

Connell Wise

Study of the Future of Money: Is Crypto-currency the Future?

Table of Contents

Contents

Abstract	3
Study of the Future of Money: Is Crypto-currency the Future?	4
Bitcoin?	5
How to earn bitcoin?	7
Marketing.....	7
Getting Paid in Bitcoin.....	8
Regulations	8
Challenge facing Crypto currencies	10
Tax Prevention.....	12
Security Issues	13
Challenges for Tax Authorities.....	14
Control against fraud	15
Global accessibility	15
Cost efficiency	15
REGULATION.....	16
Who regulates it?	17
FinCEN.....	17
CFTC	18
SEC	18
Legislative branch.....	18
The States	19
Private sector companies (banks)	19
Taxation.....	19
What is the Future of money?	20
GLOSSARY	20
GLOSSARY compliment of the (Bitcoin Foundation,2013)	22
References	23

1. Abstract

Exploring the commercial possibilities of Bitcoin, a fascinating, innovative and complex technical architecture and an intricate balance of market forces, social norms, and group consensus. Bitcoin has grown considerably from its original specification and it's often unclear the extent to which Bitcoin's rules are technical versus social in nature. This paper will educate the reader by doing the following.

- 1) Giving the reader a basic knowledge of the subject
- 2) Discussing the pro and cons
- 3) Transparency & Regulation of Digital Currency
- 4) Future of Money.

(Please refer to the word Glossary for reference in this paper to any term that you may not be use to using.)

Study of the Future of Money: Is Crypto-currency the Future?

This paper describes Crypto-currencies and focus on Bitcoin the most well knows of this digital money. Throughout history currency has taken some amazing new forms such as in the 17th Century when the country of Holland used flower-arrangements as a form of currency. This, as all of history, can teach us is a lesson about the constantly evolving state of currency.

While the Dutch were selling single tulip bulbs for 10 times a craftsman's annual income, the British were panicking about their own economic crisis. The silver coinage that had been the basis of the national economy for centuries was rapidly becoming unfit for purpose: it was constrained in supply and too easy to forge (Bill Analysis,2013).

Bitcoin is a crypto-currency in which has gained massive media attention recently as a growing number of businesses have started to accept it as a form payment. Long before the introduction of digital currencies, various businesses have created points or internal store currency models that reward consumers with points for completion of various tasks such as spending a certain dollar amount, or even by purchasing items or points with dollars. These point systems effectively operate as currency allowing the consumers to buy a retail item or pay for some type of service (Hern, 2013). Thus While the future of Bitcoin is still undecided. This paper will try to provide evidence of whether “Bitcoin” become the new dominant reserve currency of the world over shadowing the U.S. dollar or just new way to pay online? Throughout this paper the reader will be given a brief but detail history of this growing sensation.

2. Bitcoin?

The currency was created in 2009 by Satoshi Nakamoto Bitcoin or (BTC) for short became a fresh type of electronic/ digital currency, using cryptographic keys, which can be decentralized towards a system of computers, employed by people and miners worldwide and is never managed by a solitary business or government. This is the initial electronic cryptocurrency which has acquired the public's interest and is approved by an increasing number of retailers. Similar to other currencies, customers can utilize the electronic currency to purchase goods as well as services on the internet in addition to in some real shops that acknowledge it like a type of settlement. Currency dealers can additionally trade Bitcoins throughout Bitcoin exchanges (Shamir & Dorit ,2012).

Presently there are many main variations among Bitcoin and conventional currencies (e. g. USD):

1. Bitcoin lacks a centralized recognition or clearing property (e. g. government, main bank, and MasterCard as well as Visa system). The peer-to-peer repayment system is maintained by customers and miners worldwide. The currency will be anonymously shifted directly among users via the internet devoid of dealing with a clearing property. This indicates that exchange fees are reduced.
2. Bitcoin is produced through a procedure known as "Bitcoin mining". Professionals worldwide employ mining program and computer systems to fix complicated Bitcoin algorithms plus to accept Bitcoin dealings. They are granted with exchange fees and fresh Bitcoins produced from fixing Bitcoin algorithms.
3. A community ledger known as 'Blockchain' documents all Bitcoin dealings and displays each Bitcoin user's particular holdings. Anyone may access the community journal to confirm dealings. This creates the electronic currency more translucent and foreseeable. Furthermore, the visibility stops scam and double investing of the identical Bitcoins.
4. Presently there will be a limited quantity of Bitcoins in circulation. Based on Blockchain,

