Advances in Economics and Business Management (AEBM)
p-ISSN: 2394-1545; e-ISSN: 2394-1553; Volume 3, Issue 5; April-June, 2016, pp. 505-511

http://www.krishisanskriti.org/Publication.html

The New Age of Decentralized Digital Currency System: The Bitcoins

Farhat Fatima

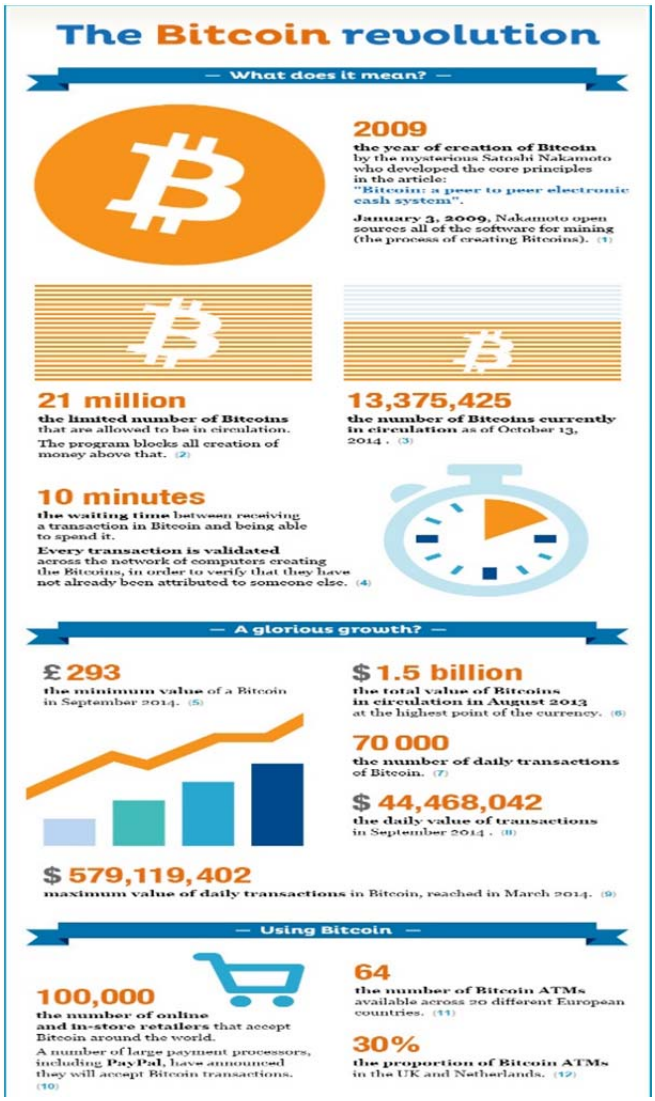
Periyar Management and Computer College, Jasola, New Delhi
E-mail: farhat.fatima17@gmail.com

Abstract—*In January of 2009 an anonymous programmer Satoshi Nakomoto claimed to have invented the infamous computer code which works on the basis of cryptography called bitcoins. However, Dr. Craig Wright from Australia on the month of May 2016 has claimed to be its real Inventor which nowadays is the most circulating conversation in Tech blogs. Bitcoins have always been an interest of discussion to a very small segment of IT, perhaps it significantly gained attention when it was used by a few big companies which have accepted bitcoins as the substitute of fiat currency. Bitcoin is not only a means of payment, but also the ideology of tools, support and development of social entrepreneurship. Presently about 13.7 million Bitcoins are in the flow. Yet, the total number of Bitcoins that can be generated is arbitrarily capped at 21 million coins, which is projected to be reached in 2140. However, because a Bitcoin is divisible to eight decimal places, the maximum amount of spendable units is more than 2 quadrillion (i.e., 2,000 trillion). The distinguished unique and decentralized management of the public ledger of Bitcoin resolves the double spending problem and the attendant need for a trusted third party to verify the integrity of electronic transactions between a buyer and a seller. The source code of Bitcoins was made open source at its inception to show its integrity and to allow others to experiment in the domain of decentralized payment systems.*
The following research has three major sections which briefly discusses bitcoins as the new age currency. It highlights the procedure of transactions from peer to peer to the digital decentralized public ledger and also its advantages and disadvantages. It is not the only digital currency but perhaps the most famous and the most controversial currency right now.

