UDC: 336.744 ; 004.738.5:339 JEL: E42. F31 ID: 207707660
ORIGINAL SCIENTIFIC PAPER

Demystifying Bitcoin: Sleight of Hand or Major Global Currency Alternative?

Malović Marko[1], Institute of Economic Sciences, Belgrade, Serbia

ABSTRACT *– Bitcoin, a peculiar crypto-currency has been the loudest buzzword in global finance over the last year or so, both for its spectacular and seemingly robust appreciation trend as well as for more recent equally ostentatious demise. After reviewing the history of bitcoin and specificities of its cyber-construct, this paper adds to the critical analysis of bitcoin as an international currency alternative. Lately, its volatility has been so excessive that it arguably cannot serve as a store of value. In addition, notwithstanding bitcoin's rising if bumpy credibility as a medium of exchange, since it has been immediately converted (by chief vendors) in either of the leading world currencies upon payment due to its extraordinary exchange rate volatility, bitcoin's unit of account potential appears to be dubious too. Moreover, bitcoin's next to none correlation with other major currencies' movements renders it unsuitable for managing FX risk or hedging purposes. Finally, having in mind that it lacks formal reserves or deposit-insurance scheme to back it up yet it's also prone to hacking, bitcoin resembles and behaves more like a pyramidal investment vehicle than a global currency alternative. Nevertheless, technology that made it be may still spawn an evolution in the way we posses things, transfer ownership and pay for goods and services in the near IT-ridden future.*

KEY WORDS*: bitcoin, crypto-currency, functions of money, global currency alternative, litecoin*

Introduction

Bitcoin, a peculiar crypto-currency has been the loudest buzzword in international finance over the last year or so, both for its spectacular and seemingly robust appreciation trend as well as for more recent equally ostentatious demise. It's maximum historical value hovered around 1300US$ in early December 2013 (although maximum daily close stopped at 1238US$), where from it fell to as low as 125US$ on February 21st this year. Bitcoin is encrypted digital floating currency used within a computerized or phabletised peer-to-peer network and whose value and raison d'etre is generated and approved only by the spontaneous consensus of its users. *Stricto sensu*, Bitcoin with capital 'B' denotes the entire technology and an open-source software network released in 2009, while bitcoin with

[1] Institute of Economic Sciences, Belgrade, marko.malovic@ien.bg.ac.rs. This paper is a part of research projects: 179015 (Challenges and prospects of structural changes in Serbia: Strategic directions for economic development and harmonization with EU requirements) and 47009 (European integrations and social and economic changes in Serbian economy on the way to the EU), financed by the Ministry of Education, Science and Technological Development of the Republic of Serbia. The usual disclaimer applies.

lowercase 'b“ denotes the actual virtual currency devised back in 2008 when its specification and proof of concept was originally published via cryptography mailing list by an unknown entity pseudo-named „Satoshi Nakamoto“. Strange as it may sound, bitcoin won the hearts of not only cyber-geeks but also much wider audience practically overnight and in less than two years became widely accepted and passionately sought global electronic currency.

After reviewing the history of bitcoin and specificities of its cyber-construct, this paper adds to the critical analysis of bitcoin as an international currency alternative. Just before - and in the early days of- internet, prominent figures in international finance like Paul Krugman or Joseph Stiglitz frequently repeated that world is not an optimum currency area and that cannot be such thing as the 'globo', *i.e.* truly international worldwide accepted pecuniary denominator which could be secure, politically unbiased, practical, fast to deploy and resilient to printing press abuse. However, can there be a globo in cyber space after all? Could cyber space constitute an optimum currency area? May it happen that Bitcoin/bitcoin overpowers American dollar and Chinese renminbi on its way to the currency throne of international trade facilitator? Is it conceivable for bitcoin to become a leading international reserve currency too at some point?

In trying to answer these and related pertinent questions troubling bitcoin's volatile existence and robust popularity, the rest of this paper is structured as follows. Section 2 reviews the history of bitcoin and its cyber-construct. Section 3 deals with critical analysis of bitcoin as an international currency alternative, tackling both its peculiarities and more conventional functions of money. Section 4 draws lessons from the essay and sheds some light on future allies of arguably fruitful research in this regard.