Running head: STUDY ON THE FUTURE OF MONEY

right now there are approximately 12.1 million within flow by December 20, 2013. The trouble to use Bitcoins (fix algorithms) gets more difficult as additional Bitcoins are produced, and the highest quantity in flow is assigned from 21 million. The actual restriction may not be attained until around the year of 2140. This creates Bitcoins extra useful as more individuals utilize them.

5. The electronic currency may be obtained via Bitcoin mining as well as Bitcoin transactions.

6. The electronic currency is recognized by a restricted quantity of retailers online and throughout a few brick-and-mortar merchants.

7. Bitcoin accessories (comparable to PayPal balances) are utilized for keeping Bitcoins, personal keys along with public addresses in addition to for anonymously shifting Bitcoins among customers.

8. Bitcoins aren't covered and will not be guarded by government companies. Therefore, they can't be retrieved when the secret codes are compromised by any hacker or displaced to an unsuccessful hard disk, or even because of the ending of the Bitcoin exchange. When the secret codes are displaced, the connected Bitcoins can't be restored and might be away from movement.

Bitcoin may obtain more popularity from the community because customers can stay unknown while purchasing products and services on the internet, dealings costs are reduced compared to credit card transaction systems; the community ledger is obtainable by anyone, that may be utilized to prevent scam; the currency source is assigned with 21 million, along with the transaction system is managed by customers and miners rather than a fundamental power. Nevertheless, this does not meant that it will be a fantastic expenditure vehicle since it is quite unstable and is not very secure. For instance, the Bitcoin value increased from about \$14 to the maximum of \$1, 200 this year prior to shedding to \$632 for each BTC recently (Daily Tec, June 2011).

3. How to earn bitcoin?

When a consumer needs Bitcoin he or she can either buy it or create it on the internet. Bitcoin will be the planet's first expert to export cryptocurrency which isn't managed by any fundamental issuing company but is instead an open resource process that is adopted by most of the individuals who take part in the financial system. No one person may adjust the supply associated with Bitcoins and almost all dealings that happen in this financial system are cryptographically confirmed via a procedure known as Bitcoin mining. The Bitcoins tend to be as safe as community key cryptography may be (The Bitcoin Project,2009). As soon as idea of Bitcoin is valued, another reasonable issue is, exactly how would are Bitcoins generated? There are many suggestions which include generating money on the internet and transforming this to Bitcoin. Surprisingly, it is nevertheless much simpler to generate United States currency and then trade the money you earn for Bitcoin in any of several exchanges including Bitstamp or even Coinbase when you're situated within the US.

Consumers can also generate Bitcoin directly inside the Bitcoin financial system. For example, you may do part-time work for Bitcoin in Coinality or perhaps you may turn out with a little gig in Coingig. These tend to be real life comparative of sites such as Elance as well as Fiverr within the Bitcoin environment.

4. Marketing

The marketing of the Bitcoin financial system is, unsurprisingly, fairly strong. This is because there are lot of fresh Bitcoin dependent services which keep approaching constantly and these all require a great advertising system.

CoinURL enables the consumer to spot Google AdSense-designed advertisements on his or her site, and additional services, such as Bitads, let marketers bid regarding banner space on a blog. Presently, there are additional ads that enable money to be generated via ad impressions devoid of reference in the clicks (thus it is not pay per click). Managers, bloggers, or even webmasters, may earn a few Bitcoins via this option.

5. Getting Paid in Bitcoin

There are websites that will pay you for work done on certain tasks. Sites like CoinChat are possibly the most common site to pay people for such work. These sites give freelancers a some milli-Bitcoins for talking in their ad-sponsored chatrooms. The payments tend to be arbitrary and managed by a protocol that considers your action and how nicely you're adding to the conversations available.

