BITCOIN – LIGHT AT THE END OF THE TUNNEL FOR CYBER-LIBERTARIANS?

by

ROBERT KUTIŠ*

In the Internet pre-commercial era, much of the most influential writing about cyberspace was written from a cyber-libertarian perspective. But then, times and the Internet changed, as well as the opinions on the future of Internet regulation. Nevertheless, there still are some technical developments which give libertarians hope that the future of the cyberspace will greatly differ from the dystopian views of it. Bitcoin is one of those technical developments and questions whether it really provides anonymity for individuals, demonstrates unregulability of certain aspects of cyberspace or makes the regulation of cyberspace less possible in general, lie at the heart of this paper. After finding answers to these questions, a more general one can be answered – is Bitcoin really a light at the end of the tunnel for digital libertarianism or just a false hope which will soon become a prey of cyber-paternalism?

KEYWORDS

e-currencies; Bitcoin; regulation of cyberspace; anonymity; privacy; cyber-libertarianism; cyber-paternalism

1. THE RISE AND FALL OF CYBER-LIBERTARIANISM

In the early 1990s Internet was seen as some kid of mythological space, existing outside of the physical boundaries of the "real space" providing its users with unprecedented freedom. But apart from freedom to pursue their own tastes and interests online with no or little involvement of the state, Internet also offered its users the freedom of choice of the ways and extent of

* Mgr. Robert Kutiš, LL.M. - PhD. candidate, Department of Theory of law and Constitutional law, Faculty of Law, Trnava University in Trnava, robert@kutis.sk

Work on this manuscript was supported by the Slovak Agency for Advancement of Science and Research under the grant no. APVV-0562-11.

regulation within its own digital boundaries. Under such a frame of thinking, pillars of the cyber-libertarianism arose.

The whole existence of an individual in this new disembodied space was based "*on the primacy of the individual liberty and a commitment to pluralism, diversity, and community*"[1]. Any type of state´s coercion was seen as the biggest threat to both political and economic freedoms of individuals within the new digital space and thus the approach of none, or minimal, state coercion with preference for bottom-up spontaneous approach to address the code failures as an equivalent of the market failures[2] represented the core of cyber-libertarian thinking. Moreover, the idea of the lack of legitimacy of the states existing in the physical world to regulate actions carried out in the Internet caused by the disappearance of the locus of the actions gave rise to the more radical cyber-libertarian ways of thinking. The basic idea of such cyber-exceptionalism could be best seen in the influential works of the mid 1990s – A Magna Carta for the Knowledge Age[3] or John Perry Barlow´s Declaration of the Independence of Cyberspace.[4]

By understanding the users of the Internet as citizens of cyberspace, those works challenged the very notion of Internet governance by national states, working also with traditional concepts of the theory of the state – for example Barlow pointed to the nation-states´ lack of legitimacy to govern cyberspace that stems from the absence of the social contract.[5] The other line

---

1 Kapor, M. 1993, *Where is the Digital Highway Really Going?,* Wired 1(3), p. 53–59

2 See: Bator, F.M. 1958, *The Anatomy of Market Failure*, Quarterly Journal of Economics, 72(3) pp. 351–379

3 "*As humankind explores this new "electronic frontier" of knowledge, it must confront again the most profound questions of how to organize itself for the common good. The meaning of freedom, structures of self-government, definition of property, nature of competition, conditions for cooperation, sense of community and nature of progress will each be redefined for the Knowledge Age -- just as they were redefined for a new age of industry some 250 years ago*."Dyson, E., Gilder, G., Keyworth, G.,Toffler, A. 1994, *Cyberspace and the American Dream: A Magna Carta for the Knowledge Age*, Future Insight, Release 1.2, August 1994.

4 "*Governments of the Industrial World, you weary giants of flesh and steel, I come from Cyberspace, the new home of Mind. On behalf of the future, I ask you of the past to leave us alone. You are not welcome among us. You have no sovereignty where we gather. We have no elected government, nor are we likely to have one, so I address you with no greater authority than that with which liberty itself always speaks. I declare the global social space we are building to be naturally independent of the tyrannies you seek to impose on us. You have no moral right to rule us nor do you possess any methods of enforcement we have true reason to fear.[…] Cyberspace does not lie within your borders.[...] We are forming our own Social Contract . This governance will arise according to the conditions of our world, not yours*."Barlow, J. P. 1996, *A Declaration of the Independence of Cyberspace*, Davos, Switzerland, February 1996