Keywords*: Bitcoins, Decentralized transaction system, Public and Private Key, Digital currency.*

1. INTRODUCTION

The use of bitcoins is increasing rapidly, it is also used in e-commerce to purchase both legal and illegal goods. They are transferred and traded and companies like CoinMonk, UnoCoin provide opportunity to other companies to invest in bitcoins and bitcoin mining related initiatives. Bitcoin is defined by wikipedia as a cryptocurrency where the creation and transfer of bitcoins is based on an open-source cryptographic protocol that is independent of any central authority. Bitcoins can be transferred through a computer or smartphone without an intermediate financial institution. The concept was introduced in a 2009 paper by pseudonymous developer Satoshi Nakamoto, who called it a peer-to-peer, electronic cash system (CoinMonk, 2013).



Source: Capgamini, 2015
Fig. 1: The Bitcoin Revolution

As Bitcoin approaches its seventh birthday, we see things changing. It is turning into that curious, wide-eyed technology with ideas as widespread as any normal 7-year-old would imgine. Cross-border payments, machine-to-machine transactions, smart contracts, microtransactions, and stock settlements all have been discussed and developed. Nothing is off limits; no question goes unasked (BitcoinMagazine, 2015). There is no third party middleman in a Bitcoin transaction. Buyer and the Seller can network directly, however their identities are encoded and kept personal which is unknown to each other. But the record of the transaction of each Bitcoin and the user's identity is been maintained and recorded on the public ledger.

In past few years the growing e-commerce has substantially increased the use of online payment system which further gave birth to Bitcoin. The Bitcoin system is private, but with no traditional financial institutions involved in transactions. The below diagram will explain its revolutionary growth from 2009 till year 2014 (See Fig 1)

The complete decentralized system of Bitcoin in which the transactions are done by the system differentiates it from fiat and digital currency usually controlled by some person and entity. Bitcoin offers users the advantages of lower transaction costs, increased privacy, and long-term protection of loss of purchasing power from inflation. Though, it also has a number of disadvantages that could hinder wider use. These include sizable volatility of the price of Bitcoins, uncertain security from theft and fraud, and a long-term deflationary bias that encourages the hoarding of Bitcoins (Murphy et al, 2015).

2. REVIEW OF LITERATURE

Cryptographic currencies date back to Chaum's proposal for "untraceable payments" in 1983 (D. Chaum, 1982), a system involving bank-issued cash in the form of blindly signed coins. Unblinded coins are transferred between users and merchants, and redeemable after the bank verifies they have not been previously redeemed. Blind signatures prevent the bank from linking users to coins, providing unlinkability akin to cash. Throughout the 1990s, many variations and extensions of this scheme were proposed. Significant contributions include removing the need for the bank to be online at purchase time (D. Chaum, 1990), allowing coins to be divided into smaller units and improving efficiency (J. Camenisch, S. Hohenberger, and A. Lysyanskaya, 2005). Several startup companies including DigiCash (D. Schwartz, N. Youngs, and A. Britto, 1998) and Peppercoin (D. Schwartz, N. Youngs, and A. Britto, 2014) attempted to bring electronic cash protocols into practice but ultimately failed in the market. No schemes from this "first wave" of cryptocurrency research achieved significant deployment. A key building block of Bitcoin, moderately hard "proof of work" puzzles, was proposed in the early 1990s for combating email spam (J. C. Dwork and M. Naor, 1992) proposed in the early 1990s, enable parties to formally specify a cryptographically enforceable agreement, portending Bitcoin's scripting capabilities.

