JETIR.ORG ISSN: 2349-5162 | ESTD Year : 2014 | Monthly Issue
JOURNAL OF EMERGING TECHNOLOGIES AND INNOVATIVE RESEARCH (JETIR)
An International Scholarly Open Access, Peer-reviewed, Refereed Journal

# Conceptual Study of Bit coin and its working

**Prof. Malusare L.B.**

**S.N. Arts D.J.M. Commerce and B.N.S. Science college Sangamner – Ahmednagar**

**Omsairammalusare@gmail.com**

**Abstract :** The finance system in India is developing in the age of digitalisation, it is turning toward the digitalisation and avail to society digital transaction platform. But today also some types of currencies are not included in our finance system therefore Indian society also not aware with these new trend and changes in the fiancé system. Some of the people are aware about this crypto currency but they also not fully known about the crypto currency therefore it is important to clarify the concept and how it works in the digital platform. The research paper is conceptual research paper and it focus on the concept of bitcoin and how it works and what is the advantages and drawback of the bitcoin. It is also going to explain about the status of bit coin in India

**Introduction:** The financial literacy in India is fundamentally low in the situation bitcoin is a quit new concept therefore it is necessary to know the concept and how it works. Bitcoin is a digital Crypto currency, the. In 2009, Satoshi Nakamoto, an engineer, coined the concept of Bitcoin

There are about 25 sites like Bitcoin India where we can make these transactions. But Bitcoin was not legally recognized, therefore it is not very popular in India but The Supreme Court has lifted the ban on the use of virtual currency (cryptocurrency) and allowed its use in transactions. The Reserve Bank of India (RBI) had in April 2018 banned the trading of virtual currencies like Bitcoin. The RBI had tightened rules on Bitcoin and other virtual currencies. This time, they banned banks and other financial institutions from providing any services, but now the ban has been lifted. therefore, it is necessary to know the concept and its working in the finance mechanism.

Now a days India is looking toward the bitcoin as a investing opportunity and now it is now in trend to purchase and sale bit coin.

**Concept Bitcoin:** Bitcoin is a currency like the rupee, dollar or any other currency. It is only online and encrypted by a computer code. 'Bitcoin' came into being by performing mathematical calculations in a computer program. Over the past decade, hundreds of types of cryptocurrencies have emerged in the computer world.

Bitcoins can be used to buy merchandise anonymously. In addition, international payments are easy and cheap because bitcoins are not tied to any country or subject to regulation. Small businesses may like them because there are no credit card fees. Some people just buy bitcoins as an investment, hoping that they'll go up in value.

**History :** Bitcoin is the first implementation of a concept called "cryptocurrency", which was first described in 1998 by Wei Dai on the cypher punks mailing list, suggesting the idea of a new form of money that uses cryptography to control its creation and transactions, rather than a central authority. The first Bitcoin specification and proof of concept was published in 2009 in a cryptography mailing list by Satoshi Nakamoto. Satoshi left the project in late 2010 without revealing much about himself. The community has since grown exponentially with many developers working on Bitcoin.

Satoshi's anonymity often raised unjustified concerns, many of which are linked to misunderstanding of the open-source nature of Bitcoin. The Bitcoin protocol and software are published openly and any developer around the world can review the code or make their own modified version of the Bitcoin software. Just like current developers, Satoshi's influence was limited to the changes he made being adopted by others and therefore he did not control Bitcoin. As such, the identity of Bitcoin's inventor is probably as relevant today as the identity of the person who invented paper.

**How works the Digital Crypto currency:** Bit coin is just a program or mobile application which provided mobile wallets to the bitcoin user. The Bitcoin network is sharing a public ledger called the "block chain". The basic steps are as follows:

1. **Blockchain:** Blockchain is a shared public ledger on that entire network of bitcoin transaction occurs and get completes. All confirmed transactions are included in the blockchain. It also allows Bitcoin wallets to calculate their spendable balance so that new transactions can be verified so that they actually own the cost. Blockchain integrity and chronological cryptography are implemented.

2. **Transactions: private keys:** A transaction is a transfer of value between Bitcoin wallets that gets included in the blockchain. Bitcoin wallets keep a secret piece of data called a private key or seed, which is used to sign transactions, providing a mathematical proof that they have come from the owner of the wallet. The signature also prevents the transaction from being altered by anybody once it has been issued. All transactions are broadcast to the network and usually begin to be confirmed within 10-20 minutes, through a process called mining.
3. **Mining:** Mining is Distribution agreement system in which pending transaction used to confirm using block chain. Blockchain works in a sequence, protects the neutrality of the network, and allows different computers to agree on the state of the system. To be confirmed, transactions must be packed in a *block* that fits very strict cryptographic rules that will be verified by the network. These rules prevent previous blocks from being modified because doing so would invalidate all the subsequent blocks. Mining also creates the equivalent of a competitive lottery that prevents any individual from easily adding new blocks consecutively to the block chain. In this way, no group or individuals can control what is included in the block chain or replace parts of the block chain to roll back their own spends.

