International Journal of Scientific Research in Science, Engineering and Technology
Print ISSN: 2395-1990 | Online ISSN : 2394-4099 (www.ijsrset.com)
doi : https://doi.org/10.32628/IJSRSET

Bitcoin and Cryptocurrency: Challenges, Opportunities and Future Works

Shubham Kisan Kadam, Afsha Akkalkot, Jareena Shaikh
Department of Computer Engineering, Zeal College of Engineering and Research, Pune, Maharashtra, India

Article Info
Volume 9, Issue 2
Page Number : 437-448

Publication Issue :
March-April-2022

Article History
Accepted : 15 March 2022
Published: 30 March 2022

ABSTRACT

Bitcoin and other prominent cryptocurrencies have gained much attention since the last several years. Globally known as digital coin and virtual currency, this cryptocurrency is gained and traded within the blockchain system. The blockchain technology adopted in using the cryptocurrency has raised the eyebrows within the banking sector, government, stakeholders and individual investors. The rise of the cryptocurrency within this decade since the inception of Bitcoin in 2009 has taken the market by storm. Cryptocurrency is anticipated as the future currency that might replace the current paper currency worldwide. Even though the interest has caught the attention of users, many are not aware of its opportunities, drawbacks and challenges for the future. Researches on cryptocurrencies are still lacking and still at its infancy stage. In providing substantial guide and view to the academic field and users, this paper will discuss the opportunities in the cryptocurrency such as the security of its technology, low transaction cost and high investment return. The originality of this paper is on the discussion within law and regulation, high energy consumption, possibility of crash and bubble, and attacks on network. The future undertakings of cryptocurrency and its application will be systematically reviewed in this paper.

Keywords: Cryptocurrency, Blockchain, Mining, Investment

I. INTRODUCTION

Since the inception of the fiat money, people have been using it for everyday transaction. Trading and transaction has been much easier. In the year 2009, after the global crash of 2008, the first form of cryptocurrency has emerged in the form of Bitcoin. It was first introduced by Nakamoto (2008), an anonymous group or individual that has introduced Bitcoin as the first digital currency for easier day-to-day transaction from individual to individual. Bitcoin is operated without the middle man such as banks and monetary institutions. It is a form of peer-to-peer transaction, without the need to reveal one's identity for a transaction to happen. Unlike the current practice, the bank functions as the middleman or the go-between, knows the identity of buyer and seller, thus engendering the issues of personal data protection. Bitcoin platform has made the trading and transaction of cryptocurrency much easier and more independent,

without compromising personal information and details. To some, opting for this method of transaction has entitled them to transact freely and anonymously.

Bitcoin is the first digital coin in the world to have used the blockchain platform. It is created within a transaction log with computers participated across a network (Bohme et al., 2015). This blockchain has one of the highest security systems by not allowing fraudsters to use the currency more than once. The blockchain protocol rely on proof of work where it ensures miners converge to this structure. The computational operation is known as hashing where the term hashing power refers to the computational power of mining the currencies (Kiayias & Panagiotakos, 2015).

The system in the cryptocurrency market is rather complex and quite difficult to understand, even for the players in the industry and researchers doing studies in this field (Fry & Cheach, 2016). There have been many researchers revealing the benefits of Bitcoin such as security (Bariviera et al., 2017), low transaction cost (Kim, 2017), high return (Ciaian et al., 2016; Kristoufek; 2013; Hong, 2017) and as for alternative instrument for a country's bailout mechanism (Bouri et al., 2017) and use for employees' wages (Angel & McCabe, 2015). Despite that, there are also researchers pointing on the risk and drawbacks of using this digital coin, in term of lack of regulation (Cheung et al., 2015; Böhme et al., 2015), high electricity bill due to energy consumption (Hayes, 2017; Vranken, 2017), lack of security (Bradbury, 2013; Conte De Leon et al., 2017) and other issues such as anonymity (Androulaki et al., 2013) and switching cost (Luther, 2015).

