An Analysis of Cryptocurrency, Bitcoin and the Future

Mr. Shubham Kadoo[1] and Ms. Khushboo Sodi[2]
Student, M.Sc. I.T., I. C. S. College, Khed, Ratnagiri, Maharashtra, India[1]
Asst. Prof., Department of I.T., I. C. S. College, Khed, Ratnagiri, Maharashtra, India[2]

Abstract: *A technology that was developed eight years ago is cryptocurrency, which is an encrypted, peer-to-peer network for facilitating digital barter. The first and most widely used cryptocurrency, Bitcoin, is paving the way as a disruptive technology for decades-old financial payment systems that have remained unchanged. Although cryptocurrencies are unlikely to replace conventional fiat currency, they have the potential to alter how Internet-connected global markets interact with one another, removing barriers to exchange rates and standard national currencies. The market in which a technology aims to improve is almost entirely responsible for its success. Technology advances at a rapid rate. By creating a fee-free trading system, cryptocurrencies may revolutionize digital trade markets. A SWOT analysis of Bitcoin is provided, which sheds light on some of the most recent happenings and trends that may have an impact on whether or not Bitcoin contributes to a paradigm shift in the economic system.*

Keywords: Cryptocurrency, Bitcoin, Encrypted, Currency, Bitpay, Exchange Rates

I. INTRODUCTION

The most widely used and well-known cryptocurrency in the world, Bitcoin, is getting more and more popular. Although it retains the same fundamental structure as when it was first created in 2008, subsequent shifts in the global market have resulted in a new demand for cryptocurrencies that is significantly greater than its initial showing. Users are able to digitally exchange value without the oversight of a third party by using cryptocurrencies. Cryptocurrency is based on the idea that solving encryption algorithms yields a finite number of unique hashes. Users are able to exchange hashes as if they were exchanging physical currency when paired with a computer network that verifies transactions. A limited number of bitcoins will ever be created, ensuring its rarity and preventing an oversupply. Despite its necessity as a life-sustaining substance, water is generally regarded as free or inexpensive due to its abundance. Diamonds would be more valuable than water if it were scarce. According to Kelly (2014), the value of bitcoin stems from its users' trust that if they accept it as payment, they will be able to use it elsewhere to purchase something they desire or require. The valued object can be anything so long as the users continue to have faith in it. Similar to how Native Americans used wampum, a seashell, as their currency, Bitcoin's value exists in its ecosystem (Kelly, 2014).In the same way that gold does not have an intrinsic value, Bitcoin cannot be used to make valuable physical objects like jewelry. Nevertheless, trust and acceptance ensure that value persists.

Legal and financial structures of today were not designed with this kind of technology in mind. The foundation of financial institutions is based on much older forms of currency. It is comparable to the computing industry in some ways. Even though there are only two dimensions of input, the fundamentals of computing still rely on transmitting and processing 1s and 0s.However, this technologically dated system is utilized by all of our current technology as a result of adoption, cultivation, and a lack of demand for newer systems. To deal with this kind of competition, established trade systems would need to be completely reformed if cryptocurrencies became the global standard for transactions. As a result, cryptocurrencies have the potential to be the technology that causes the greatest disruption to global financial and economic systems.

According to Team (2016), BitPay, the world's largest bitcoin processor, has recently seen a 115 percent increase in transaction rates over the past year.

An increase in transactions is a sign that user acceptance is growing. A "fire triangle" of conditions exists for the widespread use of Bitcoin. where heat, oxygen, and fuel are required for fire to exist; To get going, Bitcoin needs innovation, vendor acceptance, and user acceptance. It's possible that bitcoin won't truly become a mainstream currency if it doesn't have all three aspects. The other two aspects of the "fire triangle" are being driven by Bitcoin's current rise in user acceptance and usage. Because it has the potential to be a truly transformative technology that alters the way

money is exchanged worldwide, the adoption of cryptocurrencies will be an important topic to keep an eye on in the future. The shifts in global markets have played a significant role in the rise in adoption of Bitcoin. The global market that is currently fueled by the Internet is extremely entangled. It's easy for other regional markets to follow suit if one starts to fall. Like the Euro, Bitcoin can move freely across many national borders, fostering global trade, mutual prosperity, and even peace.

