

Review Paper on Emergence of Bitcoin in India, its Technological Aspects and Legal Implications

Swamy T^a, Pramanshu Shukla, Shreyas Ganesan Iyer, Rishi Gupta

^a Associate Professor, VIT Business School, VIT University, Vellore – 632014 | swamy.t@vit.ac.in

Abstract

India is witnessing an epidemic growth in the field of digital payment these days. With the advancement of technology, e-commerce giants are establishing themselves, which hints of a massive surge in the acceptance of digital payment in the form of bitcoins. Bitcoin is a digital code which is hidden in “data blocks” and could be mined by solving those datablocks. It allows the transactions to be performed without any centralized banking system. It was started by Satoshi Nakamoto in 2009. A tremendous amount of research has been done in this field but that is just a drop in an ocean and there is still a lot to achieve. Limited number of published literature creates a demand for further research in this area. This paper mainly aims at reviewing the available literature work and creates a framework for further studies in this field while summarizing the challenges faced in using bitcoins and its future aspects..

Keywords: Bitcoins, BTC, Mining, datablocks, fungibility, digital currency, money, e-commerce.

INTRODUCTION

Bitcoins is a digital currency created in 2009 by Satoshi Nakamoto (A pseudonym whose identity is still unknown). Since then it has emerged as a replacement of fiat money in various domains, some thinkers believe it to be a viable solution as a medium of exchange. The original use case for bitcoin is Satoshi Nakamoto’s white paper in 2009 on the proposed “Peer to Peer” cash system in which transactions can be done without an intermediary unlike the currency notes which are controlled by central authorities.

For a simple user, it can be considered as cash on internet or an e-wallet. It is also known as crypto currency since it reckons with cryptography for generating electronic currency and validating online transactions. However it does not completely satisfy the “double coincidence of wants” (the situation where the supplier of good A wants good B and the supplier of good B wants good A). As everyone is not well versed with technology even in today’s era a person cannot exchange bitcoins with a farmer to purchase goods, But bitcoins gained huge

popularity in e-commerce industry because of its versatility and ease of exchange and no

one wonder if in future it completely replaces the present money exchange system.

Working Mechanism

There are two ways to get/earn bitcoins:

Mining	Exchange
1. Bitcoins are hidden in various data blocks, which can be extracted by applying various complex algorithms known as mining. Various software are available in market to mine bitcoins. 2. Rewards are given if those hidden blocks are discovered, it is 25BTC for one block and it can be max up to 21 million in a system.	1. If a person does not know mining of bitcoins, he can directly exchange the bitcoins from someone who already has bitcoins. 2. Now exchange can be done by Either, giving them money or, offering them service.

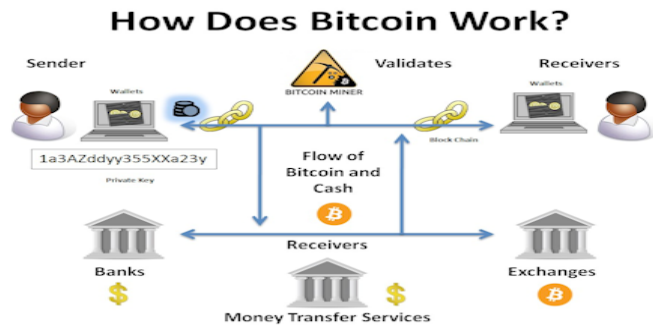


Image source : <https://www.bitcoinsnitch.com>

Figure 1

When a sender enters a key (which can either be in the form of PIN or password) which is private, it validates the user and connects it to the network, in which a public ledger named block chain records are the transactions happened (refer Figure1). Thus by entering addresses you can pay to anyone in the server.

Advantages Over Fiat Money

No Regulating Authority: The first and foremost advantage of bitcoin over money exchange system is that there is no regulating authority to control the transaction as it works on peer-to-peer basis which does not need any centralised banks as they are not issued by any bank.