Bitcoin fanatics can also earn a few Bitcoins by offering their community signatures in Bitcointalk boards. A large number of marketers are prepared to perform this, as well as regarding the socially productive participant who values conversation via this community (it will be similar to the forum in which Satoshi Nakamoto released Bitcoin in the community), selling signatures may be profitable (Jon Matonis, 17 September 2013).

6. Regulations

Bitcoin has almost turned out to be a household name with escalating coverage throughout the media, as well as reasonable to claim its notoriety carries on to improve. Thus one may wonder what the hassle is all about. Bitcoin came out about in 2009 as a fresh type of electronic currency that had been created from an open-source by a single person or a group of people who is or are known as Satoshi Nakamoto Satoshi Nakamoto has released a statement that his specific identity will be

Running head: STUDY ON THE FUTURE OF MONEY

'shrouded throughout mystery' like a superhero's mild-mannered alter ego (O'Brien, 2014). However this may simply indicate that he's a tremendous geek, but there's no issue, he's definitely a leader. Thus what's this supposed to be about?

Bitcoin will be a type of currency just like any other; nonetheless it is never under the command of any kind of government or monetary organization. The idea can be regarding this to be held and maintained by its individual group. Bitcoin can be de-centralized and handled by peer-to-peer associates who all participate in fresh purchase action and store prior task in exactly what are called 'block chains'. That indicates that a complete 'copy' associated with all dealings are kept locally and utilized to confirm, among individuals, new task, thereby avoiding any one individual from malforming, including or making fake dealings inside the actual block sequence. This 'consensus' strategy safeguards the protection of Bitcoin dealings (Matonis, January 2013).

Bitcoin operates in a similar method to PayPal where the consumer possess an electronic wallet using a distinctive address where individuals can send him Bitcoins. He merely sets up a wallet on his computer or wireless device, or he may obtain the complete Bitcoin wallet as well as take part in the system like a node.

Bitcoin's worth is really as much a result of supply and demand with dangerous traders betting on the altitudes. Presently a solitary Bitcoin (demonstrated as 1. 0000000) will be value £573 or \$935. However, Bitcoins can be purchased in up to 8 decimal spots. Therefore, as an example, 0. 0100000 would cost £5.70 and 0. 1000000 would cost £57. 00, respectively. It's not difficult to see where Bitcoin got its name!

So, where can Bitcoins be purchased?

Unless Bitcoins have been earned through one of the previously mentioned transactions, the consumers will need to buy Bitcoins with his country's current currency. Initially, buying Bitcoins will be all about confidence as it can be not controlled, nevertheless that's exactly how eBay began - a

Running head: STUDY ON THE FUTURE OF MONEY

community where customers trusted one another to purchase and deliver products, and they've carried out instead nicely for on their own.

The particular Bitcoin coal experience

Bitcoin exploration, as it is known, will be the procedure of creating (and acquiring) Bitcoins as well as payment as Bitcoins tend to be compensation for the persistence of your equipment as it is utilized as well as your stage of involvement. This is carried out through numerous techniques from utilizing your personal computer's processor or even GPU (not different to additional grid dependent BOINC projects like Seti @ Home) to utilizing ASIC miners (Application Specific Integrated Circuits), these are created for the unique objective regarding which they tend to be constructed, which however is producing Bitcoins. Until you have substantial expenditure to buy effective ASIC miners like those through butterflylabs.com which may run on 600GH/s (Hash's for each second), you may have to examine USB ASIC Miners like the favorite BlockErupter that produce 336MH/s. Utilizing the actual BlockErupters you may create your personal USB hub type rig operating plenty of them at the same time (Maria,2013).