History of Bitcoin and its Cyber-construct

When launched and embraced six years ago by a handful of computer nerds, bitcoin was an exotic, stateless, nerd-related digital currency equipped with original software by Satoshi Nakamoto (pseudonym[2]) released under the MIT licence that traded for couple of dollar cents and much curiosity. Bitcoin hasn't been secured by sovereign inventories of monetary gold or FX reserves of any kind nor it relies on any central clearing authority. And yet bitcoin has managed to grow in value almost geometrically[3] and attract many a user because it apparently has found a way to by-pass the proverbial weaknesses of gold-linked and fiat currencies. Namely, not a single government nor supranational authority can possibly interfere with existing or future supply of bitcoin, since the crypto-currency has been envisaged as an electronic money delivered and driven by complicated mathematical algorithms which are closely tying the growth rate of money supply to the amount of

[2] In an online profile, he/she or them said he/she/they lived in Japan. His/her/their email address was from a free German service. Google searches for the name turned up no relevant information [Benjamin Wallace, 2011]. Nevertheless, one of the main reasons why the author or authors of bitcoin haven't been identified as yet is the fact that he/she/they never foresaw nor subsequently claimed any royalties from or property rights over the Bitcoin platform [David Yermack, 2013].

[3] Only during November 2013 bitcoin's exchange rate relative to US$ strengthened fivefold, whereas even contemporary much lower parity stands substantially taller than original 4.9 US cents which was bitcoin's introductory value back in 2009 [Yermack, 2013].

bitcoins already in circulation and up to the predetermined absolute limit [Satoshi Nakamoto, 2008]. According to problem-set algorithms made by Nakamoto (2008), new bitcoins are "forged", or rather awarded to PC users whose computers successfully solve(d) prespecified mathematical tasks. As a matter of fact, financial platforms take a lot of power to run and are expensive and insecure to be launched and maintained by one entity only. With Bitcoin, individuals and/or groups willing to dedicate computer processing power to support the network are rewarded with bitcoins. There are 12 million bitcoins circulating presently, while the total of 21 million could be 'discovered' at most, by or near the year of 2140.[4] Bitcoin's subunit is called satoshi, where one satoshi equals 10^{-8} of a bitcoin. Therefore, bitcoin is designed around the idea of cryptography as a way of protecting the creation of liquidity while enabling utmost public transparency of money transfer, rather than relying on banks, clearing houses or otherwise defined central(ised) authority. Limited and to the extent inevitable reflation is being distributed evenly (by central processing units' power of devices engaged in money creation) between the so-called miners and consequently all network members. Miners are owners of computers responsible for world-wide-web prospecting, uncovering, claiming, activating or, if you will, injecting newly acquired bitcoins into the global monetary circulation.

In addition to mathematically limiting money creation and denying forgery, Nakamoto (2008) developed an operating procedure for preventing the so called double spending, the long standing weakness of digital currency that one and the same electronic money unit may be illegally spent over and over again. His novel idea introduces an on-line ledger that records every single bitcoin transaction. The ledger is created through code-breaking work, done by a network of powerful personal computers owned by Bitcoin "miners", that validates each transaction [Carter Dougherty, 2014]. Bitcoin uses public-key cryptography[5], peer-to-peer network, and Hashcash CPU cost protocol[6] to process and verify digitally made payments. Bitcoins are sent (or signed over) from one address to another with each user potentially in possession of multiple addresses. Each order flow is publicly broadcast by being included in the so-called blockchain of Bitcoin transactions with common origination, so that none of the coins can be spent twice. Soon enough (after a 100 minutes give or take) each payment is locked in time by processing power which further extends the blockchain. Namely, data blocks are randomly assigned with a header, which miners compete in trying to match with a 'nonce', an arbitrary number used only once, to get alphanumeric code (called hash) of prespecified dynamic difficulty. All in all, one can obtain bitcoins either by outright buying them or by receiving them in exchange for goods and/or services, other than

[4] See Chart 1 in the Appendix.

[5] Public-key cryptography is a method of digital data protection which consists of an encrypted algorithm that is turn requires two keys to operate. Public key is informatics datum or mathematical parameter that serves the purpose of encrypting plaintext or confirming a digital signature, while private key unlocks (deciphers) text or creates a cyber-version of 'John Hancock'.