Fungibility: Fungibility is the ease of exchange of one good with another, before exchange of money was invented, people

used to exchange goods with each other (barter system), but those goods could not be divided into smaller units, also there might be a case where a seller does not want a good which buyer has or it is larger in quantity, for e.g : A person wants a mobile phone in exchange of a laptop, but if the worth of laptop is more than the mobile then this system fails. Using money as a medium of exchange has solved this problem to an extent but it does not work when there is need of smaller units such as paisa, because circulation of it has been stopped. Bitcoins are fungible compared to money because it can be divided into smaller units such as microbitcoin (μ BTC) or millibitcoin (mBTC), which makes exchange easier.

Durability: It is more durable than paper currency because it cannot be destroyed as they are stored electronically.

Hard to counterfeit: Bitcoins are hard to counterfeit compared to money because it is not in printable format but in a password protected chain of crypto currency mathematical algorithm, which could not be accessed easily unless and until there is no hacking.

Limitations

Low acceptance Rate: In developing countries like India, where only 18 out of 100 people have access to the internet. Acceptance rate of BTC lags behind money. If a buyer wants to give bitcoins to a nearby store, it won't accept. However an IT professional may accept bitcoins.

National Security issue: Because of its anonymity and having no regulation of transaction, it can be used by terrorists,

druglords or tax evaders. However there are various softwares which can validate "good"(earned through legal activities) or "bad"(earned through illegal activities) bitcoins by analysing its transaction history and origin. But if everyone will start validating it, BTCs will lose their fungibility because Out of fear most of the users will deny using BTC which originated illegally. Hence those coins will lose their worth.

No Regulatory Authority if Stolen: If a user has a bank account and his money has been stolen, then the bank will take care of it but in this case because of anonymity No one will reimburse the value of his stolen bitcoins.

Selfish Mining: Selfish mining is a well-known attack where a selfish miner, under certain conditions, can gain a disproportionate share of reward by deviating from the honest behaviour.

According to professor Ittay Eyal of Cornell University USA, selfish mining can be defined as: "You know that blocks are generated one after the other. When a miner generates a block, it's supposed to publish it to the network, and then everybody works to try to create a block that will follow this original block. With selfish mining, the attacker keeps the block to itself and mines on top of it without exposing it to the network. [The selfish miner] only exposes this secret chain — the local secret chain — when it has to in order to maximize its revenue. It turns out by doing that a miner can actually increase its revenue and earn more than it should, more than its fair share of the mining power, and this is the essence of the attack."

LEGAL ISSUES

Virtual Currencies pose a various legal implications which are addressed here:

- Bitcoin is relatively new and has not yet received the public assurance that it needs to thrive in India. The government policies do not line up in accordance with Bitcoin either, thus posing a hindrance for the increase of value of Bitcoin.
- It also proves to be an unnecessary gamble for the public, especially due to the lack of financial protection provided by the government with respect to virtual currency. The law for public protection in accordance with virtual currency is still at an embryonic stage.
- Double spending, which causes hackers to spend more money than what is available to them is also cause for concern in the case of virtual currencies.
- Flagitious activities brought about due to the elementary stage at which virtual currency is perceived in India establishes itself as an inhibitory cause for government backing of virtual currencies.
- India, not unlike any other country, already has an extensive framework revolving around the existing currency. Many of these laws may not apply to the digital currency such as Bitcoin, thus forcing many private as well public institutions and companies to not provide its complete backing for the same.

Pros and Cons of Bitcoins

Pros	Cons
1. Does not have a central authority, making it hassle free.	1. Due to no controlling authority, risk of forgery is there.
2. Fungibility	2. Limited no. of coins (about 21 millions)
3. Indian banks like SBI, have ceilings on transfer in retail banking, NEFT: upto 2 lakhs and RTGS: upto 5 lakhs, more than this can be done via corporate banking only. No such ceiling system is present in bitcoins transfer.	3. Bitcoins cannot be sent more than once, which is known as double sending. Double sending is not possible.
4. Low Inflation risk compared to money. (as only 21 million bitcoins are released)	4. Not accepted everywhere in India.
5. No transaction charges in transfer unlike money transfer.	5. RBI neither regulates nor supports bitcoins.