In 2008, Bitcoin was announced and a white paper penned under the pseudonym Satoshi Nakamoto was posted to the Cypherpunks mailing list (S. Nakamoto, 2008), followed quickly by the source code of the original reference client. Bitcoin's genesis block was mined on or around January 3, 2009. The First use of Bitcoin as a currency is thought to be a transactionin May 2010, where one user ordered pizza delivery for another in exchange for 10,000 bitcoins (Bonneau, Millerx, Clark, Narayanan, Kroll, Felten, 2014). From then, a large Fig. of merchants and services have adopted Bitcoin and the price has generally escalated, reaching a peak of approximately US$1200 per bitcoin in late 2013 (Bonneau, Millerx, Clark, Narayanan, Kroll, Felten, 2014). Like the U.S. dollar, the Bitcoin has no intrinsic value in that it is not redeemable for some amount of another commodity, such as an ounce of gold. Unlike a dollar, a Bitcoin has no physical form, is not legal tender, and is not backed by any government or any other legal entity, and its supply is not determined by a central bank. The Bitcoin system is private, but with no traditional financial institutions involved in transactions (E. Murphy, M. Murphy, Seitzinger, 2015). This is why the rate of crime is also associated with its past. In 2014, a computer virus called CryptoLocker extorted millions of dollars from victims by encrypting their files and demanding a Bitcoin ransom to release the decryption key (Garber, 2014). Many users' Bitcoins have been lost due to theft (Dree, 2014) and collapsed exchanges (Moore and Christin, 2013). Bitcoin is not just in the fringes anymore; it is everywhere. Whether its miners or payment processors, wallets or developer tools, the reality is simple: Bitcoin is growing up. And its ambitions are as vast as the many great technologies that came before it (BitcoinMagzine.com, 2016).

3. OBJECTIVES OF THE STUDY

To understand the Bitcoin Mining

To examine advantages and disadvantages of Bitcoin

Bitcoin: From An Indian Perspective

Controversies and Threat on the go

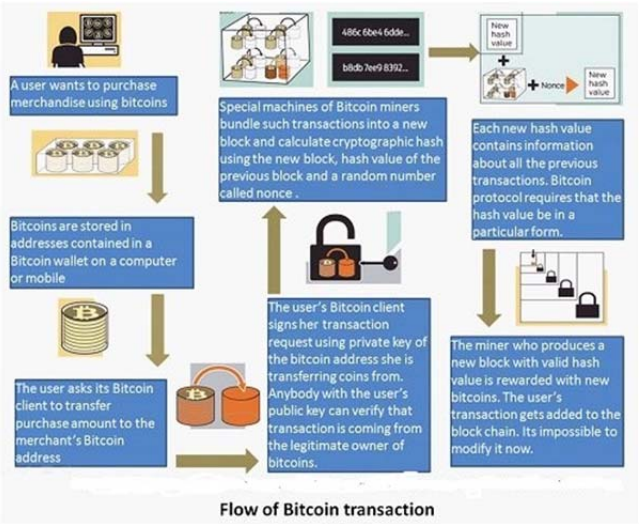
4. RESEARCH METHODOLOGY

This research paper is descriptive in nature and is based on the secondary data attained from the various secondary resources such as old research papers various e-journals, books, websites, whitepapers, newspapers and some of the governmental data etc.

4.1 The Bitcoin Mining

Bitcoin, like cryptocurrencies usually, is a complex system. Its application involves an amalgamation of cryptography, distributed algorithms and incentive driven behavior.

Furthermore, these are recent phenomena and there is thin academic literature, an ascent policy debate, and limited understanding by the public about cryptocurrencies overall. New bitcoins are created by carrying out mathematical operations which become progressively harder as the bitcoin space is explored—like calculating ever-larger prime numbers, they get further apart. (See fig 1). 'Mining' is discovering new Bitcoin. In reality, it's simply the verification of Bitcoin transactions. In order to make sure a Bitcoin is genuine, miners verify the transaction. There are many transactions that individuals are trying to verify and not just one. These transactions are gathered into boxes with a virtual padlock on them which make up the 'block chains'. 'Miners' run software to find the key to open that padlock. Once the computer finds it, the box pops open and the transactions are verified. Hence, it can be said that while Bitcoin are "mined" by individuals, they are "issued" by the software. A 'centralized' currency system is one where all of the currency is monitored by a central agency. Certain centralized forms of virtual currencies also exist in centralized forms, such as Facebook credits. These are also subject to similar regulation, and are monitored by banks and governments. The authenticity of each transaction is protected by digital signatures corresponding to the sending addresses, allowing all users to have full control over sending bitcoins from their own Bitcoin addresses. In addition, anyone can process transactions using the computing power of specialized hardware and earn a reward in bitcoins for this service. This is often called "mining". An address is like a bank account into which a user can receive, store, and send bitcoins. Instead of being physically secured in a vault, bitcoins are secured with public-key cryptography. Each address consists of a public key, which is published, and a private key, which the owner must keep secret (See Fig 2).