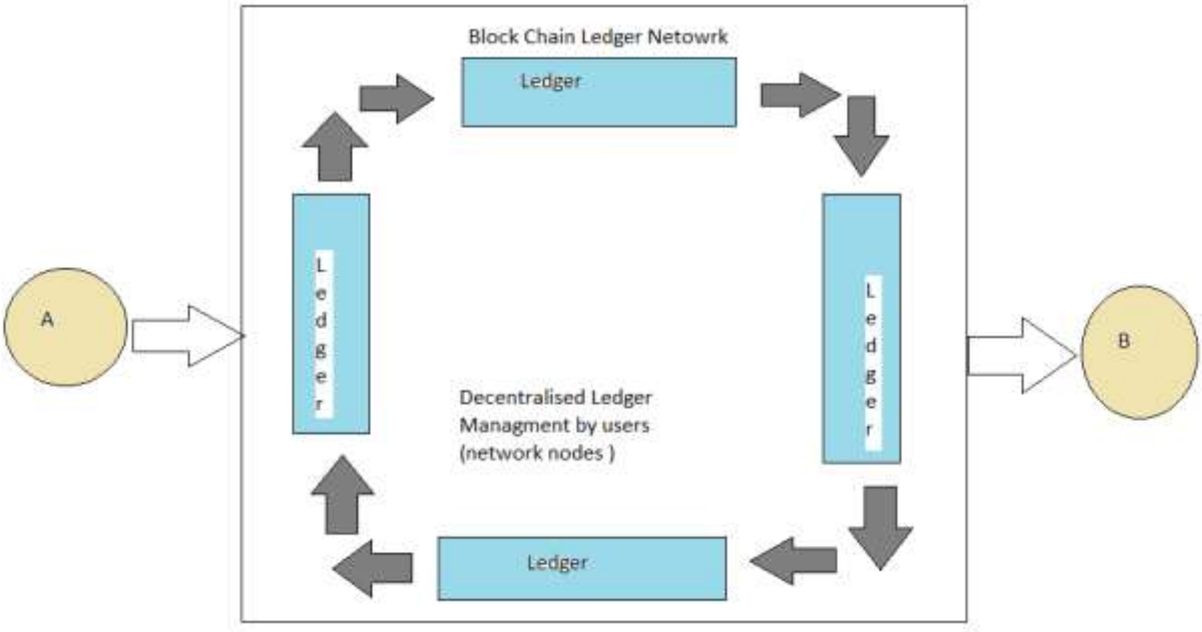

Fig 1 : cryptocurrency transaction procedure

Figure 1 shows the cryptocurrency transaction procedure. If user A would like to transfer digital currency to user B, the transaction needs to go through the blockchain path. The blockchain in the ledger system that monitored and validated by the users in involved in ledger validation system using a computer system. Cryptocurrencies make it easier to transfer funds between two parties in a transaction; these transfers are facilitated using public and private keys for security purposes. These fund transfers are done with minimal processing fees, allowing users to avoid the steep fees charged by most banks and financial institutions for wire transfers. There are no physical bitcoins; only balances kept on a public ledger in the cloud. All Bitcoin transactions are verified by a massive amount of computing power.

1. **Establish an account**. Select an approach and third-party providers that are appropriate for the type and quantity of cryptocurrency being donated and your organization's capacity to manage complexity and risk. Use a two-factor authentication application, such as Duo, Authy, or Google Authenticator, to add an additional layer of protection beyond passwords.

2. **Receive a donation.** Once your account is established, you can share your account number or "public address" with the donor. The donor will then transfer the cryptocurrency to that address. With BitPay, the public address is incorporated into the invoice for payment.

3. **Sell the asset and transfer the proceeds**. With BitPay, the sale and transfer of proceeds is processed for you. On Coinbase, you simply enter the amount to sell and the proceeds are transferred to the bank account you designated at initial setup. Bitstamp offers more sophisticated trading options, requiring you to choose between placing an instant, market, limit, or stop order. Online guidance is available. Once sold, you will have a credit for U.S. dollars that can be transferred to the bank account you designated at initial setup. Bitstamp has additional security measures that require confirmation of the transfer through an email sent to the address on record.

