International Research Journal of Management and Commerce
ISSN: (2348-9766)
Impact Factor- 5.564, Volume 4, Issue 12, December 2017
Website- www.aarf.asia, **Email** : editor@aarf.asia , editoraarf@gmail.com

VIRTUAL CURRENCY- BIT COIN

Mahesh K.M[1], Arabhi Krishna K.A[2]

[1] Department of Commerce, Rajagiri College of social sciences (Autonomous), India

[2] Department of Commerce, St. Alberts College, Ernakulam

ABSTRACT

The development of technology and the increased use of the internet have led to the creation of virtual communities. Some of these communities have created and circulated their own currency for exchanging goods and services. Bitcoin is currently the most popular among these virtual or digital currencies and has been in news recently because of the wild fluctuations in its 'value' and also significant venture capital investment in entities associated with it. Bitcoin has emerged as the most successful crypto currency since its appearance back in 2009. Besides its security robustness, two main properties have probably been its key to success: anonymity and decentralization. In this paper, we provide a comprehensive description on the details that make such cryptocurrency an interesting research topic in the privacy community.

KEYWORDS : Virtual currency; Criptoghraphy; Mining; Anonymity,Private key,Public key

1.INTRODUCTION

Bitcoin, world's first decentralized digital person-to-person crypto currency, is considered to be a revolution in present currency market. This virtual currency is gaining huge popularity worldwide and mass adoption. The countries that had initially banned Bitcoin are now looking to legalize it. Initially, Bitcoin faced a lot of criticism from each part of the world and was considered to be a scam due to its several negative factors. But over the time when experts from various sectors started examining Bitcoin, they understood the power of digital

currencies and started to look it in a positive way. Bitcoin is a so-called virtual currency that has been devised for anonymous payments made entirely independently of governments and banks. In recent years, Bitcoin has generated a great deal of attention on several fronts. Bitcoin payments are based on a new interesting technical solution and function differently to traditional payments. In certain payment situations, Bitcoin can bring advantages in the form of lower costs, rapidity, anonymity, etc. over traditional payment methods. However, usage can also be more risky because Bitcoin is not directly covered by the laws that govern other payment mediation. Weak consumer protection is also a reason for why it may be difficult for Bitcoin to become generally accepted and viable as a means of payment. Use of Bitcoin for payments is low today, and although Bitcoin's future is uncertain, it is an interesting innovation worthy of description.

2. ADVANTAGES OF BIT CION

Anonymous and Private: Bitcoin transactions are completely anonymous and private. Unlike in payments through bank, where the transactions can be tracked and identified, bitcoin transactions cannot be identified. A person can only know the addresses of bitcoins on which the payment has been sent and received. But to whom these addresses belong cannot be identified. It's like payment to a particular bank account can be tracked but to whom these accounts belong cannot be known.

Payment Freedom: Paying through bitcoins provide us utmost freedom. Bitcoins can be sent to any person in any part of the world. No intermediaries in between. No bank holidays/strikes. No boundaries or borders. No payment limit.

Minimal Fees: Paying through Bitcoin has very low and sometimes no transaction fees at all. It all depends on the priority of the person. If a person wishes that his/her transaction gets processed fast, he has to pay a transaction fees which is still very low as compared to any financial intermediary or digital wallets.

Fewer risks for merchants: Bitcoin transactions are secure, irreversible, and do not contain any customers' sensitive or personal information. This protects merchants from losses caused by fraud or fraudulent chargebacks.

Transaction speed is high: Bitcoin transactions are very fast if compared to banking channels. A bitcoin transaction is as fast an e-mail and can be processed within 10 minutes. Also it can be instantly processed if they are "zero-confirmation" transactions, meaning that

the merchant takes on the risk of accepting a transaction that hasn't yet been confirmed by the bitcoin blockchain. Bitcoin has very low transaction fees even for being super-fast in terms of processing.

Non-Inflationary: The central government can get fiat currencies printed as much as they want. When the economy is slowing down it is not able to pay off its national debt, the government orders to print more currency and inject it into the economy. This causes the value of currency to decrease as more people have more currency. Also printing more notes creates inflation and increases the prices of commodity. It is because now more people is willing to pay for a particular commodity and the seller has to increase the price in order to make the sale. Thus, the person who had gained when government injected more currency can now buy more but those people who were not benefitted from have limited currency and now the prices of commodity has also increased.

Create your own money: As central government can print its own money, similarly any person can also produce bitcoins by himself. This can be done my mining bitcoins through computers. It is not any kind of physical mining. Bitcoin mining is simply a case of leaving the computer switched on, and keep the bitcoin mining software running.