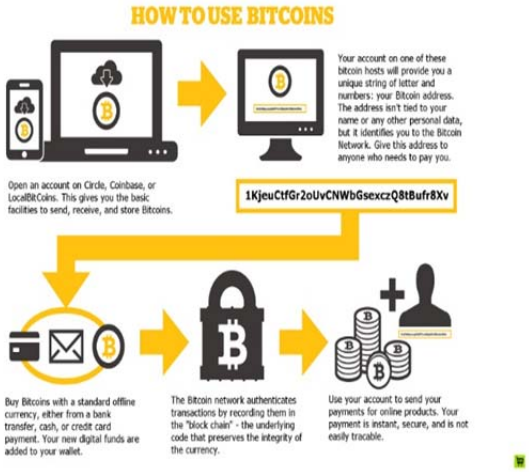


Source: Specptrum.Ieee.org, 2014p

Fig 2 The Bitcoin Mining and Transaction

Anyone can send bitcoins to any public key, but only the person with the private key can spend them. While addresses are public, nobody knows which addresses belong to which people; Bitcoin addresses are pseudonymous. After depositing your bitcoins into a "wallet", the wallet alerts ("broadcasts") every other user of bitcoins that it contains bitcoins (See Fig 3).

The central authority makes controlling and monitoring customers and their transactions much easier. Since, money is traditionally centrally regulated, the surge in Bitcoin has invited mixed reactions from regulators across the globe. It has been treated differently in different parts of the world as regards to taxation and other issues. The recent past has seen an enormous growth in Bitcoin as a form of payment. This is because the fee charged in case of making payments with the use of Bitcoin is lower than the general 2-3% interest imposed by credit card processors (NishithDesai, 2015).



Source: GoldeneagleCoin.com, 2016

Fig. 3 How to use Bitcoin

4.2 To examine advantages and disadvantages of Bitcoin

4.2.1 Advantages

As a payment system, Bitcoin has certain benefits over existing electronic systems. These benefits largely accrue to the recipient of a Bitcoin transaction, but certain benefits may be realized by senders of transactions (i.e., consumers or spenders) as well.

Transparency- All Bitcoin Network transactions are cleared in the Blockchain, meaning a complete, auditable and immutable record of all activity exists No individual or organization can control or manipulate the Bitcoin protocol because it is cryptographically secure. This allows the core of Bitcoin to be trusted for being completely neutral, transparent, and predictable.

Low fees and Friction- Bitcoin payments are currently processed with either no fees or extremely small fees. Users may include fees with transactions to receive priority processing, which results in faster confirmation of transactions by the network. In addition, services exist to assist merchants in processing transactions, converting bitcoins to fiat currency, and depositing funds directly into merchants' bank accounts daily. As these services are based on Bitcoin, they can be offered for much lower fees than with PayPal or credit card networks.

Sovereignty of Payment – It is possible to send and receive any amount of money instantly anywhere in the world at any time. No bank holidays, no borders, no imposed limits. Bitcoin allows its users to be in full control of their money.

Network security- The Bitcoin Network itself is highly secure due to the use of cryptographic and decentralized Blockchain protocols. The public-private key pairs used provide ample security against the risk of a brute force hack or an accidental instance of two users generating the same private key. Additionally, there is no single, centralized point of failure, which limits the susceptibility of the Bitcoin Network to downtime and hacking

Protection of financial information. Bitcoin transactions can be performed without having to reveal sensitive personal and financial information to the recipient, limiting the potential exposure of such information to database hacks.

