Siddiqi *et al.LGU (IJECI)* 2017

LGU (IJECI)
ISSN: 2522-3429

LGU International Journal for
Electronic Crime Investigation

Research Article

Vol. 1 issue 1 Dec 2017

Crypto Currency in Cyber world

Mohsin Ali[1]
Digital Forensics Research and Service Centre
Lahore Garrison University, Lahore, Pakistan
mohsinaly@lgu.edu.pk

Abstract:

The Article covers the key aspect of the evolution of Cryptocurrency as a future mode of payment for merchant and consumers, the paper will highlight all the key elements that plays a pivotal role in influencing the market value of the Cryptocurrency, with respect to the acceptance of Cryptocurrency within general people, government regulations for this means of transaction, the security aspect of the currency, and where, how and who is using this currency, the perks and the disadvantage that have taken birth due to the advent of this currency which includes bitcoin, ethereum, and other alt-coins. More over the paper concludes with author's analysis on digital currency.

Keywords: Cryptocurrency, Security, transaction, bitcoins, ethereum, Government regulations, payment.

1. Introduction

The evolving trends have change people lives to great extent, every day every instant our standards of living is changing because of the acceptance of new improved items that are arriving the market. These items have not only brought comfort to our lives, but is also source of revenue generation for many individuals. There was an era when all our capital was the gold or silver coins that we had in our hands, then paper money came into existence, then banker's cheque, and then online payments, and now the emerging currency is crypto currency.

It's certainly not wrong to say that over the recent years, the production and the usage of digital currencies also known as crypto currency has increased a lot. The famous among these electronic currency is Bitcoin [1], because of the great market worth, usage and merchant acceptance. There are numerous currencies available in market which are functioning primarily on the same principles as Bitcoin. All these crypto currencies are collectively termed as "altcoins". During the past few years, the altcoins have gained monetary worth and acceptance to great extent.

The total value of crypto currency worth billions of dollar, in a survey conducted in 2015 the total net worth of this industry was $3.8 billion, in which only bitcoin worth was $3.3 billion alone. This shows the acceptance of crypto currency among the people during the recent years [2]. Many of the altcoins available within the market are the replica of the functionality of Bitcoin, it's because of the code being open source, the slight difference in these altcoins, and Bitcoin is of the tweaks, which can be easily enhanced by anyone who has fundamental skills of programming. Though undoubtedly the adoption of crypto currency is increasing day by day, and the market worth of these digital currencies are touching the sky, there are many factors that are issues of concern for developing world, which includes the fragility of the value of this currency, and anonymity. The biggest threat to the world is anonymity of this currency at the moment, where hackers are asking for ransom as an amount to be paid in these crypto currency, where the identity of a hacker is unknown to the victim, and it's a source for them to easily flee the scene. There was a time when the many of the cybercrimes were related to the physical ransom, and the crime end scene had somehow connection with the physical world, but due to the presence of cryptocurrency now this factor has moved more into to virtual world, and has increased the anonymity of the person online to great extent [3].

The mechanism of a crypto currencies like bitcoin, and other same kind of altcoins is just based on "a chain of digital signatures" where for every transaction the owner of the coin must digitally enter the hash value of the last transaction and must generate public key for the next coin holder of crypto coin, which is to be attached at the end portion of the coin, to complete the process of transfer of transferring coin ownership dynamically. Now after purchasing coin there is an additional process of storing these coins either there is an option of storing it on physical hard drives or to store online using wallets available online like coinbase. As every invention has some pros and cons, cryptocurrency has negative features too, Since everything is done online or saved in hard drive there are chances of these currency to be stolen or loss or destroyed, as happened to Mt. Gox in the incident where approximately $ 350 million worth of bitcoin were stolen which caused the company to declare bankruptcy and this has made the concern of money lost in cryptocurrency more prominent, though its matter of 2014 but till the date people are very conscious when it comes to transaction through bitcoins. Apart from the risks within this industry there are more than 5 ton of cryptocurrencies that are available in market, and the success ratio is high, though not as high as bitcoin, but certainly they are playing role in giving boast to this industry. Still there is a lot to be researched of this industry as most of the research focuses on Bitcoin, and research on other altcoins is not done as effectively as done on bitcoin. The advent of this cryptocurrency has not only brought new way to digital payments, but has brought significant development in technological progression, and alarming factor for government entities, for the issuance of new laws for carrying out transactions legally. According to many experts even after these years of Bit coin within the global market there are still mixed perspectives about the future of bit coin and currencies related to this industry. According to [4] he believes that the ratio of electronic

transactions will increase. Block chain mechanism will be greatly used by the stake holders for handling digital transactions [5]. Considering all these elements, the paper will give a brief yet comprehensive analysis on the industry of crypto currency.

