
ФИНАНСИЈСКА ТРЖИШТА

Rainer KULMS, Priv.-Doz., Dr. iur., LL.M.
Senior Research Fellow, Max Planck Institute for Comparative and
International Private Law, Hamburg, Germany

BITCOIN – A DIGITAL CURRENCY BETWEEN PRIVATE ORDERING AND REGULATORY INTERVENTION

Summary

Bitcoin has become the most innovative and controversial form of digital money. It operates cross-border as a virtual currency without having the attributes of a real currency, since government backing is absent. Bitcoin depends crucially on the internet. It is open to everybody and has brought forth rudimentary organisational structures with the potential for creating externalities. Internal incentive mechanisms are in effect to maintain the stability of the private currency in an unstable legal environment. This paper reviews the technical aspects and governance mechanisms of Bitcoin in the light of the literature on the tragedy of the (anti-) commons. Government intervention into virtual currencies is still in its infancy. Regulators are currently assessing the benefits of private financial networks against the fall-out from money laundering and tax evasion practices. The future of the virtual currency critically depends on the interface between efficient private ordering and the fight against crime.

Key words: *virtual currencies, the tragedy of the (anti-) commons, regulation of private financial networks.*

I What is Bitcoin?

1. A Currency in a Legal No-man's Land

“Bitcoin is a decentralised, peer-to-peer network-based virtual currency that is traded on-line and exchanged into US dollars and other currencies.”¹ But, according to the former president of the Dutch Central Bank, “this is worse than the tulip mania; at least then you got a tulip (at the end)”² Late in February 2014, the largest exchange for bitcoins, the Tokyo-based Mt. Gox Co., Ltd., went bankrupt, citing losses of bitcoins and customer funds.³ Illinois investors filed a class-action law suit alleging fraud, negligence and breach of fiduciary duties, as they could not withdraw bitcoins from Mt. Gox.⁴ Eventually, a Texas federal district court stayed the action pending the Japanese bankruptcy proceeding.⁵ Later, the insolvent Mt. Gox made it known that it had retrieved in a digital storage file about one quarter of the missing bitcoins.⁶

The Japanese (bankruptcy) application for the commencement of a ‘Procedure of Civil Rehabilitation’ expressly refers to the possibility of an illicit removal of bitcoins from the Mt. Gox.⁷ This seems to confirm warn-

1 US Federal Bureau of Investigation Intelligence Assessment, (U) Bitcoin Virtual Currency – Unique Features Present Distinct Challenges for Deterring Illicit Activity, 24 April 2012 (available at http://www.wired.com/images_blogs/threatlevel/2012/05/Bitcoin-FBI.pdf).

2 Quoted from the The Guardian on line 4 December 2013, “Bitcoin hype worse than tulip mania, says Dutch central banker” (available at <http://www.theguardian.com/technology/2013/dec/04/bitcoin-bubble-tulip-dutch-banker>).

3 Financial Times online 25 February 2014, B. McLannahan, “Fate of Mt. Gox questioned after Bitcoin trading suspended” (available at <http://www.ft.com/intl/cms/s/0/f13bf822-9de4-11e3-95fe-00144feab7de.html#axzz2v6cwn3vK>); Reuters US edition 28 February 2014, “Mt. Gox files for bankruptcy, hit with lawsuit” (available at <http://www.reuters.com/article/2014/02/28/us-bitcoin-mtgox-bankruptcy-idUSBREA1R0FX20140228>).

4 Ars technical (Cyrus Farivar) 28 February 2014, “Illinois man files class-action law suit against Bitcoin exchange MtGox” (available at <http://arstechnica.com/tech-policy/2014/02/illinois-man-files-class-action-lawsuit-against-bitcoin-exchange-mtgox/>); see also Reuters online 15 March 2014, “U.S. class action over bitcoin losses names Mitsuho as defendant” (available at <http://www.reuters.com/article/2014/03/15/us-bitcoin-mtgox-mitsuho-idUSBR EA2E01V20140315>).

5 BBC News Technology online 11 March 2014, “Bitcoin firm Mt Gox wins brief US bankruptcy protection” (available at <http://www.bbc.com/news/technology-26523826>).

6 UPI News online 21 March 2014, “Mt. Gox has found 200,000 bitcoins worth around \$ 114 million” (available at http://www.upi.com/Business_News/2014/03/21/Mt-Gox-has-found-200000-bitcoins-worth-around-114-million/3691395413831/).

7 See translation from the Japanese of 28 February 2014 (available at <https://www.mtgox.com/>).

ings voiced by the US Federal Bureau of Investigation (FBI) in 2013. The FBI felt that the very features of Bitcoin invite criminal activities such as the purchase of illicit goods and money laundering.⁸ In January 2014, New York state officials held hearings on whether to regulate bitcoin trading.⁹ Obviously, supporters of Bitcoin take a much more optimistic approach, highlighting the beneficial effects of a digital currency which is said to be largely inflation-proof. They claim that Friedrich August von Hayek would have approved Bitcoin,¹⁰ since Bitcoin is a private, denationalised currency, totally independent of Central Bank intervention.¹¹ Bitcoin presents a fascinating challenge to lawyers and financial market regulators.¹² It appears to stand for the benefits of private ordering, the fall-out from financial bubbles and its potential for money laundering. Bitcoin is not a new-comer in the field of privately sponsored virtual currencies. But it is the first scheme for a private, digital currency which operates without a centralised steering-mechanism and without direct intervention of central private regulator. Bitcoin by-passes more or less current national securities rules and it does not come under the European Union (EU) rules on electronic cash. The 'external' value of Bitcoin fluctuates, and central Banks (including the European Central Bank) warn consumers about Bitcoin's highly speculative nature.¹³

Bitcoin depends crucially on the internet. It is open to everybody and has brought forth rudimentary organisational structures which require closer

8 See supra sub FN 1. See also Statement by J. Shasky Calvery, Director of the Financial Crimes Enforcement Network, US Department of the Treasury, before the US Senate Committee on Homeland Security and Government Affairs, Washington, D.C., 18 November 2013 (available at <https://www.hsdl.org/?view&did=747209>).

9 See infra sub III.3.b.

10 See F.A. Hayek, "Denationalisation of Money – The Argument Refined, An Analysis of the Theory and Practices of Concurrent Currencies" (The Institute of Economic Affairs, London, 3rd ed., 1990) (available at <http://mises.org/books/denationalisation.pdf>).

11 J. Brito/A. Castillo, "Bitcoin: A Primer for Policy Makers" (Mercatus Center at George Mason University, 2013, available at http://mercatus.org/sites/default/files/Brito_Bitcoin_Primer_embargoed.pdf).

12 See news analysis: The Guardian online 25 November 2013, "Is Bitcoin about to change the world?" (available at <http://www.theguardian.com/technology/2013/nov/25/is-bitcoin-about-to-change-the-world-peer-to-peer-cryptocurrency-virtual-wallet>).