4.2.2 Disadvantages

Bitcoin had a rough road ahead of it, as did many early technologies including the Internet. It dealt with newspaper headlines lambasting Bitcoin because of its connection to Silk Road and drugs. Early adopters suffered millions of dollars in losses when early exchange Mt. Gox imploded. “Bitcoin is Dead,” many prophesied. The total amount of bitcoins is fixed. However, if you use it as a money, i.e. for goods and services, the amount of those goods and services available for that money is not fixed. So the cost, which is simply the ratio of good is completely tied to the goods. In an economy, the ratio of goods and services vs available money is an important indicator of the working of the economy. In relation to these advantages, the abstract nature of Bitcoin poses a challenge to regulators. Like any form of monetary value, including cash, e-money, and credit cards, Bitcoin can be used for both legitimate and illicit purposes.

Privacy Issues - However the cryptographic protocols and the Blockchain that trigger Bitcoin are protected, users must safely store and use their private keys in order to safeguard their bitcoins either on a computer or other mediums which requires proper personal computing.

Instability and Lacks protections against mistakes- The total value of bitcoins in circulation and the number of businesses using Bitcoin are still very small. Therefore, relatively small events, trades, or business activities can significantly affect the price. In theory, this volatility will decrease as Bitcoin markets and the technology matures.

Difficult to use and access - Many people are still unaware of Bitcoin. Every day, more businesses accept bitcoins because they want the advantages of doing so, but the list remains small and still needs to grow in order to benefit from network effects. Most software to control, custody or transact in bitcoins is complex or difficult to use. Often, third-party software and solutions that can simplify this use involve entrusting bitcoins to such third party. Although the Bitcoin Network is open access and liquid markets (relative to current demand and use) exist in the United States and certain other economies, few of the exchanges and services that allow the purchase of bitcoins are regulated and have a significant operational history. Furthermore, the opening of accounts with regulated exchanges requires anti-money laundering and “know your client” verification and account funding that makes it difficult for new users to acquire bitcoins quickly (Wash and Lee, 2013).

Bitcoin is still experimental – Bitcoin software is still in beta with many incomplete features in active development. New tools, features, and services are being developed to make Bitcoin more secure and accessible to the masses. Some of these are still not ready for everyone. Most Bitcoin businesses are new and still offer no insurance. In general, Bitcoin is still maturing.

Government taxes and regulations- Bitcoin is not an official currency. That said, most jurisdictions still require you to pay income, sales, payroll, and capital gains taxes on anything that has value, including bitcoins. It is your responsibility to ensure that you adhere to tax and other legal or regulatory mandates issued by your government and/or local municipalities (Bitcoins.org, 2016).

4.3. Bitcoin: From the Indian Perspective

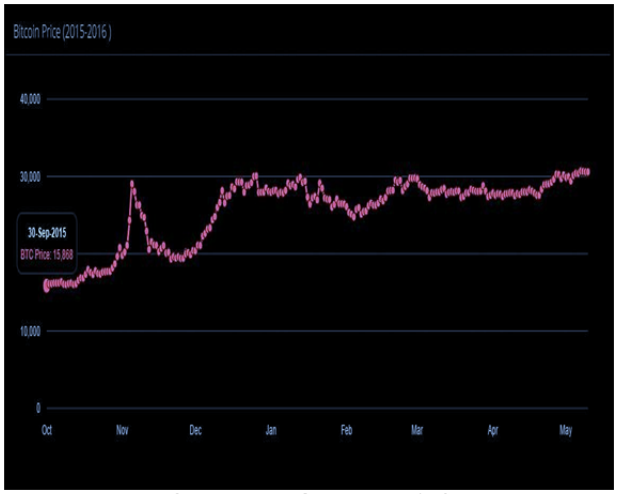
In December 2013, the RBI had cautioned users, holders and traders of virtual currencies (VCs), including bitcoins, about the potential financial, operational, legal, customer protection and security-related risks that they are exposing themselves to. Exactly two years after RBI has come around to appreciate the strengths of the underlying 'blockchain' technology. It’s still too early to throw away your credit card, but bitcoins are making inroads in India as a mode of payment. India currently has around 50,000 bitcoin enthusiasts, with 30,000 of them actually owning the currency

- The concept of bitcoin is new, so some retailers in India have realized the advantages like lower transaction fees, fraud prevention and quick payment etc. of accepting the currency.
- Madovercoins.in is an Indian e-commerce website that accepts only Bitcoins and is targeted mainly at NRIs who want to buy Indian products.