3. DISADVANTAGES OF BITCOINS

Degree of acceptance: Many people are still unaware of Bitcoin. Every day, more businesses accept bitcoins because they want the advantages of doing so, but the list remains small and still needs to grow in order to benefit from network effects.
Instability: Bitcoin prices are uncertain and increases or decreases at a very high pace. Speculators wish to take advantage of it but genuine investor's thinks of it as too risky and therefore all the investors does not invest in Bitcoins.

Developing nature: Bitcoin software is still in beta with many incomplete features in active development. New tools, features, and services are being developed to make Bitcoin more secure and accessible to the masses. Some of these are still not ready for everyone. Most Bitcoin businesses are new and still offer no insurance.
Possible Government Interference: Well the government may not take Bitcoins away but can ban it in the country, which forces bitcoin wallets and companies to shut down. The bitcoins in these wallets are freezed and access to them becomes difficult.
Lack of recourse: If you lose the wallet which had bitcoins stored in it, you have lost all of your bitcoins in that wallet. You cannot regain it and they are simply lost forever. In case

credit card/debit card stolen, we can call the merchant to cancel the card and request for a new one but in case of Bitcoins, as it is decentralized and no one has control over it , we don't have any person to call.

Money Laundering: Initially bitcoins were used for money laundering and people operating in black markets, which did not wanted to reveal their personal information and get payment secured. In money laundering middleman/intermediaries would collect money from one source and transfer it to another source through Bitcoins.

4. HOW DOES BITCOIN WORK?

As a new user, you can get started with Bitcoin without understanding the technical details. Once you have installed a Bitcoin wallet on your computer or mobile phone, it will generate your first Bitcoin address and you can create more whenever you need one. You can disclose your addresses to your friends so that they can pay you or vice versa. In fact, this is pretty similar to how email works, except that Bitcoin addresses should only be used once. **Balances - block chain**: The block chain is a shared public ledger on which the entire Bitcoin network relies. All confirmed transactions are included in the block chain. This way, Bitcoin wallets can calculate their spendable balance and new transactions can be verified to be spending bitcoins that are actually owned by the spender. The integrity and the chronological order of the block chain are enforced with cryptography.

Transactions - private keys: A transaction is a transfer of value between Bitcoin wallets that gets included in the block chain. Bitcoin wallets keep a secret piece of data called a private key or seed, which is used to sign transactions, providing a mathematical proof that they have come from the owner of the wallet. The signature also prevents the transaction from being altered by anybody once it has been issued. All transactions are broadcast between users and usually begin to be confirmed by the network in the following 10 minutes, through a process called mining.

Processing – mining: Mining is a distributed consensus system that is used to confirm waiting transactions by including them in the block chain. It enforces a chronological order in the block chain, protects the neutrality of the network, and allows different computers to agree on the state of the system. To be confirmed, transactions must be packed in a block that fits very strict cryptographic rules that will be verified by the network. These rules prevent previous blocks from being modified because doing so would invalidate all following blocks. Mining also creates the equivalent of a competitive lottery that prevents

any individual from easily adding new blocks consecutively in the block chain. This way, no individuals can control what is included in the block chain or replace parts of the block chain to roll back their own spends.

5. SECURITY ISSUES & RISK OF THEFT

Taken together, the security risks around Bitcoin are the currency's single greatest drawback, and are worthy of special consideration for anyone considering converting U.S. dollars into Bitcoin. The fact that Bitcoin units are virtually impossible to duplicate does not mean that Bitcoin users are immune to theft or fraud.

The Bitcoin system has some imperfections and weak points that can be exploited by sophisticated hackers looking to steal Bitcoin for their own use. The Mt. Gox incident, as well as a host of smaller, less publicized incidents, underscore that Bitcoin exchanges are particularly vulnerable to theft by hacking. Two of Bitcoin's perceived strengths – its political independence and strong anonymity protections – actually make it more attractive to thieves and fraudsters.

In many jurisdictions, Bitcoin occupies a legal gray area, meaning local law enforcement authorities view theft prevention as a relatively low priority. Moreover, it's often difficult for the authorities to prosecute those responsible for Bitcoin heists, many of which originate in politically unstable or unfriendly nations and affect a global population of Bitcoin holders.

Those who use Bitcoin for illicit purposes face additional risks. Dark web marketplaces – online, international black markets whose users buy and sell illicit substances, stolen goods, and prohibited services – are frequent heist targets. Bitcoin users who participate in the dark web are likely already breaking the law, and thus have limited recourse in the event of a hack or theft – they can't very well contact local authorities and say that the funds they received for selling illegal drugs were stolen.

