Sinteza
Međunarodna naučna konferencija Univerziteta Singidunum

Impact of Internet on Business Activities in Serbia and Worldwide
Uticaj Interneta na poslovanje u Srbiji i svetu

DOI: 10.15308/SINTEZA-2014-1-7

648K-BITS ABOUT BITCOIN

Nancy Neslund[1,*]
[1] Ohio Northern University, USA

Abstract:
This paper explores the recent development of digital currencies—currencies which are creatures of the Internet, self-authenticating, and usable worldwide by members of the general public to engage in the same types of direct, one-to-one transactions that daily occur using government-issued currencies. At present, the most developed digital currency measured by market capitalization is Bitcoin, which will be used as a proxy for the general phenomenon. Not surprisingly, as Bitcoin's circulation and visibility has increased, so have the number of practical and legal issues surrounding its use. Some of these will be explored in this paper, with a view to considering the utility and viability of such currencies for widespread, global use.

Key words:
Bitcoin,
digital currencies,
crypto-currencies.

INTRODUCTION

This paper explores the recent development of digital currencies[1]—currencies which are creatures of the Internet, self-authenticating,[2] and usable worldwide by members of the general public to engage in the same types of direct, one-to-one transactions that daily occur using government-issued currencies. At present, the most developed digital currency measured by market capitalization is Bitcoin, which will be used as a proxy for the general phenomenon. Not surprisingly, as Bitcoin's circulation and visibility has increased, so have the number of practical and legal issues surrounding its use. Some of these will be explored in this paper, with a view to considering the utility and viability of such currencies for widespread, global use.

WHAT IS BITCOIN?

Bitcoin began with a paper published anonymously in 2008 that outlined how to create a digital currency which could be exchanged on a "peer-to-peer" basis, would not be susceptible to unauthorized duplication, and would have no issuing or central authority. The first Bitcoins were "mined" in 2009 using an open-source program which constrains how many coins can be created and at what intervals (currently 25 approximately every ten minutes, but the number drops by half approximately every four years, with the preprogrammed cap of 21 million reached around 2025). As of this writing, one Bitcoin is trading for about 640 USD (€460).[3] Since approximately 12.5 million coins have been mined, the value of the total supply is just under 8 billion USD (compared to the roughly 10 trillion actual U.S. dollars in circulation).

Mining Bitcoins

In the language of Bitcoin, new coins are "mined" by self-selected "miners," who have downloaded the software used to verify all Bitcoin transactions which occur during a set period of time, condense it into a block of data, and add the new block to a chain of other blocks recording earlier transactions. This chain is effectively a public ledger of all past Bitcoin transactions. The current payment of 25 Bitcoins is transferred to the miner who is the first to

1 These currencies have also been referred to as electronic currencies, virtual currencies and crypto-currencies.
2 That is, no third party is necessary to verify the authenticity of a particular Bitcoin; the program performs that function automatically.
3 The number of Bitcoins, current values, trading prices and market capitalization were taken from www.coindesk.com on March 13, 2014. CoinDesk maintains a price index for Bitcoin based on a weighted average of prices on the largest Bitcoin exchanges.

produce the latest block. Thus, the infrastructure necessary to keep the system running is provided by miners motivated by Bitcoin rewards. The program is designed to increase the computational challenge if the solution rate drops below ten minutes or decrease the challenge if the rate grows longer than ten minutes.

As recently as January 2013 when Bitcoins were trading for around 15 USD, it was possible for a miner with a personal computer to earn Bitcoins. No more. A computer programmer in Britain started out just that way, but now has a mining operation using purpose-built machines—166 of them in a secure facility close to the Arctic Circle in Iceland, with more computers being built for a second installation in Texas [1]. Even as of November 2013, the collective computing power sustaining the Bitcoin network equaled 100 times the collective computing power of the world's top 500 supercomputers [2]. As the trading price of Bitcoins has increased, more miners have entered the race; as more have entered the race, winning has required ever-faster computing power, which has driven the investment in infrastructure higher.