7. Challenge facing Crypto currencies

Throughout 2009, a fresh idea of currency had been released. The idea appeared slightly obscure regarding using this currency; however, within two years after, Bitcoin has become a rapidly-catching trend. Announced like a decentralized electronic currency, additional individuals and enterprise have begun using Bitcoins. Although this currency continues to be in the experimental phase regular modernizing and repeated tweaking is carried out to enhance it in any way feasible. Unlike other financial systems Bitcoins are never managed by anybody. The system offers a couple of methods guarded by cryptography. It is a new transaction method that has no fundamental power besides the cryptography (available supply application operating with the regulations of mathematics) that addresses the development and exchange, making it impossible to cheat the program. The Bitcoins

Running head: STUDY ON THE FUTURE OF MONEY

promote a community journal (block sequence ledger) where each transaction is documented creating it a notable multiple entry bookkeeping program and a translucent recorder. Utilizing the expert to expert program and the cryptographic key, dealings are refined among customers. Since the key can't be deciphered it is a much more secure type of internet money than carrying out dealings with credit as well as debit cards (Castillo, 2013).

With each new rising pattern, Bitcoins possess pros and cons. However if the hurdles are eliminated, it might assist re-imaging of Worldwide financing. The benefits of Bitcoins tend to be:

- Customers have total command over the cash; they may send and get any quantity of repayments in time regarding the day. Since these dealings are not carried out by banks or businesses but among people it's as simple as delivering a document.
- The dealings need no or really less cash in comparison to additional online cash exchanges that significantly increase the charge, the mere support through Bitcoins is carried out through the miners in order to help the deal documenting in the actual block along with that doesn't charge a lot.
- This will be the most protected and permanent form of money dealings where no individual data is exchanged. Most individuals will choose this technique as it eliminates major problems included in additional dealings.
- Large market segments and small companies alike have broadly recognized it since it assists in faster and dependable money exchanges with very small management charge.
- When additional currencies are impacted by cost variances, the identical can't be stated regarding Bitcoins.

The drawbacks of Bitcoins are to be listed below in no specific order. The new guidelines and improvements are being continuously handled by numerous trustworthy parties.

- There will be no assurance and no buying power supplied as of yet.

Running head: STUDY ON THE FUTURE OF MONEY

- The particular Bitcoin value has still to support, which may only occur when the quantity of customers and companies using bitcoins improve.
- Client plans utilized as wallets can't assure or supply insurance in the Bitcoins.
- The actual currency has however to develop fully and obtain a greater support on the marketplace.

The issues confronted by Bitcoins may be effortlessly deterred. However, the currency requires a tougher existence and greater warranties on the security prior to it may be recognized broadly by the open public like the simplest type of internet currency. The idea currently is a prosperous online currency opportunity which will be on an exciting path it has however being legalized as well as changed through a trial and error currency. Although the future associated with Bitcoins will be nothing however speculation, this has a good reaction through all its customers and may simply be the following big factor (Ryan,2013).

8. Tax Prevention

Tax prevention is a fairly typical exercise among corporate entities. Although the title may seem a bit deceptive, it is both completely legitimate and urged by the US government. Utilizing tax prevention means that a company doesn't completely bypass all of the spending of a company on taxation; rather, the company monetizes on the numerous reductions and loopholes available.

There are numerous methods a company may execute to maximize its tax avoidance. Numerous businesses choose to commit portions of their cash within municipal bonds that are never taxable. Based on exactly how much cash they select to spend, they might be capable to decrease their taxation considerably. Another typical tactic will be to form another organization in an overseas legislation, where business taxation is not used.

Finally, proprietors of the organization can prevent taxation by giving almost all of their individual property to the company. Since the company possesses almost all of the money the

individual generates, he is no longer susceptible to the associated personal taxation. However, they may have to spend business taxation, nonetheless (Andrey,2014).

Tax Evasion

Individuals who do not know precisely what tax evasion, may inadvertently participate in this unlawful practice in their endeavours to reduce taxation. This is really regarded as defrauding the government, therefore regardless of whether the practice conserves lots of cash when from the beginning; whenever the practitioner is captured he can encounter high penalties and years inside federal jail. Tax evasion is committed whenever a tax payer actively prevents, without the existence of any loophole, paying the appropriate taxes – either on an individual basis, business, or both (Andrey,2014). Government entities are currently investigation the likelihood and proliferation of individuals and companies utilizing Bitcoin as a method of tax evasion.

9. Security Issues

Bitcoin has attracted the hacker community because it lends itself to an anarchist or anti-federalist swing due to its development as a method that allows the anonymous and untraceable trade of money. This occurs because bitcoin exchanges don't trace where the money is going.