5 Kline, J. 2010, *Property and Control: Cyber-libertarianism and Public Policy in the Internet Age*, [on-line] http://thesis.kline.ca/documents/lit-review.pdf [Accessed: 15.11.2013]See: Barlow, J. P. 1996, *A Declaration of the Independence of Cyberspace*, Davos, Switzerland, February 1996
See also: Hobbes, T. 1651, *Leviathan*, Renaissance Books, Riverside, CA, U.S.A., October 2013
Rousseau, J.J. 1968, *The Social Contract*, Penguin Classics, London

of reasoning was connected with the libertarian notion that the intrinsic role of the state is to protect its citizens from physical harm[6] and since such harm is not possible in the cyberspace, there is no need for government protection. Thus, cyber-exceptionalists had seen the Internet as a space with its own culture and social norms, which as a whole stay outside the jurisdiction of the nation-states.

Such insight also inherently brings into the light the questions of Internet governance and regulation of the actions which take place in this independent (cyber)space. The original cyber-libertarian stance was set by Johnson´s and Post´s vision of post-national state of being, where traditional, on the states´ sovereignty based, regulatory systems simply cannot be used for cyberspace regulation and governance.[7] Instead, self-regulation, where consensus of the "citizens" of the cyberspace plays the main role should prevail[8], or as later Murray put it – any regulator within cyberspace will act only as agents of individual or group interests.[9]

With regard to the character of the Internet and the climate embracing its functioning in most of the 1990s, the cyber-libertarian rhetoric predominated and the freedom, liberty and self-regulation became the holy trinity[10] of much of the influential works in those days.[11] However, further commercionalisation of the cyberspace and changes in the possibilities of the Internet regulation caused that cyber-libertarian way of thinking became less prevalent in the literature, or at least many authors changed their rhetoric.[12] As Dahlberg aptly wrote *"[b]y the beginning of the new millennium, the Inter-*

---

6 See: Rand, A. 1981. *The Virtue of Selfishness*, New American Library, New York, p. 109

7 See: Johnson, D. R, Post, D. G. 1996, *Law and Borders: The Rise of Law in Cyberspace*, 48 Stanford Law Review, p. 1367

8 *Id* at p.1391

9 See: Murray, A. 2002, Free Expression and Censorship Through Design Protocols: A Misapplication of the ICANN UDRP, 17th Bileta Annual Conference, p.9 [on-line]http://www.bileta.ac.uk/content/files/conference%20papers/2002/Free%20Expression%20and%20Censorship%20Through%20Design%20Protocols%20-%20A%20Misapplication%20of%20the%20ICANN%20UDRP.pdf, [Accessed: 29.11.2013]

See also: Klang, M. 2005, *Controlling Online Information: Censorship & Cultural Protection*, A presentation given at "WSIS, Internet Governance and Human Rights" Uppsala, October 3, 2005, [on-line] http://www.kus.uu.se/pdf/publications/ICT/klang_03_oct.pdf [Accessed: 09.11.2013]

10 See: Boyle,J. 1997, *Foucault in Cyberspace: Surveillance, Sovereignty, and Hardwired Censors*, University of Cincinnati Law Review Vol. 66, pp. 177–79, p. 177

11 However that does not mean that such insights were without a critique. See: Aoki, K. 1998, *Considering Multiple and Overlapping Sovereignties: Liberalism, Libertarianism, National Sovereignty, "Global" Intellectual Property, and the Internet*, Indiana Journal of Global Legal Studies Vol. 5, Issue 2, pp. 443-4473

See also: Reidenberg, J. 1998, *Lex Informatica: The Formation of Information Policy Rules Through Technology*, Texas Law Review Vol. 76. Number 3, pp. 553-594

net was generally seen as part and parcel of "everyday life" – simply an extension of existing social systems, rather than being a revolutionary medium transcending offline political and economic constraints."[13]

Such continuous change in the nature of the Internet proved that many sceptical views on the Internet future unveiled the weaknesses of the cyber-libertarian optimistic reasoning with great accuracy. Goldsmith observed very soon that cyber-libertarians overstated the Internet and territory separateness, not recognizing that the question of Internet controllability is not about the mere possibility, but rather about its cost.[14]