Clearly, the "digital" in "digital currency" does not mean no physical infrastructure. To the contrary, the reality raises questions of whether the system is sustainable—economically, technologically or environmentally. Economically, an investment that makes sense when Bitcoins trade for over 1000 USD, as they did for a time in December 2013, may precipitate bankruptcy if the value drops into the 600 USD range, as it is at present. An investment that is remunerative when the reward is 25 Bitcoins, may not be remunerative when the reward is only 12.5 Bitcoins. In addition, when the 21 million Bitcoin cap is reached,[4] there will still be a need for a substantial infrastructure to verify transactions and maintain the public ledger. Apparently the intention is that Bitcoin users will then pay a transaction fee, but there is no guarantee the fee necessary to support the infrastructure will be a fee users will be willing to pay. Technologically, as more coins are mined and more users participate over time, the public ledger block chain will grow ever longer. At what point does it become unwieldy? At the time of this writing, the block chain had already reached 15 gigabytes [4] and it could take days to establish a new wallet on one's own computer.[5]

Environmentally, the electricity used to operate the computers mining new coins is already a significant cost constraint. Those costs factored into the decision of the miner previously mentioned to establish his operations in Iceland, where "geothermal and hydroelectric energy are plentiful and cheap. And the arctic air is free and piped in to cool the machines" [1].

4 One author has asserted that the cap can be "adjusted or eliminated altogether" by the agreement of miners "representing more than half of the system's computing power" [3].

5 Creating a wallet requires downloading the Bitcoin client. To be able to independently verify the authenticity of the owner's transactions, the program needs to have verified all preceding transactions since the mining of the first Bitcoin. This also means that each time the wallet's owner wants to engage in a transaction, the computer must verify all transactions added since the prior transaction. One user told this author that, for this reason, he leaves the program running in the background whenever his computer is on.

Doing Business with Bitcoins

There are several ways to acquire Bitcoins for trading other than mining. One way is to purchase some from an individual willing to sell. Websites exist that identify persons willing to sell (or buy) by locale and by payment method, including cash.[6] In a few cities, you can use an ATM machine to buy Bitcoins by inserting cash [5]. You can also purchase coins from some online wallet services or from an established exchange.[7] Because these services generally seek to be both legitimate and secure, an initial purchase may take several days to allow for verification of one's identity and purchase funds. One can also acquire Bitcoins simply by accepting them in exchange for goods or services. Whatever the acquisition method, the purchaser will need to set up a digital wallet to receive the Bitcoins, which can be installed on a personal computer (or a removable drive) or with online wallet service. Once a wallet has been established, a smartphone app can be used to make transfers.[8]

As relatively few businesses presently accept payment in Bitcoin, Coinmap.org displays a world map from which local vendors and charities accepting Bitcoin can be identified. Not surprisingly, the United States and Europe have the largest concentrations, although Buenos Aires lists almost as many as New York City.[9] There are also online merchants, such as Overstock.com, that accept Bitcoin for payment. For both in person and online purchases, the easiest way to complete a transaction is to scan the vendor's code with a smartphone. The relevant code can also be typed in, but it is likely to be long and cumbersome (e.g., a 34-digit alphanumeric string).

COMPARISON TO OTHER MEDIA OF EXCHANGE

Comparison to National Currencies

Not long ago, currency transactions were almost completely accomplished through physical means: via cash, both paper and coin, and negotiable instruments, most commonly checks. Today, digital transactions far outstrip cash transactions. The bulk of one's annual income can easily be both received and spent digitally. The cash-only economy is now largely the preserve of those with the lowest incomes and those engaged in criminal activities—the former substantially for reasons of cost and accessibility and the latter to preserve anonymity. At present, digital transactions require the use of an intermediary—the banking system—and often involve fees, either direct or indirect. These transactions can take several days to clear. In contrast, cash transactions require no intermediary, trigger no fees and are completed instantaneously. However, they generally require an actual meeting of the two parties to the transaction. Under appropriate cir-

6 For example, localbitcoins.com.

7 Well established exchanges include www.bitstamp.net (US) and btc-e.com (Bulgaria). Coinbase.com (US) is a wallet service that will also trade Bitcoins for USD.