- The interest is not limited to e-commerce sites. Dharwad International School in Karnataka introduced bitcoins as an online payment facility for school fee this academic year.
- eTravelSmart, which offers 80,000-plus bus routes, started the facility in May and sees averagely five bitcoin transactions per month. Customers now pay their ticket fare in bitcoins. For instance, if the fare is Rs 1,000, bitcoins equal to this value are deducted from the customer's wallet.
- Zebpay buys vouchers from e-commerce companies and sell these online against bitcoins and seeing a monthly growth of 100%.
- ePaisa has convinced around 100s of brick and mortar stores to accept bitcoin.
- The bitcoin user base in India is increasing and cannot be ignored.
- With increasing ease of using them for purchases through mobile apps, bitcoins are quickly transitioning from being trading units to shopping currency (Kably, 2015).

Unocoin, an Indian bitcoin exchange, has launched a 'merchant gateway' which enables business entities to accept bitcoins. Sellers like Sapna Book House, bus ticket booking

- Portal eTravelSmart, Dharwad International School, fashion portal Fashiondiva.me, and internet platform service provider Indsoft.net are among those who have signed up and are now accepting bitcoins from their customers.
- Coinsecure, another Indian bitcoin exchange, is likely to introduce a merchant gateway in the coming months. The present value of a Bitcoin in Indian currency is 30947.31 Rupee (see fig 4).



Source: UnoCoin.com, 2016

Fig. 4: Bitcoin Price Fluctuation in India Market

Furthermore, The Constitution of India provides for matters in respect of which the Central Government has powers to regulate and legislate. To understand if Bitcoin are capable of government review, an analysis of the Indian Constitution has been undertaken. In this regard, Article 246 read with Seventh Schedule of the Constitution enumerates the list of activities that the Central Government and the State Governments are allowed to legislate. Entry 36 and 46 of List I of the Seventh Schedule of the Constitution states that the Central Government is allowed to legislate in respect of currency, coinage, legal tender, foreign exchange and bills of exchange, cheques, promissory notes and other like instruments respectively. If Bitcoin (as discussed below) falls within the purview of any of the above outlined categories of instruments, then the Central Government would have exclusive powers to legislate. In the hierarchy of laws, the Constitution is supreme. All laws are subordinate to the Constitution. A law may be struck down as being unconstitutional due to lack of legislative competence or because it violates fundamental rights. Decisions of the Union or State Executive, including decisions of statutory authorities, constitutional functionaries and quasi-judicial authorities may be challenged in a State High Court under the Constitution. Rules, regulations, notifications and circulars passed by authorities under the relevant statute may also be challenged on the ground that the same violate the Constitution. The Constitution empowers, and the Supreme Court of India ("Supreme Court") has recognized, authorities created under a statute to delegate certain functions to subordinate authorities. To facilitate in the effective implementation of government policies certain executive authorities have the power to pass rules and regulations which have the force of law. These rules and regulations are subordinate to the parent law and cannot transgress the limits set out by the parent law. Rules and regulations cannot confer excessive discretion on subordinate authorities. It is also settled law that authorities acting in furtherance of a statute must carry out their functions in a manner that best achieves the objectives of the statute. These principles are designed to reduce the scope of discretion and eliminate arbitrariness in executive action. Ordinarily, decisions of these authorities may be challenged in appeal before an appellate authority. However, in exceptional circumstances, where there is an egregious violation of fundamental rights, principles of natural justice or when an authority acts in violation of its jurisdiction, an aggrieved party may file a petition in the State High Court. It is important to note that while challenging the decision of a statutory authority, generally the scope of appeal is limited and there is a high degree of deference by courts. The Supreme Court has recognized that in matters relating to economic policy, courts must not interfere unless arbitrariness is writ large in the decision making process. Even in cases where intervention of the court is justified, the court would only examine the decision making process and not the decision itself (NishithDesaiAssociates, 2015).