Common Modes of Bitcoin Theft

It usually takes more technical skill to steal Bitcoin than physical cash. Most Bitcoin heists involve sophisticated hack attacks by highly accomplished outsiders or rogue exchange employees. Common modes of Bitcoin theft include the following:

- **Stealing Private Keys**. Private keys stored in publicly accessible digital repositories, such as Bitcoin exchanges or personal cloud storage drives, are vulnerable to theft by

hacking. The thieves use these private keys to access and transfer the corresponding Bitcoin holdings, relieving their rightful owners of their funds.

- **Exploiting Wallet Vulnerabilities**. Some Bitcoin wallets have security flaws that render them vulnerable to attack. As a convenience, some service providers store private keys in the same virtual wallets as Bitcoin funds themselves, allowing hackers to steal the funds and keys in one fell swoop.

- **Operating Fraudulent Exchanges and Investment Funds**. Some seemingly legitimate companies dealing in Bitcoin are actually fronts for financial crimes. For instance, a boutique "Bitcoin investment fund" called Bitcoin Savings & Trust made a name for itself in the early 2010s by providing outsize returns to early investors.

- **Attacking Legitimate Exchanges Directly**. Since they attract thousands of users and store millions of dollars in Bitcoin, exchanges are attractive targets. Bitcoin can be stolen from exchanges' own Bitcoin wallets (which they use to store Bitcoin units taken as exchange fees), from users' wallets (as many users store Bitcoin balances with exchanges for convenience, similar to a brokerage account's cash balance), or during exchanges and transactions themselves.

- **Attacking Dark Web Marketplaces**. The vulnerabilities of dark web marketplaces are similar to those of Bitcoin exchanges. The second largest Bitcoin heist, after the Mt. Gox hack, affected a dark web marketplace called Sheep Marketplace. Losses approached $100 million at then-current exchange rates.

6. STRATEGIES FOR REDUCING SECURITY RISKS

The cyber security industry is locked in a constant arms race with hackers and other cyber-criminals, whose sophistication and operational scope increase by the week. In this environment, there's no such thing as a complete guarantee of security – particularly when money is involved. However, prudent Bitcoin users employ these common-sense strategies to reduce their exposure to theft and general security breaches:

- Securing Private Keys. Savvy Bitcoin users store copies of their private keys offline, in physical storage media or even on paper printouts, rather than in online locations that can easily be accessed by hackers. Since you have to provide your private key during a Bitcoin transaction, storing your key offline isn't completely foolproof – but it's preferable to leaving it in a static online location all the time.

- Using Highly Secure Bitcoin Wallets. Even if you're not an advanced computer programmer capable of evaluating wallet code or technical security protocols directly, do your best to research a particular wallet service's track record. Speak with current users or read online reviews, if possible. Think twice about using services that have been hacked in the past and have yet to publicly state that they've made security enhancements.

- Researching Bitcoin Exchanges and Other Services. To avoid getting caught up in a Ponzi scheme or simply being robbed blind by a seemingly legitimate Bitcoin exchange, do your own due diligence before transferring or storing Bitcoin units with a new platform. Treat any promises that sound too good to be true (such as rapid or outsize returns on your funds) as red flags – and avoid working with platforms that make them.

- Avoiding the Dark Web. Like real-world black markets, the dark web is an unsavory and sometimes dangerous place. Avoiding marketplaces like the now-defunct Silk Road and its successors is an easy way to avoid needless exposure to security risks. Additionally, avoid using Bitcoin for "gray market" activity that, while possibly legal in your jurisdiction, might be illegal or frowned upon in others – such as sports betting. It may be impossible to recover your funds after a heist that targets a gray market platform found to be operating illegally, even if you're not criminally liable.

7. FACTORS AFFECTING THE PRICE OF BITCOIN

1**. Government Regulation:** Each time a government releases official statements about the regulation of digital currencies, the price of bitcoin is normally affected. Even if the actions of that government are not related to the virtual currencies directly, the impact will still be felt. A good example of this can be derived from the Cyprus banking crisis, where the government seized funds. This prompted discussions on whether Cyprus should adopt Bitcoins as their new currency. Anytime there are restrictions on the use of bitcoins, their price changes drastically. However, because of the anonymous nature of the bitcoin transactions, most governments are proposing certain rules to eliminate this anonymity. For instance, there have been proposals to create a third party supervision mechanism for bitcoin exchanges. This is bound to significantly affect the bitcoin price.

