An Analytical Paper on Bitcoin

M. Vivek Anand, Department Of Computer Science and Engineering
Galgotias University, Yamuna Expressway Greater Noida, Uttar Pradesh

Abstract:Bitcoin is an electronic type of "money". It is digitally generated and carried onto a device. Bitcoins are not paper money from central banks or monetary agencies such as pounds or dollar. Bitcoin is the example of a block chain that is generated globally by people and businesses utilizing advanced computer tools to solve mathematical problems.Bitcoin does not flow via the banking system; instead it transfers from one wallet to another computer. Bitcoin cannot be stored or retained as money in a purse or wallet; it is simply a means of exchange built on a computer system.Every Bitcoin is simply a computer file which is saved on a computer or phone in a digital wallet app.People send Bitcoins to digital wallet, and one can transfer Bitcoins to others. Each single transaction is registered in a block chain-called public list, it helps tracking the past of Coins to prevent people from spending coins that they don't own, making copies or undoing payments.Bitcoin was created for the first time, inventor Satoshi Nakamoto published 50 bitcoin which he retained. Going on, he or she received 25 bitcoin when a miner solved a puzzle. That was halved again in the summer of 2016, to 12.5. The number will continue to be halved annually until it has published all 21 million bitcoins.

Keywords: Bitcoin, Coin, Coin base, Miner, Nakamoto.

INTRODUCTION

Bitcoin is an electronic type of "money". It is digitally generated and carried onto a device. Bitcoins are not paper money from central banks or monetary agencies such as pounds or dollar. Bitcoin is the example of a block chain that is generated globally by people and businesses utilizing advanced computer tools to solve mathematical problems.[1], [2]. The Figure 1 show the bitcoin logo.



Fig.1: The Figure Portrays the Logo of Bitcoin

Satoshi Nakamoto initially suggested Bitcoin as a payment method based on mathematics. Bitcoin is a process of payment or cashless transaction that is independent from governmental authorities such as central banks that typically control money supply and currency availability in the market. Bitcoin is in many aspects a pan-global means of exchange. Transfers are done immediately through device with small transaction fees.

Bitcoin does not flow via the banking system; instead it transfers from one wallet to another computer. Bitcoin cannot be stored or retained as money in a purse or wallet; it is simply a means of exchange built on a computer system.

Bitcoin is a financial asset; there are just 21 million coins in all. Solution of complex mathematical problems contributes to Bitcoins mining. Bitcoin is however divisible so that the exchange medium's potential for growth is unlimited. The block chain or distributed ledger technology is among the most interesting innovations that came along with bitcoin. In terms of traditional operations and settlement ramifications, DLT has incredible potential for companies in the economic and other industries. DLT monitors possession, which enables Bitcoin to be exchanged quickly and efficiently.

Bitcoin has several characteristics that set it apart as a pan-global medium of exchange from the traditional currencies. The amount of Bitcoins is not regulated by central banks or financial authorities; it is decentralized and allows it global. To receive or transfer Bitcoins in seconds, anybody with a computer can established a Bitcoin address. Bitcoin is anonymous; the cryptocurrency allows the user to maintain different addresses, and no personal data is required to set up an address. The DLT technology makes Bitcoin totally transparent; it saves full details by every account address that ever occurred.

Bitcoin transactions are immediate and they're final once done. At the very same time there are minimal fees, and foreign exchange rates and transfer fees do not apply to international and domestic transfers. When it applies to Bitcoin there are no frontiers.[3], [4]. Figure 2 portrays how bitcoin works.

Is Bitcoin a product?

The approval of the CFTC came as a reaction to an auction of Bitcoin that provided futures contracts or options on cryptocurrency valuation. Bitcoin, though, is one of those assets that doesn't fall well into either description, and a historical understanding of what a currency is, and what a product sheds light on the case.

How Bitcoins Works?

Every Bitcoin is simply a computer file which is saved on a computer or phone in a digital wallet app.People send Bitcoins to digital wallet, and one can transfer Bitcoins to others. Each single transaction is registered in a block chain-called public list,it helps tracking the past of Coins to prevent people from spending coins that they don't own, making copies or undoing payments.