1.1 Background and History

Nakamoto introduced Bitcoin in 2009 and had initially brought up 50 Bitcoin in circulation. In this early phase, the hype was taken lightly only from the computer enthusiasts around the world (Wallace, 2011). In 2010, Mt Gox, a Japanese company had created a platform in using Bitcoin as trading mechanism with 20 coins changing hand at 4.951 cents. The total volume was approximately one U.S dollar. As the use of Bitcoin had increased, the price had escalated tremendously, and at the time this paper was written, the price had surged drastically to U.S dollar of 6,777 (Bitcoin Chart, 2018). According to Bohme et al (2015), the basis of the bitcoin value is based on scarcity. It serves as the foundation to put a value to any form of money. In the current practice of using the fiat currency, the monetary authority or the central bank hold and reserve the money. Central bank of a country has the power in adjusting the circulation of money and its absolute quantity. The bank is able to produce only limited amount of these paper money for regulating fiscal economic of a country, therefore creating scarcity. This scarcity will be recorded in the bank bookkeeping and will be preserved by the legal rules.

The big question that arise as Bitcoin was introduced, are these cryptocurrencies considered as real money? According to Ali et al. (2014), the history has outlined that money must have the following criteria: (1) A store of value. It is a purchasing power that users can manipulate to buy goods in the current time to the future. (2) A medium of exchange. The ability to make payments and (3) A unit of account. The value that can be measured of any goods for sale. Money theoretically must meet all these criteria but it is not always the case. Analyzing Bitcoin and other cryptocurrency in their current form, all the three criteria are debatable. One can postulate that it does have a store value due to the ability for purchasing power, but due to uncertainty, one cannot estimate whether Bitcoin can be used in the future as it is being used now. For medium of exchange, some can justify that cryptocurrency can be used for a medium of exchange, but to others the goods that can be exchanged are limited.

If all these three criteria are set to be the pre-requirement for any commodity to be given the stature of money, therefore it should be accepted within the context of its use and application. Radford (1945) reported that cigarettes met all these criteria during the hard time of World War 2 where prisoners in war camps used it for transaction. Further back in time,

cooking salt can be regarded as having value in the time of Roman empire where the troops wages were paid in salt. As for cryptocurrency, it can be regarded as money to people who are computer and internet enabled. The problem lies on the fact that only a small fraction of the people worldwide has the access to internet devices. Therefore, within this context, similar to the prisoner in the war camp and the Roman troops, cryptocurrency only is limited to those having access to the internet. Ali et al. (2014) reported that only about 20,000 Bitcoin holders in the United Kingdom with only 300 transactions each day. This number would be even smaller in emerging and developing countries due to the lack of internet access. Bohme et al. (2015) suggested that cryptocurrency, particularly Bitcoin is more of a platform for payment rather than currency due to its real time convertible to a conventional currency in fixed value. This cryptocurrency is different from other assets in term of its portfolio analysis, risk management and sentiment analysis (Dyhrberg, 2016). Compared to other assets such as gold, property, stocks and equity, cryptocurrency does possess similar portfolio in term of having certain value. Cryptocurrency however, resembles people's sentiment as when the value elevates with more and more people willing to accept them as payment. These differences create various opportunities to the market where investors and stakeholders alike can benefit from it. Therefore, to acknowledge cryptocurrency as the replacement for the fiat money in today's economics is still premature and requires further understanding in application, theoretically and practically.

1.2 Mining and the Blockchain System

How was cryptocurrency initially gained or received? As to fiat money, it is issued by the central bank, while cryptocurrency is created by mining via the blockchain using cryptography technology. This is the method of issuing new cryptocurrency. The blockchain system consisting of users, developers, miners, node maintainers and the interactions that ensure the functionality of the distributed ledgers (Dos Santos, 2017). Such mining process requires miners to have capital expenses in purchasing the software and hardware. The software includes GUIMiner, BFGminer and CGminer are the examples used in Bitcoin mining (Kethineni et al., 2017). While the hardware's are AntMiner, Avalon and ASICMiner. Mining of other currencies that uses many different algorithm requires the use of high-end and high-speed graphic cards. For a new miner, one needs to register a wallet and an encrypted banking online that can store and accept the cryptocurrency (Kethineni et al., 2017). When a miner is able to solve the puzzle in the blockchain system, the digital coins will be rewarded and transferred to the wallet that has been predetermined earlier.

According to many of the cryptocurrency protocols, the way mining works is by validating transaction by linking to the block that was accepted earlier (O'Dwyer & Malone, 2014). The blockchain technology will record every transaction in its unit (Eyal & Sirer, 2014). A unique ID is assigned on each block and the block preceding it. This is called the proof of work protocol. Proof of work is a protocol of verifying a transaction and informing others about it. Users or miners have to do work in validating or proofing that they are the real identities. These works revolve around algorithm and puzzle that can be solved by computers mathematical process (Tschorsch & Scheuermann, 2016). Proof of work adapted in cryptocurrency working principle is to replace the centralized payment system imposed by the banking system. The main basis of this system is to charge the user i.e. the service requester in solving a problem that is considered to be hard to solve compared to verifying it (Becker et al., 2013). By this, proof of work principle would be able to limit the access to any given service in mining and trading the cryptocurrency.