Later, Lessig came up with the position that most of the features that portray the Internet as a space which is inherently unregulable are not stemming from some inherent libertarian nature of the Internet as cyber-libertarians tend to see it, but they are purely coding choices – and those can be rather easily changed.[15] Although this position may not seem so disastrous for the cyber-libertarians on the first sight since it means that cyber-libertarian values can also be promoted by means of the code, Lessig rightly foresaw that the biggest threat for the future of the cyberspace from the cyber-libertarian perspective lies at the hands of private entities with their own commercial or political interests. Arguing that *"[t]he invisible hand, through commerce, is constructing an architecture that perfects control—an architecture that makes possible highly efficient regulation"*[16] Lessig point out that those entities, offered with powerful control have only little motivation to protect fundamental cyber-libertarian values.[17]

---

[12] For instance, Barlow changed his rather courageous rhetoric from the Declaration of the Independence of Cyberspace to more cautious statements – for example when later claimed that at least the some of his ideas expressed in the declaration were right because „*the Internet continues to be an anti-sovereign social space, endowing billions with capacities for free expression*". Dahlberg, L. 2010, *Cyber-libertarianism 2.0: A discourse theory/critical political economy examination*, Cultural Politics Vol. 6, Issue 3, pp. 331-356, p. 333

[13] Dahlberg, L. 2010, *Cyber-libertarianism 2.0: A discourse theory/critical political economy examination*, Cultural Politics Vol. 6, Issue 3, pp. 331-356, p.333See also: Margolis, M., Resnick, D. 2000, *Politics as Usual: The Cyberspace"Revolution"*, Sage, London

[14] Goldsmith, J. L. 1998, *The Internet and the Abiding Significance of Territorial Sovereignty*, Indiana Journal of Global Legal Studies Vol.5, Issue 2, pp. 475-491

[15] Lessig,L. 1999, *Code and Other Laws of Cyberspace*, Basic Books, New York, p.217 See also: Holland, B. 2007, *In Defense of Online Intermediary Immunity: Facilitating Communities of Modified Exceptionalism*, Kansas Law Review Vol 56, pp. 101-137, p. 113

[16] Lessig,L. 1999, *Code and Other Laws of Cyberspace*, Basic Books, New York, p.6

[17] See also: Holland, B. 2007, *In Defense of Online Intermediary Immunity: Facilitating Communities of Modified Exceptionalism*, Kansas Law Review Vol 56, pp. 101-137, p. 114

2. GLIMMERS OF HOPE FOR CYBER-LIBERTARIANS

After some time passed, it could now be said that Lessig and many other authors who were rather sceptical about the cyber-libertarian views on the future of the Internet were right in a number of things. Put very simply, development of the character of the Internet in the last two decades too closely resembles the content of the thesis of Debra Spar that society's reaction to new technologies follows a predictable sequence of stages starting with the innovation, followed by chaos and creative anarchy, self-regulation, commercial exploitation, piracy, attempts to monopolize the field and finally with government rules and control.[18] However, apart from rules imposed by terrestrial sovereigns, market forces foresaw by Lessig play also big role in today´s Internet nature. Thus, ironically, most of the norms and values associated with today´s Internet are emerging from the field of commercial entities and now and then even cyber-libertarians call for intervention of sovereign governments in order to protect individuals acting in cyberspace.[19]

Nevertheless, there still is a number of glimmers of hope for cyber-libertarians including cyber-exceptionalists that encourages many to say "cyber-libertarianism´s not dead"[20] - one might see them in the end-to-end design of the Internet architecture,[21] free software, cryptography,[22] mere opportunity for anonymity,[23] technologies that enhance anonymity,[24] or emerging e-currencies with Bitcoin on the forefront. Building upon the previ-

---

[18] Spar, D.L. 2001, *Ruling the Waves: Cycles of Discovery, Chaos, and Wealth from the Compass to the Internet*, Harcourt Trade Publishers, Sand Diego, CASee also: MacCarthy, M. *Internet Exceptionalism Revisited* In. Marcus, A., Szoka, B. (eds.) 2010, *The Next Digital Decade: Essays on the Future of the Internet*, pp. 209 -237, p. 210, Techfreedom, Washington, D.C.

[19] The debate over online privacy and data protection is a good example.