2. Literature Review:

This topic of research is taking great strength over the years, the crypto currency is a matter of concern that's been highlighted in most of the research write ups, and the top among all these is Bit coins. There have been several researches done on Bitcoin value, some researchers have actually tried to compare the value of this "moneyless" digital currencies with the actual available currencies like 'digital gold' [6][7]. According to another study carried out by Yermack there are several weakness in Bitcoin currency which can cause fluctuation in the value of this currency. Even though, the value of Bitcoin can change because of many reasons.

Yermack believes there are many weakness in the bitcoins currency which can easily alter its price on a given day. Even though, the price of bitcoins can vary over various exchanges but the bitcoins price in dollars is a bit too high considering alt-coins are not exactly money in the traditional sense and there will be issues of acceptance by people of these crypto currencies [8]. Crypto currency track has been wild over the last half decade even though the traction it has got at the moment. The hype it had at the time it was publically emerged in 2009 was more than the performance of anarchic crypto currency. The future of crypto currency and how it will affect us in future is still unknown, though the demand of alt-coins have increased over the years but when it started in 2009 it was only traded for pennies. It was later that when a slight alteration was made to the code by a community of coders and its value rose from $1 in February of 2011 to $30 after just four months to roughly $290 in 2015 [9]. The remaining portion of this article will highlight the factors which influence the price, and the repute of this digital currency.

2.1 Government Regulations for Cryptocurrency:

It is believed that there is still room for improvement when it comes to the government regulations, and because of this there is hesitation among the investors. Still there are a lot countries which doesn't accept the use these crypto currencies but Japan is one where it's is legitimately allowed to use Cryptocurrency as the legal means of transaction, after implementing changes in the Payment Service Act, which officially recognize the bitcoin and ethereum as legal medium for payment transactions, but it's not piece of cake to use it straight away, any organisation that wish to use this medium should register first with government by paying 10 million yen ($90,000), should ensure that they have proper Secure IT system, to avoid fraud and theft, and an every year audit by certified accountant. Apart from Japan, United States is also making use of digital currency as legal currency, but the process is lengthier, and difficult one needs to go through many channels before getting final approval, while in Japan it's only Financial Services Agencies FSA. [10]

While the growing cryptographic money popularity can possibly reform the mode of

transaction, its presentation into worldwide settings is full of challenges and possible problems linked to it. Since virtual currency standards are not generally perceived as legitimate methods for paying to merchandise and enterprises, creating systematic frameworks for their operation is fundamental. For the monetary reforms to be rational, their legal status must be built up. Administrative frameworks are blooming, with horde approaches being taken by different governments. Current administrative steps are in their initial stages and is changing with rapid growth of the industry [11].

Controls will highlight more prominent genuineness to a cash, which will result in increased mass acknowledgment. They will institutionalize mechanism of the market and limit in any events that can cause instability. While governments are trying administrative steps, their end objective is the same: to confine fraud, protect buyers, regard financial agreements, and create appropriate tax evaluation techniques [12].

2.2 Public Perception about Cryptocurrency:

The acceptance of virtual currencies among general public is growing day by day, according to a survey by Boston Federal Reserve in 2015 a negligible percentage of 0.87% of American consumers were estimated to have Cryptocurrency, which worth's approximately 2.8 million people in United States only. Carrying this calculation ahead, coin based and ARK Research projected that in 2016 roughly 10 million people around the world will own bitcoin. Their survey clearly shows that people have started to adopt digital currency, for business and transaction purposes.

According to another research conducted in America in April 2015 not many Americans knows about the crypto currency, what actually it is and how it works or how can be used. Only 4.5% of the surveyed people had used crypto currency weather in payment or transactions [13]. At that particular instance this stat show very discouraging depiction of how the crypto currency is useful and how only few people are using it.