13 See European Banking Authority, Warning to Consumers on Virtual Currencies (EBA/WRG/2013/01, 12 December 2013, available at <http://www.centralbank.ie/public/information/Documents/EBA%20Warning%20on%20Virtual%20Currencies.pdf>); and Wall Street Journal Europe online 5 December 2013, R. Sidel et al., "Central Banks Warn of Bitcoin Risks" (available at <http://online.wsj.com/news/articles/SB10001424052702303497804579239451297424842>); Deutsche Bundesbank, "Interview mit Carl-Ludwig Thiele, Bitcoins sind hochspekulativ", 7 January 2014 (available at http://www.bundesbank.de/Redaktion/DE/Interviews/2014_01_08_thiele_handelsblatt).

inspection with respect to potential externalities.¹⁴ Being open-source and largely unregulated, it has to be ascertained whether Bitcoin will run the risk of becoming a victim of the tragedy of the commons.¹⁵ Closer inspection suggests that Bitcoin may have ‘amended’ the commons of the internet by offering a communitarian governance structure to its users. A potentially tragic fate of the commons may have been averted by Bitcoin’s rudimentary organisation designed to address some collective action problems. This calls for an analysis of whether Bitcoin’s governance structure has *de facto* created property rights as incentive mechanisms for the administrators. Conversely, an uneven distribution of (*de facto*) property rights might result in a tragedy of the anti-commons if incentive mechanisms malfunction. This in turn, raises the question whether regulators’ interest in Bitcoin is purely motivated by a fight against cybercrime or whether regulatory efforts aim at interfering with ill-devised *de facto* private property rights.

2. Outline of the Paper

This paper will first study the technical aspects of Bitcoin in order to ascertain the organisational structure for administering a digital currency scheme. It will then place Bitcoin and its specific internet features in the broader context of the literature on the tragedy of the (anti-) commons in order to appreciate current regulatory attitudes towards digital currencies. This is both a process of legalisation and potentially repressive enforcement strategies against illicit practices. Current government strategies are still in their infancy.¹⁶ In some jurisdictions, Bitcoin is recognised as a digital currency or a unit of account which may give rise to taxation. Other jurisdictions have taken a more hostile stance towards digital currencies introducing an outright prohibition of business transactions in digital currencies.¹⁷ A section on the future of digital currencies at the crossroads between efficient private ordering and the fight against crime concludes.

14 See *infra* sub III.2, 3.b.

15 Cf. on the tragedy of the commons in non-property based schemes for structuring cooperation: Y. Benkler, “Coase’s Penguins, or, Linux and the Nature of the Firm”, 112 *Yale L. J.* 369 (378) (2002).

16 The Library of Congress, Global Research Center, Regulation of Bitcoin in Selected Jurisdictions (January 2014), p. 1 (available at http://www.loc.gov/law/help/bitcoin-survey/2014-010233%20Compiled%20Report_.pdf?loclr=bloglaw).

17 *Ibid.*, country reports.

II Bitcoin and Virtual Currencies in the Age of the Internet

1. Virtual Currencies – The Basics¹⁸

A ‘virtual currency’ operates as a medium of exchange over a network without having the attributes of a real currency; it operates without government backing.¹⁹ Nonetheless, virtual currencies have an equivalent value in real currency or commodities or may serve as a substitute for real currency²⁰. Under art. 2 (2) of the EU’s Electronic Money Directive, ‘electronic money’ means “electronically stored monetary value as represented by a claim on the issuer which is issued on receipt of funds for the purpose of making payment(s) ...”²¹ Electronic money maintains the link with the traditional money format as funds are always expressed in the same unit of account (i.e. traditional currencies).²² Electronic money gets virtual as soon as the ties with a traditional currency unit of account are severed. Proponents of electronic, virtual money tend to emphasise that a global electronic currency reduces or eliminates exchange fees prevalent in international trade.²³ As a corollary, it is the issuer who controls the virtual currency, but neither Central Banks nor

18 For literature survey on alternative currency concepts, see: P. Degens, “Alternative Geldkonzepte – ein Literaturbericht”, Max Planck Institute for the Study of Societies, Discussion Paper 13/1, 2013 (available at http://www.mpifg.de/pu/mpifg_dp/dp13-1.pdf).

19 U.S. Department of the Treasury (Financial Crimes Enforcement Network), Guidance FIN-2013-G001 of 18 March 2013 on the Application of FinCEN’s Regulations to Persons Administering, Exchanging, or Using Virtual Currencies (available at http://fincen.gov/statutes_regs/guidance/html/FIN-2013-G001.html); Statement of M. Raman, Acting Assistant Attorney General, Criminal Division, before the US Senate Committee on Homeland Security and Governmental Affairs, “Beyond the Silk Road: Potential Risks, Threats and Promises of Virtual Currencies”, Washington, D.C., 18 November 2013 (available at <http://www.mainjustice.com/2013/11/18/raman-statement-for-hearing-beyond-silk-road-potential-risks-threats-and-promises-of-virtual-currencies/>); Connecticut General Assembly, Office of Legislative Research, Bitcoins – Virtual Currency (Research Report 2014 – R 0050), 28 February 2014 (available at <http://www.cga.ct.gov/2014/rpt/pdf/2014-R-0050.pdf>).

20 *Ibid.*

21 Directive 2009/110/EC of the European Parliament and of the Council of 16 September 2009 on the taking up, pursuit and prudential supervisions of the business of electronic money institutions, O.J. L 267/ of 10 October 2009. See also the definition in United Kingdom Financial Conduct Authority, The Electronic Money Regulations 2011 (sub 2, available at http://www.legislation.gov.uk/uksi/2011/99/pdfs/uksi_20110099_en.pdf).

22 European Central Bank (ECB), Virtual Currency Schemes (October 2012), at p. 16 (available at <http://www.ecb.europa.eu/pub/pdf/other/virtualcurrencyschemes201210en.pdf>).

23 K. L. Macintosh, “How to Encourage Global Electronic Commerce: The Case for Private Currencies on the Internet”, 11 *Harv. J. L. & Tech.* 733 (757 et seq.) (1998).

other regulatory authorities. In this context, PayPal relies on virtual accounts, but still transfers traditional currencies.²⁴

a) The ECB's Categories

The European Central Bank (ECB) distinguishes between three types of virtual currency schemes. Closed virtual currencies do largely ignore the real economy. They function as 'in-game only' schemes where users, upon payment of a subscription fee, may earn virtual money to be spent within the virtual community. Frequent flyer-programmes by airlines figure prominently among virtual currency schemes with unidirectional flow. Real currency is spent for purchasing virtual currency. This virtual currency cannot be exchanged back to traditional 'real' money. Moreover, the airlines determine the conversion of virtual currency into goods and services.²⁵ By applying different regimes of bonus miles, the airlines do actually control the supply of virtual currency. A virtual currency scheme becomes bidirectional once the users are entitled to buy and sell based upon exchange rates. Like any other currency, a virtual (bidirectional) currency may be used for purchasing real and virtual goods and services.

b) The US Department of the Treasury on Virtual Currency Systems

In its Guidance on virtual currencies, the US Department of the Treasury emphasises the administrative structure of virtual currency systems.²⁶ Centralised virtual (convertible) currencies revolve around a centralised repository. The administrator of this repository is charged with transferring value between persons or locations.²⁷ This transfer of value may also be based on a *de facto* sale of convertible currency to the extent that an exchanger credits the user with an amount of convertible virtual currency on an account held with the administrator.²⁸ The exchanger will then transfer this

24 Cf. ECB, Virtual Currency Schemes, at p. 17 et seq.; I. Kobayashi, "Private Contracting and Business Models of Electronic Commerce", 13 *U. Miami Bus. L. Rev.* 161 (209 et seq.) (2005); *Comb v. PayPal, Inc.*, 218 FS 2d 1165 (1166 et seq.) (N.D. Cal., 2002).