II. STRENGTHS

By design, bitcoin has the strength to be a viable currency, which has elevated its status over time, particularly the fixed bitcoin limit. Every four years, bitcoin will be mined with decreasing returns until the maximum number of bitcoins is reached:21 million in all (King, 2013).Because of its value, this aspect of Bitcoin is significant. It will never rise in value as a result of an excessive amount of bitcoins because there are only so many of them. Also, cryptocurrencies like bitcoin are generally thought to protect against inflation caused by changes or restrictions imposed by national governments (Magro, 2016).Because it generally does not lose value in response to inflation, this creates a "safe haven" for investors to invest their wealth in. As a haven from inflated national currencies, Bitcoin is quickly demonstrating its strength. However, just like it is the case with the majority of commodities, a wide range of other external factors can influence the price. According to Desjardins (2016), the price volatility and demand for a safe haven helped Bitcoin become the best-performing currency in 2015 using the US Dollar Index. This indicates that at the end of last year, Bitcoin was the world's most valuable currency. In a global economy dominated by giants like China and the United States, this is no small feat.

Bitcoin transactions in South America increased by 5150 percent between 2014 and 2015 (Bitcoin:2015, A New Global Economy Due to its extremely high inflation rate and large unbanked population, Argentina is a hotbed for increased cryptocurrency use (Magro, 2016).To maintain its value, Argentinians used to exchange their currency for US dollars. However, in recent times, Argentina has restricted the amount of US dollars that its citizens can exchange. According to Magro (2016), as a result, there has been an increase in bitcoin adoption as well as a black market for purchasing USD at a higher price. Argentinians have made it very clear that they want to keep their currency's value, and cryptocurrencies are a popular legal way to meet that demand.

Vendors will be more likely to accept Bitcoin if there is an increase in the flow. This would theoretically be a cyclical effect. Users will use cryptocurrency technology to benefit from its advantages as more vendors adopt it.

III. WEAKNESSES

As part of its design, Bitcoin has a number of internal flaws that cannot be easily changed. Every user has access to every transaction thanks to the public ledger, also known as the block chain. Although the owners of bitcoin wallets cannot be directly identified, there is a degree of anonymity, which can be slightly nerve-wracking for some potential adopters. Because the public block chain is shared by all users, it is easy to access and vulnerable to attacks (King, 2013).Multiple DDoS attacks, or "stress tests," have been conducted on the Bitcoin network thus far (Hileman, 2016).Exchanges and miners initiated these "tests" in an effort to demonstrate a point about the design of Bitcoin: that the network cannot accommodate high transaction rates under load. An unfortunate feature of the code's design is that participants in Bitcoin's operation can bring the network down to demonstrate their point. These two aspects of Bitcoin's design cannot be altered because they are necessary for its operation. Despite these characteristics, users who are hesitant to adopt must do so.

Recent events have given Bitcoin a questionable reputation. Stories like "Silk Road" have the potential to paint a negative picture of digital currencies in general, not just Bitcoin. Silk Road was an underground online marketplace that enabled thousands of drug dealers and nearly a million customers to engage in illegal drug transactions. Due to the lack of government tracking and semi-anonymity of Bitcoin, they used it as their primary method of transaction. According to Bearman (2015), it operated from 2011 to 2013 and generated nearly one billion dollars in sales. Because people want criminals to face justice, bitcoin's semi-anonymity appears to be harmful to law-abiding citizens. The general user base will believe that cryptocurrencies are only used by criminals unless positive marketing promotes the value of semi-anonymity for normal users.

Additionally, cryptocurrencies have acquired a reputation for questionable security. According to McMillan (2014), Mt Gox, which stands for Magic the Gathering Online Exchange, was the primary bitcoin exchange in the world until it went out of business in 2011 following a hacker robbery that took away approximately 460 million USD. Mark Karpeles, the CEO and main programmer, did not use version control for new code. Additionally, he would permit security and bug fixes to languish for weeks (McMillan, 2014).The exchange's security flaws and oversights made it possible for hackers to steal bitcoin. As a result of this breach, users sold their bitcoins out of fear that it would be stolen. According to Price (2016), another digital currency called Etherium recently experienced a similar theft that cost 50 million USD. Large holders of cryptocurrencies who fail to keep their security measures up to date are typically the targets of these hacks. They do the most damage to the image of cryptocurrencies and are the primary factor in the decline in their value. These incidents will continue to impede adoption until organizations that exchange cryptocurrency in the future comprehend how security flaws can result in attacks like these.