8 Blockchain.info/wallet is a wallet service that provides apps for use with both Apple and Android phones.

9 At the time of this writing, five sites were listed in Belgrade.

cumstances, many digital transactions can be unwound through the intersession of the intermediary; cash transactions are generally final. Bank accounts can be hacked and access codes stolen; cash and checks can be lost or stolen. Depositors may be protected against bank failures, but only because laws have been enacted to do so, not because of any inherent characteristic of the system.

That Bitcoin transactions are digital, therefore, is not what makes them intriguing. Rather, what is new is the peer-to-peer characteristic, which makes them function more like cash: the buyer and seller need not know each other, no intermediary is necessary and, if no intermediary is used, no material fees are incurred. All transactions are final. Significantly, however, in contrast to cash, the two parties to a Bitcoin transaction need not meet to conclude their business. Further, in contrast to digital transactions involving national currencies, Bitcoin transactions close in a dramatically shorter amount of time.

Other characteristics of national currencies have analogs in the Bitcoin world. If not held off-line, digital wallets can be hacked, whether stored by a third party or on one's own computer. Bitcoins can be lost in a variety of ways. For example, if the owner keeps his wallet on his personal computer and the hard disk fails, the Bitcoins will simply vanish. The government does not insure commercial digital wallet services against the failure of the service provider, but some who are active in the Bitcoin world are seeking to create insurance mechanisms that would protect against the downfall of an exchange like Mt. Gox and other catastrophic losses [6].

National currencies have their advantages: Bitcoins are nowhere near as widely accepted as national currencies and their market value is very volatile, two factors which are not unrelated. Merchants that have chosen to accept Bitcoins in payment may be able to mitigate the volatility risk by converting Bitcoins received into local currency on a daily basis. Because there is no need to "make change" in a Bitcoin transaction, there is no need for a merchant to maintain a ready Bitcoin stock. The same cannot be said of the consumer who wishes to transact purchases with Bitcoin, unless they have an readily accessible location at which to purchase Bitcoins with cash (such as an ATM).

Comparison to Credit Cards, PayPal Accounts and Debit Cards

Neither credit cards nor PayPal are media of exchange; rather, they are simply methods of payment. To use them, both parties to the transaction must have an account through which to process the transaction. The transactions are not anonymous and can be traced. Vendors typically incur a transaction fee of 2-3%; buyers may also be subject to a charge, such as an annual fee. Accounts can be hacked and access information stolen. However in the case of credit cards, the holder (at least in the U.S.) is financially protected from unauthorized use of the account as long as the misuse is timely reported. With both of these payment methods, transactions can and will be unwound by the intermediary under appropriate circumstances. This is primarily a benefit to the purchaser.

Merchants may prefer to receive Bitcoin payments so as to avoid the fees associated with both credit cards and PayPal accounts. The speed with which Bitcoin transactions are finalized may also be attractive. Both of these factors must still be weighed against the volatility risk associated with Bitcoins although, as previously mentioned, merchants can protect themselves from much of this risk.

Debit cards are also a method of payment tied to an institutional account, rather than a medium of exchange. However, the fee paid by the merchant when the buyer uses a debit card is considerably less than with credit cards. Amazingly, debit transactions may not clear the buyer's account any faster than a credit transaction. In other respects, debit cards are similar to the prior two payment methods.