[20] Although cyber-libertarian thinking in form of cyber-exceptionalism is no more the topic of the day, cyber-libertarianism is still quite widely held belief shaping many debates over Internet regulation. See: Holland, B. *Section 230 of the CDA: Internet Exceptionalism as a Statutory Construct* In. Marcus, A., Szoka, B. (eds.) 2010, *The Next Digital Decade: Essays on the Future of the Internet*, pp. 189-209 - an adapted version of Holland, B. 2007, *In Defense of Online Intermediary Immunity: Facilitating Communities of Modified Exceptionalism*, Kansas Law Review Vol 56, pp. 101-137

[21] See: Lessig, L. 2002, *The Architecture of Innovation*, Duke Law Journal Vol. 51, pp. 1783-1801, p. 1789 See als: Holland, B. 2007, *In Defense of Online Intermediary Immunity: Facilitating Communities of Modified Exceptionalism*, Kansas Law Review Vol 56, pp. 101-137, p. 114

[22] More specifically - wide use of strong cryptography as an ideal response to today´s problems of Internet as it is seen by „cypherpunks".See: Applelbaum, J., Assange, J., Müller-Maguhn, A., Zimmermann, J., 2012, *Cypherpunks, Freedom and the Future of the Internet*, OR Books, London

[23] See: Reidenberg, J. 1998, *Lex Informatica: The Formation of Information Policy Rules Through Technology*, Texas Law Review Vol. 76. Number 3, pp. 553-594See also: Strasser,M. 2001, *Beyond Napster: How the Law Might Respond to a Changing Internet Architecture*, Northern Kentucky Law Review, Number 28, p. 760–712

ously used analogy with the music genre – the only question now stands whether any of those bearers of hope for cyber-libertarians will hit the right "tune" to bring cyber-libertarianism, or even cyber-exceptionalism back on the main scene. With regard to maybe even unexpected success, Bitcoin seems capable of doing exactly that.

3. BITCOIN

Bitcoin can be described as a decentralized electronic currency scheme and at the same time as quickly emerging electronic payment system, introduced by a rather mystical, or better said pseudonymous[25] Satoshi Nakamoto in 2008[26] and deployed in the beginning of the year 2009. The main rationale of Bitcoin launch was Nakamoto´s belief that electronic payment system based not on trust in financial institutions acting as intermediaries, but cryptography, allowing to carry out transactions directly between two parties without the need for a trusted third party, is needed.[27] Such system design offers users the electronic currency which can be used for electronic payments which are performed faster and cheaper than with traditional trust based payment methods.

Apart from cryptography, Bitcoin is based also on the peer-to-peer network and the proof-of-work system.[28] While the former mainly relates to the way how are Bitcoin transactions carried out, the latter relates also to the way how bitcoins are "minted". Since Bitcoin, as a digital currency, can be briefly described as a chain of digital signatures, the transaction represent the process where owner of the Bitcoin, using secret key corresponding to his public key, digitally signs a hash of the previous transactions and the public key of the next owner which is then added to the end of the electronic coin itself – thus creating the above mentioned chain.[29] Since such design

---

[24] For example the Tor Project, https://www.torproject.org/about/overview.html.en [Accessed: 07.01.2014]

[25] I reffer to Satoshi Nakamoto as "pseudonymous", because his real identity was never truly unveiled.

[26] See: Nakamoto, S. 2008, *Bitcoin: A Peer-to-Peer Electronic Cash System*, http://bitcoin.org/bitcoin.pdf [Accessed: 27.10.2013]

[27] *Id* at p.1

[28] More specifically, Hashcash is (with minor changes) the proof-of-work system used by Bitcoin.For more about Hashcash see: Back, A. 2002, *Hashcash - A Denial of Service Counter-Measure*, http://www.hashcash.org/papers/hashcash.pdf [Accessed: 02.11.2013]

[29] Meiklejohn, S., et al. 2013, *A Fistful of Bitcoins: Characterizing Payments Among Men with No Names*, http://cseweb.ucsd.edu/~smeiklejohn/files/imc13.pdf, [Accessed: 16.11.2013], p.2Nakamoto, S. 2008, *Bitcoin: A Peer-to-Peer Electronic Cash System*, http://bitcoin.org/bitcoin.pdf [Accessed: 27.10.2013], p.2

does not in itself prevent double spending of the Bitcoins, creator(s)[30] decided for a solution based on timestamps.[31] Transactions are thus grouped into blocks in which they are timestamped. Those blocks are then formed into a block chain which is then publicly available.[32] This is the point where not only proof-of-work system modified by Bitcoin come into use,[33] but also when the process of the Bitcoin "minting" is introduced because, using very simplified explanation, Bitcoin is "minted" during the process of forming a block. Since all tasks needed to be performed during the process of Bitcoin transaction are carried out by number of participants, the incentive to support the network lies right in the convention that the first transaction in a block starts a new coin owned by the creator of the block.[34]

With regard to above mentioned description of cornerstones of Bitcoin functioning, Bitcoin can be viewed as a virtual currency scheme and digital payment system based on a peer-to peer network which does not have a central clearing house, nor central authority in charge of money supply, operating without any involvement of financial institutions acting as trusted third parties in the transactions, since users perform all these tasks themselves.[35]

4. CYBER-LIBERTARIANISM, BITCOIN AND THE FUTURE OF BOTH

Reading the lines above, many characteristics of Bitcoin must have pleased the heart of every cyber-libertarian, however two are of particular importance – its decentralised nature and the promise of anonymity.