There are three primary ways in which people are using Bitcoins:

- Bitcoins can be purchased using the ' real ' currency.
- One can sell products with Bitcoins, and let people pay
- Or one could create them using a computer.



Fig.2: The Figure Portrays How Bitcoin Works

One could start with Bitcoin as a new user, without knowing the technical details. One has enabled a Bitcoin wallet on device or mobile phone, first Bitcoin address will be created, and one can build more whenever one needs more. One should show his/her addresses to mates so they can reimburse one or vice

versa. This is actually quite similar to how email operates, except that the Bitcoin addresses should only be used once.

Where precisely to categorize Bitcoin is contentious. Was it a kind of money, a value market, a network of payments or an asset class?Thankfully it's easier to define what Bitcoin is in reality. They're apps. Don't be deceived by stock images emblazoned with updated Thai baht labels with polished coins. Bitcoin is a purely digital technology, a collection of protocols and procedures. It is also the most popular of hundreds of attempts by cryptography, the technique of making and breaking codes to create virtual currency. Bitcoin has spawned hundreds of imitators, but by market capitalization it remains the largest cryptocurrency, a distinction it has retained throughout its decade-plus.[5], [6]

- Key Features

Bitcoin is a digital currency, a cryptographic network that tracks transactions called a database in a distributed ledger.

Bitcoin miners operate complex computer hardware to solve difficult puzzles in an attempt to validate transaction groups called blocks; after completion, these blocks are applied to the block chain database, and the miners are credited with a small number of bitcoins.

Certain Bitcoin market players may buy or sell tokens through cryptocurrency exchanges.

The Bitcoin network is secured against abuse through a trust less system; Bitcoin exchanges often operate to shield themselves from future hacking, but there have been high-profile robberies.

No, the system is meant to cap out at a capacity of 21 million bitcoin. Bitcoin would stop releasing at that stage. Many people believe this is going to be around the year 2140.

One knows, miners are not building blocks just out of the kindness of their hearts. When a miner constructs a stone, a set of complex math puzzles need to be solved too. If they could do it before any other miner, they can release a guaranteed amount of bitcoin they can keep — a bonus for being smart and quick. The way in which this bitcoin rivalry will last until 2140 is via halving activities. Figure 3 portrays how bitcoin can be achieved. The Figure 4 shows the minor rewards of bitcoin.



Fig.3: The Figure Portrays How Bitcoin Can Be Won



Fig.4: The Figure Portrays the Minor Rewards of Bitcoin

Bitcoin was created for the first time, inventor Satoshi Nakamoto published 50 bitcoin which he retained. Going on, he or she received 25 bitcoin when a miner solved a puzzle. That was halved again in the summer of 2016, to 12.5. The number will continue to be halved annually until it has published all 21 million bitcoins.[7], [8]

- Is it safe to invest in bitcoin

Many bitcoin analysts claim that decentralized block chain is fairly bulletproof. one will not only need to use a lot of computing power to change the ledger, but one would also need to do so in very public space where thousands of other machines and people can see precisely what one is doing. The whole network is influenced by what one person or machine does and everyone can control the transactions.

At present, when one invests thousands of dollars purchasing it in bulk, bitcoin is nothing more than a warehouse, though the inventors would struggle to have it described that way. Over time, it could become a reasonable means to buy goods and services— Japan currently, constitutionally, recognizes it. But it's rather an expense for now. And if one is clever enough, one might make money, as long as the bubble doesn't break out. The Figure 5 Portrays the value chart of bitcoin.