4.4 Controversies and Threat on the go

The currency then fell below the key levels of both $450 and $445 between 06:00 and 08:59 UTC on 2nd May, additional BPI data show – the day Wright proclaimed himself the creator of bitcoin. Gavin Andresen, a noted developer and maintainer of Bitcoin Core, and Jon Matonis, a Bitcoin Foundation founding director, both wrote blog posts supporting Wright's claims. Yet his assertion generated skepticism, and the proof he provided to support his claim was quickly debunked, as members of the bitcoin community revealed that could be owned only by Satoshi Nakamoto. However, the proof was dubbed a "scam" by computer security experts who found the signature but later reneged on the promise and deleted those related blog posts (CoinDesk.com, 2016). On May 5th, 2016 Wright issued a new post saying he would not provide further proof that he is a bitcoin creator, as he fears it would result in personal attacks. Wright also apologised to cryptocurrency consultant Jon Matonis and bitcoin developer Gavin Andresen, who supported his declaration before it was revealed.

In a blog Dr. Wright wrote by quoting, "I'm sorry. I believed that I could do this. I believed that I could put the years of anonymity and hiding behind me," he wrote in the post. "But, as the events of this week unfolded and I prepared to publish the proof of access to the earliest keys, I broke. I do not have the courage. I cannot. When the rumors began, my qualifications and character were attacked. When those allegations were proven false, new allegations have already begun. I know now that I am not strong enough for this, they were not deceived, but I know that the world will never believe that now. I can only say I'm sorry. And goodbye," (Coinspeaker.com, 2016).

5. CONCLUSION

If triumphalism drove adoption, Bitcoin use would already be widespread, and its price in other currencies would be stratospheric. But the existence of a genius protocol does not guarantee its success. For Bitcoin to thrive, there must be a great deal of social and economic change. To foster such change, the Bitcoin ecosystem needs better and more mature communications. It's a deficit that is costing the Bitcoin ecosystem in lost potential each day it persists. Bitcoin and the blockchain are brilliant and fascinating technologies. But Bitcoin's social capital needs are manifold. To deliver on its promises of global financial inclusion, user-defined privacy, enhanced liberty and a stable money supply for all the world's people, the Bitcoin ecosystem needs a larger and more sophisticated community of software and protocol developers, greater assurance against mining centralization, and a thriving community of node operators. The embrace of the financial services community would speed adoption. Bitcoin needs the reality and perception of low volatility; it needs protocols and practices that assure privacy, flourishing marketplaces, a congenial regulatory environment and a positive reputation. (bitcoinMagzine.com, 2016).

While the broader bitcoin community might have been temporarily distracted by Wright's claims to be the digital currency's founder, several developments are brewing that could potentially bolster bitcoin's credibility and push its price higher.

REFERENCES

[1] Andrychowicz, S. Dziembowski, D. Malinowski, andL. Mazurek. *On the Malleability of Bitcoin Transactions*, In Workshop on Bitcoin Research, 2015

[2] Androulaki, G. O. Karame, M. Roeschlin, T. Scherer, and S. Capkun. *Evaluating User Privacy in Bitcoin*, In Financial Cryptography, 2013.

[3] BTC-Planet, \Complete List of Bitcoin Exchanges," Available at http://planetbtc.com/complete-list-of-bitcoin-exchanges/ (2014-09-17) 2014.

[4] A. Biryukov and I. Pustogarov, *Bitcoin over Tor isn't a good idea*, In IEEE Symposium on Security and Privacy, 2015

[5] G. Bissias, A. P. Ozisik, B. N. Levine, and M. Liberatore, *Sybil Resistant Mixing for Bitcoin*, In WPES'14: Workshop on Privacy in the Electronic Society, 2014.

[6] J. Bonneau, A. Miller, J. Clark, A. Narayanan, J. A. Kroll, and E. W. Felten. *Research Perspectives and Challenges for Bitcoin and Cryptocurrencies (Extended Version)*, Cryptology ePrint Archive, Report 2015/261, 2015.

[7] S. Barber, X. Boyen, E. Shi, and E. *Uzun. Bitter to Better—How to Make Bitcoin a Better Currency*, In Financial Cryptography, 2012.