GOVERNMENTAL RESPONSES

Governmental response to the use of Bitcoins has been quite varied. Thailand and Russia have banned its use [7]. China has forbidden financial institutions from engaging in Bitcoin-related business; its largest e-commerce website, Alibaba, has banned its use as a medium of payment; a major Bitcoin exchange located in China no longer accepts deposits in China's own currency [8]. In contrast, Japan does not consider it a currency, thereby providing its Financial Services Agency an argument for not regulating it [9]. More favorably, the former Chairman of the U.S. Federal Reserve, Ben Bernanke, stated that virtual currencies "may hold long-term promise, particularly if the innovations promote a faster, more secure, and more efficient payment system" [10]. It has been suggested that both US and UK bankers would prefer to see the end of physical currency and, thus, might like to see a form of digital cash gain popular acceptance [11]. Perhaps most favorably of all to Bitcoin, Germany has recognized it as a "unit of account," which permits it to be used like cash in some contexts [7]. In direct contrast to Japan's position, some view regulation as necessary to ensure the integrity of Bitcoin transactions and thereby support their continued development.

REGULATION OF EXCHANGES AND TRANSFER AGENTS: CONTROLLING CRIMINAL USE

One of the most common regulatory concerns raised is the need to address and minimize the ability of Bitcoin and other digital currencies to facilitate illicit activities, such as money laundering and the purchase of illegal goods. The most infamous example of its use for such purposes thus far was the arrest in October 2013 of the owner of the Silk Road website (a digital marketplace) and the seizure of nearly 175,000 Bitcoins by the U.S. government. The owner has been charged with drug trafficking and money laundering. Three additional individuals associated with the website were arrested in December. Then in January 2014, Charlie Shrem, an outspoken Bitcoin advocate, was also charged with money-laundering in connection with Silk Road's online activities. No trials have yet been held.

It has become apparent that the early vaunting of Bitcoin's transactional anonymity was substantially overstated. The transaction ledger previously discuss is a public record of all trades with respect to each Bitcoin ever mined. Although encoded and lacking the parties' names, the ledger can be read and the transaction amounts and public keys[10] of the parties uncovered. "You can track specific Bitcoin movements just as you would the serial number on a U.S. dollar" [12].

The U.S. has determined that all digital currency exchanges and businesses facilitating the transfer of Bitcoins, such as the providers of commercial wallets, are "money services businesses" (MSB) and, therefore, subject to the Bank Secrecy Act. This places them under the regulatory authority of the U.S. Department of Treasury's Financial Crimes Enforcement Network (FinCen). The Act requires MSBs to be licensed and to report transactions over 10,000 USD. Further, the Money Laundering Control Act requires them to comply with its know-your-customer requirements. In May 2013, the U.S. seized accounts of the U.S. affiliate of the Mt. Gox exchange because it was not FinCen compliant.

In a similar move, in December 2012 France officially licensed a Bitcoin exchange as a "payment services provider" [13].

TAXATION OF BITCOIN TRANSACTIONS

Along with concerns about the facilitation of criminal activities, governments have been concerned about tax avoidance that could result from economic transactions occurring in Bitcoin. Australia, Canada and the Netherlands have each addressed the tax treatment applicable to Bitcoin transactions under their respective laws. In the U.S., although the U.S. Government Accountability Office has recommended that the Internal Revenue Service (IRS) issue informal guidelines on the taxation of transactions in digital currencies, the IRS has not yet done so.[11] Rather than developing new principles or promulgating new rules, the challenge for countries seems to be how to determine the proper characterization of Bitcoin transactions within the scope of existing law. Two alternative conceptual frameworks have been advanced: 1) treat it as a currency and use the approaches that govern transactions in foreign national currencies or 2) treat it as property and analyze transactions as exchanges of property.[12] The following discussion uses U.S. tax law to illustrate the possible implications of these alternative treatments.

Is Bitcoin a currency?