The issue with the bitcoin anonymity does not end with the anonymous addresses. In the case of the LulzSec¹ donations, the group has used money laundering techniques to obscure large donations. Bitcoin software allows for creating as many unique addresses as one needs. Large donations to LulzSec were quickly broken down into smaller amounts that moved from one address to another to the point where they could be hidden within the other transactions through the bitcoin system.

What should be of concern for governments is that the bitcoin could allow for the movement of large amounts of money easily without the controls that apply to the banking sector such as reporting

¹ a black hat computer hacker group that claimed responsibility for several high profile attacks, including the compromise of user accounts from Sony Pictures in 2011

requirements on large transactions.

Currently, there are limited venues for converting bitcoins into tangible goods. Exchanges allow for the conversion of bitcoins back into national currencies and a limited number of retailers have opened that allow bitcoins to be used to purchase legitimate goods while others sell illicit substances.

Some websites offer online gambling that uses bitcoins to circumvent restrictions on funding online gaming accounts. While some merchants are engaging in questionable practices, others are selling legal goods. Legitimate Bitcoin retailers offer clothing, computer hardware, and coffee.

10. Challenges for Tax Authorities

Although bitcoin is still evolving, there are signs that the currency is on government agencies' radars, particularly in the United States. The FBI, for example, compiled an intelligence report entitled "Bitcoin Virtual Currency: Unique Features Present Distinct Challenges for Deterring Illicit Activity," in which the agency expressed its concerns about bitcoin's popularity with criminals engaged in money laundering and other criminal activity. The lack of response by governments at the moment could be due in part to the relatively small bitcoin market which hasn't reached a critical mass (Tax Analysts, 2013)

Tax Analysts' have requested that the IRS and FinCEN comment on the U.S. government's focus on Bitcoins. Tax Analysts was able to reach the Intra-European Organisation of Tax Administrations (IOTA) to get a sense of how aware European tax authorities are about this emerging digital currency.

Some governments may not be devoting immediate attention and resources to figuring out how to treat digital currencies such as bitcoin because of more pressing economic concerns, particularly in the European Union.

Continual education to make administrations more aware of the tax issues that arise from

Internet currencies is the key for governments to prepare themselves and move toward more concrete answers to questions surrounding government treatment of digital currencies.

The Bitcoin currency brought some advantages to analyst attention. Please follow them below:

11. Control against fraud

A great level of security is possible with Bitcoin. The network provides users with protection against frauds like chargebacks or unwanted charges, and bitcoins are impossible to counterfeit. Users have the possibility to backup or encrypt their wallet and it will make very difficult to steal or lose money in the future. Bitcoin is designed to allow its users to have complete control over their money.

12. Global accessibility

All payments in the world are interconnected. Bitcoin allows any bank, business or individual to be protected when sending and receiving payments anywhere at any time, with or without a bank account. Bitcoin became available in a large number of countries. Bitcoin increases global access to commerce.

13. Cost efficiency

With the use of cryptography, secure payments are cheaper because they eliminate the cost for intermediaries. Transactions with bitcoin are cheaper as cost and as time.

While the accounting treatment of the five year-old currency should be treated in much the same way as any other foreign currency, businesses need to be aware of the risks of keeping Bitcoins on their balance sheet as exchange rate fluctuations have the potential to cause significant gains or losses that could ruin underlying performance.

14. REGULATION

Bitcoin has proven to be a contentious issue for regulators and law enforcers, both of which have targeted the virtual currency in an attempt to control its use. Many legal authorities are still struggling to understand the cryptocurrency and the regulation process is hard to be accomplished.

Tax Analysts sought out members of the bitcoin community as well as tax experts to identify what the implications are for tax administrators (O'Brien, 2014). Some believe that the system could be used to facilitate tax evasion, while others contend that the open nature of the transactions would deter such evasion. All believe, however, that bitcoins raise significant questions. For tax administrators, the challenge is how to approach a system that is outside the traditional streams of commerce and finance. For users, the challenge is how to navigate an ambiguous regulatory climate in which guidance is difficult to come by².