The bitcoin network is beginning to stabilize, but investors are beginning to realize that immediate returns on investments are not guaranteed. Since June 2016, the source code has made it harder to figure out the algorithm, which has made mining bitcoins more expensive. A "halving event" occurs when the number of bitcoins returned to miners is reduced by half. Because it would be more expensive to run the older computers than it would cost to mine bitcoin, this could effectively eliminate 25% of the bitcoin network (Kar, 2016).The mining community's shift could compromise the network's security and make it more susceptible to attack. Due to the limited returns on mining and the higher overhead that must be paid, it also reduces the likelihood that new miners will join the network. Until all of the bitcoin has been mined, the largest miners will remain as the halving events continue.

The fact that cryptocurrencies can be traded like commodities can also be a weakness. Values in commodity-based markets fluctuate significantly in response to a variety of market factors. Investor confidence in the commodities is ultimately reduced as a result of this fluctuating value. An unanticipated occurrence could result in a significant loss for an investor, lowering investor confidence. Additionally, the price of bitcoin has not been accurately determined, resulting in an uncertain trading environment. Investors with a "buy low, sell high" mentality also frequently trade commodities, which has far-reaching consequences for those who use bitcoin as a currency and causes value fluctuations. According to PwC (2015), price volatility creates risk, which discourages both merchants and consumers from holding cryptocurrency for an extended period of time. Consumer trust is eroded as a result of excessive risk, which limits legitimacy validation. Despite having the highest capacity of any cryptocurrency, Bitcoin's price is also at risk due to its shallow market.

According to Kasiyanto (2016), a person who wants to buy a lot of bitcoin will not be able to do so without affecting the current price. For other cryptocurrencies, which have a much smaller capacity, this is exponentially greater. In the current state of their market and currency, cryptocurrencies do not appear to be mature. Theoretically, this issue would be resolved by expanding adoption and capacity.

IV. OPPORTUNITIES

Because it is a forerunner in a technology that has the potential to change established financial systems, cryptocurrencies are in a unique position. Because it is a peer-to-peer system, it is able to fill in the gaps in existing financial technologies and assist in resolving typical banking issues. Another peer-to-peer system, Napster, eliminated the middleman and revolutionized the music industry (Kelly, 2014).Transformational technologies begin by addressing a specific industry issue. For instance, cryptocurrencies have the potential to assist in resolving issues pertaining to unbanked customers. In developing nations, a significant number of people do not have access to a bank account.60% of the 600 million people living in Latin America do not have access to a bank account (Magro, 2016).The technology behind Bitcoin enables individuals to exchange currencies without the need for a trusted third party, such as a bank, to supervise the transaction .According to Magro (2016), all that is required to use Bitcoin is a mobile phone, which 70 percent of Latin Americans do possess. By scanning QR codes that are displayed on their phones and printed out by the application, two users can trade bitcoin with one another due to bitcoin's ad-hoc networking capability. This is a truly original solution to a problem that some people have had for a long time. The demand for better cryptocurrency networks and applications will rise to the forefront as the user base expands invariably. As this technology could affect any industry that relies on a reputable third-party clearing system, there is a huge market for potential developers of

these applications (PwC, 2015).Any developers who improve bitcoin's application and graphical user interface to make it more user-friendly will succeed greatly. The ability of Bitcoin to solve long-standing issues and the community of developers and users that supports and grows it are the driving forces behind the technology's transformation into a transformative one.

When international transactions need to be completed quickly in response to an emergency, businesses are beginning to realize the value of using cryptocurrencies. Due to the peer-to-peer system's speed and ease of transaction, only cryptocurrencies can address this issue. Money can be wired internationally, but it typically does not arrive in its entirety and takes days to arrive (Team, 2016).As the transaction crosses borders, it may be hit with any number of unknown fees, making it difficult to send the correct amount to another business. An online business facing a denial-of-service attack and seeking immediate protection from a network security company is a good illustration of this kind of emergency need (Team, 2016).In this scenario, transaction speed is critical because profits are being lost for every minute that the company's website is down. Due to its adaptability when it comes to swift peer-to-peer transactions, especially in international business-to-business contexts, cryptocurrencies have a significant advantage over conventional currencies.