There are few researcher who believes that the hike in the price of bitcoins is simply a marketing technique of making money, as there is no basic value to support this currency [14]. In contrast to his study Woo, and his fellow researchers states that bitcoin may have some rational value because of its money like properties and can be used in transactions and payments, without any fundamental basis [15]. The advancement in technological aspects can impact the bitcoin value. E.g. the blend of bitcoins in PayPal's instalment framework has brought issues into consideration and encourage a substantial measure of eagerness for advanced financial systems among many people. Besides, many new organisations have begun using crowd funding stages which recognize cryptographic forms of money, with Ethereum being one of the best case. Block stream is another progress that could provide enhanced functionalities to bitcoins, which will ultimately support their general esteem and cost. The purpose of stage was begun to develop better approaches for speeding up developments process in these kind of financial methods and particular contracts.

Only few large retailer have accepted crypto currency as a mode of payment during the initial 6 years of crypto currency. Many of the major vendors like Zhanga, Overstock.com and TigerDirect only used to deal in bitcoins [16]. This shows that there is a positive development of this industries and still it's in developing phase. A paper written by William J. Luther and Josiah Olson, in 2013 stated that hardly any retailers accepts Bitcoin as a type of payment because of the little client base; and many of the customers won't consider utilizing Bitcoin till the time that a critical number of retailers started accepting Bitcoin payments. Basically: arrange impacts support the status quo.... Bitcoin may neglect to gain broad acknowledgment regardless of the prospect that it was better than existing currencies [17].

Block chain technology is new to many of the business, and few of the businesses have already started to adopt this technology. NASDAQ proclaimed that it will launch a block chain-style digital record technology to manage equities with its Nasdaq Private Market stage [18]. The consultancy firm Deloitte has established the Deloitte Crypto Currency Community to direct instructions to its customers on the advantage of the block chain for trading funds and overseeing staff payments, among other things [19]. Even the Federal Reserve System in 2015 has considered the block chain or in other words "digital value transfer vehicle" to process interbank transaction. It is expected that more organisations will adopt this technology as more people will be more familiar.

2.3 Cyber Terrorism and Cryptocurrency:

Though the internet terrorism is not as intense deadly as the conventional terrorism like (bombings, mass killing, and other kind of violence), the reason why it's dangerous is because it's used as a medium to recruit, convert and to establish an easier medium of communication with terrorist cells, with greater degree of anonymity from Intelligence Communities and Law enforcement agencies. Now the question that arises here is that how these terrorist organisation do works? It is believed that they are terrorist groups that have created their websites that have information regarding the history of the group, details about the famous members, and the founder of the group, goals of the organisation and how they are going to achieve their set goals, it's not necessary that all the groups will write their goals directly, there is a possibility that they may not state it directly. The main way to identify their intention is the content they will write against their enemies. There are few groups like Hezbollah and Hamas discuss the operation they have been involved in. Moreover the news that's cited on their website is generally accurate in terms of their "enemies", attack, martyrs and the enemies they have killed in an attack [3].

There have been many cases were terrorist have tried to used crypto currency, for transferring money, Though they are not using it to great extent as they are using the "hawala" system, as they area where they are operating are not IT infrastructure wise as strong as other countries. According to Haaretz in January 2015 one of the support of ISIS Abu-Mustafa was able to raise five bitcoins (approximately $1000) at that time, his account was then shut by FBI, and he was not able to further proceed. Then in May 2015 one of the member Abu Ahmed al-Raqqa had appeal ISIS supporters to

submit their donations on dark web through bitcoins. Then in 2015 another member of ISIS from Virginia had instructed donors through social media to submit donation using bitcoins. It is further reported that one of the ISIS linked hacker "Albanian Hacker" had demanded to bitcoins in order to remove bugs from the system of an Illinois internet retailer, at that time the worth of bitcoin was app $250. In July 2016 a terrorist organisation had received 0.929 bitcoins in 2 different transactions after they have added option of donating those funds through bitcoin. Recently in January 2017 Indonesian financial agency has announced that Bitcoin and other online Services were used by ISIS militants to fund terrorist events in Indonesia [20].