4.1 ANONYMITY

Generally speaking, anonymity is not a good in itself. One may use his anonymity as he wishes – to exercise the freedom of expression in the fight against totalitarian regimes, support and promote human rights by other means, purchase weapons, or to sell drugs. Nevertheless, anonymity is inherently good for protecting and strengthening one´s sphere of freedom,

---

30 See *supra* note 26.

31 In order to avoid involving trusted third party.

32 See: Nakamoto, S. 2008, *Bitcoin: A Peer-to-Peer Electronic Cash System*, http://bitcoin.org/bitcoin.pdf [Accessed: 27.10.2013], p. 2

33 *Id* at p. 3-4

34 See: *Id* at, p.3

35 See: ECB, 2012, *Virtual Currency Schemes*, http://www.ecb.europa.eu/pub/pdf/other/virtualcurrencysche mes201210en.pdf [Accessed: 03.11.2013], p.6

which puts it naturally into the position of a good from the cyber-libertarian or, even more so, from the crypto-anarchistic perspective.[36] Since anonymity in business transactions promised by Bitcoin facilitates fulfilment of the economic and other freedoms, from the point of cyber-libertarianism, anonymity represents a characteristic of particular significance.

Despite the fact that Bitcoin is often referred to as "digital cash"[37] there is number of substantial differences between them – for example, the "real world cash" does not allow one to see all previous transactions done with particular bill or coin, as Bitcoin does. Thus, one´s ownership of Bitcoins is genuinely anonymous only until he decides to cash out or spend them. This feature of Bitcoin is connected to design choice, where creator(s), in order to leave out intermediaries in form of various financial institutions, decided to use system where payee is aware of all transactions of the coin. Thus, in order to prevent double spending, all transactions must be publicly announced[38] to global peer-to-peer network of participants who are verifying them. Aware of such trait, one may easily come to conclusion that Bitcoin is not as completely anonymous as it may seem on the first sight. Then, it is only up to computer scientists to confirm such notion - as they very recently did.

Results of research made by researchers from ETH Zurich and NEC Laboratories Europe - who mimicked the use of Bitcoin in university environment on a simulator - show that the profiles of almost 40% of the users can be, to a large extent, recovered even when users adopt privacy measures recommended by Bitcoin.[39] Also second research, done very recently by researchers from University of California and George Mason University came to similar conclusions - researchers noticed growing gap between the potential anonymity offered by the Bitcoin protocol design and the actual anonymity achieved by users.[40] Moreover, after tracking the thief who stole Bitcoins from other individual users using trojan they stated that "*even the*

[36] Crypto-anarchism is a branch of cyber-anarchism. Put very simply, cypto-anarchists employ robust cryptographic software in order to oppose to the regulatory efforts of not only states, but also private entities.

[37] Brito, J., Castillo, A. 2013, *Bitcoin: A Primer for Policymakers*, Mercatus Center at George Mason University, http://mercatus.org/sites/default/files/Brito_BitcoinPrimer_embargoed.pdf [Accessed: 11.01.2014]

[38] Nakamoto, S. 2008, *Bitcoin: A Peer-to-Peer Electronic Cash System*, http://bitcoin.org/bitcoin.pdf [Accessed: 27.10.2013], p.2

[39] Androulaki, E., et al., 2013, *Evaluating User Privacy in Bitcoin*, Lecture Notes in Computer Science, Vol. 7859, pp. 34-51

[40] Meiklejohn, S. et al. 2013, *A Fistful of Bitcoins: Characterizing Payments Among Men with No Names*, http://cseweb.ucsd.edu/~smeiklejohn/files/imc13.pdf, [Accessed: 16.11.2013],p. 12-13

most motivated Bitcoin users (i.e., criminals) are engaging in idioms of use that allow us to erode their anonymity".[41] After using clustering heuristic allowing them to cluster addresses belonging to the same user which is however not really fully robust they argue that among average users this gap is more likely to widen: "[*w*]*e argue that to completely thwart our heuristics would require a significant effort on the part of the user, and that this loss of usability is unlikely to appeal to all but the most motivated users (such as criminals)*".[42]