25 There has been some litigation about the airlines' practice to change the conditions of a bonus programme *ex post*. This litigation also demonstrates that transactions in virtual currencies may be predicated upon the existence of property rights. These property rights may be created by the parties to an on-line transaction; they are occasionally recognised by the law.

26 See *supra* FN 19; cf. *passim* J. S. Gans/H. Halaburda, „Some Economics of Private Digital Currency“, Bank of Canada Working Paper 2013/38 (available at <http://www.bankofcanada.ca/wp-content/uploads/2013/11/wp2013-38.pdf>).

27 See *supra* FN 19.

28 See *supra* FN 19.

value to a third party at the user's instruction. From an economic point of view, this amounts to transmission of virtual money to another person on the part of the exchanger. These financial processes do radically change once a de-centralised convertible virtual currency scheme is implemented. Such a de-centralised virtual currency would dispense with a central depository and a single administrator.²⁹ The necessary computing for transmitting (virtual) value is undertaken by the very participants of this currency scheme.

The US Department of the Treasury applies a very fine distinction to decide whether the participants of virtual currency scheme are subject to specific financial market regulations: In a de-centralised scheme for a virtual currency this convertible virtual currency is created by the users themselves who buy real or virtual goods with this new currency.³⁰ Value to this currency is attached by the very willingness of the parties to use this virtual currency as an instrument for settling debt. As long as the person who creates units of this convertible virtual currency employs one a person-to-person basis, he will not be deemed a money transmitter under US Treasury regulations. However, if the creator of virtual currency units sells them to another person for real currency or transfers virtual units to another person upon instruction, the US money transmitter regime applies.³¹

2. The Making of Bitcoin

a) *The 2008 Paper*

Bitcoin saw the light of the digital world in 2008 when a paper on "A Peer-to-Peer System Electronic Cash System" for on-line transactions was published.³² The authenticity of the author has remained obscure. It is unclear whether a group of computer specialists or an individual fathered Bitcoin.³³ The 2008 paper proposes a virtual currency without a central administrator. Instead, it is claimed that the network will be able to police potential double-spending by relying on cryptographic time-stamps which will generate computational proof of the chronological sequence of the transactions undertaken in virtual currency units.³⁴ An electronic coin is defined as an electronic

29 See supra FN 19.

30 See supra FN 19.

31 See supra FN 19.

32 Available at <https://bitcoin.org/bitcoin.pdf>.

33 Banque de France, "Les dangers liés au développement des monnaies virtuelles: l'exemple du bitcoin", Focus no. 10 – 5 December 2013 (available at http://www.banque-france.fr/fileadmin/user_upload/banque_de_france/publications/Focus-10-stabilite-financiere.pdf).

34 See Testimony of P. Murck, General Counsel, the Bitcoin Foundation to the Senate Committee on Homeland Security and Governmental Affairs, "Beyond Silk Road:

signature. In order to effectuate an electronic transfer of payment each owner of a bitcoin will attach his or her electronic signature to the virtual currency unit so that the recipient will not be supplied with electronic cash doubly spent.³⁵ Each bitcoin received carries its cryptographic history with it so that double-use problems can be avoided.³⁶

To ascertain the functionality of Bitcoin it is useful to reflect on the initial transaction with bitcoins and the ensuing acceleration of the system. If the web and the aficionados of digital currencies are to be believed, the first transaction in bitcoins took place early in 2009.³⁷ The creator of the virtual currency sent the amount of 50 bitcoins to another client who at that time maintained both a block database and a transaction database.³⁸ Once the block database had cleared the transaction, the owner of the database had earned his commission (i.e. new bitcoins, ‘mining’) and the digital money could be passed to third parties being also members of the developing bitcoin network.³⁹ Subsequent transactions would create new blocks since the need to prevent double-use by the owner of bitcoins is permanent. A bitcoin protocol was negotiated among the ‘founding fathers’ laying down the ground rules for the operation of the network.⁴⁰

b) Joining Bitcoin

Bitcoin software is open-source and non-proprietary. New ‘entrants’ will be automatically admitted once they subscribe to the Bitcoin protocol.

Potential Risks, Threats, and Promises of Virtual Currencies”, Washington, D.C., 18 November 2013 (available at <http://www.hsgac.senate.gov/hearings/beyond-silk-road-potential-risks-threats-and-promises-of-virtual-currencies>).

35 S. Barber et al., “Bitter to Better – How to Make Bitcoin a Better Currency” (available at <http://crypto.stanford.edu/~xb/fc12/bitcoin.pdf>).

36 Thus a valid bitcoin which may be used for future transactions consists of two electronic signatures: It is the personal signature of the owner of the wallet of bitcoins and a ‘public’ signature will be attached as a consequence of the checking process undertaken with respect to each block of transactions. A valid bitcoin documents its history of previous use. However, in order to reclaim disk space the previous history can be discarded once the transaction has been cleared in the ‘block-building’ process.

37 S. Barber et al., “Bitter to Better”, supra sub FN 35.

38 See information supplied under “The first 50 BTC block reward can’t be spent. Why?” (available at http://www.reddit.com/r/Bitcoin/comments/1nc13r/the_first_50btc_block_reward_cant_be_spent_why/).

39 For details see J. Brito/A. Castillo, “Bitcoin: A Primer for Policymakers”, supra sub FN 11.

40 See Bitcoin Protocol Specification (available at https://en.bitcoin.it/wiki/Protocol_specification); D. T. Rice, “The Past and Future of Bitcoins in Worldwide Commerce”, 2013-Nov Bus. L. Today 1 et seq.; S. Gruber, “Note – Trust, Identity, and Disclosure – Are Bitcoin Exchanges the Next Virtual Havens for Money Laundering and Tax Evasion?”, 32 *Quinnipiac L. Rev.* 135 (143 et seq.) (2013).

'Subscription' to the protocol and its digital payment network is realised by downloading the bitcoin software. Since bitcoins are not represented by physical coins there is a technical need to store the 'memory of the system' in a public ledger.⁴¹ Once the bitcoin software is downloaded to a computer, the new user is entitled to establishing an individual wallet, and a copy of the universal ledger will be automatically stored.⁴² This universal ledger consists of the blocks of transactions and each block builds on previous ones, as only transactions with non-double use bitcoins will be ratified. The initial transactions have created a network of bitcoin software users who depend on the public ledger and a personal wallet of bitcoins, i.e. a Bitcoin address in the form of a cryptographic 'public key'.⁴³ There is a matching 'private key which allows individual access to the network.⁴⁴ Payment from one user to another is triggered by a message from the payor to the payee. The combination of private and public keys will ensure that the valid virtual money will be sent via the bitcoin network.

c) The Division of Labour and Mining

New transactions in bitcoins are sent to all nodes of the network. These nodes will group new transactions into blocks, updated every ten minutes. Once such a node identifies a transaction as difficult to be verified, it will be effectively thrown out, thereby invalidating the transaction as an attempt to double-spend a bitcoin. The result of this verification process will be transmitted to all other nodes in order to inform the participants of the system of 'false' money.⁴⁵ Once a node has ratified a block of transaction for payment purposes, it will automatically create the next block.