Experts consider Bitcoin as a digital commodity while other considers it as being a currency. However, at its most basic level as a medium for exchange within the community, bitcoins do function as a currency. Users began using the code BTC to designate bitcoins, but BTC is not recognized by the International Standards Organization, which has authority over currency codes.

The bitcoin economy functions similarly to one of the many economies in the world in which U.S. dollars trade in parallel to the local currency. In such cases, buyers and sellers agree to a price using a reference currency with the exchange rate determining the price in the secondary currency.

The coins themselves have no physical form and transfer from computer to computer via a system of cryptographic hashes. Bitcoin users can store their currency using software on their computer or use a web-based service to hold the coins in an account known as a wallet. Moving coins from user to user is done through a peer-to-peer system that operates through unique addresses. These 30-plus character addresses are visible on the network, but only the address creator knows to whom the address

² Reuters website: www.reuters.com

belongs. Because of the length and complexity of the addresses, the bitcoin system makes extensive use of QR codes³, which convert text into an image that can be read by any smartphone. Ownership of an address is known only to the address creator. However, larger transactions, which require more extensive hashes, could, in theory, be traceable. To circumvent this, some users that want to maintain anonymity have used techniques developed for money laundering to break down large blocks into smaller amounts that can be hidden within the system.

Government agencies are increasingly worried about the implications of bitcoin, as it has the ability to be used anonymously, and is therefore a potential instrument for money laundering. In particular, law enforcers seem to be concerned about the decentralized nature of the currency.

The U.S. Federal Bureau of Investigation published a document highlighting its fears around bitcoin specifically, drawing a distinction between it and centralized digital currencies such as eGold and WebMoney. It voiced concerns that while US-based exchanges are regulated, offshore services may not be, and could be a haven for criminals to use bitcoin for illicit activities without being traced.

15. Who regulates it?

Regulators will vary on a per-country basis, but one can expect to see national financial regulators interested in bitcoin and other virtual currencies, potentially along with regional regulators at a sub-country level.

FinCEN

In the US, the Financial Crimes Enforcement Network (FinCEN), an agency within the US

³ Wikipedia Free Encyclopedia: **QR code** (abbreviated from **Quick Response Code**) is the trademark for a type of matrix barcode (or two-dimensional barcode) first designed for the automotive industry in Japan. A barcode is an optically machine-readable label that is attached to an item and that records information related to that item. The information encoded by a QR code may be made up of four standardized types ("modes") of data (numeric, alphanumeric, byte / binary, [kanji](#)) or, through supported extensions, virtually any type of data

Treasury Department, took the initiative. It published guidelines about the use of virtual currencies. FinCEN's guidance defined the circumstances under which virtual currency users could be categorized as money services businesses (also commonly known as money transmitting business or MTBs). MTBs must enforce Anti-Money Laundering (AML) and Know Your Client (KYC) measures, identifying the people that they're doing business with.

16. CFTC

The US Commodity Futures Trading Commission (CFTC), which looks after financial derivatives, hasn't announced regulation yet, but has made it clear that it could if it wanted to.

17. SEC

The US Securities and Exchange Commission (SEC) hasn't issued solid regulations on virtual currencies, but its Office of Investor Education and Advocacy published an investor alert to warn people about fraudulent investment schemes involving bitcoin. In particular, it warned of Ponzi schemes, after charging Texas resident Trendon T Shavers, identified by the online alias 'pirateat40', founder and operator of Bitcoin Savings and Trust, with allegedly raising 700,000 bitcoins by promising investors up to 7% weekly interest.

18. Legislative branch

The SEC case has forced the legislative branch of government to consider bitcoin's legal status. Shavers had claimed that he could not be prosecuted for securities fraud, as bitcoin wasn't money. However, Judge Amos Mazzant issued a memorandum arguing that bitcoin can be used as money. US Senate wrote to several law enforcement agencies, inquiring about the threats and risks relating to virtual currency. It requested policies and guidance related to the treatment of virtual currencies, and information about any ongoing strategic efforts in the area.

19. The States

Each US state has its own financial regulators and laws, and each approaches bitcoin differently. California and New York have been particularly aggressive in their pursuit of bitcoin-related organizations, for example, while others, such as New Mexico, South Carolina, and Montana, don't regulate money transmitting businesses.