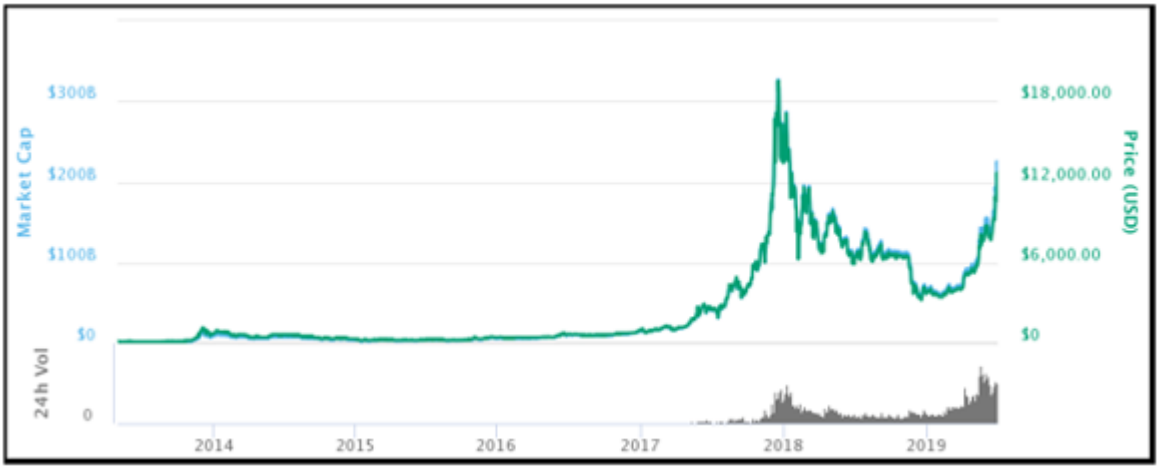


Fig.5: The Figure Portrays the Value Chart of Bitcoin

- How to invest?

As with any company, finding someone who is well knowledgeable with making investments is safest. But a simple rule is not to pay more than you wish to lose. In terms of price, cryptocurrencies can be unpredictable, increasing and plummeting every day. If one is still interested, there are a number of apps that you can access to get started investing on your computer, such as Coinbase and Bitstamp. Such software are likewise "digital wallets" that house the money.[9], [10]

Coinbase seems to be the more accessible and common. It's an app which you can access and spend up to $750 a week on your computer. It's free, but then again last week it received some cheeky attention for insider trading. Figure 6 shows how to buy bitcoin.

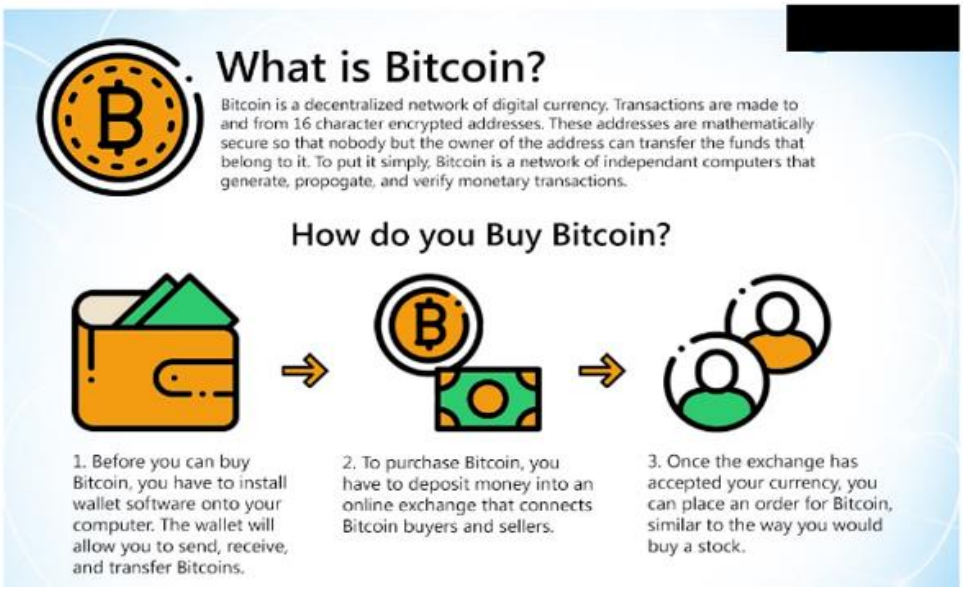


Fig.6: The Figure Portrays the Process to Buy Bitcoin

CONCLUSION

Bitcoin is an electronic type of "money". It is digitally generated and carried onto a device. Bitcoins are not paper money from central banks or monetary agencies such as pounds or dollar. Bitcoin is the example of a block chain that is generated globally by people and businesses utilizing advanced computer tools to solve mathematical problems.Bitcoin does not flow via the banking system; instead it transfers from one wallet to another computer. Bitcoin cannot be stored or retained as money in a purse or wallet; it is simply a means of exchange built on a computer system.Every Bitcoin is simply a computer file which is saved on a computer or phone in a digital wallet app.People send Bitcoins to digital wallet, and one can transfer Bitcoins to others.Each single transaction is registered in a block chain-called public list it helps tracking the past of Coins to prevent people from spending coins that they don't own, making copies or undoing payments.