Although Bitcoin operates as a peer-to-peer network without a central agency, the ratification procedure has brought forth a special class of members of the community.⁴⁶ In fact, the ratification procedure demonstrates a division of labour. Only sophisticated users will dispose of highly complex

41 See Bitcoin, How does Bitcoin Work? (available at <https://bitcoin.org/en/how-it-works>); P. Noizat, *Bitcoin Book* (in French, edition 2012, Pierre Noizat), p. 19 et seq.

42 Testimony of P. Murck to the Senate Committee on Homeland Security and Governmental Affairs, "Beyond Silk Road: Potential Risks, Threats, and Promises of Virtual Currencies", Washington D.C., 18 November 2013; ECB, Virtual Currency Schemes, supra sub FN 22; see also P. Noizat, *Bitcoin Book*, p. 25 et seq., 71.

43 N. Passaras, "Comment – Regulating Digital Currencies: Bringing Bitcoin Within the Reach of the IMF", 14 *Chi. J. Int'l. L.* 377 (385 et seq.) (2013).

44 *Ibid.*

45 S. Barber et al., "Bitter to Better", supra sub FN 35.

46 See R. Grinberg, "Bitcoin: An Innovative Alternative Digital Currency", 4 *Hastings Sci. & Tech. L. J.* 159 (162 et seq.) (2012).

computer facilities to analyse the validity of the transaction. Other will just want to use the system for transmitting bitcoins across the network, relying on the block-services rendered by others.⁴⁷ This division of labour is enshrined by the system of incentives underlying the verification process for the benefit of the whole network. Once the owner of the complex verification computer facilities starts checking the validity of a block, a bitcoin is earned as a commission (i.e. a reward for undertaking verification voluntarily). Thus the first transaction in a block under exam is the creation of a new bitcoin. In the language of the Bitcoin community, the owners of the computer facilities to undertake to analysis of the transactions are called miners, since new bitcoins can only be issued as a result of this ‘block examination’.⁴⁸ It is as yet unclear whether this division of labour generates de facto property rights. Miners might acquire more relevant information than normal users who just ‘place’ their transaction on the network, trusting the efficiency of the ledger and those who update it.

Since its inception ‘block examinations have taken place at an ever accelerating pace so that in April 2013, the total value of bitcoins in circulation reached 1.5 bn US \$.⁴⁹ For technical reasons, the production of new bitcoins will not exceed 21 m Bitcoins.⁵⁰ It is obvious that the end of the ‘coining’ process will affect the economic incentives to undertake the creation of new blocks and the examination of transactions to avoid double-spending.

III Bitcoin between *Laissez-faire* and Regulation

1. A Tragedy of the Commons or Successful Joint Management?

When Bitcoin was first introduced as a currency and a *de facto* organisation, it was heralded as an instrument to save transaction costs in an atmosphere of great privacy.⁵¹ The organisational structure of the network

47 Cf. D. T. Rice, “The Past and Future of Bitcoin in Worldwide Commerce”, 2013-Nov *Bus. L. Today* 1 (2013).

48 P. Noizat, *Bitcoin Book*, 45 et seq.; K.L. Penrose, “Banking on Bitcoin: Applying Anti-Money Laundering and Money Transmitter Laws”, North Carolina Banking Institute, 18 *N.C. Banking Inst.* 529 (532 et seq.) (2014); R. Grinberg, 4 *Hastings Sci. & Tech. L. J.* 159 (163 et seq.) (2012).

49 N.A. Plassaras, “Regulating Digital Currencies; Bringing Bitcoin Within the Reach of the IMF”, 14 *Chi. J. Int’l L.* 377 (392) (2013).

50 There is some controversy when this cap on the production of new bitcoins will take effect: Speculations vary considerably between 2025 and 2140. See N. M. Kaplanov, “Nerdy Money: Bitcoin, the Private Digital Currency, and the Case Against its Regulation – Student Comment”, 25 *Loy. Consumer L. Rev.* 111 (121) (2012); Banque de France, “Les dangers liés au développement des monnaies virtuelles”, supra sub FN 33.

51 See Financial Times online 24 February 2014, J. Einhorn, “Bitcoin is still a useful bludgeon” (available at <http://www.ft.com/cms/s/0/d0530f6e-998f-11e3-b3a2-00144feab7de.html>).

is relatively straight-forward, thus adding to the legitimacy of Bitcoin as a convertible virtual currency. Traditional currencies are converted into bitcoins and vice versa at specific exchanges. Due to the conceptual design of the Bitcoin currency the amount of bitcoins created during the mining process is finite, as the complexity of verifying transactions puts an effective cap on the production of money. Bitcoin is therefore to produce long-term anti-inflationist effects. On the other hand, the future of Bitcoin is hard to predict due to its vulnerability to external shocks and its potential for abuse through money laundering and fraud.⁵² Thus, bitcoins have come to be considered as investments promising high returns in a decidedly speculative environment. It is this latter aspect which has motivated criticism of Bitcoin as a financial instrument creating bubbles and inviting investments by individuals being less than risk-averse.⁵³ Regulatory policy debates focus on Bitcoin's potential for creating negative externalities,⁵⁴ but tend to overlook the distribution of property rights, the specific characteristics of a transnational internet and the efforts to avoid both a tragedy of the commons and the anti-commons. Thus any meaningful attempt to regulate trading in bitcoins is predicated on an analysis of Bitcoin's communitarian governance mechanism as an attempt to protect the internet from a tragedy of the commons.

In the law literature, 'commons' generally describes 'land owned by the government' or 'something free for everyone'.⁵⁵ A definition has been proposed which focuses on exclusionary powers and the decision-making power over the use of a resource.⁵⁶ Charlotte Hess and Elinor Ostrom caution however against a dichotomy between common-pool resources and property regimes.⁵⁷ In fact, many common-property regimes have succeeded administering the joint management of a resource.⁵⁸ It is Ostrom's conclusion that the traditional policy recommendation to address the tragedy of the commons by a private property rights regime is overly simplistic. Instead she observes that commons problems have been overcome by introducing a community-organisation which restricts the use of the commons while maintaining its

52 Cf. New York Times online, 17 February 2014, N. Popper, "Regulators and Hackers Put Bitcoin to the Test" (available at http://dealbook.nytimes.com/2014/02/17/regulators-and-hackers-put-bitcoin-to-the-test/?_php=true&_type=blogs&_r=0).

53 See The Economist online 30 November 2013 (available at <http://www.economist.com/news/leaders/21590901-it-looks-overvalued-even-if-digital-currency-crashes-others-will-follow-bitcoin>).

54 See *infra* sub III.3.b.

55 C. Hess/E. Ostrom, "Ideas, Artifacts, and Facilities: Information as Common-Pool Resource", 66 *L. & Contemp. Probs.* 111 (114 et seq.) (2003).

56 Y. Benkler, 112 *Yale L.J.* 369 (410 et seq.) (2002).

57 C. Hess/Ostrom, 66 *L. & Contemp. Probs.* 111 (121 et seq.) (2003).

58 *Ibid.* at p. 123 et seq.

general accessibility without imposing private property rights.⁵⁹ In this, Ostrom maintains that the idea of the commons and an autonomous institution averting the tragedy of the commons are not mutually exclusive. A commons needs not be privatised to be administered efficiently.⁶⁰ Bitcoin's intricate electronic structure has replaced the 'commons of the internet'. Bitcoin's supporters implicitly claim that the quasi-organisational character of the network and its inherent incentive mechanisms will contribute to maintaining the stability of the virtual currency. Ostrom has shown that incentive mechanisms can be easily reconciled with the notion of an organised commons.⁶¹ In fact, commissions which accrue to the 'policemen' of the organised commons, the bitcoin miners, are intended to support the stability of the network. Commons communities can be organised by a contractual mechanism as long as they do not experience collaborative failure by the participants.⁶² In this context, newcomers to Bitcoin do not challenge the quasi-contractual mechanism of the system as they cannot participate in the currency network without pledging allegiance to the original protocol.