4. **Determine the gift value.** The gift value can be determined several ways, including:

a. the actual price at the time of the contribution,
b. the closing price for the day of the contribution,
c. the volume weighted average price, or
d. the average of the high and low price.

For consistency with the valuation method used for gifts of public stock, the average of the high and low price should be used. For a better measure of the average price at which the asset was traded over the day, the volume weighted average price is preferable. Prices can be found on a variety of websites that chart price history. Substantiating the value of the donation for tax **purposes** is the donor's responsibility, as is obtaining a qualified appraisal for donations over $5,000.

**Buy on an Exchange:** Many marketplaces called "bitcoin exchanges" allow people to buy or sell bitcoins using different currencies. Coinbase is a leading exchange, along with Bitstamp and Bitfinex. But security can be a concern: bitcoins worth tens of millions of dollars were stolen from Bitfinex when it was hacked in 2016.

**Transfers:** People can send bitcoins to each other using mobile apps or their computers. It's similar to sending cash digitally.

**Mining:** People compete to "mine" bitcoins using computers to solve complex math puzzles. This is how bitcoins are created. Currently, a winner is rewarded with 12.5 bitcoins roughly every 10 minutes.

Bitcoin wallet: Bitcoins are stored in a "digital wallet," which exists either in the cloud or on a user's computer. The wallet is a kind of virtual bank account that allows users to send or receive bitcoins, pay for goods or save their money. Unlike bank accounts, bitcoin wallets are not insured by the FDIC.

**The anonymity of bitcoin**

Though each bitcoin transaction is recorded in a public log, names of buyers and sellers are never revealed – only their wallet IDs. While that keeps bitcoin users' transactions private, it also lets them buy or sell anything without easily tracing it back to them. That's why it has become the currency of choice for people online buying drugs or other illicit activities.

**Comparison between traditional digital currency transaction and cryptocurrency transaction:**

| | | |
|---|---|---|
| Definition | Money in any form in actual use or circulation as a medium of exchange, especially circulating banknotes and coins. Money is government-issued currencies. | Digital currency in which encryption techniques are used to regulate the generation of units of currency. Type of currency that is non-physical, of which no banknotes and coins exist, and which can only be transmitted via electronic means, typically allowing for instantaneous transactions and borderless transfer of ownership |
| Example | Two monetary systems: fiat money and commodity money | Virtual currencies and cryptocurrencies |
| Verification | The transaction using code from financial institution | A transaction using a digital signature that represented by a code that is generated by the algorithm. |
| Transaction path | The transaction path is monitored by trusted third part | Ledgers in blockchain monitor the transaction path. This ledger is open for public access and maintained by users. |
| Transaction cost | There is transaction cost | Minimal transaction cost that lower compared to traditional money transfer method |
| Volatility | Price of exchange rate fluctuates according to economic condition. | Price of Bitcoin is based on supply and demand. The exchange rate of cryptocurrency fluctuates widely depending on the news |

**Status of Bitcoin in India:** The government of India used to not accept the bitcoin and declared as an illegal currency due to unknown control of bitcoin. In early 2018 India's central bank, the Reserve Bank of India (RBI) announced a ban on the sale or purchase of cryptocurrency for entities regulated by RBI. But In March 2020, the Supreme Court of India passed the verdict, revoking the RBI ban on cryptocurrency trade. The current price of the bit coin in the rupees is 7,87,661 per bit coin in 2020.

**Conclusion :** The bit coin is a crypto currency and it working using digital networking with high security. The bit coin pricing is depends demand and acceptance of the bit coin. The bit coin transfer using facilitated using public and private keys for security purposes. These fund transfers are done with minimal processing fees,

**Reference:**

1. bdalla, M., Boyen, X., Chevalier, C., Pointcheval, D.: Distributed Public-Key Cryptography
2. om Weak Secrets. In: Jarecki, S., Tsudik, G. (eds.) PKC 2009. LNCS, vol. 5443, pp. 139–159. Springer, Heidelberg (2009) Corssref