2.4 Stability of Crypto Currency:

Another problematic issue with these virtual currency is that their value is unpredictable, which is one of the reason that plays critical role in user acceptability, just as happened in the case of ZCash where the value of one coin was over $4000 on October 28th, the day when it has launched, and a week later the value dropped to $1000, and now the worth of one coin is below $100 [21]. As happened recently when the rumor of the death of the owner of ethereum broke out, which resulted in loss of $4 million to the ethereum. Ethereum is the second leading crypto currency after bitcoin.

To keep user identity anonymous the efficient methods have been developed for bitcoins and other altcoins. Bitcoin is a digital currency which relies on a systematic set of mineworkers to mine coins, and a distributed system that is responsible for communicating the exchange. The character of Bitcoin clients are concealed behind the pseudonyms (keys) which changes time to time with a set target to increase the exchange. One of the significant feature of bitcoin design is the mining mechanism which involves the participants to solve the computational puzzles in order to gather payment. This helps in understanding the weak points and technical problems such as the inconsistencies in the crypto currency disrupted log data structure [19].

The work that's done on Bitcoin can generally be divided into couple of streams. The main stream of studies are focuses on the strategy and the innovation fundamental decentralized foundation of Bitcoin, i.e. its convention and hazards developing on a specialized level. Different systems in light of system hypothesis have been connected to direct inquiries in regards to exchange irregularities and conceivable results of de-anonym zing single substances in the Block chain. For example, Reid and Harrigan in their study have validated that clients and Bitcoin addresses might be drawn latently by the use of focused administrations, for example, online wallets and money traders also, [20]. On the premise of an everyday utilization situation of Bitcoin on a college grounds, Karame and his co researchers have split their approach with a semi simulative approach the secrecy of Bitcoin-clients. They locate that 40% of the understudies can be profiled inactively which subsequently additionally drives them to dismiss the namelessness theory with respect to Bitcoin. Furthermore, [22] demonstrate that twofold spending is imaginable under the situation of a quick installment (i.e. an installment which is not checked in the Block chain) and in this way they suggest an

alteration of the current Bitcoin execution. Clark what's more, Essex use the Bitcoin-framework to explain a technique with safely timestamp [23].

Though there have been several researches carried out to monitor stability of this type of currency, but till the date its considered to be most fragile currency unlike international currencies like dollars, euros, pound etc. The graph (figure 1) clearly illustrates how the value of bitcoin has changed over the recent months.

Figure 1: Bitcoin Stats

The figure 1 shows the value of one bitcoin against dollar, over the time, according to the figure the value of one bitcoin in early September was around $3400, which was further dropped in mid-September to approximate $3200, and now recently it has achieved the maximum high price of all time of $6034 on 21st October. This shows that the price is never stable and there are always chances of ups and down like stock market prices.

2.5 Critical Infrastructure, and Cryptocurrency:

In 2007 Estonia's Critical Infrastructure (CI) was hacked, which is believed to be caused by Russian hackers or a group of hackers who were upset because Estonian government had moved the Soviet WWII memorial out of city center to their capital of Tallinn, they initiated Distributed Denial of Service attack (DDOS) on the CI of the Estonia, which includes communication systems, and few big name in banking industry there. It is said that most of the banking transaction (98% of the transactions) in Estonia are performed online, and due to this attack there was a huge impact on the financial system. [24]

The United State has initiated the initial steps to counter this threat, by following the Executive Orders (EO) 13.636, and Presidential Policy Directive (PPD) -21; "Improving Critical Infrastructure Cyber Security" and "Critical Infrastructure Security and Resilience" respectively. EO acknowledges the issues that are faced by the CI, and to priorities the national security, wellbeing of the digital world. This EO 13.636 strategies to successfully increase the degree of sharing information regarding cyber security. The plan is to come up with a process that can track, disseminate, record report, and deliver said reports to the necessary agency or agencies with the coordination of National Intelligence. Not only physically but virtually the amount of sharing information among agencies and security providers will improve by this order. The order also states that the information sharing objective will be further improved by temporarily hiring Subject Matter Experts (SMEs), who will provide information to the Critical Infrastructure Operators so that they can provide sufficient security to the CIs. The order further states that agencies will consider all action and courses to make sure that they comply with privacy standards. Annually all Sector Specific Agencies (SSAs) and Subject Matter Experts will spot the CIs by the risks level they are on, and shall work accordingly. [25]