REFERENCES

[1] C. S. Wright, “Bitcoin: A Peer-to-Peer Electronic Cash System,” SSRN Electron. J., 2019.

[2] I. Eyal, A. E. Gencer, E. G. Sirer, and R. Van Renesse, “Bitcoin-NG: A scalable blockchain protocol,” in Proceedings of the 13th USENIX Symposium on Networked Systems Design and Implementation, NSDI 2016, 2016.

[3] E. Portmann, “Rezension „Blockchain: Blueprint for a New Economy“,” HMD Prax. der Wirtschaftsinformatik, 2018.

[4] R. Böhme, N. Christin, B. Edelman, and T. Moore, “Bitcoin: Economics, technology, and governance,” J. Econ. Perspect., 2015.

[5] J. a Kroll, I. C. Davey, and E. W. Felten, “The Economics of Bitcoin Mining, or Bitcoin in the Presence of Adversaries,” Twelfth Work. Econ. Inf. Secur. (WEIS 2013), 2013.

[6] P. Ciaian, M. Rajcaniova, and d’Artis Kancs, “The economics of BitCoin price formation,” Appl. Econ., 2016.

[7] F. Reid and M. Harrigan, “An analysis of anonymity in the bitcoin system,” in Security and Privacy in Social Networks, 2013.

[8] I. Eyal and E. G. Sirer, “Majority is not enough: Bitcoin mining is vulnerable,” in Lecture Notes in Computer Science (including subseries Lecture Notes in Artificial Intelligence and Lecture Notes in Bioinformatics), 2014.

[9] I. Eyal and E. G. Sirer, "Majority Is Not Enough: Bitcoin mining is vulnerable," Commun. ACM, 2018.

[10] M. Conti, K. E. Sandeep, C. Lal, and S. Ruj, "A survey on security and privacy issues of bitcoin," IEEE Commun. Surv. Tutorials, 2018.

- Usha Yadav, Gagandeep Singh Narula, Neelam Duhan, Vishal Jain, "Ontology Engineering and Development Aspects: A Survey", International Journal of Education and Management Engineering (IJEME), Hongkong, Vol. 6, No. 3, May 2016, page no. 9 – 19 having ISSN No. 2305-3623.

- Vishal Assija, Anupam Baliyan and Vishal Jain, "Effective & Efficient Digital Advertisement Algorithms", CSI-2015; 50th Golden Jubilee Annual Convention on "Digital Life", held on 02nd to 05th December, 2015 at New Delhi, published by the Springer under ICT Based Innovations, Advances in Intelligent Systems and Computing having ISBN 978-981-10-6602-3 from page no. 83 to 91.

- Vishal Jain and Dr. S. V. A. V. Prasad, "Analysis of RDBMS and Semantic Web Search in University System", International Journal of Engineering Sciences & Emerging Technologies (IJESET), Volume 7, Issue 2, October 2014, page no. 604-621 having ISSN No. 2231-6604.

- S. Balamurugan, K. Amarnath, J.Saravanan and S. Sangeeth Kumar, "Scheduling IoT on to the Cloud : A New Algorithm", European Journal of Applied Sciences 9 (5): 249-257, 2017.

- S.Balamurugan et.al., "Smart Healthcare: A New Paradigm", European Journal of Applied Sciences 9 (4), 212-218, 2017

- S Balamurugan, N Divyabharathi, K Jayashruthi, M Bowiya, RP Shermy, R Shanker, "Internet of agriculture: Applying IoT to improve food and farming technology," International Research Journal of Engineering and Technology (IRJET), Volume 3 issue 10, pp.713-719,e-ISSN: 2395 -0056, p-ISSN: 2395-0072, 2016