Miners would have to solve the puzzle embedded in the block, which contain the hash of the previous block, the current block transaction hash and address that will be rewarded after the puzzle is solved. This is

the basic of the mining process. This in turn created a block chain, a trace of the transaction that happened. This blockchain technology will prevent any fraudsters to double spend of cryptocurrency by tampering the transactions in the ledger (Vranken, 2017).

II. CRITICS OF CRYPTOCURRENCY

There have been considerable critics of cryptocurrency, one of them is whether it is a form of an asset currency. In its current form, having the ability to perform monetary transaction, according to Kim (2017), bitcoin and cryptocurrencies are much closer and meet the definition of currency. Even though cryptocurrencies do have complete criteria of the three main characteristics of currency which are store value, unit of account and method of transaction, it does have majority of the elements.

2.1. Opportunities and Advantages

Being a relatively new commodity, the opportunities of cryptocurrency looks promising. Despite having escalated in term of its price and value, the fruits and the future opportunities are still being sought after. The following discusses on the realistic opportunities of cryptocurrency for the users, investors and including the government.

2.1.1. Secure Technology

The blockchain is deemed to be one of the best platforms and most sophisticated technology since the discovery of the internet. It provides efficiency for online transaction, in term of its security and confidentiality. Ying et al. (2018) in their case study they concluded that, apart from enabling the use of cryptocurrency, the blockchain is able to protect confidential information and also eliminate the intermediation from any institutions. Even though there were reports stating that Bitcoin was found to reveal 40% of the user's identity (Androulaki et al., 2013). This report was claimed after the users had followed the recommendation set by Bitcoin. This issue of identity privacy is important based on the features of the cryptocurrency that protect the user's profile by decentralizing system. Two flaws in this study is that it does not use actual blockchain system but simulation, and the simulation was only done in one faculty only consisting of students. Other than this, no other studies up to author's reading that have revealed the flaws of using Bitcoin and cryptocurrency that exposed the risk of exposing user's personal information One of the risks in owning digital coins is double transaction, which means somebody is able to issue two transactions parallel by granting the same coin to two different recipients (Tschorsch & Scheuermann, 2016). In the case of centralized and online transaction, the bank operational system is able to detect such suspicious activity. The blockchain technology is very secured. Fraudsters will not be able to commit such crime because one cannot change nor validate several ledgers at the same time (Bariviera et al., 2017). According to a claim by Bentov et al. (2014), security of the cryptocurrency can be broken if fraudsters are able to control a huge amount stake in the proof of work hash power. Hash power is the computing power controlling capability. Khatwani (2018) stated that hash power is the power needed by the cryptocurrency network to be function continuously. The hash power is counted in an average of 10 minutes that power is consumed. By controlling majority of the stake in the proof of work, fraudsters can double-spend on the same block by secretly preparing the blockchain branch beforehand prior broadcasting it to the chain network. Theoretically, fraud can be done in a large scale provided that fraudsters are able to control at certain percentage of the hash power. From the Bitcoin's algorithm of binomial random walk, fraudster is able to double spend if they control 51% of the computing power (Shi, 2016). In the proof of work protocol, the verification of whether there is double transaction or not is based solely on the hash power, instead the possibility of multiple fake identities (Tschorsch & Scheuermann,

2016). This has ensured that the issue of fraudsters being able to control majority of the hash power is undermining by the verification of other method rather than relying solely on the hash power. The assumption is that it is much more difficult in controlling majority of the system hash power than controlling the identities of the majority.

Cryptocurrency algorithm is more secured and is better than using credit cards. Even though it is still understudied, cryptocurrency has much lower processing fees with the secure transaction it provides. Van Alstyne (2014) explained that using cryptocurrency is more secure when doing transaction. The mechanism of transferring cryptocurrency is by authentication by the buyers and sellers. The authentication between both parties will prevent fraudsters in forging any new transaction or delaying any refund transaction. Compared to credit card, these forge had happened and will continue to persist due to its mechanism (Van Alstyne, 2014). The technology behind credit card transaction is working within the cardholder, merchant, merchant bank, credit card network, issuing bank and service provider (Papadimitriou, 2009). For any single transaction, the process is more complicated than meets the eye. It has to go through to all these entities before a transaction can be finalized. Fraudsters and opportunity for committing fraud can exist in any of these stages. Even though certain measures have been taken in reducing credit card fraud (Van Vlasselaer et al., 2014), the system is more vulnerable when compared to blockchain. The system applied by the credit card technology is still not secure as the cryptography technology possess by the cryptocurrency.