4.2 DECENTRALISED NATURE

As stated above, the cornerstones of Bitcoin functioning are based on a peer-to-peer network by means of which, without any involvement of a central clearing house or financial institutions acting as trusted third parties, users perform all of the necessary tasks by themselves. Bitcoins are minted and transactions are verified by users who are, aided by the software, de facto exchanging their CPU power and energy for a share of newly minted Bitcoins.[43] Such design provides sufficient incentives not only to support the functioning of Bitcoin, but also an incentive to stay „honest" within this system. The idea is that even if a person is able to assemble more CPU power than all the „honest" users, „*he ought to find it more profitable to play by the rules, such rules that favour him with more new coins than everyone else combined, than to undermine the system and the validity of his own wealth*."[44]

However, such constructed and maintained character of the Bitcoin is not necessarily permanent. Incentive for centralisation may stem from the ambitions of subjects other than users seeking to maximize their profits – for example sovereign states.[45] Furthermore, "greedy" users do not necessarily behave according to the pattern presumed by the creators of Bitcoin – this is true all the more when other practices than "honest" use of CPU power can achieve much higher revenues than those offered by Bitcoin scheme.

---

[41] *Id* at p. 12

[42] *Id* at p. 13

[43] With regard to above mentioned users who with the help of the software verify Bitcoin transactions are called miners. Nakamoto, S. 2008, *Bitcoin: A Peer-to-Peer Electronic Cash System*, http://bitcoin.org/bitcoin.pdf [Accessed: 27.10.2013], s. 4

[44] Nakamoto, S. 2008, *Bitcoin: A Peer-to-Peer Electronic Cash System*, http://bitcoin.org/bitcoin.pdf [Accessed: 27.10.2013], p. 4

[45] Such incentive may stem for example from the need to stabilize own "real-world" currency to the detriment of electronic currencies.

This was very recently confirmed by the results of research focused on the decentralised nature of Bitcoin, published by the Department of Computer Science at the Cornell University. Their conclusions suggest that the creator(s) of the Bitcoin overstated the power of incentives offered to users by Bitcoin design to stay "honest"[46] since they found out that the Bitcoin ecosystem is facing the challenge of potential takeover and manipulation by miners who seek to maximize their rewards.[47] The paper presented a Bitcoin mining strategy that enables pools of colluding miners to earn revenues higher than their fair share, what can lead new miners to join the "selfish" miners with possible catastrophic outcomes for decentralized currency since the colluding group will increase in size until it becomes a majority – and in that point "*the Bitcoin system ceases to be a decentralized currency*".[48]

5. CONCLUSIONS

The purpose of this paper is to shed some light on the answer to the question whether Bitcoin truly represent such technological innovation that is able to bring the cyber-libertarian, or even cyber-exceptionalist views on the future of Internet regulation back on the track of the mainstream public debate.

Despite noticeable shift in the Internet governance, Bitcoin proved that even today one may - pushing the notion of decentralisation to a new level - create something that functions within the scope of today´s setting of the Internet and nevertheless seem unregulable again. Combining this characteristic with the promise of anonymity[49] that is provided, Bitcoin is empowering individuals acting on the Internet to really materialize their economical freedoms and together with those also political and other freedoms.[50]

Nevertheless, I do not believe that Bitcoin is a dream come true for cyber-libertarians - mainly because neither of those two core characteristics can be understood as permanent and their sustainability for the future is more than uncertain. Even though it can be argued that Bitcoin represents

---

[46] Nakamoto, S. 2008, *Bitcoin: A Peer-to-Peer Electronic Cash System*, http://bitcoin.org/bitcoin.pdf [Accessed: 27.10.2013], p.4

[47] Eyal, I., Sirer, G. E., 2013, *Majority is not Enough: Bitcoin Mining is Vulnerable*, arXiv:1311.0243 [cs.CR], http://arxiv.org/abs/1311.0243 [Acccessed: 02.11.2013], p.15

[48] *Id* at p. 1, 2 and 12

[49] Fuelling the functioning of various services, repressed movements etc. financing whose seemed before almost unimaginable. (not only recently closed SilkRoad, but also Wikileaks, revolutionary movements in some countries etc.)