Under U.S. law the question is whether Bitcoins fall into the narrow category of "nonfunctional currency"[13] [16] or the general category of "property" (which does not include money) [17]. If Bitcoins are currency, but not the taxpayer's functional currency, every use of a Bitcoin to acquire a good or service would subject the user to taxation (at the taxpayer's highest marginal tax rate—presently as high as 39.6%) on the gain or loss from the exchange. For example, if the taxpayer a piano worth 800 USD using a Bitcoin presently worth 800 USD (but originally acquired for 700 USD), the taxpayer would have a 100 USD gain and would be required to pay a tax of up to 39.6 USD. If Bitcoins are not currency, Bitcoin transactions will be taxed as property transactions, discussed below.

As thoroughly analyzed in [7], the most likely result is that Bitcoins, at least at this time, would not be classified as currency for one or more of the following reasons:

- It is not predominantly used as a medium of exchange rather than for investment,[14]
- It is not "widely or commonly accepted by a community or a group in exchange for goods,"
- It is not used as a standard of value,[15]
- It does not function as a unit of account,[16] or
- It is not legal tender in any jurisdiction.

Taxation of Bitcoins as Property

If Bitcoin is not a currency, it seems most likely that Bitcoin transactions will be analyzed as property transactions under national tax laws. In the U.S., the tax treatment of property transactions depends both on why a taxpayer is holding the property and how long the property is held. A key question for Bitcoins would be whether, in the hands of a particular taxpayer, they will be classified as "ordinary" assets or "capital" assets [17]. Gains

10 When Bitcoin payments are made, the transferor encrypts the transaction using the recipient's public key and the recipient unencrypts the transaction with the related private key, which is known only by the owner. Maintaining the security of the private key is one of the primary protections against theft built into the Bitcoin program.

11 The IRS has issued no formal guidelines, but two other agencies of the U.S. government have. A federal district court held that Bitcoin was a currency for purposes of the Securities Act of 1933 [14], while FinCen held that digital currencies are not currencies [15]. The difference in these decisions can be traced, in part, to the specific statutory and regulatory authorities that were being interpreted, including the differing purposes animating those regulatory schemes.

12 For example, it has been reported that Norway will not treat Bitcoin as currency, but as an investment asset or, more broadly, property [8].

13 The currency of a nation other than that of which the taxpayer is a citizen or permanent resident.

14 As several commentators have noted, at this point in time what prevents Bitcoins from effectively functioning as a medium of exchange is that many, if not most, holders seem to be speculating on it being a good investment (that is, that its value will continue to rise considerably), rather than using it as a supplement to their existing monetary system. The more Bitcoins are held for investment, the less they are available to facilitate exchange transactions. The proof generally offered for this includes its wild fluctuation in price [18].

15 Use as a standard of value is precluded by the same volatility referenced in the prior footnote. Stated another way, it is not a stable store of value as measured, for example, against other currencies or against goods and services in the marketplace.

16 This concept is very close to its predecessor. The argument is that Bitcoin's value is not sufficiently stable forto it could act as an effective standard with which to measure one's economic activity. However, Germany has recognized Bitcoin as a "unit of account," which might in turn lead it to characterize it as a currency. This author to date has found no information on Germany's tax treatment of Bitcoin transactions.

and losses on ordinary assets are, like the nonfunctional currencies previously discussed, taxed at an individual's highest marginal rate. Gains and losses on capital assets, if held more than one year, are taxed at a maximum rate of 20%. Capital assets held for one year or less are taxed like an ordinary assets.