Recent experiences with the organised commons of Bitcoin suggest, however, that the currency is not free from deficiencies. In fact, the fathers of Bitcoin might be accused of ignoring Ostrom's advice on how to organise a communitarian governance structure while ensuring the best available service by the organised commons to its users. Once Bitcoin reaches the maximum amount of available currency units the incentive structure for its policemen, the miners, will change dramatically. Admittedly, virtual property rights in an internet-based currency system will not automatically create an anti-commons with negative side-effects.⁶³ What is at stake in the context of Bitcoins is whether the organisational properties of the currency will not generate discrimination among its users and encourage moral and security hazards.⁶⁴ In the following, the potential for creating inefficient distribution of property rights within Bitcoin will be examined as this might ultimately trigger a tragedy of the anti-commons.

59 E. Ostrom, *Governing the Commons – The Evolution of Institutions for Collective Action* (New York, Cambridge University Press 1990), at p. 29 seq.

60 E. Ostrom, *Governing the Commons*, p. 33 on organising 'common-pool resources'. See also B. Hudson/J. Rosenbloom, "Uncommon Approaches to Commons Problems: Nested Governance Commons and Climate Change", 64 *Hastings L.J.* 1273 (1284 et seq.) (2013).

61 E. Ostrom, *Governing the Commons*, pp. 61 et seq., 69 et seq.

62 J.-A. Lee, "Organizing the Unorganized: The Role of Nonprofit Organizations in the Commons Communities", 50 *Jurimetrics J.* 275 (310 et seq.) (2010).

63 See J.A.T. Fairfield, "Virtual Property", 85 *B.U.L. Rev.* 1047 (1073 et seq.) (2005). For an analysis of the tragedy of the digital anticommons: D. Hunter, "Cyberspace as Place and the Tragedy of the Digital Anticommons", 91 *Cal. L. Rev.* 439 (509 et seq.) (2003).

64 Cf. S.J. Shackelford, "Toward Cyberspace: Managing Cyberattacks Through Polycentric Governance", 62 *Am. U. L. Rev.* 1273 (1321 et seq.) (2013).

2. How Common is Bitcoin?

Mining is at the core of the Bitcoin organisation. It checks the reliability of transactions and is crucial for the issuance of new bitcoins. The technical capability of administering the mining process creates a potential for property rights, a hierarchy in the system and requests for commissions.⁶⁵ Thus, there is considerable economic value in the mining process. Contracts offered via the internet confirm this finding: Interested users can acquire the necessary software to become a 'miner' by signing a 'Cloud Hashing Contract' for three to six months.⁶⁶ But so far, it is unclear whether efficient policing by miners can be ensured when the currency will no longer expand. This might create imbalances as miners in their capacity of policemen could then acquire *de facto* property rights which thwart Ostrom's incentive system of enforcement officers working for the communitarian governance structure of the commons.⁶⁷ Moreover, 'third party mixers' might exploit their position by obscuring the identity of those behind the transactions.⁶⁸ Deficiencies or delays in the verification process currently go unpunished.⁶⁹

When in February 2014, trading in bitcoins temporarily broke down, a core group of six developers had to devise amended software so that the process of verifying software could be resumed.⁷⁰ Thus Bitcoin's current vulnerability results from small number of experts sufficiently knowledgeable to repair the system and abolish delays in processing transactions for verification.⁷¹ This suggests that the founding fathers of Bitcoin still retain considerable control of the system.⁷² There is a powerful incentive for the founding fathers to remedy defaults of the system, but there is also a potential for mor-

65 See P. Noizat, *Bitcoin Book*, 65, who emphasises that without a commission regime there is a risk of delay in the verification process which might amount to three days.

66 See Bitcoin Cloud Hashing, Mining Contracts (available at <https://www.bitcoinclouddhashing.com/product-category/mining-contracts/>).

67 On the economics of the 'mining process': P. Noizat, *Bitcoin Book*, 64 et seq.

68 See remarks on <http://bitcoinmagazine.com/5161/bitcoin-is-not-losing-its-soul-or-why-the-regulation-hysteria-is-missing-the-point/>.

69 Cf. S. Barber et al., "Bitter to Better", supra sub FN 35. For P. Noizat, *Bitcoin Book*, 64 et seq., a system of commissions would be sufficient to incentivise miners to check expeditiously. On the other hand, miners will only amend the verification process if significant competitive advantages are to be expected (P. Noizat, *ibid.*, at p. 65).

70 Financial Times on-line, 14 February 2014, "Bitcoin's volunteer army tested by attack" (available at <http://www.ft.com/cms/s/0/cc63ad06-9592-11e3-8371-00144feab7de.html>).

71 See Financial Times online 14 February 2014, "Bitcoin's volunteer army tested by attack" (available at <http://www.ft.com/intl/cms/s/0/cc63ad06-9592-11e3-8371-00144feab7de.html#axzz2v76XvvRK>).

72 To that extent, Bitcoin is characterised by information asymmetry: ECB, Virtual Currency Schemes, supra sub FN 22, at p. 27.

al hazard and the potential for abuse as the reward regime of new bitcoins will gradually be replaced by commissions. Current proposals to modify the Bitcoin protocol assume that the community-based system of managing the virtual currency might be adapted to fending off signature falsifications and other malware attacks.⁷³ This would require a modified threshold cryptography and a restructuring of wallets. Moreover, the potential for moral hazard and abuse will have to be addressed as ‘third party mixers’ obscure the identity of those behind the transactions. A ‘Fair Exchange Protocol’ is advocated to remedy the fallacies of the original Bitcoin protocol⁷⁴ which appears to be threatened by the rapid growth of the currency.

If Bitcoin is live up to Elinor Ostrom’s claim that community-based systems of managing the commons increase efficiency,⁷⁵ it will have to modernise. Unfortunately, modernisation of Bitcoin might be much more difficult to be implemented than in Ostrom’s self-organising common pools of resources. Plans for amendments of the original Bitcoin protocol have a potential for triggering collective action problems as a consensus to revise the protocol will have to be engineered.⁷⁶ Conversely, if the founding fathers propose changes to trading rules for bitcoins,⁷⁷ most users are likely to accept in a realistic assumption of the know-how and the balance of power. In a twist, this would again confirm that the founding fathers enjoy a position of power which amounts *de facto* to an exercise of property rights. If the founding fathers, miners and specialists fail to master the current difficulties of the system, Bitcoin both as an organisation and a currency might face tragic consequences which regulators will wish to address, albeit in an indirect way.

3. Legal Challenges

a) *The Internet*

It is a truism that the internet stands for the globalisation of information and for the free flow of data. Apart from sensitive information, gov-

73 See S. Barber et al., “Bitter to Better”, supra sub FN 35.

74 S. Barber et al., “Bitter to Better”, supra sub FN 35. In this context, it is suggested that a more demanding burden of proof should be imposed for the verification process.