Conclusion

As discussed above, virtual or digital currency like Bitcoin has its fair share of pros and cons. Despite being at an embryonic stage of development, it has laid down the basic foundation in looking for an alternative for the existing currency on the web. With the e-commerce industry booming and technological advances revolutionizing every field, an evolution in the way we handle currency will be welcomed by most people. Virtual currency when wholly implemented will shift the power of currency from the hands of central banking institutions to the hands of the people. With the Indian Rupee still struggling to get a grip on its declining value, despite boasting one of the largest economies in the world, can lead to several investments in digital currency like Bitcoin. Participation from the second largest country in the world in terms of population, will definitely lead to more research in this area to make it a strong force in the global economy.

References

- Chinmay A. Vyas, Munindra Lunagaria, (2014), "Security Concerns and Issues for Bitcoin" *International Journal of Computer Applications® (IJCA)* (0975 – 8887) National Conference cum Workshop on Bioinformatics and Computational Biology, NCWBCB-2014.
- Dr. B.S. Sawant," Technological Developments in Indian Banking Sector" , *Indian Streams Research Journal*, ISSN No-2230-7850 Vol.1, Issue.IX/Sept; 11 pp.1-4.
- Dr. Bhagwan Jagwani: "Bitcoins Demystified" *International Journal Of Marketing, Financial Services & Management Research* ISSN 2277-3622 Vol.4 (4), April, (2015), pp. 29-35
- Ghassan O. Karame, Elli Androulaki and Srdjan Capkun, "Two Bitcoins at the Price of One? Double-Spending Attacks on Fast Payments in Bitcoin," In Proceedings of the ACM Conference on Computer and Communications Security (CCS), Chicago, IL, USA, pp. 1-17, 2012.
- Jerry Brito, Andrea Castillo, *Bitcoin - A primer for policymaker*, Center Copyright © 2013.
- Ittay Eyal and Emin Gün Sirer, "Majority is not Enough: Bitcoin Mining is Vulnerable," unpublished.
- Mandar Kadam, Prahars Jha, Shравan Jaiswal Double Spending Prevention In Bitcoins Network, *International Journal of Computer Engineering and Applications*, Volume IX, Issue VIII, August 2015 www.ijcea.com ISSN 2321-3469
- Mayur Shetty (Dec 26, 2015) "Tech behind bitcoin can help check counterfeiting: RBI", Times of India/Tech news.
- Nakamoto, Satoshi (October 2008). "Bitcoin: A Peer-to-Peer Electronic Cash System" .bitcoin.org. Retrieved 28 April 2014.
- Thabiso Peter Mpofo, Budwell Masaiti, Macdonald Mukosera : "Digital Currency: The Emergence of Bitcoins", *International Journal of Science and*

Research (IJSR), ISSN (Online): 2319-7064, Impact Factor (2012): 3.358

VasudhaKapil : “BitCoin: A New Paradigm in E – Commerce”, International Journal of Advanced Research in Computer and Communication Engineering Vol. 3, Issue 9, September 2014.

W.S. Jevons (1875), Money and the Mechanism of Exchange, Chapter 1, paragraphs 5-6. London: Macmillan.

<https://www.theguardian.com/technology/2015/dec/09/bitcoin-creator-satoshi-nakamoto-alleged-to-be-australian-academic>

<https://bitcoinmagazine.com/articles/bitcoin-as-a-solution-to-e-commerce-pain-1415923213>

<https://www.bitcoinmining.com>

<https://www.bitcoinsnitch.com>

<http://www.investopedia.com/terms/f/fungibility.asp>

<https://bitcoins.org>

(<http://data.worldbank.org/indicator/IT.NET.USER.P2>).