[50] Since political and other freedoms are extremely intertwined with economical freedoms of contract and exchange.

the code which - promoting cyber-libertarian values – does not tend to be changed, its own design contains several weak points which may prove crucial in connection to future regulatory efforts. The promise of anonymity that is so appealing for cyber-libertarians is not adhered in the everyday use and the future of this promise is thus looking rather gloomy. Also the decentralised nature of Bitcoin faces many future challenges – potential takeover and manipulation with the system by the majority of "selfish" miners represent only the main one. Bearing in mind latest fragments added to the mosaic of potential future regulation of Bitcoin[51] I am rather sceptical about the outlook of this nevertheless genius technological solution – predators from the ranks of cyber-paternalists are surrounding the prey and odds are on their side.

REFERENCES

[1] Aoki, K. 1998, *Considering Multiple and Overlapping Sovereignties: Liberalism, Libertarianism, National Sovereignty, "Global" Intellectual Property, and the Internet*, Indiana Journal of Global Legal Studies Vol. 5, Issue 2, pp. 443-4473

[2] Androulaki, E., et al., 2013, *Evaluating User Privacy in Bitcoin*, Lecture Notes in Computer Science, Vol. 7859

[3] Applelbaum, J., Assange, J., Müller-Maguhn, A., Zimmermann, J., 2012, *Cypherpunks, Freedom and the Future of the Internet*, OR Books, London

[4] Back, A. 2002, *Hashcash - A Denial of Service Counter-Measure*, http://www.hashcash.org/papers/hashcash.pdf [Accessed: 02.11.2013]

[5] Barlow, J. P. 1996, *A Declaration of the Independence of Cyberspace*, Davos, Switzerland, February 1996.

[6] Bator, F.M. 1958, *The Anatomy of Market Failure*, Quarterly Journal of Economics, 72(3) pp. 351–379.

[51] Examples of such fragments of the mosaic of the future regulation in the field range from the letter adressed to the secretary of Homeland Security stating that *„the expansive nature of this emerging technology demands a holistic and whole-government approach in order to understand and provide a sensible regulatory framework for their existence[…] the federal government must make sure that potential threats and risks are dealt with swiftly"* to the recognition of the Bitcoins as "*private money*" or "*form of money*" worldwide with regard to the need for deeper foundations of the potential future regulation.See: Jilch, N. 2013, *Onlinewährung Bitcoin gilt offiziell als "privates Geld"*, Die Presse http://diepresse.com/home/wirtschaft/international/1442631/Onlinewaehrung-Bitcoin-gilt-offiziell-als-privates-Geld [Accessed: 30.11.2013]

See: United States District Court, 2013, *Memorandum opinion regarding the court´s subject matter jurisdiction, CASE NO. 4:13-CV-416*, http://ia600904.us.archive.org/35/items/gov.uscourts.txed.146063/gov.uscourts.txed.146063.23.0.pdf [Accessed: 30.11.2013]

See also: Farivar, C. 2013, *Federal judge: Bitcoin, "a currency," can be regulated under American law*, ArsTechnica, http://arstechnica.com/tech-policy/2013/08/federal-judge-bitcoin-a-currency-can-be-regulated-under-american-law/ [Accessed: 30.11.2013]

[7] Boyle,J. 1997, *Foucault in Cyberspace: Surveillance, Sovereignty, and Hard-wired Censors*, University of Cincinnati Law Review Vol. 66, pp. 177–79, p. 177.

[8] Brito, J., Castillo, A. 2013, *Bitcoin: A Primer for Policymakers*, Mercatus Center at George Mason University, http://mercatus.org/sites/default/files/Brito_BitcoinPrimer_embargoed.pdf [Accessed: 11.01.2014]

[9] Dahlberg, L. 2010, *Cyber-libertarianism 2.0: A discourse theory/critical political economy examination*, Cultural Politics Vol. 6, Issue 3, pp. 331-356

[10] Dyson, E., Gilder, G., Keyworth, G.,Toffler, A. 1994, *Cyberspace and the American Dream: A Magna Carta for the Knowledge Age*, Future Insight, Release 1.2, August 1994.