V. THREATS

To gain widespread user acceptance, Bitcoin must overcome numerous obstacles. Users and investors alike are doubtful as a result of the cryptocurrencies' erratic value fluctuations. Ultimately, widespread acceptance is a limitation of cryptocurrency. [PWC]. The trust that a consumer's value will be retained on a daily basis is diminished by value fluctuations, which reduces faith in the currency's overall worth. According to PwC's 2015 survey, 83% of respondents had little or no knowledge of bitcoin. Because cryptocurrencies do not have centralized ownership, any attempt to address this marketing issue through advertising could theoretically benefit the investing company's rivals. A marketing strategy would not work well in this circumstance. Additionally, cryptocurrency-related theft and fraud have occurred, typically as a result of exchange companies' faulty system setups. These pranks frequently make the news and can quickly persuade the uninitiated that these sites are risky places to invest. Additionally, there is a significant void in the laws governing cryptocurrency use. User acceptance of cryptocurrencies will be limited as long as they remain in an area that is not typically covered by law. Users must have faith that any cryptocurrency transactions are legal and binding. Governments and markets have been slow to adopt the new technology. In the end, consumer trust in cryptocurrency and bitcoin is hampered by each of these factors.

Additionally, issues with investors result from this lack of trust. According to Hilleman (2016), the number of failed startups has increased to 24, with the majority citing "security" as the primary reason for closure. Before making an investment in bitcoin, this metric could be thought of as a watermark for future investors to consider. The Mt. Gox and DAO hacks demonstrate how a careless organization can not only significantly decrease the value of digital currency but also lose millions of dollars worth of it. Startups are now aware that launching haphazardly and without a plan is, at best, ill-advised, and that new market entry will be limited. Bitcoin could suffer as a result of this, as better software is essential for increasing user acceptance and security. Security implementation and fixes typically take a long time to adapt to new technologies, despite how obvious the issue may appear.(Price, 2016) Even the DAO hack exploit was documented as a potential issue weeks prior to the attack. The decentralized nature of the code prevents a coordinated effort to fully secure each server that runs the code, which is one of the security issues. Before the peer-to-peer network is truly secure, it may be necessary to establish a unified front in the cryptocurrency industry. For cryptocurrencies to develop security standards that go beyond the requirements for the bitcoin application, it may be necessary to appoint a standards committee that is similar to ANSI, the American National Standards Institute. Independent miners may leave the market as a result of this kind of regulation, which could only be implemented at the expense of the freedom of peer-to-peer networks.

Cryptocurrency's rivals are also attempting to provide an alternative to digital currency. With their product, ApplePay, Apple is one of the main rivals. They are using their infrastructure and hardware to make it possible for users to use their phones to charge their debit or credit cards that are linked to their iTunes account. As long as they can keep their fees, traditional credit card companies like Visa and MasterCard are happy to join ApplePay's infrastructure (Gerber, 2015). Bitcoin will always struggle to compete with these well-known brands. As the eBay exchange system, PayPal

has had a lot of success, and it could be expanded to mobile payment. With full marketing budgets and a foothold in the mobile application market, Apple, Google, and Amazon have a significant advantage over Bitcoin's relatively inexperienced players. Bitcoin would have a difficult time uniting as a community to outperform rivals because mobile consumers want to be able to directly purchase goods and services with their phones.