Dos Santos (2017) stated that despite algorithmically complicated, the blockchain system is not complex. The complexity only exists in the node and mathematical puzzle that will be solved by the mining process. Other than that, the blockchain technology provides useful functions to all users. It is unlikely to precede to chaotic system based on the resilience and irreversibility. The records of digital documents online and identification is well preserved within the blockchain system for now and the near future (Dos Santos, 2017).

2.1.2. Cost of Transaction

Throughout history, people have been using some kind of monetary form for day-to-day transaction. As early as a trading system, the barter system had got the business going, where people exchanged or bartered their goods, with the agreement from both sides. As the time changes, the fiat money was designed for people to trade with ease, without having to bring big commodities to trade. As the world enters the 21st century, the cryptocurrency has taken the market by storm. There have been big multinational companies using Bitcoin as their form of currency, and even using it to pay the employees monthly wages (Angel & McCabe, 2015).

As the current cost of transaction, cryptocurrency and Bitcoin transaction charges are lower compared to other normal currencies. With the prominent features of cryptocurrency, decentralized and deregulated, accounted to its low cost of transaction (Kim, 2017). There have been considerable issues in the current payment system that is being practiced by credit and payroll cards. The interest being charged for users who default on their payments is way too high and that can jeopardize a user into financial despair (Angel & McCabe, 2015). This has not been the case for cryptocurrency, where trading occurs when end to end users agreed and only then will remittance of money be made.

In addition, cryptocurrency can be operated for 24 hours a day, 7 days a week throughout the year. The data pricing is available instantly whereby anyone in the world can trade without any cost as long as the internet is accessible (Pieter & Vivanco, 2017). As the world is bombarded with recent development of the internet of things (IoT) and reliance on big data, having the ability to trade without time limitation is an ease for users. This method of payment would facilitate the younger generation who are in the future are expected

to become business owners and working within their own time frame, without having to attach with conventional working hours. This way of trading is also suitable for the internet savvy without having to fork out additional cost that comes with using other payment system.

2.1.3. High Return

The distinctive features of cryptocurrency and its ability to suit to economic function making it a unique asset (Briere et al., 2015). History shows that Bitcoin is a very volatile currency but having substantial return for investors. Apart from that, Bitcoin risk is low due to its proportion in many and diversified portfolios. As known to investors, to make profit from investment is by purchasing any commodities at low price and sell at high. For those who had been holding Bitcoin in its early days of introduction, they may have raked in and profited from 1000-10000 percent of profit from what they had invested (Bohme et al., 2015).

Ciaian et al. (2016) studied on both the traditional currency determinants of supply and demand, and the modern indicator such as currency attractiveness. He also studied on the interaction between the determinants of price. It is posited that due to the demand of the market, the price of Bitcoin per se will be increased particularly when the supply of Bitcoin in circulation is larger than what it is now. After every four years when the amount of the Bitcoin will be halved, it indicates lesser new Bitcoin will be introduced, hence will be more stable. The scarcity of Bitcoin will only make the price higher, apart being the major currency used in a worldwide trading. At this stable period, Bitcoin will be demanded by investors and users alike. Kristoufek (2013) has shown that the price of Bitcoin has risen, parallel with the queries search on Wikipedia and Google Trends. It shows that the relationship of the search queries and Bitcoin price is co-related. This indicates that as the mass gets to know the existence of cryptocurrency, and how it can benefit them in such a way, the price will reasonably be higher. In the near future, when more people are computer and internet oriented, the price of cryptocurrency will be stabilized and thus people who had held on to their coins will reap the fruits of their investment.

The use of cryptocurrency is simply like the use of fiat money or by using credit cards in purchasing legitimate goods from retailers. Apart from that, Wingfield (2013) suggests that Bitcoin can be used for wider purposes. The popularity of cryptocurrency, Bitcoin in particular was further accelerated due to several particular events that implied on its usability such as in the banking crisis in Cyprus from 2012 to 2013 and the European sovereign debt crisis (ESDC) of 2010- 2013 (Bouri et al., 2017). Cyprus had taken the steps in using cryptocurrency into taking a bailout by making levy on bank deposits. This is due to the insecurity of using traditional deposits (Luther & Salter, 2017).