[6] CPU cost protocol forces a moderately hard data processing time on behalf of service requester which enables service provider to easily verify counterparty authentication and hopefully prevent denial of service attacks, spam abuse and alike. It is arguably simple and does not rely of central server, but it's also prone to both type 1 and type 2 errors. In other words, it might either stuck the good transaction sent from computer with insufficient computing power or the malevolent illegitimate transaction might get through if the complexity net were lowered.

originally claiming the currency through the 'mining' process [Wallace, 2011]. Users ought to have an internet access and downloaded Bitcoin in order to be able to make or receive payments to/from another public address. Apart from the keys briefly explained above, Bitcoin generates a virtual 'wallet', i.e. digital account, or multiplicity of them, for network's clients. A transfer request floats on the Bitcoin cyber network until picked up and packaged within a data block [Thomson-Reuters, 2014]. When proper hash is computed, respective network clients are, for the time being, credited with 25 bitcoins per data block.[7] Hash is then assigned to the next transaction block, binding them forever in transparent and neat public history ledger which Nakamoto (2008) dubbed a blockchain.

Thus, internationally mobile digital currency was born and accepted in less than four years on a tide of user-enthusiasm amidst and in spite of pressing financial and economic crisis worldwide. Nonetheless, how safe is to tell it a fortune? What does it take for a currency to become the truly global, omnipresent, world money?

Critical analysis of Bitcoin as an International Currency Alternative

In my opinion, if bitcoin were to claim a seat in the leading global currencies club, let alone crowd out any of the regular members, it would have to fulfil four criteria: *1)* to be safe, secure and reliable to buy, use or hold *2)* to capture significant share of denomination in both invoicing and financing international trade, *3)* to develop reasonably liquid derivative markets for risk management purposes and finally *4)* to become respectful reserve- as well as vehicle currency in international finance. Let us preliminarily reflect on the fulfilment of the aforementioned criteria, with facts and data disposable thus far.

It goes without saying that global currency acceptance criteria trace their grassroots in well-known functions of money, namely money as medium of exchange, unit of account, store of value (treasure) and world-wide common denominator.

When it comes to safety, code for Bitcoin is written beautifully, hence the probability of that being hacked is currently reasonably small, but security of wallets and supporting platforms on its way to outside world is simply appalling. The recent demise of Mt. Gox, one of the chief exchanges for bitcoin both in Japan and more globally, is the case in point.[8] Even before 127,000 customers were mugged online in this particular Mt. Gox incident, bitcoin showed signs of weakness in that it's encrypted format is difficult, but not impossible for

[7] Every four years (or exactly every 210,000 blocks later), number of bitcoins assigned to miners halves. For instance, first couple of thousand blocks earned their miners 50 bitcoins even though consisted of one birth transaction only. Today, and approximately until 2017, blockchains will be worth 25 bitcoins a piece, while burdened with hundreds of thousands of transactions per block [Wallace, 2011], [Thompson-Reuters, 2014]. From thereon, as the number on miners and claims goes up, the number of bitcoins awarded will exponentially decrease, e.g. transaction blocks assembled in 2139 will yield only one satoshi each, whereas those made in 2140 would have to rely on imposing a small transaction fee in the secondary market [Ian Gordon-Vadim Iaralov-David Woo, 2013].

[8] Mt. Gox, a Tokyo-based exchange, filed for bankruptcy in February after realising hackers had nicked some 850,000 bitcoins/480 mill.US$ in cyberspace, or circa 6% of all bitcoins in circulation [Dougherty, 2014]. Similarly, Flexcoin bank storing bitcoins in hot wallets (online accounts) was closed down after being robbed just a week after Mt.Gox's bankruptcy when hackers stole another 896 bitcoins worth over 600,000 US$ [Kiran Moodley, 2014]

hackers to break and electronically steal. In other words, for all the users not able or not willing to mine their own bitcoins, an hour or two time lag before payment receipt information is received will henceforth prohibit wider audience utilisation of bitcoin. As pointed out by Gordon, Iaralov and Woo (2013), when dealing with anonymous counterparty, a minimum 50 minutes wait is presently inevitable for enough blocks to be mounted to the chain, thereby protecting the transactors from double-spending. Alas, exactly this window of opportunity represents a security breech in Bitcoin exchanges, adding a credit risk on a top of FX risk exposure for bitcoin owners. Ironically, the very anonymity guaranteed to counterparties which gave bitcoin such abrupt and widespread popularity, in these cases leave many bitcoin users/investors with little recourse as to retrieval of stolen funds while dealing with outside financial world [*Ibidem*]. In conclusion, as to the first criterion of truly international currency status, bitcoin is generally very safe and attractive to buy and hold, especially as compared to cash. As a medium of exchange, it is visibly superior to e-banking and money wiring due to much lower transaction costs and astounding speed of transfer. It's rather convenient to move around, since it comes in fairly large appreciated denomination as opposed to leading sovereign currencies (the largest dollar and yuan bill is 100 units only). In addition, a considerable anonymity it offers draws users in large numbers not only from the economic and (il)legal underworld, but also those wishing to evade abnormally steep taxation, capital controls or full-fledged confiscation. All the pros notwithstanding, bitcoin appears to be extremely unsafe to use for purchases, since it is currently vulnerable to hacking, especially when exchanged for other conventional currencies.