75 See supra sub FN 59–61.

76 See passim on collective action problems in decentralised networks: N. Plassaras, 14 *Chi. J. Int’l. L.* 377 (406) (2013).

77 See White Paper, “A Next-Generation Smart Contract and Decentralized Application Platform”, ethereum wiki (available at <https://github.com/ethereum/wiki/wiki/%5BEnglish%5D-White-Paper>), and CNN Money 21 January 2014, “Bitcoin is not just digital currency. It’s Napster for Finance” (available at <http://finance.fortune.cnn.com/2014/01/21/bitcoin-platform/>).

ernments have never interfered with the free cross-border flow of data even if intellectual property rights (under licensing agreements) were affected.⁷⁸ ‘Borderlessness’ of the internet, however, does not imply lawlessness.⁷⁹ For more than a decade the internet has been subject to private regulatory efforts to assure technical standardisation and geo-identification.⁸⁰ It is noteworthy, however, that the transnational nature of the internet has largely precluded public authorities from addressing potential externalities of the web. This has ushered in private, self-regulation mechanisms designed to become self-enforceable in the face of practical difficulties of public regulation in a cross-border context. As far as public authorities would disapprove of a virtual currency traded via the internet they are confined to warning the general public of the speculative nature of the currency.

b) Status quo and Plans for Regulation

The survey of ‘Regulation of Bitcoin in Selected Jurisdictions’ undertaken by the Law Library of the US Congress⁸¹ Library of the US Congress reveals a diversity in regulatory attitudes. Some countries flatly outlaw transactions in bitcoins since a virtual currency is not recognised as legal tender.⁸² Others recognise contracts for or in bitcoins as valid under the respective civil codes so that parties might claims damages and tax authorities have a basis for taxing income or imposing value-added-tax.⁸³ Some jurisdictions classify bitcoin exchanges or special service providers as financial service providers who require licensing under the respective financial market laws.⁸⁴ There has

78 J. Basedow, ‘The Law of Open Societies – Private Ordering and Public Regulation of International Relations’, *Académie de Droit International, Recueil des Cours* 360 (2012), 1 (91 et seq.).

79 See D. Jerker/B. Svantesson, *Private International Law and the Internet* (Wolters Kluwer, 2nd ed. Alphen aan den Rijn, 2012), 34, and their critique of traditional jurisdictional concepts, 50 et seq.

80 B. du Marais, in: G. Chatillon, 286 et seq.; D. Jerker/B. Svantesson, 414 et seq.

81 See supra FN 16.

82 *Ibid.*, see also Financial Times online 2 April 2014, ‘Bitcoin set for fresh Chinese regulatory attack’ (available at <http://www.ft.com/cms/s/0/ed3ee914-ba4f-11e3-aeb0-00144feabdc0.html#axzz2yNbNFOXW>).

83 *Ibid.* See also California Assembly Bill AB 129 of 23 January 2014 recognising Bitcoin as a lawful alternative currency (available at http://www.leginfo.ca.gov/pub/13-14/bill/asm/ab_0101-0150/ab_129_cfa_20140128_174724_asm_floor.html).

84 See e.g. the German regulatory approach towards bitcoin service providers: Bundesanstalt für Finanzdienstleistungsaufsicht (BaFin), J. Münzer, ‘Bitcoins, Aufsicht-rechtliche Bewertung für Nutzer’, *BaFin Journal* 1/2014, 26 et seq. (available at https://www.bafin.de/SharedDocs/Downloads/DE/BaFinJournal/2014/bj_1401.pdf?__blob=publicationFile&v=4).

been litigation on the scope of this licensing or registration requirement;⁸⁵ but current regulations on financial service providers do not offer much guidance on specific behavioural duties for online trading in virtual currencies.

In August 2013, the New York Department of Financial Services launched an inquiry into virtual currencies in order to determine the need for regulatory action. In a public notice, the Department referred to evidence that virtual currencies were instrumental in supporting drug smuggling, money laundering, gun running and child pornography.⁸⁶ In January 2014 hearings were held in order to ascertain at what stage of trading in bitcoin a regulator should intervene.⁸⁷ It soon became clear that the sheer magnitude of transactions and the multi-national dimension of bitcoin trading require a fine-tuned approach to virtual currencies⁸⁸ which would have to combine domestic regulation with an appreciation of specificities of a global internet.⁸⁹ This led the New York state superintendent of financial services to caution against comprehensive oversight for every single peer-to-peer transaction unless specific criminal or civil wrongdoing could be established.⁹⁰

85 See US SEC v. Trendon T. Shavers and Bitcoin Savings and Trust, 2013 WL 4028182 (E.D. Tex., 2013), and US Department of Justice, Press Release, “Manhattan U.S. Attorney Announces Charges Against Bitcoin Exchangers, Including CEO of Bitcoin Exchange Company, For Scheme To Sell and Launder Over \$ 1 Million in Bitcoins Related to Silk Road Drug Trafficking”, 27 January 2014 (available at <http://www.justice.gov/usao/nys/pressreleases/January14/SchremFaiellaChargesPR.php>).

86 New York State Department of Financial Services, Notice to Hold Hearing on Virtual Currencies, Including Potential NYDFS Issuance of a ‘BitLicense’, 14 November 2013 (available at <http://www.dfs.ny.gov/about/press2013/virtual-currency-131114.pdf>).

87 See the agenda of the hearing: New State Department of Financial Services, NYDFS Outlines Additional Details on Witness and Panels for Currency Hearing on January 28 and 29 in New York City (available at http://www.dfs.ny.gov/about/panels_witnesses_virtual_currency_hearing.pdf).

88 For an account of the hearing see M. Ferranti, “Bitcoin investors, legal experts grilled by New York regulators”, 28 January 2014 (available at <http://news.idg.no/cw/art.cfm?id=894D54F8-CC1B-B169-CD070473C48DB1D1>), and I. Marritz, “New York Looks To Bring Bitcoin Out of the Shadows”, 30 January 2014 (available at <http://www.npr.org/blogs/alltechconsidered/2014/01/30/268686547/new-york-could-become-the-center-of-legitimate-bitcoin-commerce>).

89 See Testimony of Marco Santori, Chairman, Regulatory Affairs Committee, The Bitcoin Foundation, to the New York Department of Financial Services Hearing on Virtual Currencies, 28 January 2014 (available at <https://bitcoinfoundation.org/blog/wp-content/uploads/2014/01/Bitcoin-Foundation-Marco-Santori-NYDFS-Hearing-on-Virtual-Currencies-Testimony.pdf>).

90 Remarks of Benjamin M. Lawsky, Superintendent of Financial Services for the State of New York, on the Regulation of Virtual Currencies at the New Age Foundation in Washington, D.C., 11 February 2014 (available at http://www.dfs.ny.gov/about/speeches_testimony/sp140212.htm).