The threat to CIs is inevitable to great extent, many of the banks in London have started to stock Bitcoins, so that if there is threat to their system they can pay in bit coins, it's because criminals prefer to have ransom in shape of virtual currency, which is difficult to be traced. [26]

2.6 Security for Cryptocurrency:

When we talk about online payment transfer procedures or virtual currencies among many other factors, security is one of the major factors that needs to be considered, people still have trust issues with this type of currency because it's something that doesn't exists physically. People still have doubts about the transaction being secure and real, and this is

exactly what people should understand that it's secure and real. There have been many mechanism developed in order to make sure that the digital transaction are secured. For digital transactions. Decentralized trusted Time stamping technique is used to store anonymous record for digital content transaction through online web based service. The service enables clients to hash records, for photographs, content, or recordings, and save the generated hashes in the Bitcoin square chain. Clients would then be able to retrieve and verify the timestamps that have been focused on the piece chain [27].

Crypto currency can work as decentralized trusted time stamping only if digital data of the transaction, and the hash values are embedded together, which keeps record in the block chains of the alt-coins or crypto currency [23].

In addition to all the techniques mentioned above another way of verification of-work in light of looking for prime numbers is presented in shared digital money plans. Three sorts of prime chains known as Cunningham chain of first kind, Cunningham chain of second kind and bi-twin chain are qualified as evidence of-work. Main quickest is connected to piece hash to protect the security property of Nakamoto's Bitcoin, while a consistent trouble assessment conspire is intended to enable prime tie to go about as customizable trouble evidence of-work in a Bitcoin like digital money [28].

3. Conclusion:

After discussing all the key elements above the author would like to conclude the article with the statement that certainly there is no doubt that Cryptocurrency will be the future global currency for the means of transaction.

4. References

1 Hayes Adam, "What Factors Give Cryptocurrencies Their Value: An Empirical Analysis". (16th March 2015) University of Wisconsin - Madison - Department of Sociology; The New School - Department of Economics. Available at SSRN: https://ssrn.com/abstract=2579445

2 Ujan, M., Anthony, S., Oluwakemi, H., Jon, O., Lu, Y. and Richard, B. (2017). " A brief survey of Cryptocurrency systems" - IEEE Conference Publication. [online] Ieeexplore.ieee.org. Available at: http://ieeexplore.ieee.org/document/7906988/

3 Jesse D. Bray, "Anonymity, Cybercrime, and the Connection to Cryptocurrency" (January 2016) Eastern Kentucky University [online] Available at : http://encompass.eku.edu/cgi/viewcontent.cgi?article=1342&context=etd

4 Luther, William J. and Josiah Olson. "Bitcoin is Memory." Journal of Prices & Markets, 3, 3 (2015): 22-33.

5 Nahorniak, I., Leonova, K. and Skorokhod, V. (2016). CRYPTOCURRENCY IN THE CONTEXT OF DEVELOPMENT OF DIGITAL SINGLE MARKET IN EUROPEAN UNION. 3(1).

6 Gertchev, Nikolay. "The Moneyness of Bitcoin.", Available at: www.mises.org (2013).

7 Harwick, Cameron. "Crypto-Currency and the Problem of Intermediation." Available at : SSRN 2523771 (2014).

8 Yermack, David. "Is Bitcoin a Real Currency?". No. w19747. National Bureau of Economic Research, 2013.

9 Luther, W. (2017). Bitcoin and the Future of Digital Payments. [online] Papers.ssrn.com. Available at: https://papers.ssrn.com/sol3/papers.cfm?abstract_id=2631314

10 Boyd, J. (2017). "Japan Takes Lead in Legitimizing Digital Currencies". [online] IEEE Spectrum: Technology, Engineering, and Science News. Available at: https://spectrum.ieee.org/tech-talk/computing/it/japan-takes-lead-in-legitimizing-digital-currencies

11 Raymaekers, "Cryptocurrency Bitcoin: distribution, challenges and opportunities," Journal of Payments Strategy & Systems, vol. 9, no. 1, pp. 30-40, Spring 2015.