Ha and Moon (2018) adapted a genetic programming in evaluating the profit pattern in investing in cryptocurrency. The finding shows that there were frequent and profitable signals in the pattern from the analysis. It was further simulated in trading with the pattern and the signals shows it can be profitable for any given portfolio of the cryptocurrency. Hong (2017) found that Bitcoin return was significant using time series momentum. For a continuous 8 weeks, it was found that there was a strong return on Bitcoin. Based on the famous asset theories, the prediction was proven by the evidence of empirical return continuation and reversal with the predictability of the time series. As discussed, due to the volatility of the cryptocurrencies, Bitcoin's time length continuation and reversal were shorter as compared to another asset. Institutional investors can gain profit by investing in Bitcoin contemplating with their portfolio as such in equities.

2.2. Challenges

Despite the opportunities in cryptocurrency, there are still many challenges waiting to be faced by the cryptocurrency. Onlookers and new investors have probably taken precautious step whether to invest

heavily or not is because the risk and challenges pose by trading and investing in cryptocurrency.

2.2.1. Law

As the fiat money is concerned, it is safe for users to use since it is regulated by the central bank of a country. Every policy and the outcome of a country's monetary stand is within the full authority of the central bank. As for cryptocurrency, anyone can have multiple account, with no cost to create it. No proper centralized vetting procedures and also not compulsory to use their real name (Böhme et al., 2015). This process is rather vague where the notion of illegal activities behind all the cryptocurrency registration and trading might be a hoax in some way or another. Being anonymous on the web is the perfect ground for criminals and fraudsters in committing their action. Cybercriminals would use this trading platform to perform their illegitimate activities and to the extent of scamming and cheating. Kethineni et al. (2017) believe that cryptocurrency is more likely to be used by criminals in engaging with frauds such as money laundering and drug trafficking. Despite the blockchain technology is invented to facilitate users around the world with easiness, criminals will always find ways to make profit.

Previously, some regulatory authorities had declined in endorsing Bitcoin as a currency for example in China (Cheung et al., 2015). China had banned the application of Bitcoin or any other digital currencies in financial institutions and any forms of business. This action taken by the authority is understandable because cryptocurrency trading and business activities cannot be traced on its trading platform and the anonymity of the personnel involved. Even though some countries supported the use of digital currency, China might have banned it due to its potential in rising economy and being as one of world's economic superpowers.

2.2.2. Electricity Bills

Apart from the initial cost of investing in the hardware, other main expense a miner has to pay is the consumption of energy (Hayes, 2017). It has been found that mining the digital currency has taken up more electricity bills compared to the rewards granted by solving a block (O'Dwyer & Malone, 2014). The mining of cryptocurrency has taken a huge energy. The cost of mining differs from the hardware performance. It is reported that the generation of electricity from mining cryptocurrencies ranging from 10MW (equivalent to a small power plant) to 3-6 GW (the estimated energy consumes by small to medium size country such as Bangladesh and Denmark) (Vranken, 2017).

Vranken (2017) stressed on the sustainability aspect of cryptocurrencies. He explored that the proof of work in mining these digital currencies is consuming high energy and requires intensive computer capabilities. Nevertheless, these sophisticated computers which include CPUs, GPUs is necessary in mining within the blockchain to prevent double spending that revolve around the security aspect. It is expected that the mining activities will be slowed down within the next decade, and only those with a substantial up-to-date hardware will survive in the mining business and the ability to reduce cost of electricity consumption.

Becker et al. (2013) encapsulated the cost of mining cryptocurrency. Due to a vast majority of these currencies adapting proof of work, it requires consuming large amount of power due to the mathematical work by the hardware involved. This is especially harmful in large scale mining activities. This in turn, will make mining cryptocurrency as the villain contributing to emission of carbon dioxide and would destroy the earth through global warming. More studies on the effect of cryptocurrency on the environment should be studied. It is not worth sacrificing the earth for a short-term profit. If proven that the mining process would do more harm than good, the governments or even the United Nation

should intervene in ensuring the environment will not be jeopardized.