2. Media Influence: The media can also influence the bitcoin price significantly. Media hype can easily lead to an increase in the price, while negative news can lead to a decline in the

price. For instance, news about bankruptcy or hacks on bitcoin-related websites and services can cause panic and disruption among bitcoin users, leading to price dips. Negative news about government involvement and regulations as well as news on the use of bitcoins in illegal dealings such as drug transactions and money laundering tends to have the same impact on the bitcoin price.

3. Stability of the Bitcoin Network: Stability of the bitcoin network is a major factor that most bitcoin enthusiasts are concerned about. Most people want a secure network where they will not lose their money. Unlike the conventional currencies like euros and dollars, bitcoins are largely perceived as economic bubbles as they are only valuable when exchanged with other currencies, but do not have any inherent value on their own. If most people and business organizations stopped accepting bitcoins, the "bubble" would burst, leading to a fall in the bitcoin price.

4. The Bitcoin Demand and Supply: The price of bitcoins is largely depended on the demand and supply. This means that high demand and low supply often leads to an increase in the price. Note that bitcoins have a controlled supply whereby the total number of bitcoins in circulation must never be more than 21 million. Due to the limited supply, there are speculations that the bitcoin price will continue to rise with time.

5. Wider Mainstream Acceptance: This is another major factor that influences the price of this crypto-currency significantly. Even if it has faced a number of challenges and detractors, many well-known companies and businesses have started accepting bitcoins as a means of transaction. For instance, sites such as Reddit and WordPress are currently accepting bitcoins as a means of payment. A number of Brick and Mortar enterprises in the US have also started accepting bitcoins as payment for their services. An increase in the number of venders accepting this type of currency will definitely lead to an increase in the price of bitcoins.

6. Large Businesses Dumping to Fiat Currency: Given that bitcoins are not widely accepted as a means of transactions or payment, not many people and institutions can accept them. Because most things still have to be paid for in fiat currencies, many businesses often sell large portions of bitcoins so as to pay for their business expenses. This is normally referred to as "dumping" and it can keep the value and price of bitcoins in a depressed state.

8. Conclusion

Since the establishment of Bitcoin 2009, its uses as a cryptocurrency have been debated extensively as it has become a highly controversial topic. The debates are stimulated by the

fact that some argue it has the potential to disrupt the financial system as we know it. On a positive note, the minimal fees and lack of regulations makes it much easier and cheaper to send money internationally. This ultimately makes capital available in the places that need it the most and were previously unable to gain access to capital flows. However, when looking at the negatives, the implementation of this currency also allows for the facilitation of criminal activity, and it takes away from the ability of the government to generate revenue through taxation. This tradeoff highlights the importance of cost-benefit analysis when evaluating the issue. Furthermore, it is critical to note that any alterations made to the existing infrastructure could radically change the nature of the currency and eliminate some of the greatest benefits it was designed to retain

Bitcoins can be helpful to a lot of people. Since they are an international currency, you can use them in any country without having to convert between currencies. The Blockchain is really secure and it lets you make sure your money goes to/comes from the right person. People receiving Bitcoins won't have to pay anything for the transactions, and Bitcoins have a lot of support. All of these will definitely help Bitcoin get more users, and if everyone uses Bitcoin it could replace official currencies. Sure, it has some disadvantages, but some of those are because Bitcoin is a new thing, so as time goes on they will be less of a problem. The others can easily be avoided.

References

[1] Satoshi Nakamoto. Bitcoin: A Peer-to-Peer Electronic Cash System.

[2] http://bitcoin.org/bitcoin.pdf

[3] Scott Driscoll. How Bitcoin Works Under the Hood.

[4] http://www.imponderablethings.com/2013/07/how-bitcoin-worksunder-hood.html

[5] Adam Back. Hashcash. http://www.hashcash.org/

[6] Bitcoin Wiki, Available from https://en.bitcoin.it/wiki/.

[7] Evaluating User Privacy in Bitcoin, In Proceedings of Financial Cryptography and Data Security Conference (FC), 2013. Available from http://eprint.iacr.org/2012/596.pdf.

[8] IRC Bitcoin incident resolution, Available from http://bitcoinstats.com/irc/ bitcoin-dev/logs/2013/03/11.

[9] [Bitcoin-development] Revisiting the BIPS process, Available from https://www.mail-archive.com/bitcoin-development@lists.sourceforge.net/msg02982.html.

[10] Bitcointalk Forum - Available from https://bitcointalk.org/.