It has been suggested that the permission to use software is an incident of application service providing, subject to a specific contract under the law of obligations.⁹¹ There are licensing elements in this which would entitle the parties to damages in case of a breach of contract.⁹² However, in view of the technical idiosyncrasies of bitcoin this is not a very realistic alternative. Unless verification and mining services are outsourced to highly sophisticated service providers,⁹³ the miners will remain anonymous and if known, any legal action would present formidable private international law problems. Outsourcing verification might also accommodate incentive problems once miners can no longer create new bitcoins as the finite cap is reached. Judging from the hearing before New York state financial regulators, the negative externalities of mining and verification may be contained by employing specific regulated service providers.⁹⁴ In this context, it should be recalled that the EU's directive 1999/93/EC on a Community framework for electronic signatures provides for 'certification-service-providers' who provide for services related to electronic signatures.⁹⁵ The directive also lays down ground rules on liability of certification-service-providers.⁹⁶

Under the current legal situation, several layers for potential regulation have to be identified. Registration under the Bitcoin protocol basically opens access to free trading facilities over the internet. This raises questions about the legal relationship between the new entrant and the miners who verify transactions and might create externalities by inappropriate behaviour. As a corollary, the safety of technical procedures will have to be ascertained.

If not earned during the mining process, Bitcoins can be purchased at local exchanges. From a conflict of laws perspective, these transactions are less difficult to regulate. They also inspire regulators' creativity with respect to proposing a licensing system.⁹⁷

Apart from these archetypes of bitcoin transactions, more sophisticated transactions can be envisaged where mining is outsourced or financial companies offer specific services with respect to transmitting virtual money from a payor to a payee.

91 H. Redeker, *IT-Recht* (Verlag C.H. Beck, Munich 5th ed. 2012), 361.

92 *Id.*, at p. 364 et seq.

93 See e.g. the homepage of BIPS Denmark (available at <https://bips.me/merchants>).

94 See supra FN 89 et seq.

95 See art. 1 (11) of the Directive 1999/93/EC of the European Parliament and of the Council of 13 December 1999, O.J. L 13/12 of 19 January 2000.

96 *Ibid.*, art. 6.

97 See K. Hill, "New York May Give 'BitLicenses' to Bitcoin Companies", 14 November 2013 (available at <http://www.forbes.com/sites/kashmirhill/2013/11/14/new-york-may-give-bitlicenses-to-virtual-currency-companies/>).

c) *Bitcoin Exchanges, Money Storage Facilities and Special Service Providers*

In spite of its transnational character Bitcoin, both as a currency and an organisation does not completely escape national jurisdictions. In fact, Bitcoin has to ‘touch’ down on national, decentralised trading platforms or exchanges where local customers convert national currencies into bitcoins or vice versa.⁹⁸ Frequently, these institutions offer additional facilities such as accounts where customers may store their amounts in virtual currency. In 2013/2013, Bitcoins registered as a payment services provider under European Union law.⁹⁹ Technically, payment or exchange services by Bitcoin are offered by legal entities which operate as an agent for a national financial institution in a Member State of the European Union. This has led to a decentralised market for buying bitcoins. Potential users of bitcoin who do not make virtual money by ‘mining’ will have to register an account with a respective national trading platform. Users have voiced concerns that this practice leaves considerable room for arbitraging if the exchange rate for bitcoin varies.¹⁰⁰

In opening an account with one of the national Bitcoin trading platforms, the user will have to accept the Standard Conditions of the respective national law.¹⁰¹ National Consumer Protection laws will then control the interpretation of the contracts on opening an account. This will not ensure harmonised standards on bitcoin trading platforms since the applicable law may vary from jurisdiction to jurisdiction. Nonetheless, financial regulators have come to classify these local platforms as a minimum-contact instrumentality which creates jurisdiction over Bitcoin and foreign exchanges.¹⁰² On 14 May 2013, the US District Court for Maryland ordered the seizure of Mt. Gox’s funds in an account with Dwolla, an online payment service provider for

98 When traded at various exchanges, Bitcoin floats against other currencies on the basis of demand: Kaplanov, 25 *Loy. Consumer L. Rev.* 111 (121 et seq.) (2012).

99 The Guardian 7 December 2012 on-line, “Virtual currency Bitcoin registers with European regulators” (available at <http://www.theguardian.com/technology/2012/dec/07/virtual-currency-bitcoin-registers>).

100 See the discussion on the Bitcoin Forum on Bitcoin Exchange Arbitrage Opportunities (available at <https://bitcointalk.org/index.php?topic=8399.0>).

101 See e.g. the Standard Conditions of Bitcoin Deutschland GmbH (Geschäftsbedingungen der Bitcoin Deutschland GmbH, available at <https://www.bitcoin.de/de/agb>).

102 Cf. the studies on Internet Jurisdiction: D. Jaeger-Fine et al., “Internet Jurisdiction: A Survey of German Scholarship and Cases, Center on Law and Information Policy at Fordham Law School”, 30 June 2013 (available at http://papers.ssrn.com/sol3/papers.cfm?abstract_id=2309575) and J. R. Reidenberg et al., “Internet Jurisdiction: A Survey of Legal Scholarship Published in English and United States Case Law”, Center on Law and Information Policy at Fordham Law School, 30 June 2013 (available at http://papers.ssrn.com/sol3/papers.cfm?abstract_id=2309526).

customers interested in buying bitcoins.¹⁰³ Mt. Gox, the now defunct bitcoin exchange, had operated out of Tokyo, using a number of US instrumentalities which were to collect customer money for engineering bitcoin transactions via Japan. US authorities had established that domestic instrumentalities had been active in undertaking unlawful trading in currencies as a ‘money transmitter’.¹⁰⁴ In the aftermath of the New York hearing, regulators ponder about whether to introduce a licensing scheme for financial institutions dealing in virtual currencies.¹⁰⁵ Public regulation would create safe harbour provisions whereby financial institutions would be allowed to continue trading as long as anti-money laundering provisions and consumer protection standards are observed.¹⁰⁶

From a long-term perspective, local special service providers might operate in a growth business which warrants closer scrutiny and stricter behavioural standards. If users contract for bitcoin accounts with these service providers,¹⁰⁷ some specific protective devices are apposite. Otherwise users would be relegated to normal bankruptcy law proceedings where most of their deposits could be lost.¹⁰⁸ In the past, members of the community have described these service providers as ‘bitcoin laundries’,¹⁰⁹ but it would seem that regulatory efforts should go beyond anti-money laundering devices. In the case of Bitcoin’s prolonged success, future currency contracts could be envisaged which are tied to Bitcoin mining companies envisaging a return on the amount of Bitcoins mined.¹¹⁰

103 US District Court for the District of Maryland, Seizure Warrant of 14 May 2013, Case Number 13-1162 SKG (available at <https://s3.amazonaws.com/s3.documentcloud.org/documents/701175/mt-gox-dwolla-warrant-idg-news-service.pdf>).

104 See the Seizure order of the US District Court of 14 May 2013.

105 See K. Hill, 14 November 2013, supra FN 98; Remarks by B.M Lawsky, supra FN 91, and the Testimony by M. Santori, supra FN 90.

106 See analysis A. Greenberg, Forbes online 28 January 2014, “Bitcoin Investors Ask for ‘Safe Harbor’ Exceptions in Proposed ‘BitLicense’ Regulations” (available at <http://www.forbes.com/sites/andygreenberg/2014/01/28/bitcoin-investors-ask-for-safe-harbor-exceptions-in-proposed-bitlicense-regulations/>).

107 See e.g. information on the services offered by the French bitcoin trading platform Paymium (available at <http://paymium.com/>).