2.2.3. Crash and Bubble

According to Fama (1970) an efficient market is where past information is available that can fully reflect the prices of its history. Cryptocurrency is said to be a weak form of commodity because investors are not able to predict the future prospect because there is no available information from the past (Urquhart, 2016). This is true since the inception of cryptocurrency has only emerged in 2009, nearly a decade ago. An investment in this short length of time surely has no past records and investors cannot rely on the history to ensure the investment can be profitable. Fry and Cheah (2015) and Urquhart (2016) postulated that, if cryptocurrency have true form of account and storing value, it would not be so volatile. Such as facing risk of crashes and bubbles. It is anticipated that cryptocurrency would reach its bubble face in the near future. Despite this, no real bubble that would ultimately diminish Bitcoin or any other cryptocurrency had actually happened.

The volatility returns for monthly average for cryptocurrency as in Bitcoin is much higher gold. On the other hand, the monthly highest volatilities for gold and other currencies are higher than the lowest monthly volatilities for Bitcoin (Dwyer, 2015). This volatility in Bitcoin provides the indication that cryptocurrency would be a non-confidence commodity for long term investment. It provides the opportunity for bubble and crash to happen according to this trend of volatility according to Dwyer (2015). Cheung et al. (2015) had investigated that Bitcoin had suffered three big bubbles burst from 2011 to 2013 which had prolonged from 66 to 106 days. The biggest scandal in this bubble tragedy had cost the Mt Gox exchange (Yermack, 2013).

Prior research has shown that speculation can lead to assets being destabilized (Blau, 2018). The volatility possessed by Bitcoin price shows that it is driven by trading marred by speculation. The speculation can possibly eliminate its status as viable currency. The price of Bitcoin in its early trading price was only a few cents, had climbed to $1,132.26 towards the end of 2013. Few months later the price plunged nearly 60% (Blau, 2018). This was a clear sign of asset bubble. Due to only limited people using Bitcoin as the main cryptocurrency today, it is difficult to assess it as fair a value (Bariviera et al., 2017). There is no account required to trade Bitcoin without any interest rates. Worldwide, there are approximately less than 9000 retailers who accept Bitcoin as mode of payment (Yermack, 2013). This uncertain application of Bitcoin might lead to scam and other scheme that can lead to lost in monetary investment. Investors would like to make profits from cryptocurrency, seeking for their potentially saving them from any risks of speculation (Li et al., 2018). It is anticipated that bubbles would eventually occur when the authorities and economic policy intervene by not favoring the cryptocurrency, as evident from the minor Bitcoin bubble burst in several cases reported above.

2.2.4. Attack on network

Kshetri (2017) posited that technology of the blockchain having decentralized feature has low susceptibility and security. It opens the door to manipulation and forgery. The blockchain technology has many challenges regarding its identity and access management system related to Internet of Things (IoT). The mining activities using pool creation are vulnerable to two types of attack. It is either by malicious pool members or pool operators. A Sybil attack targeting on the network can be done by the malicious pool operators by combining the resources in their pool. While malicious pool members can potentially increase the computational power in a particular mining pools and later in the future, destabilize it. These users hop from one pool to another in order to sabotage the pools mining returns and

withholding the effectiveness of the mined block (Conte De Leon et al., 2017).

Another shortcoming of cryptocurrency is the attack on the code-based. The founder, Nakamoto's coding of the network is open for bug attack. This network is now maintained by a core group on the open source through the Github. An attack had already happened in June 2013, where the Bitcoin nodes were attacked by an unknown attacker on its path that relayed the information on the network that did not involve in mining activities (Bradbury, 2013). As the history showed, future attack on the blockchain network is imminent. Although being successful so far, fraudsters will eventually find ways to attack on the cryptography network of the blockchain, if this issue of vulnerability is not earnestly addressed.

III. DISCUSSION

The critics surrounding cryptocurrency have been raised since the first day of its inception. The illegal activity accusation of cryptocurrency was realized when the Silk Road scandal has stopped its operation by the FBI. Silk Road was a popular market where users trade using Bitcoin. Silk Road was accused as a platform for business involving drug and other illegal activities. But, according to Alstyne (2014), the shutdown of Silk Road was not the fault of Blockchain nor cryptocurrency. Instead, it was the criminals and fraudster who had exploited this technology for their own lust for profits, just like other platform that can benefit them. The second such case was the Mt Gox where it has lost money summed up to 350 million dollars (McMillan, 2014). One would have imagined, before a system is fully developed and becomes a trustworthy and robust technology, time factor is a huge consideration. Cryptocurrency requires ample time before it can be used and applied by the mass people throughout the world. Even Paypal, the electronic payment system that was introduced in the year 1999 had several times been the target for fraudsters. It had actually been attacked at least 5 times after being fully robust and had established as an efficient and trustworthy electronic payment system in the world (Jackson & Grey, 2014).