With regard to the second criterion, bitcoin has come a long way and still offers a reasonably promising future. As bunch of commerce hastily migrates online these days, growing number of producers and merchants seem to be ready to accept digital crypto-currency as means of payment.[9] The first purchase of goods&services with bitcoin was a pizza, yet more recently, people have been using bitcoins to buy overseas villas, foreign automobiles, drugs&narcotics, arms, proprietary software etc. In a nutshell, international trade facilitated by bitcoin attracts either technology-enthusiasts or anarcho-libertarians who abstain from currencies connected with sovereign governments or indeed the mainstream international financial order. However, governments may and in all likelihood will, at some point - unilaterally or multilaterally, impose series of controls and fees on Bitcoin platforms in order to minimise illicit and black market activities or simply to do way with digital competitions which might bite into their shares of international seignorage [Gordon-Iaralov-Woo, 2013]. Moreover, the use of Bitcoin's decently encoded and pretty transparent transactions ledger can in fact be traced back by governments with enough funds and know-how to do so, which will probably drive out (and away) some of money laundering and other illegal transactions from bitcoin as their denominator, rendering it with ambiguous popularity consequence. Further still, ambiguities don't stop here: in Denmark and a number of other countries, one doesn't have to pay taxes on transactions carried out through Bitcoin which is definitely prosperous for bitcoin as medium of trade. To top it all off, however, vast

[9] The list of famous e-commerce platforms that are accepting bitcoins includes among others: e-Bay, PayPal, Tesla Automotives, The Pirate Bay, SilkRoad (cracked down by US authorities), Virgin Galactic, Zynga and so forth.

majority of contemporary trade invoiced in bitcoin comes either from China or the USA, while both of their governments have severely limited -and publicly distanced themselves from- utilisation of bitcoins [Yermack, 2013]. According to American IRS classification, for example, bitcoin is not even considered to be a currency, but property, which invokes capital gain tax as an undesirable repercussion for bitcoins prominence in international trade. Additional problem represents the practice of involving third party intermediation that accepts bitcoins and pays with conventional internationally accepted fiat money or gold, either already upon or immediately after the exchange of goods&services has been made. Finally, bitcoin is in no way connected with national or international banking system, is not protected by any sovereign or supranational deposit insurance scheme and hence does not feature as international loans denominator at all. To the extent, conventional financial industry has pretty much abstained from the whole crypto-currency mania thus far. Instead, investment euphoria seems to have been enhanced if not sparked by lobbying efforts of computer manufacturing and energy producing industry, since the whole business heavily relies on powerful CPUs rarely encountered in regular PCs and enormous consumption of electricity.[10] The latest novelty - the introduction of litecoin[11], financially diluted and (in respect to thus far required computer power) less demanding light-weight version of bitcoin, which is to roam those same Bitcoin networks in parallel with original bitcoins, arguably lends itself to overall confusion, information asymmetry and downgrading sentiment towards the indigenous digital currency's standing.

In terms of the third criterion, bitcoin's exchange rates vis-à-vis other leading currencies in the world exhibit next to no correlation whatsoever with values of either currencies or other financial assets for that matter, which makes it utterly useless for hedging FX risk in any direction [Yermack, 2013]. Perhaps that explains why there are no (not even plain-vanilla) derivative contracts out there in the market offering the usual forward exchange rate agreements for bitcoin.

At last, bitcoin's global store of value function must be evaluated through the lens of its unprecedented volatility, ranging from less than five cents to over 1200US$ and back to in-between 300/400US$ at the time of this writing, which makes it spot-on evident that bitcoin's instability cannot be matched by those of otherwise notoriously volatile gold and silver, let alone the leading reserve currencies.[12] Put differently, bitcoin stands no chance of becoming internationally embraced reserve currency nor inter-currency unit of account vehicle for as long as it demonstrates such an unacceptable volatility.[13] Therefore, it should come as no surprise that some of the leading figures in international finance designated it as speculative investment at best or poorly masked Ponzi game even [Alex Crippen, 2014], [Nouriel

[10] See Chart 2 in the Appendix.