108 See Spiegel online 4 April 2013, “Virtuelle Wahrung: Hack-Attacken bremsen Bitcoin-Rallye” (available at <http://www.spiegel.de/netzwelt/web/hacker-angriff-auf-bitcoin-dienstinstawallet-kurs-steigt-nicht-mehr-a-892438.html>).

109 See information on ‘The hidden politics of bitcoin mixing services’, available under <http://www.howtogetbitcoins.info/the-hidden-politics-of-bitcoin-mixing-services/>.

110 See Testimony of Deputy US Attorney R.B. Zabel of 29 January 2014 at the New York State Department of Financial Services Hearing on Law Enforcement and Virtual Currencies (available at <http://www.justice.gov/usao/nys/pressspeeches/2014/DFSLawEnforcementandVirtualCurrenciesHearing2014.php>).

3. *Whither Bitcoin?*

Bitcoin is an open-source network, demonstrating the classic features of a commons with a rudimentary, community-based organisation designed to fend off signature falsifications and other malware attacks. The connoisseurs of Bitcoin argue that the system is relatively safe from abuse and outsider attacks.¹¹¹ Nonetheless, it should not be overlooked that an attacker might attempt to re-write the history of transactions in order to create additional bitcoins for his or her own benefit. The temptation to shirk within Bitcoin is triggered by in-built deflationist tendencies.¹¹² As the money-creating process approaches the finite cap, the value of the individual digital coin is likely to explode, hence inviting theft. Moreover, as the checking activities will reach the ultimate frontier of electronic money-printing, the disincentives to verify transactions are bound to increase. This development can only be averted by improving the system of commissions which operate as incentives to maintain verifying computer facilities.

It would seem that change will only come by amending the original Bitcoin protocol. It remains to be seen how Bitcoin can evolve and consensus to amend a digital currency can be achieved. It has been suggested that a revision of Bitcoin should also extend to the verifying process by requiring a more demanding burden of proof. This, however, assumes that the distribution of property rights is such that the verifiers will accept change.

By focusing on Bitcoin's local trading platforms law enforcement officials have pledged to remedy some of the negative externalities of a virtual currency. But with a dose of realism, they refrain from curing organisational deficiencies of Bitcoin as such. Rather, regulators plan to attack fraud, money laundering and plans to operate on-line Ponzi schemes.¹¹³ A licensing requirement for traders will not affect Bitcoin's potential for facilitating tax evasion and its vulnerability to theft. In its current form bitcoin is likely to operate as a tax haven as national tax authorities experience difficulties in tracing

111 According to J. Brito/A. Castillo, "Bitcoin: A Primer for Policymakers", supra sub FN 11, criminal use of the Bitcoin technology does not warrant an outright prohibition of the virtual currency. As Bitcoin expands, legitimate uses are to outweigh criminal transactions. See also the endorsement of electronic currencies by K. L. Macintosh, "How to Encourage Global Electronic Commerce: The Case for Private Currencies on the Internet", 11 *Harv. J.L. & Tech.* 733 (792 et seq.) (1998).

112 S. Barber et al., "Bitter to Better", supra sub FN 35.

113 Testimony of R.B. Zabel, supra sub FN 111. According to the US Securities and Exchange Commission, "(a) Ponzi scheme is an investment scam that involves the payment of purported returns to existing investors from funds contributed by new investors": US SEC, Office of Investor Education and Advocacy, Investor Alert – Ponzi Schemes Using Virtual Currencies (SEC Pub. No. 153 (7/13), available at https://www.sec.gov/investor/alerts/ia_virtualcurrencies.pdf).

a breach of tax law to one jurisdiction.¹¹⁴ In this context, US and German tax authorities have recognised Bitcoin as a trading unit in order to establish a basis for taxing income derived from trade in virtual currencies.¹¹⁵

In comparing the statements of New York financial regulators with the pronouncements of central banks it is interesting to see that the prevention of bubbles or speculative investments does not figure prominently on the regulatory agenda.¹¹⁶ Value to Bitcoin is attached by private agreement to accept bitcoins as an instrument of payment. Contrary to Hayek's scheme on private currencies, commodities do not necessarily serve as instruments for reference for Bitcoin. Bitcoin is as yet the most successful and most controversial virtual currency scheme. It might fail. But whatever its fate it will offer crucial insights for more sophisticated and less fraud-prone structures of virtual exchanges of money.¹¹⁷ In the denationalised world of virtual currencies local regulated service providers might not just exchange real money for electronic money, they might as well assume the role of commission-earning miners verifying the authenticity of an electronic transaction.¹¹⁸

114 See O. Marian, "Are Cryptocurrencies Super Tax Havens?", 112 *Mich. L. Rev. First Impressions* 38 (43 et seq.) (2013).

115 See US Government Accountability Office, Report to the Committee on Finance, US Senate, Virtual Economies and Currencies – Additional IRS Guidance Could Reduce Tax Compliance Risks (GAO-13-516), May 2013 (available at <http://www.gao.gov/assets/660/654620.pdf>); CNBC.com online 19 August 2013, "Bitcoin recognized by Germany as 'private money'" (available at <http://www.cnbc.com/id/100971898>) and Handelsblatt online 17 August 2013, "Finanzministerium erkennt Bitcoins an" (available at <http://www.handelsblatt.com/finanzen/rohstoffe-devisen/devisen/internet-geld-finanzministerium-erkennt-bitcoins-an/8653802.html>).

116 See Remarks of B.M. Lawsky, supra FN 91 and Testimony of R.B. Zabel, supra FN 111.

117 Cf. N. Popper, "Regulators and Hackers Put Bitcoin to the Test", supra sub FN 52, commenting on Professor Susan Athey's remarks on Bitcoin and its potential for inspiring less vulnerable money transfer programmes.

118 See also The Economist 15 March 2014, "Bitcoin's Future – Hidden Flipside – How the Cryptocurrency could become the internet of money" (available at <http://www.economist.com/node/21599054/print>), on global banks exploring Bitcoin-like currencies for money transfers between subsidiaries.

др Рајнер КУЛМС, LL.M.

Виши научни сарадник на Макс Планк Институту за упоредно и међународно приватно право, Хамбург, Немачка

БИТКОИН – ДИГИТАЛНА ВАЛУТА ИЗМЕЂУ ПРИВАТНОГ УРЕЂЕЊА И РЕГУЛАТОРНЕ ИНТЕРВЕНЦИЈЕ

Резиме

Биткоин је постао најиновативнији и најконкретнији облик дигиталног новца. Он функционише прекогранично као виртуелна валута и нема карактеристике стварне валуте, јер нема подршку државе. Биткоин у популарности зависи од интернета. Он је отворен за све и довео је до настанка рудиментарних организационих структура које могу да изазову екстерне ефекте. Тренутно постоје интерни подстицајни механизми који одржавају стабилност ове приватне валуте у нестабилном правном окружењу. Овај рад објашњава техничке аспекте и механизме управљања биткоином у светлу литературе на тему праједије искључивих права, односно општег добра. Законодавна интервенција у области виртуелних валута је још увек у зачетку. Законодавци тренутно процењују користи приватних финансијских мрежа у поређењу са неинвентивним последицама збој праксе прања новца и пореске евазије. Будућност виртуелне валуте пре свега зависи од интеракције између ефикасне приватне уређења и борбе против криминала.

Кључне речи: виртуелне валуте, праједија искључивих права, односно општег добра, регулатива приватних финансијских мрежа.