As the history of the Bitcoin is concerned, the bubbles are affected by the speculation and price drop was affected by the intervention by the government and central monetary agencies. Therefore, for the interest of the public in anticipating the benefits of the cryptocurrency, government should make a proper policies and regulation that can safeguard the public interest as well as main players in the economic market. A stabilized market would ensure that the fiscal policy of a country can be balanced without subduing the interaction from the central bank. All this depends on how the government acts on the current cryptocurrency market, either favoring or diminishing its existence once and for all.

IV. IMPROVEMENT AND FUTURE WORK ON CRYPTOCURRENCIES

It is undeniable that the emergence of cryptocurrency will play a significant role in the world's economic fabric. It is the fact that every economist, researchers, investors alike has to act and considerable measures to strengthen their knowledge on the blockchain technology in general (Fauzi et al., 2019; Fauzi et al., 2018a). As cryptocurrency has not yet reached maturity in term of time frame, further studies on its technology, potential and risk should be studied to ensure that the opportunities are not just a mere fluke. Also, the upcoming challenges do not mitigate stakeholders into the doldrums of financial failures.

Future research on reducing the 51% attack on the blockchain mining network should be further enhanced (Shi, 2016). The security protocol should be better, if not the same than the conventional centralized banking system in protecting the customer's monetary assets. Security aspect of users warrants the ground-breaking testimonial from the players in this new industry so that the confidence and trust of the blockchain technology would allow it to be

the norm for users in doing their daily transaction via the internet.

In reducing the cost of mining the currency, a proof of stake would provide lesser energy consumption in mining these digital coins (Vranken, 2017). In proof of stake methodology, a person needs to validate the coins that they own and the amount possessed. The person needs to create a transaction of their coins that they send to their account as a reward with the information of predefined percentage. The proof of stake resembles a raffle-like scheme that provide the same chance for all miners. Furthermore, a hybrid method that consists of both proof of work and proof of stake had been suggested, by rewarding fraction of the proof of work to all nodes that are active and at the same time the stake determines the ticket gained to all raffle. Bentove et al. (2014) suggested Proof of Activity (PoA) that combines the proof of work and proof of stake. In PoA, the activity term refers to active users that maintain the full online node and the one that should be rewarded. Contrarily, in proof of stake, offline users can still accumulate the coins over time and this can lead to double spending of the same block. PoA provides much better security in facing future threat on the cryptocurrency. It has a bigger storage space and the network communication permits low penalty. Plus, PoA also has low transaction fees, consuming less energy and the topology of the network can be improvised. Thus, PoA alternative serve as a better platform for cryptocurrency due to its ability to fend of double spending and most importantly the cost in acquiring the cryptocurrency compared to proof of work.

The market has been plunged with many new cryptocurrencies that had already made it into the market and there are many still waiting to be released. There have been many emerging currencies that are challenging and competing Bitcoin in term of its price and market capitalization. Even though at the time of writing, only Ethereum and Ripple had reached three figure prices. Bornholdt and Sneppen (2014) proposed a model called Moran process on new emerging cryptocurrency. The model does simulation on the market where the currencies are traded. The model is able to simulate the constant rate of new mined coins, trading activities of the agents and the communication among users trading on the markets (Cocco et al., 2017). All the currencies are interchangeable among themselves, with the acknowledgement of the account holders. It was also found that Bitcoin can be traded with other coins and the future might see that the highly warranted Bitcoin be replaced by other fascinating coins that may have better features. Therefore, studying on these features such as security, return on investment and low mining cost can determine which of the new and emerging digital coin can replace Bitcoin in the near futures.

Future work on using the proof of work has been discussed in Becker et al. (2013). One of it is to maximize the byproduct of the proof of work by reusing it. Reusing this byproduct in the sense that the resource in solving any mathematical puzzle by an already awarded user can reuse it by rewarding other user from the formulated solved problem. Another suggestion is to use the energy generated by the mining process from electrical energy to heat energy. This can be realized in cold climate countries, where the considerably high heat energy released from the computation of solving the mathematical puzzle can be used to heat residential houses and other household chores requiring heat energy.