[11] Apparently, litecoin is envisaged to provide faster transaction confirmation and yield less value per more realistic mining effort tuned down to CPU's most households already posses up until the entire supply of 84 mill. litecoins is claimed.

[12] Yermack (2013), for instance, calculates bitcoin's 2013 volatility (i.e. before the great plunge of early 2014) in the vicinity of 133%, whereas volatility of gold amounts to about 20% and that of the leading world currencies falls between 8 and 12% (see Chart 3 in the Appendix). By mid April 2014, bitcoin lost more than 60% of its value since the late 2013 peak.

[13] See Chart 4 in the Appendix.

Roubini, 2014]. Worse still, spectacular volatility of bitcoin is in turn additionally hurting its medium of exchange and unit of account functions, thereby closing the vicious circle bitcoin's been spinning in as of late [Gordon-Iaralov-Woo, 2013].

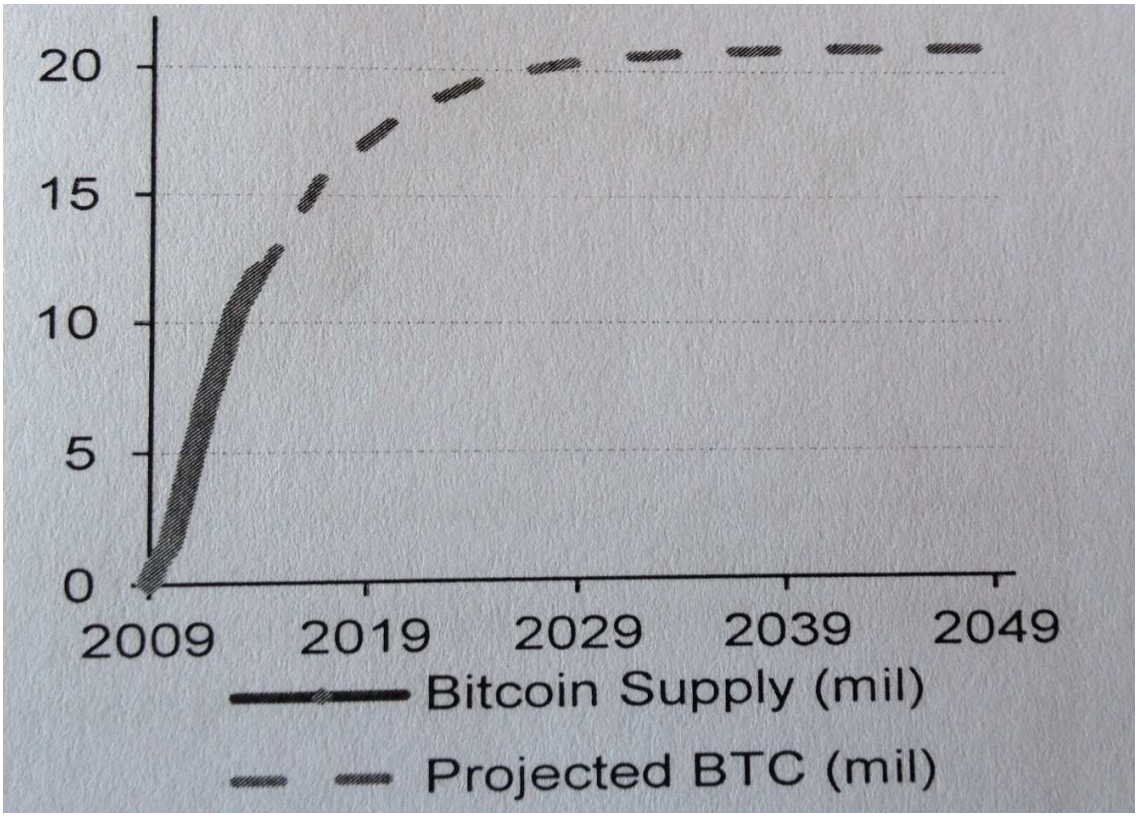
Even though bitcoin's wild gyrations in worth effectively relate it more closely to speculative investment vehicle than to a major global currency, clever technical design that bitcoin rests upon and respectful post-bubble purchasing power of more than 7 billion US$ may still spear-lead the process of pretty futuristic metamorphosis of the consumer-finance industry as we know it [The Economist, 2014*]. Open source software and public observance (i.e. peer-to-peer audit) of each and every transaction crack-opens the door for third parties to take and tweak existing technology to many different directions and fascinating offspring. For example, funds could be programmed to lend or collect themselves following a contractual decryptying clause, banks might start using crypto-currencies for inter-affiliate cash management, flats and cars soon could be entered/jump-started only with temporary (lease) or permanent (sale) set of public and private digital keys [The Economist, 2014]. This may well sound like Sci-Fi curiosity at the moment, but as a matter of fact, many tech-startups are deeply involved in developing precisely such commercial applications already. Thus, despite the fact that bitcoin arguably failed to meet at least three out of four criteria for becoming a major global currency, incredible technological legacy it stems from may define entirely new and formidably important functions of money that digital crypto-currencies and crypto-currencies only could serve. One of those futuristic functions may prove to bring about that crucial junction which irrevocably transforms society over time. Such a change, consequently, might reserve a currency throne and historical memory for bitcoin after all.