With regard to Bitcoin, there are six taxpayer categories:

- Investors, who buy Bitcoins primarily for appreciation in value. They are required to track the price paid for their Bitcoins so that, when sold, their gain or loss on can be measured. The length of time held (one year or less versus over one year) will determine whether the gains and losses will be taxed like ordinary assets or like capital assets. Investors subject to U.S. laws are used to keeping such records, so complying with the law would be relatively straightforward.[17]
- Traders, who buy and sell Bitcoins for their own account, principally to profit from short-term market swings. Although some unique rules apply to traders as compared to investors, the basic rules are the same. Because of the short-term holding period, their gains and losses will be ordinary. Again, traders in the U.S. are familiar with the recordkeeping requirements and so are likely already maintaining records for compliance.
- Miners, who earn income either from the services they provide or from being in the business of Bitcoin mining. The ultimate tax outcome will be the same as for ordinary assets. Under U.S. law, the tax treatment for earned income is the same, whether payment is in the form of money or property [19] (here, Bitcoins).
- Exchanges, which generate their income by earning brokers fees from the clients matched up in Bitcoin buy-sell transactions. This will be classified again as fees for services and, therefore, ordinary income. The tax treatment will be the same as for miners. Note that some exchanges may also be Bitcoin traders.
- Sellers of goods and services who accept Bitcoin in payment. The tax treatment will be the same as for miners.
- Individuals who buy Bitcoins and then use them to buy goods and services. These will be characterized as barter transactions, which will be taxed like the transactions of investors or traders, depending on how long the individual had held the Bitcoins used in the transaction.

The above may initially seem straightforward but, except for investors and traders, two enormous challenges confront those required to report these transactions for tax purposes—the twin challenges of valuation and recording-keeping.

Taxpayers must be able to demonstrate the fair market value in USDs of any Bitcoin used in a transaction, on the dates both of acquisition and of disposition, in order to be able to prove the amount of taxable gain or loss [20]. Unlike investors and traders, those in the other four categories may not have mechanisms in place for tracking these values. Sellers of goods and services and perhaps miners and exchanges might be able to avoid this issue, but only by converting any Bitcoin revenues received to USD on a daily basis.

The challenge will be hardest for those individuals who use Bitcoin primarily to buy services and consumer goods. Assuming most of these individuals do not receive their wages in Bitcoin, in order to purchase items with Bitcoin, they will first have to buy Bitcoins (and record the purchase price of each transaction). When they purchase goods or services, each transaction will be treated as a separate property transaction. U.S. law specifies that the amount realized equals the amount of money received "plus the fair market value of property" received in exchange for the Bitcoins given up [21]. Thus, these individuals will also need to record the value of everything they buy with their Bitcoins. Finally, they will need to devise a reasonable system for determining which Bitcoins in their wallet were used to purchase which goods or services, in order to compute the gain on each transaction. For anyone who regularly uses Bitcoin as a medium of exchange, maintaining such records will be a substantial burden.

THE FUTURE OF BITCOIN

Bitcoin seems most like a noble experiment—it shines a light on possibilities, while seeming to carry the seeds of its own destruction. Let us look first at the latter:

- Built in to its program is a public ledger, which is one key to its success because it permits any user (actually, the computer holding a user's wallet) to authenticate a proffered Bitcoin by verifying it against the ledger, thereby doing away with the need for a central clearing house and speeding up transactions. At the same time, the enormous and growing size of the ledger is, as a practical matter, forcing individual users to turn to third-party services to hold their wallets because the verification process can overwhelm the capacity of a personal computer. This puts users back in the position of having to rely on third parties to facilitate their transactions, with the attendant costs and delays.
- The size of the ledger creates another significant problem: Maintaining it requires an ever-larger allotment of society's resources. With the number of Bitcoins presently in circulation at just over half of the preprogrammed cap, and with the number of active users as yet tiny in comparison to the number required if Bitcoin is ever to reach the status of a currency, the system is already consuming computing resources equivalent to 100 times the fast-

17 That is not to say that they will have no issues. For example, if they buy and sell Bitcoins at various times, but generally own at least some minimum amount, they will have to select an approach for determining the cost paid for the Bitcoins sold in each transaction. There are several possible methods. But Bitcoins, like corporate stock, are essentially fungible, so a consistent, acceptable method has to be established for determining when and at what price the particular Bitcoin now being sold had been acquired.

est 500 supercomputers the world has to offer, as well as a tremendous amount of electricity. Digital the currency may be, but the infrastructure to support it is not part of the solution to climate change.