Dyhrberg (2016) has found that Bitcoin is able to hedge against the financial stock market and the US dollars. It was posited that similar to gold that does not depend on the central authority, Bitcoin can diminish any risk in the market. In the short term, Bitcoin's active trading frequency among users enables it by showing the hedging capabilities. This indicates that Bitcoin has a clear and potential in the portfolio analysis of the world stock market, as well as its low risk management. Dyhrberg (2016) further suggests that Bitcoin and gold are efficient instrument in reducing the risk in investment. Although this statement is still rather premature in valuing Bitcoin as the same par as gold,

the potential is there and opens the floodgate to the possibility for future research.

It is realized that having considerable knowledge in the blockchain technology would be essential in controlling the negative impact of using cryptocurrency in day-to-day activities (Fauzi, 2019). Hence, expertise in this field should collaborate with policy makers and the government agencies in making regulations and policies pertaining to a country's stand in using cryptocurrency. Knowledge management among industry players and researchers should be enhanced to make the people understand the potential and risk in using cryptocurrency. Even experts from the institution of higher learning should be engaged with the public as they have the knowledge resource that facilitating the community in having better knowledge on certain issues (Fauzi et al., 2018b).

V. CONCLUSION

Cryptocurrencies are here to stay. The future of trading lies well with new emerging technologies that are able to benefit mankind. Needless to say that, users and industry player can evaluate whether cryptocurrency can benefit or harm them, in accordance with their objectives and perspectives in owning it. This paper has reviewed the opportunities in cryptocurrency in term of its security of its technology, low transaction cost and high investment return. For the challenges, the discussion revolved around law and regulation, high energy consumption, possibility of crash and bubble, and attacks on network. The improvement and future work on cryptocurrency include improving the security protocol, working on proof of activity, using the byproduct of proof of work and applying the knowledge management system. Looking at the positive outlook of the blockchain technology and the prospect of government in regulating cryptocurrency, more in-depth studies on several aspects of cryptocurrency should be done. Taking the opportunities from part of the pie in the cryptocurrency and blockchain technology can be beneficial for researchers. From then, application in using cryptocurrency in the best of its ability would be one of the most prominent discoveries in the 21st century.

VI. REFERENCES

[1]. Ali, R., Barrdear, J., Clews, R., & Southgate, J. (2014). The economics of digital currencies. Bank of England Quarterly Bulletin, 276-286. https://papers.ssrn.com/sol3/ papers. cfm?abstract_id=2499418

[2]. Androulaki, E., Karame, G. O., Roeschlin, M., Scherer, T., & Capkun, S. (2013, April). Evaluating user privacy in bitcoin. In: International Conference on Financial Cryptography and Data Security (pp. 34-51). Berlin/Heidelberg, Germany: Springer.

[3]. Angel, J. J., & McCabe, D. (2015). The ethics of payments: Paper, plastic, or Bitcoin? Journal of Business Ethics, 132(3), 603- 611. DOI 10.1007/s10551-014-2354-x

[4]. Bariviera, A. F., Basgall, M. J., Hasperué, W., & Naiouf, M. (2017). Some stylized facts of the Bitcoin market. Physica A: Statistical Mechanics and its Applications, 484, 82-90. https:// doi.org/10.1016/j.physa.2017.04.159

[5]. Becker, J., Breuker, D., Heide, T., Holler, J., Rauer, H. P., & Böhme, R. (2013). Can we afford integrity by proof-of-work? Scenarios inspired by the Bitcoin currency. In: The Economics of Information Security and Privacy (pp. 135-156). Berlin/ Heidelberg, Germany: Springer.

[6]. Bentov, I., Lee, C., Mizrahi, A., & Rosenfeld, M. (2014). Proof of Activity: Extending Bitcoin's Proof of Work via Proof of Stake. ACM SIGMETRICS Performance Evaluation Review, 42(3), 34-37.

[7]. Bitcoin Chart (2018). Bitcoin chart. Retrieved April 5, 2018 from: https://charts.bitcoin.com/

[8]. Blau, B. M. (2018). Price dynamics and speculative trading in Bitcoin. Research in

International Business and Finance, 43, 15-21. http://dx.doi.org/10.1016/j.ribaf.2017.07.183

[9]. Böhme, R., Christin, N., Edelman, B., & Moore, T. (2015). Bitcoin: Economics, technology, and governance. The Journal