Conclusion

Having in mind that it lacks formal reserves or deposit-insurance scheme to back it up, yet it's also prone to hacking, bitcoin resembles and behaves more like a pyramidal investment vehicle than a global currency alternative. Investment euphoria seems to have been enhanced if not sparked by lobbying efforts of computer and energy producing industry, since the whole business heavily relies on powerful CPUs rarely encountered in regular PCs and colossal consumption of electricity. Besides, bitcoin's next to none correlation with other major currencies' movements renders it unsuitable for managing FX risk or hedging purposes. It's unit of account function is practically non-existing, thus compromising it for invoicing or vehicle-currency usage. Bitcoin's role as an international store of value is dramatically conceded by its bubble-like volatility pattern. In turn, bitcoin's enormously unstable exchange rate undermines its otherwise promising utilisation as an international means of payment. Nevertheless, technology that made it be may still spawn an evolution in the way we posses things, transfer ownership and pay for goods and services in the near IT-ridden future.

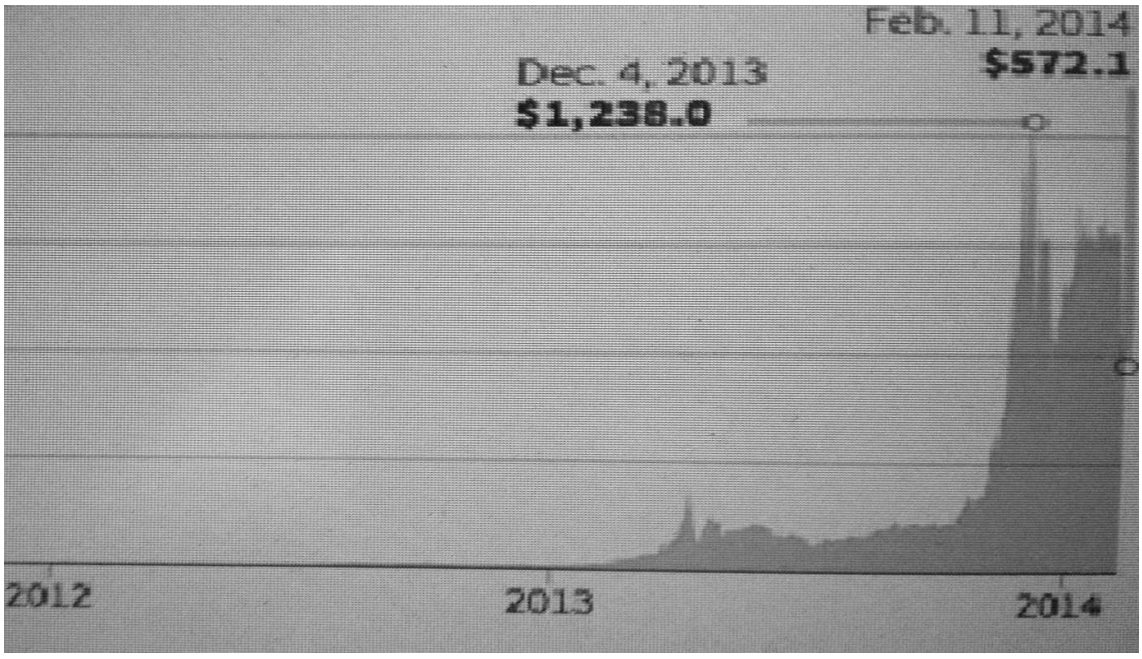
Appendix

Chart 1. Actual and projected bitcoin supply



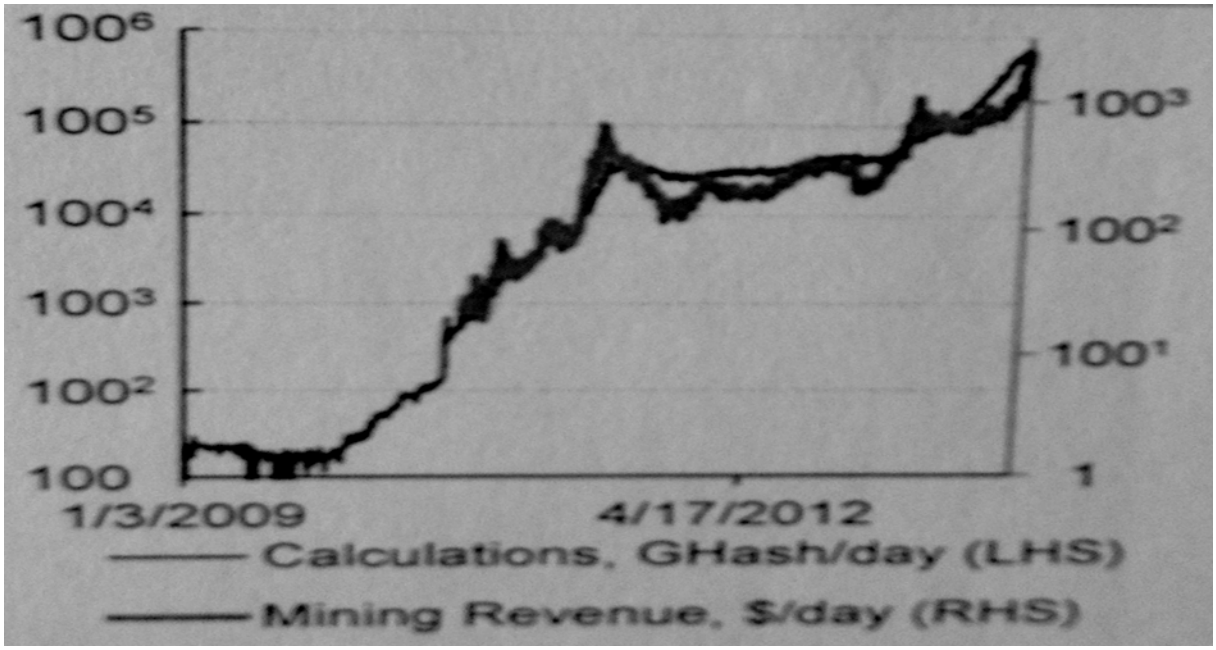
Source: Gordon, Iaralov, Woo (2013)

Chart 2. Long-term volatility of bitcoin's exchange rate



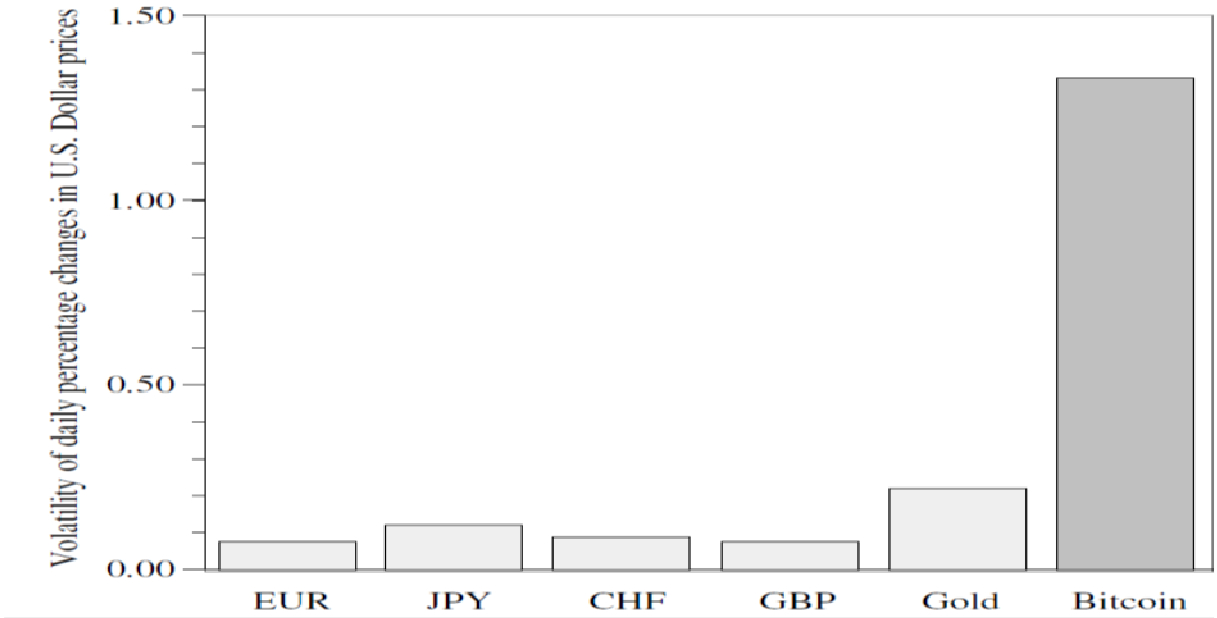
Source: Thomson-Reuters (2014)