VI. CONCLUSION

It appears that the early adoption phase of new technologies has passed for cryptocurrency. This happened to cars and trucks as well. Bitcoin has begun to establish a niche market, which may aid in the mainstreaming of cryptocurrencies; or be the primary factor in its failure. It is difficult to predict whether or not cryptocurrencies will ever gain true mainstream acceptance on global markets because they are still in their infancy. By coming up with new ideas and finding solutions to old problems, the Bitcoin community is attempting to break into the mainstream. Other forms of cryptocurrency have already appeared and attracted their own fan bases; each is a little different from Bitcoin but arguably just as reliable. According to Hofman (2014), some nations, such as Iceland, have even begun to launch their very own national cryptocurrencies. Bitcoin will play a crucial role in paving the way for cryptocurrency to flourish in the future. It is possible that cryptocurrency will be a major currency solution in the future. Bitcoin transactions are exploding in Europe and Latin America, indicating their true validity. There are numerous additional cryptocurrencies and Bitcoin-related topics to investigate. The economic effects of Bitcoin's influence on the performance of long-standing fiat currencies should be the subject of extensive research, with comparisons to countries that are just beginning to adopt state-sponsored cryptocurrencies. Although a much more in-depth market and economic analysis is required to determine this, the capacity of cryptocurrencies to carry out microtransactions may make it possible for them to close an economic gap that traditional state-sponsored currencies would not be able to fill. According to Hilleman (2016), the block chain technology that is the foundation of Bitcoin also has the potential to be put to use in other ways, such as smart contracts. These contracts are payments that are programmed to occur when a particular condition is met. Since a company's entire accounting department typically handles predetermined payment contracts, this is an extremely intriguing area for further change. Lastly, the creation of a digital property through the use of cryptography led to cryptocurrency. The transition of the music industry to a cloud-based infrastructure helped to popularize the frontier of digital property. This frontier, primarily populated by a variety of media, is still relatively new and unexplored. As cryptocurrency and music gain popularity, other forms of digital property may follow. Eight years ago, no one had ever heard of digital currency, and the person who invented Bitcoin was the only person who ever did. The underlying science of bitcoin and all cryptocurrencies, cryptology, may be the mechanism that opens the door to exciting new digital inventions.

REFERENCES

[1]. Bearman,J.(2015,May).TheUntoldStoryofSilkRoad,Pt.1.RetrievedfromWired.comWebsite:https://www.wired.com/2015/04/silk-road-1/

[2]. Bitcoin:ANewGlobalEconomy.(2015,August4).RetrievedJuly2016,fromBitPay,Inc.Website:https://blog.bitpay.com/bitcoin-a-new-global-economy/

[3]. Bovaird, C. (2016, June 24). Bitcoin Rollercoaster Rides Brexit As Ether Price Holds Amid DAO Debacle.RetrievedJune2016,fromCoinDeskWebsite:http://www.coindesk.com/bitcoin-brexit-ether-price-rollercoaster/

[4]. Desjardins, J. (2016, January 5). It's Official: Bitcoin was the Top Performing Currency of 2015. Retrieved fromTheMoneyProjectWebsite:http://money.visualcapitalist.com/its-official-bitcoin-was-the-top-performing-currency-of-2015/

[5]. Gerber, R. (2015, January 29). Why Apple Pay And Dollars Are Killing Bitcoin. Retrieved from Forbes InvestingWebsite:http://www.forbes.com/sites/greatspeculations/2015/01/29/why-apple-pay-and-dollars-are-killing-bitcoin/#23ac58a0b4b6

[6]. Hileman, G. (2016, January 28). State of Bitcoin and Blockchain 2016: Blockchain Hits Critical Mass. Retrieved from Coin desk Website: http://www.coindesk.com/state-of-bitcoin-blockchain-2016/

[7]. Hofman, A.(2014,March6). The Dawn of the National Currency–An Exploration of Country-Based Cryptocurrencies. Retrieved from Bitcoin Magazine Website: https://bitcoinmagazine.com/articles/dawn-national-currency-exploration-country-based-cryptocurrencies-1394146138

[8]. Kar,I.(2016,June30).Everythingyouneedtoknowaboutthebitcoin„halving"event.RetrievedfromQuartzwebsite:http://qz.com/681996/everything-you-need-to-know-about-the-bitcoin-halving-event/

[9]. Kasiyanto,S.(2016).Bitcoin'spotentialforgoingmainstream.JournalOfPaymentsStrategy&Systems,10(1),28-39.

[10]. Kelly,B.(2014).The Bitcoin Big Bang: How Alternative Currencies Are About to Change the World.

[11]. King, R. S. (2013, December 17). By reading this article, you"re mining bitcoins. Retrieved from Quartz. Com Website: http://qz.com/154877/by-reading-this-page-you-are-mining-bitcoins/

[12]. Magro, P. (2016, July 16). What Greece can learn from bitcoin adoption in Latin America. Retrieved July 2016,fromInternationalBusinessTimesWebsite:http://www.ibtimes.co.uk/what-greece-can-learn-bitcoin-adoption-latin-america-1511183