20. Private sector companies (banks)

Several banks have stopped accounts owned by people operating bitcoin exchanges. In at least one case, this was because the bank was unhappy that the company involved did not have a money transmitting business (MTB) account..

21. Taxation

In 2009, the US Internal Revenue Service (IRS) posted information about the tax implications of using virtual currencies inside virtual economies, arguing that taxpayers can receive income from a virtual economy and could be required to report it as taxable income. However, it based this largely on guidance related to bartering, gambling, business, and hobby income.

The IRS responded that its guidance could now be taken to cover virtual currencies as used outside of virtual economies. It added that it was also looking at the potential tax compliance risks posed by anonymous electronic payment systems, and was working with other federal agencies on the topic.

22. What is the Future of money?

In our digital age, financial transactions regularly take place electronically, online, in-store even person to person. Without the exchange of any physical currency, will Bitcoin become the money of the future? Linda Yueh Chief Business Correspondent for BBC News said it conclusion best: "Given its recent problems there are doubts as to whether Bitcoin and its contemporaries can become fully-fledged currencies. However, even if Bitcoin itself does not become the internet of money, its technology could provide the platform for future online payments systems. It can be expected that the future of money lies in the digital world; however, if this digital form is Bitcoin has yet to be seen.

GLOSSARY

Address - A Bitcoin address is similar to a physical address or an email. It is the only information you need to provide for someone to pay you with Bitcoin. An important difference, however, is that each address should only be used for a single transaction.

Bitcoin - with capitalization, is used when describing the concept of Bitcoin, or the entire network itself. e.g. "I was learning about the Bitcoin protocol today." bitcoin - without capitalization, is used to describe bitcoins as a unit of account. e.g. "I sent ten bitcoins today."; it is also often abbreviated BTC or XBT.

Block - A block is a record in the block chain that contains and confirms many waiting transactions. Roughly every 10 minutes, on average, a new block including transactions is appended to the block chain through mining.

Block Chain - The block chain is a public record of Bitcoin transactions in chronological order. The block chain is shared between all Bitcoin users. It is used to verify the permanence of Bitcoin transactions and to prevent double spending.

BTC is the common unit of Bitcoin currency. It can be used in a similar way to USD for US dollar

Running head: STUDY ON THE FUTURE OF MONEY

instead of B or \$.

Confirmation means that a transaction has been processed by the network and is highly unlikely to be reversed. Transactions receive a confirmation when they are included in a block and for each subsequent block. Even a single confirmation can be considered secure for low value transactions, although for larger amounts like 1000 US\$, it makes sense to wait for 6 confirmations or more. Each confirmation exponentially decreases the risk of a reversed transaction.

Cryptography is the branch of mathematics that lets us create mathematical proofs that provide high levels of security. Online commerce and banking already uses cryptography. In the case of Bitcoin, cryptography is used to make it impossible for anybody to spend funds from another user's wallet or to corrupt the block chain. It can also be used to encrypt a wallet, so that it cannot be used without a password.

Double Spend - If a malicious user tries to spend their bitcoins to two different recipients at the same time, this is double spending. Bitcoin mining and the block chain are there to create a consensus on the network about which of the two transactions will confirm and be considered valid.

Hash Rate is the measuring unit of the processing power of the Bitcoin network. The Bitcoin network must make intensive mathematical operations for security purposes. When the network reached a hash rate of 10 Th/s, it meant it could make 10 trillion calculations per second.

Mining - Bitcoin mining is the process of making computer hardware do mathematical calculations for the Bitcoin network to confirm transactions and increase security. As a reward for their services, Bitcoin miners can collect transaction fees for the transactions they confirm, along with newly created bitcoins. Mining is a specialized and competitive market where the rewards are divided up according to how much calculation is done. Not all Bitcoin users do Bitcoin mining, and it is not an easy way to make money.

Node - Each Bitcoin client currently running within the network is referred to as a Node of the system.

Running head: STUDY ON THE FUTURE OF MONEY

P2P - Peer-to-peer refers to systems that work like an organized collective by allowing each individual to interact directly with the others. In the case of Bitcoin, the network is built in such a way that each user is broadcasting the transactions of other users. And, crucially, no bank is required as a third party.

