitcoinem, vztahuje i na obyvatele státu New York. To v praxi znamená, že každý, kdo by chtěl prodat jeden bitcoin, si musí dávat pozor, aby neprodal tento bitcoin obyvatele New Yorku, protože by pak jednal bez licence. Stejně tak široké je i pojetí jednotlivých aktivit, ke kterým je vyžadována licence. Teoreticky lze uvažovat, že kdokoliv, kdo přepraví flash disk, který bude obsahovat privátní klíč k bitcoinu, z bodu A do státu New York a vice versa, by měl být držitelem licence.

České pojetí povinných osob a aktivit se týká pouze těch osob, které vykonávají správu bitcoinu pro jiného, popřípadě bitcoin kupují či prodávají jako předmět své podnikatelské činnosti. Tím dostáváme znatelně užší pojetí povinných osob a aktivit, které nevede k nelogickým situacím jako tomu je v případě americké právní úpravy.

Americká právní úprava nestanovuje žádnou minimální peněžní hranici, při které by nemusely být vykonávány náročné procedury identifikace klienta. To v praxi znamená, že i v okamžiku, kdy si někdo koupí bitcoin v hodnotě 10 dolarů, musí být podroben všem informačním procedurám a musí o něm být veden záznam. Česká úprava naopak vyžaduje tyto identifikační procedury až v okamžiku, kdy už je jasné, že celková transakce přesáhne hodnotu 1000 Euro. Povinná identifikace však musí být provedena vždy, když se může jednat o podezřelý obchod. Absolutní kontrola každé transakce je jistě finančně a pracovní náročnější, než jak je tomu v případě české úpravy. Česká úprava je v tomto vymezení pokročilejší, neboť zbytečně nelimituje povinné osoby.

Americká právní úprava představuje několik právních institutů, které považujeme za velmi dobré a máme za to, že by se měly objevit v české právní úpravě. Jedná se o program datového zabezpečení a celkové bezpečnosti dat. Dále se jedná o krizový plán, který má zabezpečit kontinuitu podnikání v případě neočekávané krize a v poslední řadě se jedná o speciální péči a ochranu jmění zákazníků.

První program týkající se zabezpečení dat je velmi důležitý z toho důvodu, že mnoho krádeží bitcoinů je zapříčiněno nedostatečnou ochranou dat, či dokonce absolutně nulovou ochranou, tak jako tomu bylo v jedněch z největších bitcoinových krádeží. Dle našeho názoru je tedy potřeba, aby existovalo objektivně správné hledisko zabezpečení a to jak již z důvody ochrany jmění zákazníků, ale i pro případnou odpovědnost podnikatele.

Velmi podobný je i druhý případ krizového plánu, jehož hlavním cílem je, aby se v případě krize společnost byla schopna vzpamatovat a pokračovat ve svém podnikání. Z praxe je totiž známo, že v okamžiku, kdy osobu, jejíž předmětem podnikání je Bitcoin, postihne nějaká krize, tak je to také ve většině případů její konec. Tomu by měl zabránit plán, kdy společnosti dopředu počítají s tím, že se něco takového stát může a jsou připraveny podnikat i na dále. Tím mají zákazníci větší jistotu, že nepřijdou o své jmění a popřípadě absence tohoto plánu by znamenal odpovědnost provozovatele společnosti za vzniklou škodu.

Posledním případem je speciální péče a ochrana jmění zákazníků, která spočívá v požadavcích na podnikatele, aby spravoval peněžní fond v určené výši v zákonném platidle, aby vždy disponoval stejným počtem a stejnou virtuální měnou, kterou do jeho péče vložil zákazník a posledním požadavkem je zákaz, aby podnikatel se svěřenými virtuálními měnami nakládal bez příkazu zákazníka.

Závěr

Odpovědí na naši výzkumnou otázku co je to Bitcoin je, že bitcoin je v současné době digitální prostředek směny, který ale nelze považovat za peníze v ekonomickém ani právním smyslu. Z pohledu práva lze na Bitcoin i bitcoin nahlížet různými způsoby a to i takovými, které neodpovídají pojetí věci v právním smyslu.

K Bitcoin je však třeba přistupovat především prakticky. V současnosti je nejpraktičtější řešením považovat bitcoin za oprávnění, neboť oprávnění je

považováno za věc v právním smyslu a tím se na Bitcoin vztahuje většina českých zákonů.

Nicméně naším osobním názorem zůstává, že bitcoin by si zasloužil vlastní právní kategorii, popřípadě v budoucnu podřazení pod pojetí peněz.

V rámci regulace, lze uzavřít, že Bitcoin představuje v současné době legislativně řešitelné problémy, které lze vyřešit specifickou právní úpravou cílenou na osoby, jejichž předmětem podnikání je bitcoin. Navrhujeme, aby Česká Republika přijala specifický zákon týkající se regulace podnikání s Bitcoinem. Zároveň představujeme 3 klíčové instituty, které by v takovém zákoně neměly chybět.

Je možné, že vývoj Bitcoinu povede ke vzniku dalších problémů spojených s větší decentralizací a anonymitou, ale v takovém případě je nasnadě spíše technologické než právní řešení.

Key Words: Bitcoin, Money, Currency, Regulation, Thing in a legal sense.

Klíčová slova: Bitcoin, peníze, měna, regulace, věc v právním smyslu.