[8] CoinDesk, \CoinDesk State of Bitcoin Q2 2014," Technical Report, CoinDesk July 2014. Available at http://www.coindesk.com/state-of-bitcoin-q2-2014-report-expanding-bitcoin-economy/ 2014.

[9] J. Camenisch, S. Hohenberger, and A. Lysyanskaya. *Compact ecash.* In EUROCRYPT, 2005

[10] D. Chaum, *Blind signatures for untraceable payments*, In CRYPTO, 1982.

[11] D. Chaum, A. Fiat, and M. Naor. *Untraceable electronic cash*, In CRYPTO, 1990

[12] C. Dwork and M. Naor. *Pricing via processing or combatting junk mail*, In CRYPTO, 1992.

[13] Edward V. Murphy, M. Maureen Murphy, Michael V. Seitzinger, *Bitcoin: Questions, Answers, and Analysis of Legal Issues*, Congressional Research Service, 2015.

[14] L. Garber. *Government Officials Disrupt Two Major Cyberattack Systems*, IEEE Computer, July 2014

[15] GAO, \Virtual Currencies: Emerging Regulatory, Law Enforcement, and Consumer Protection Challenges," Technical Report, United States Government Accountability Office May 2014. Available at www.gao.gov/assets/670/663678.pdf, 2014

[16] ICBA, \Virtual Currency: Risk and Regulation," Technical Report, The Clearing House June 2014. Available at www.theclearinghouse.org/~/media/Files/Research/20140623%20Virtual%20Currency%20White%20Paper.pdf (2014-09-17).

[17] Jonathan Levin, *Introduction to Bitcoin: Unique features and data availability*, Oxford Internet Institute, 2013

[18] Kroll, Joshua A., Ian C. Davey, and Edward W. Felton, *The Economics Of Bitcoin Mining, or Bitcoin in the Presence of Adversaries*," Proceedings of WEIS. Vol. 2013, 2013.
[19] Kyle and Scholar, *An Introduction to Bitcoin and BlockChain Technology*, KyleScholarLLP, 2016
[20] Ronald A. Glantz, *What is Bitcoin*, Pantera Primer, Whitepaper, 2014.
[21] S. King and S. Nadal. *PPCoin: Peer-to-Peer Crypto-Currency with Proof-of-Stake*, August 2012.
[22] T. Moore and N. Christin. *Beware the Middleman: Empirical Analysis of Bitcoin-Exchange Risk*, In Financial Cryptography, 2013.
[23] S. Nakamoto. Bitcoin: *A Peer-to-Peer Electronic Cash System*, http: //bitcoin.org/bitcoin.pdf, 2008.
[24] Sarah Rothman, *Bitcoin versus Electronic Money*, *https://www.unocoin.com/how-it-works*CGAP, 2014

Web References

[1] http://www.antipope.org/charlie/blog-static/2013/12/why-i-want-bitcoin-to-die-in-a.html

[2] https://www.bitcoinmining.com/
[3] https://bitcoinmagazine.com/articles/the-bitcoin-ecosystem-s-communications-deficits-1462286858

[4] https://bitcoinmagazine.com/articles/bitcoin-is-growing-up-an-infographic-of-the-bitcoin-ecosystem-1447865097

[5]http://bitcoin.stackexchange.com/questions/10060/how-much-energy-will-the-bitcoin-network-eventually-consume
[6] http://www.coindesk.com/bitcoin-prices-calm-craig-wright-controversy/

[7] http://www.coinspeaker.com/2014/05/05/the-past-and-future-of-bitcoin-infographic/
[8] http://www.coinspeaker.com/2016/05/08/craig-wright-failed-to-proof-bitcoin-creation/

[9]http://www.coinspeaker.com/2016/05/02/australian-entrepreneur-craig-wright-says-hes-satoshi-nakamoto-creator-bitcoin/

[10]http://indiatoday.intoday.in/story/indians-lose-crores-of-rupees-in-bitcoin-exchange-collapse/1/346596.html
[11] https://www.unocoin.com/how-it-works
[12]https://www.zebpay.com/wp-content/uploads/2016/04/Bitcoins.pdf