Chart 3. Short-term volatility of bitcoin as compared with other legal tenders



Source: Gordon, Iaralov, Woo (2013)

Chart 4. Explosive growth in effort and size of the 'mining' industry



Source: Yermack (2013)

References

Crippen, A. (2014), "Buffet blasts Bitcoin as 'Mirage': Stay Away!", CNBC News, March 14th, http://www.cnbc.com/id/101494937.

Dougherty, C. (2014), "The Rise of Bitcoin: Is it Real Currency if it doesn't come from the Mint?", Bloomberg, *mimeo.*

Gordon, I.-Iaralov, V.-Woo, D. (2013). "Cause and Effect - Bitcoin: A First Assessment", Bank of America & Merril Lynch FX and Rates Global Research, December 5th.

The Economist (2014). "Bitcoin's Future: Hidden Flipside", The Economist, March 15th.

The Economist (2014*) "Money from Nothing", The Economist, March 15th.

Moodley, K. (2014) "Another Bitcoin Site bites the Dust", CNBC News, www.cnbc.com.

Nakamoto, S. (2008). "Bitcoin: A Peer-to-Peer Electronic Cash System", MIT, Cambridge, MA, *mimeo*.

Roubini, N. (2014). "Bitcoin is a 'Ponzi Game'", The Wall Street Journal, March 10th.

Thomson Reuters (2014). "The Knowledge Effect: Bitcoin - Graphic of the Day", Thomson Reuters, *mimeo.*

Wallace, B. (2011). "The Rise and Fall of Bitcoin", Wired Magazine, November 23rd, *mimeo*.

Yermack, D. (2013). "Is Bitcoin a Real Currency?", NBER Working Paper 19747, Cambridge, MA, December.

Demistifikovanje bitnovca: lakrdija ili ključna alternativa globalno prihvaćenim valutama?

REZIME *– Bitnovčić, naročita kripto-valuta najglasnije je ponavljan termin u globalnim finansijama u poslednjih godinu dana, kako zbog svog spektakularnog trenda aprecijacije tako i zbog nešto skorijeg a jednako upadljivog gubitka vrednosti. Nakon osvrta na istoriju bitnovčića i osobenosti njegove softverske konstrukcije, članak daje skroman doprinos analizi bitnovčića kao alternativne svetske valute. U poslednje vreme, međutim, kolebljivost kursa bitnovčića je tolika da on jamačno ne može poslužiti kao čuvar vrednosti. Nadalje, ne prenebregnuvši njegovu rastuću iako truckavu kredibilnost kao razmenskog sredstva, potencijal bitnovčića za funkciju obračunskog sredstva je takođe krajnje upitan, budući da svi glavni e-trgovci smesta konvertuju prihode u bitnovčićima u neku od vodećih svetskih valuta zbog njegovog nestabilnog pariteta. Štaviše, skoro potpuno odsustvo korelacije između vrednosti bitnovčiča i kretanja vodećih svetskih valuta čini ga nepodobnim za upravljanje FX rizikom ili pak defanzivno pokrivanje rizika. Najzad, imajući u vidu da bitnovčić nije poduprt formalnim deviznim rezervama niti šemom depozitnog osiguranja, a pritom je vrlo podložan hakerskim napadima, bitnovčić podseća na i ponaša se više kao piramidalna investiciona tvorevina nego kao ozbiljna alternativa međunarodno prihvaćenom novcu. Pa ipak, tehnologija na kojoj počiva još uvek može iznedriti evoluciju u načinu na koji ćemo posedovati imovinu, prenositi vlasništvo I plaćati za dobra i usluge u doglednoj informatički vođenoj budućnosti.*

KLJUČNE REČI*: bitnovčić, kripto-valuta, funkcije novca, alternativa svetskom novcu, laganovčić*

Article history: Received: 1 April 2014
Accepted: 16 April 2014