[11] ECB, 2012, *Virtual Currency Schemes*, http://www.ecb.europa.eu/pub/pdf/other/virtualcurrencyschemes201210en.pdf [Accessed: 03.11.2013]

[12] Eyal, I., Sirer, G. E., 2013, *Majority is not Enough: Bitcoin Mining is Vulnerable*, arXiv:1311.0243 [cs.CR], http://arxiv.org/abs/1311.0243 [Acccessed: 02.11.2013]

[13] Farivar, C. 2013, *Federal judge: Bitcoin, "a currency," can be regulated under American law*, ArsTechnica, http://arstechnica.com/tech-policy/2013/08/federal-judge-bitcoin-a-currency-can-be-regulated-under-american-law/ [Accessed: 30.11.2013]

[14] Goldsmith, J. L. 1998, *The Internet and the Abiding Significance of Territorial Sovereignty*, Indiana Journal of Global Legal Studies Vol.5, Issue 2, pp. 475-491

[15] Hobbes, T. 1651, *Leviathan*, Renaissance Books, Riverside, CA, U.S.A., October 2013

[16] Holland, B. 2007, *In Defense of Online Intermediary Immunity: Facilitating Communities of Modified*

[17] *Exceptionalism*, Kansas Law Review Vol 56, pp. 101-137

[18] Jilch, N. 2013, *Onlinewährung Bitcoin gilt offiziell als "privates Geld"*, Die Presse http://diepresse.com/home/wirtschaft/international/1442631/Onlinewaehrung-Bitcoin-gilt-offiziell-als-privates-Geld [Accessed: 30.11.2013]

[19] Johnson, D. R, Post, D. G. 1996, *Law and Borders: The Rise of Law in Cyberspace*, 48 Standford Law Review, p. 1367

[20] Kapor, M. 1993, *Where is the Digital Highway Really Going?*, Wired 1(3), p. 53–59

[21] Klang, M. 2005, *Controlling Online Information: Censorship & Cultural Protection*, A presentation given at "WSIS, Internet Governance and Human Rights" Uppsala, October 3, 2005, [on-line] http://www.kus.uu.se/pdf/publications/ICT/klang_03_oct.pdf [Accessed: 09.11.2013]

[22] Kline, J. 2010, *Property and Control: Cyber-libertarianism and Public Policy in the Internet Age*, [on-line] http://thesis.kline.ca/documents/lit-review.pdf [Accessed: 15.11.2013]

[23] Lessig,L. 1999, *Code and Other Laws of Cyberspace*, Basic Books, New York

[24] Lessig, L. 2002, *The Architecture of Innovation*, Duke Law Journal Vol. 51, pp. 1783-1801

[25] Marcus, A., Szoka, B. (eds.) 2010, *The Next Digital Decade: Essays on the Future of the Internet*, pp. 209 -237, p. 210, Techfreedom, Washington, D.C.

[26] Margolis, M., Resnick, D. 2000, *Politics as Usual: The Cyberspace"Revolution"*, Sage, London

[27] Meiklejohn, S. et al. 2013, *A Fistful of Bitcoins: Characterizing Payments Among Men with No Names*, http://cseweb.ucsd.edu/~smeiklejohn/files/imc13.pdf, [Accessed: 16.11.2013]

[28] Murray, A. 2002, Free Expression and Censorship Through Design Protocols: A Misapplication of the ICANN UDRP, 17th Bileta Annual Conference, p.9 [on-line]

[29] http://www.bileta.ac.uk/content/files/conference%20papers/2002/Free%20Expression%20and%20Censorship%20Through%20Design%20Protocols%20-%20A%20Misapplication%20of%20the%20ICANN%20UDRP.pdf, [Accessed: 29.11.2013]

[30] Nakamoto, S. 2008, *Bitcoin: A Peer-to-Peer Electronic Cash System*, http://bitcoin.org/bitcoin.pdf [Accessed: 27.10.2013]

[31] Reidenberg, J. 1998, *Lex Informatica: The Formation of Information Policy Rules Through Technology*, Texas Law Review Vol. 76. Number 3, pp. 553-594

[32] Rousseau, J.J. 1968, *The Social Contract*, Penguin Classics, London

[33] Spar, D.L. 2001, *Ruling the Waves: Cycles of Discovery, Chaos, and Wealth from the Compass to the Internet*, Harcourt Trade Publishers, Sand Diego, CA

[34] Strasser,M. 2001, *Beyond Napster: How the Law Might Respond to a Changing Internet Architecture*, Northern Kentucky Law Review, Number 28, p. 760–712

[35] United States District Court, 2013, *Memorandum opinion regarding the court´s subject matter jurisdiction*, *CASE NO. 4:13-CV-416*, http://ia600904.us.archive.org/35/items/gov.uscourts.txed.146063/gov.uscourts.txed.146063.23.0.pdf [Accessed: 30.11.2013]