12 Gabi Stern. (2015, April) Bit post. [Online]. Available at:http://bit-post.com/players/bitcoin-regulation-around-the-world-the-current-state- 5627

13 Ryan Farell, "An Analysis of the Cryptocurrency Industry", pp. 15-28, (2015), Available at: http://repository.upenn.edu/cgi/viewcontent.cgi?article=1133&context=wharton_research_scholars

14 Woo, D. Gordon. I., Vadmin. I., "BITCOIN, A FIRST ASSESSMENT. FX and rates" (2013) Available at : https://www.smithandcrown.com/open-research/bank-of-america-bitcoin-a-first-assessment/

15 Robin Arnfield, Royal Canadian Mint Conducts Crypto-Currency Trial, MOBILE PAYMENTS TODAY (Feb. 7, 2014), Available at : http://www.mobilepaymentstoday.com/articles/royalcanadian-mint-conducts-crypto-currency-trial

16 Orcutt. M, "Leaderless Bitcoin Struggles to Make Its Most Crucial Decision" (May 19, 2015) Available at : https://www.technologyreview.com/s/537486/leaderless-bitcoin-struggles-to-make-its-most-crucial-decision/

17 King, R, "By reading this article you are mining bitcoins" (December 17, 2013) Available at: https://qz.com/154877/by-reading-this-page-you-are-mining-bitcoins/

18 Rizzo. P, "Crypto 2.0 in 2015: Turning Bitcoin Theory Into Big Business" (Jan 3, 2015) Available at: https://www.coindesk.com/crypto-2-0-2015-turning-bitcoin-theory-big-business/

19 Joshua A. Kroll, Ian C. Davey, and Edward W. Felten "The Economics of Bitcoin Mining, or Bitcoin in the Presence of Adversaries" (June 12, 2013) Available at:

http://www.econinfosec.org/archive/weis2013/papers/KrollDaveyFeltenWEIS2013.pdf

20 Zachary K. Goldman, Ellie Maruyama, Elizabeth Rosenberg, Edoardo Saravalle, and Julia Solomon-Strauss, "TERRORIST USE OF VIRTUAL CURRENCIES", (May 2017) Available at: http://www.lawandsecurity.org/wp-content/uploads/2017/05/CLSCNASReport-TerroristFinancing-Final.pdf

21 Peck, M. (2016). The Crazy Security Behind the Birth of Zcash, the Inside Story. [online] IEEE Spectrum: Technology, Engineering, and Science News. Available at: https://spectrum.ieee.org/tech-talk/computing/networks/the-crazy-security-behind-the-birth-of-zcash

22 Reid,.F . Harrigan,.M "An Analysis of Anonymity in the Bitcoin System" (2013) Available at : http://www.item.ntnu.no/_media/studies/courses/ttm4546/bitcoin_article.pdf

23 Karame. O. G., Androulaki. E., Capkun. S, "Double-Spending Fast Payments in Bitcoin" (October 16 - 18, 2012) Available at: https://dl.acm.org/citation.cfm?id=2382292

24 Clark, J. and Essex, A. (2012). Commitcoin: Carbon dating commitments with bitcoin. In Financial Cryptography and Data Security, volume 7397 of Lecture Notes in Computer Science, Springer

25 James, R. (2009, June 01). A brief history of cybercrime. Retrieved from http://content.time.com/time/nation/article/0,8599,1902073,00.html

26 Obama, B. Office of Press Secretary (2013). Executive order -- improving critical infrastructure cybersecurity (EO 13.636). Retrieved from The White House website: http://www.whitehouse.gov/the-pressoffice/2013/02/12/executive-order-improving-critical-infrastructure cybersecurity

27 Doward J, "City banks plan to hoard bitcoins to help them pay cyber ransoms" (22 Oct 2016) Available at: https://www.theguardian.com/technology/2016/oct/22/city-banks-plan-to-hoard-bitcoins-to-help-them-pay-cyber-ransoms

28 Gipp, Bela. Gernandt, Andre, Meuschke, Norman (2015). Decentralized Trusted Timestamping using the Crypto Currency Bitcoin Available at: https://arxiv.org/ftp/arxiv/papers/502.04015.pdf 1502/1

28 King. S. Ritchie., Williams. S., Yanofsky. D., "By reading this article, you're mining bitcoins" (December 17, 2013) Available at: https://qz.com/154877/by-reading-this-page-you-are-mining-bitcoins/