Private key is a secret piece of data that proves your right to spend bitcoins from a specific wallet through a cryptographic signature. Your private key(s) are stored in your computer if you use a software wallet; they are stored on some remote servers if you use a web wallet. Private keys must never be revealed as they allow you to spend bitcoins for their respective Bitcoin wallet.

Satoshi - The base unit of Bitcoin (0.00000001 BTC) is sometimes called a Satoshi, after Bitcoin's creator Satoshi Nakamoto

Signature - A cryptographic signature is a mathematical mechanism that allows someone to prove ownership. In the case of Bitcoin, a **Bitcoin wallet and its private key(s)** are linked by some mathematical magic. When your Bitcoin software signs a transaction with the appropriate private key, the whole network can see that the signature matches the bitcoins being spent. However, there is no way for the world to guess your private key to steal your hard-earned bitcoins.

Wallet - A Bitcoin wallet is loosely the equivalent of a physical wallet on the Bitcoin network. The wallet actually contains your private key(s) which allow you to spend the bitcoins allocated to it in the block chain. Each Bitcoin wallet can show you the total balance of all bitcoins it controls and lets you pay a specific amount to a specific person, just like a real wallet. This is different to credit cards where you are charged by the merchant.

GLOSSARY compliment of the (Bitcoin Foundation,2013)

23. References

- Brito, J. and Castillo, A. (2013). "Bitcoin: A Primer for Policymakers".Mercatus Center. George Mason University. p. 5. Retrieved 22 October 2013.
- Bustillos, M. (2 April 2013). "The Bitcoin Boom". The New Yorker. Condé Nast. Retrieved 22 December 2013.
- Dorit, R. & Shamir, A. (2012). "Quantitative Analysis of the Full Bitcoin Transaction Graph". Cryptology ePrint Archive. Retrieved 18 October 2012.
- Mick, J. (June 12, 2011) "Cracking the Bitcoin: Digging Into a \$131M USD Virtual Currency". Daily Tech. 12 June 2011. Archived from the original on 20 January 2013. Retrieved 30 September 2013.
- Matonis, J. (17 September 2013). "Bitcoin gaining market-based legitimacy as XBT". Coindesk. Retrieved 14 December 2013.
- Matonis, J. (22 January 2013). "Bitcoin Casinos Release 2012 Earnings". Forbes (New York). Archived from the original on 16 February 2013.
- News. (2014, March 19). Are Bitcoins the Future of Money or Just a Scam? NBC News. Retrieved March 20, 2014, from <http://www.nbcnews.com/feature/show-me/are-Bitcoins-future-money-or-just-scam-n56916>
- O'Brien, C. (7 March 2014). For Dorian Nakamoto, bitcoin article brings denials, intrigue. L.A.Times. Retrieved 30 September 2013. , from <http://www.latimes.com/business/la-fi-bitcoin-satoshi-20140308-story.html>
- Ostroukh, A. (10 February 2014). "Russia to crack down on virtual currencies".The Wall Street Journal.
- Rosenblum, P. (2014, January 27). Bitcoin: The Currency Of The Future?. Forbes. Retrieved March

Running head: STUDY ON THE FUTURE OF MONEY

20, 2014, from <http://www.forbes.com/sites/paularosenblum/2014/01/27/Bitcoin-the-currency-of-the-future/>

Simonite, T. (n.d.). Bitcoin's Rules May Need to be Updated. MIT Technology Review. Retrieved March 25, 2014, from <http://www.technologyreview.com/view/525836/marc-andreessen-predicts-libertarians-will-turn-on-Bitcoin/>

Steadman, I. (2013-05-11). "Wary of Bitcoin? A guide to some other cryptocurrencies". Ars Technica. Retrieved 2014-01-10.

Thinkweis "How do I get Bitcoins? (For Beginners)". The Bitcoin Bulletin. 11 March 2011. Retrieved 13 December 2013.

Tracy, R. (5 November 2013). "Bitcoin Comes Under Senate Scrutiny". The Wall Street Journal