- To reach currency status, Bitcoin needs to be substantially worldwide in its reach and use. A key strength of the concept is not that it can improve transactions in one or more specific geographic locales, but that it can make geography irrelevant. With that in mind, the preset 21 million cap seems entirely inadequate. Fractional Bitcoins can be spent—fractions as small as one 100 millionth of a Bitcoin [5]. But even if that smallest divisible portion, referred to as dust, had a value of 1 USD (making one Bitcoin worth 100 million USD), total Bitcoin capitalization would still only reach 2.1 trillion USD. There are approximately 10 trillion USD currently in circulation and even that is not enough to allow them to be used in individual transactions all over the world.
- Another strength of Bitcoin, which is critical to its ability to broaden its user base and reach into areas currently less served by existing financial institutions, is Bitcoin's low transaction costs. The system is financed currently by paying those willing to provide the necessary infrastructure with rewards of newly mined Bitcoins. However, infrastructure needs will continue to grow and the rewards, measured in Bitcoins, are programed to drop by half approximately every four years. Transaction fees will have to rise to maintain the system in the future. Already some users attach payment premiums to their transactions to incent miners to select their particular transactions for the block the miner will add to the chain [13], leaving lower fee transactions to close in later blocks. As this practice increases, low- and no-fee transactions will gradually disappear.
- The promise of low- and no-fee transactions is even a bit misleading even now because it is true only for the peer-to-peer part of the transaction. Since Bitcoin has not risen to the level of a functional currency, users of the system often have to engage in currency exchanges between Bitcoin and other currencies. Significant fees are usually associated with those transactions, which are part of the cost of doing business with Bitcoin.

Solutions for these problems are apparently available: that the block chain can be shortened "if necessary" [13], the cap could be adjusted or entirely eliminated [3], and transaction fees could simply be imposed to provide a more secure funding mechanism [22]. But how is this possible? Apparently, miners can change all these fundamental program characteristics—at least if miners representing more than half of the system's computing power agree [3]. This, if true, suggests that seemingly any portion of the program, no matter how fundamental, can be changed as long as the requisite agreement can be achieved. Remember who the miners are: anyone who chooses to download the free software and engage in the work of consolidating transactions into blocks to add to the chain. Thus, in lieu of a banking system regulated by a government, the entire Bitcoin system, which aspires to be a global financial alternative, is governed by whomever happens to be providing computing power to support its infrastructure.

Let us now reconsider some of the claims made for Bitcoin's advantages over traditional financial services. Three were just discussed: the cap on the total number of mineable Bitcoins, the lure of low- or no-fee transactions, and its peer-to-peer characteristic that alleviates the need for a third party in transactions. Others attributes ascribed to Bitcoin include:

- The transfer process is anonymous: The owner of the Silk Road website may take issue with the accuracy of this assertion. While it is true that the public ledger does not contain users names, every Bitcoin transaction is recorded there identified by a person's unique public key and a unique Bitcoin identifier. This information aided in the apprehension of the Silk Road principals. Further, for those who use wallet services, their wallets are associated with such personal information as their names and associated bank accounts.
- Transfers are nearly instantaneous: This is true if users have already established and funded their Bitcoin wallets, but it can take several days to download the Bitcoin client software to establish a wallet on one's personal computer and funding it will take additional time or, alternatively, it will also take several days to establish and fund a wallet with an online service.
- Bitcoin transactions are secure because of its two-key protocol. Users provide only their public key to other users, while keeping their associated private key information secret. Since the private key is necessary to remove funds from a wallet, the funds are protected so long as users keep their private keys confidential. As Bitcoin has attracted more attention, it has also attracted hackers. The system does seem to be fairly robust against duplication of Bitcoins, but less so against theft and destruction.
- Bitcoin may substantially increase financial services available to the world's unbanked [5]: This seems unlikely, at least at this stage, because participation requires a digital wallet. A smartphone app can facilitate Bitcoin transfers from wallet accounts, but smartphones do not have the capacity to host a wallet. For that one needs either a personal computer (with ready access to electricity) or to set up a wallet with a third-party, who then performs a bank-like function.