1. Abu Bakar, N. and Rosbi, S. (2017) Data Clustering using Autoregressive Integrated Moving Average (ARIMA) model for Islamic Country Currency: An Econometrics method for Islamic Financial Engineering, The International Journal of Engineering and Science, Vol. 6 (6), pp. 22-31 Crossref
2. Abu Bakar, N. and Rosbi, S. (2017) Data modeling diagnostics for share price performance of Islamic Bank in Malaysia using Computational Islamic Finance approach, International Journal of Advanced Engineering Research and Science, 4 (7), 174-179 Crossref
3. Alotaibi, M.N. and Asutay, M. (2015) Islamic Banking and Islamic e-commerce: Principles and Realities, International Journal of Economics, Commerce and Management, III (4), 1-14
4. Androulaki E., Karame G.O., Roeschlin M., Scherer T., Capkun S. (2013) Evaluating User Privacy in Bitcoin. In: Sadeghi AR. (eds) Financial Cryptography and Data Security. FC 2013. Lecture Notes in Computer Science, vol 7859. Springer, Berlin, Heidelberg Crossref
5. Barber, S., Boyen, X., Shi, E. and Uzun, E. "Bitter to better - how to make bitcoin a better currency," in Financial Cryptography 2012, vol. 7397 of LNCS, 2012, pp. 399-414.
6. Böhme, R., Christin, N., Edelman, B., and Moore, T. (2015). Bitcoin: Economics, technology, and governance. The Journal of Economic Perspectives, 29(2), 213-238. Crossref
7. Canard, S., Gouget, A.: Divisible E-Cash Systems Can Be Truly Anonymous. In: Naor, M. (ed.) EUROCRYPT 2007. LNCS, vol. 4515, pp. 482–497. Springer, Heidelberg (2007) Crossref
8. Decker,C. and Wattenhofer,R., "Information propagation in the Bitcoin network," IEEE P2P 2013 Proceedings, Trento, 2013, pp. 1-10.doi: 10.1109/P2P.2013.6688704 Crossref
9. Gennaro, R., Jarecki, S., Krawczyk, H., and Rabin, T. (2007) Secure distributed key generation for discrete-log based cryptosystems. Journal of Cryptology, 20(1), 51-83. Crossref
10. Grinberg, R. (2012). Bitcoin: An innovative alternative digital currency. Hastings Sci. & Tech. LJ, 4, 159.
11. Jonathan T.B. (2017). Why Is Bitcoin's Value So Volatile?
12. Kristoufek, L. (2013). BitCoin meets Google Trends and Wikipedia: Quantifying the relationship between phenomena of the Internet era. Scientific reports, 3, 3415. Crossref
13. Kroll, J. A., Davey, I. C., & Felten, E. W. (2013, June). The economics of Bitcoin mining, or Bitcoin in the presence of adversaries. In Proceedings of WEIS (Vol. 2013).
14. Miers,I.,Garman, C.,Green,M. and Rubin, A. D. "Zerocoin: Anonymous Distributed E-Cash from Bitcoin," 2013 IEEE Symposium on Security and Privacy, Berkeley, CA, 2013, pp. 397-411.doi: 10.1109/SP.2013.34 Crossref
15. Moore, T., and Christin, N. (2013, April). Beware the middleman: Empirical analysis of Bitcoin-exchange risk. International Conference on Financial Cryptography and Data Security (pp. 25-33). Springer, Berlin, Heidelberg. Crossref
16. Muhammad, M., Muhammad, M.R. and Mohammed Khalil, M, (2013) Towards Shari'ah Compliant E-Commerce Transactions: A Review of Amazon.com, Middle-East Journal of Scientific Research, 15(9), 1229-1236
17. Nakamoto, S. (2009) "Bitcoin: A peer-to-peer electronic cash system", Retrieved from http://www.bitcoin.org /bitcoin.pdf
18. Okamoto, T.: An Efficient Divisible Electronic Cash Scheme. In: Coppersmith, D. (ed.) CRYPTO 1995. LNCS, vol. 963, pp. 438–451. Springer, Heidelberg (1995) Crossref
19. Reid,F. and Harrigan,M., "An analysis of anonymity in the Bitcoin system," in Privacy, security, risk and trust (PASSAT), 2011 IEEE Third Internatiojn Conference on Social Computing (SOCIALCOM). IEEE, 2011, pp. 1318- 1326.
20. Retrieved from http://www.investopedia.com/articles/investing/052014/why-bitcoins-value-so-volatile.asp

21. Ron D., Shamir A. (2013) Quantitative Analysis of the Full Bitcoin Transaction Graph. In: Sadeghi AR. (eds) Financial Cryptography and Data Security. FC 2013. Lecture Notes in Computer Science, vol 7859. Springer, Berlin, Heidelberg Crossref
22. Yermack, D. (2013). Is Bitcoin a real currency? An economic appraisal (No. w19747). National Bureau of Economic Research. Crossre
23. https://www.loksatta.com/do-you-know-news/what-is-cryptocurrency-scsg-91-2099852/
24. https://bitcoin.org/en/how-it-works
25. https://money.cnn.com/infographic/technology/what-is-bitcoin/index.html
26. https://bitcoin.org/en/faq#who-controls-the-bitcoin-network
27. https://www.bhaskar.com/business/economy/news/bit-coin-digital-currency
28. https://blockgeeks.com/guides/what-is-bitcoin/