Having now concluded that Bitcoin has not lived up to many, if not most, of the expectations raised by its promoters, it seems appropriate to end by considering what Bitcoin has achieved. Its most significant contribution is suggesting feasible future achievements, even though Bitcoin itself is unable to reach them. For example, it has demonstrated there is a demand for the ability to cheaply and quickly transfer funds without geographic constraints; it has shown that it is technologically possible to speed up

transfer times across national borders; and it has proven that a significant portion of the population is ready to convert to a digital form of cash. That said, Bitcoin has not established that a peer-to-peer system can function without a governing body. It has simply vested that authority in the collective of self-selected miners. With any system designed to securely transfer and store significant amounts of global wealth, it would seem considerably more prudent that such a governing body be expressly created and authorized to act, while having protocols in place imposing an appropriate degree of accountability upon it. In other words, may have demonstrated that it is time for a governing body with a global portfolio to develop a universally accessible digital currency capable of peer-to-peer transactions.

ACKNOWLEDGMENT

The author would like to thank Lawrence L. King for his assistance, particularly with regard to Bitcoin technology. Any errors herein remain solely the responsibility of the author.

REFERENCES

[1] Nathaniel Popper, "Into the Bitcoin mines," The New York Times, December 21, 2013.

[2] "Bitcoin under pressure," The Economist, p. 17, November 30, 2013.

[3] "New money," The Economist, March 17, 2014.

[4] "Hidden flipside," The Economist, March 15, 2014.

[5] "America launches its first Bitcoin ATMs," Investopedia.com, March 17, 2014.

[6] Farhad Manjoo, "For Bitcoin, secure future might need oversight," The New York Times, March 5, 2014.

[7] H. Wiener, J. Zelnik, I. Tarshish, and M. Rodgers, "Chomping at the bit: U.S. federal income taxation of Bitcoin," Worldwide Tax Daily, January 27, 2014; N. Popper, "Regulators and hackers put Bitcoin to the test," The New York Times, February 17, 2014.

[8] N. Popper and N. Gough, "Bitcoin, nationless currency, still feels governmnets' pinch," The New York Times, December 18, 2013.

[9] T. Mochizuki and M. Obe, "Japan set to clarify stance on Bitcoin," The Wall Street Journal, March 5, 2014.

[10] Ryan Tracy, "Authorities see worth of Bitcoin," The Wall Street Journal, November 18, 2013.

[11] Lee A. Sheppard, "Busting the Bitcoin myths," Tax Notes Today, March 3, 2014.

[12] Nicole Perlroth, "Anonymous payment schemes thriving on web," The New York Times, May 29, 2013.

[13] W. Luther and J. Olson, "Bitcoin is memory," unpublished.

[14] Securities and Exchange Commission v. Shavers and Bitcoin Savings and Trust, 2013 U.S. Dist. LEXIS 110018 (E.D. Tex. 2013).

[15] U.S. Dept. of Treasury, Financial Crimes Enforcement Network, Guidance, FIN-2013-G001, March 18, 2013.

[16] 26 United States Code § 988.

[17] 26 United States Code § 1221(a).

[18] Paul Krugman, "Golden cyberfetters," The New York Times, September 7, 2011; James Surowiecki, "Cryptocurrency," MIT Technology Review, August 23, 2011.

[19] 26 Code of Federal Regulations § 1.61-1(a).

[20] 26 Code of Federal Regulations § 1.61-2(d).

[21] 26 United States Code § 1001(a).

[22] "Money from nothing," The Economist, March 15, 2014.