iJRASET
International Journal For Research in Applied Science and Engineering Technology

# INTERNATIONAL JOURNAL FOR RESEARCH

IN APPLIED SCIENCE & ENGINEERING TECHNOLOGY

**Volume:** 8 **Issue:** III **Month of publication:** March 2020

**DOI:** http://doi.org/10.22214/ijraset.2020.3186

www.ijraset.com

Call: 08813907089 | E-mail ID: ijraset@gmail.com

International Journal for Research in Applied Science & Engineering Technology (IJRASET)
*ISSN: 2321-9653; IC Value: 45.98; SJ Impact Factor: 7.429*
*Volume 8 Issue III Mar 2020- Available at www.ijraset.com*

# Bitcoin: Mystery, History and Background Innovative Technology Involved

Praveen Singh Rathore
*Senior Quantitative Analyst (Remote), Smart Forex Authorities.*

***Abstract: Bitcoin has been a renowned and most eminent cryptocurrency since it's inception in 2008. It is a hot topic of debate and created a lot of buzz in the financial world as well as the technology sector. Consequently there are critics as well as admirers of Bitcoin. There are many intricate features like Anonymity, Decentralization, Privacy, Peer to Peer network, Security and Robustness etc which led to the worldwide fame and exponential growth in price of Bitcoin. In this paper we will throw light on the complex features and technology behind Bitcoin. I have performed a comprehensive study of the Bitcoin. I have performed an exhaustive study on the Bitcoin price speculation and technology behind it and found it very interesting and innovative. In this research I will be evaluating all the complex features of the Bitcoin and present it in a limpid and intelligible way. I will try to clear all the buzz around the hype of the Bitcoin.***
***Keywords: Bitcoin, Cryptocurrency, Decentralized, Blockchain.***

## I. BACKGROUND AND HISTORY

The chain of events that followed the financial crisis of 2008 led to the Birth of cryptocurrency. The downfall of the banks, the massive decline in consumer wealth, along with the downturn of economic activity: all these factors led to an increased interest in decentralized currency. It was, as it seemed at that time, the answer to so many problems, like bank failures and collapses, which the usual monetary system, also known as fiat money, had failed to keep under control for so long. The 2008 was the year of the rise of Bitcoin. It all started when the infamous Satoshi Nakamoto published his paper on the Internet that talked about the peer-to-peer electronic cash system. Many people tried to uncover Satoshi Nakamoto's identity. However, their efforts were futile, as true name of the creator of Bitcoin remains unsolved mystery until these days. The concept of Bitcoin lies in its decentralized system. It is a digital currency that operates without a single administrator or a central bank, in other words, it does not need intermediaries, and it can be sent from user to user on the peer-to-peer Bitcoin block chain network. It is run using open-source software. As a response to the crisis of 2008, the pioneers of Bitcoin wanted to put the seller in charge, therefore eliminate the "middleman". They wanted to launch a monetary system that would focus primarily on transparent transactions. In simple words it is to let people control their own funds. Thus people would always be able to know where and for what cause their money went. The idea of Bitcoin was ideal for fighting corruption and cutting fees.

Bitcoin.org was officially registered on 18th August 2008. A whitepaper named "Bitcoin: A peer to peer Electronic Cash System" was penned or drafted by Satoshi Nakamoto. It's Link was posted to a cryptographic mailing list on 28th October 2008. Satoshi Nakamoto (Pseudoname) implemented the Bitcoin software as open source code and released it in January 2009. The Bitcoin Network was created on 3rd January 2009 when Satoshi Nakamoto mined the pioneer or the first block of the chain. This block is known as "Genesis Block".The Genesis block was hardcoded into the Bitcoin software with the newly created 50 BTC, which cannot be spent, due to the protocol and the set of rules made by Nakamoto written in the code. The very first Bitcoin transaction took place on 12th January, 2009 when Late Hal Finney received 10 Bitcoins from Nakamoto. After that Finney started mining blocks himself. Another important milestone was achieved on 5th October, 2009 when the New Standard set the first ever Bitcoin exchange rate against dollar which stood at $1 equal to 2300.03 Bitcoins. The first ever commercial transaction of Bitcoin took place on 22nd May 2010 when Laszlo Hanyecz bought two Papa John's pizzas for 10,000 BTC. This transaction took place between Laszlo Hanyecz and Jeremy Sturdivant (Nicknamed Jercos).

As it was earlier mentioned Bitcoin was created in the light of problems that were rising for decades, finally accumulating and bursting out in 2008 in a form of financial crisis. Historically speaking, virtual money has been in use of sedentary human civilization for a long time, before it was replaced by tangible types of alternatives, like coins following with paper money only to be supplanted by virtual money again. David Graeber, an American anthropologist, anarchist activist and an author, described this phenomenon as a series of long-cycles of money instruments and debt. It would be historically inaccurate to say that Bitcoin was the first virtual cash, as some vehicles existed before Bitcoin. However the mechanics behind them was not as nearly sophisticated as

that of the Bitcoin. There were digital currencies that incorporated the same concept as Bitcoin, such as proof-of-work and digital scarcity. Probably the earliest example of such currencies would be the issuer-based e-cash, created by Brands and Chaum. It had a proof-of-work scheme. Its algorithm was in hashcash, which later evolved into a reusable proof-of-work. B-money and Bit Gold, examples of cryptocurrencies that administered digital scarcity, were also predecessors of Bitcoin. Wei Dai and Hal Finney, creators of the mentioned above cryptocurrencies, have been thought to be the operators behind the pseudoname Satoshi Nakomoto, nevertheless both of them denied the claims. The Nakamoto's creation became a world phenomenon. It was a very successful project, the capital market of which reached 10 billion dollars in 2016. Nowadays the word cryptocurrencies is closely associated with Bitcoin. Cryptocurrencies are classified as a subset of digital currencies and alternative currencies. With the invention of Bitcoin, it became possible for two parties to transact electronically without the third party being involved. This innovation helped prevent double-spending. For a long time the double-spending was thought to be the problem that could be solved only be employing a third-party. Satoshi Nakomoto announced a solution for the problem. The Bitcoin is essentially an electronic cash. It allows for a quick and safe transfer of money, without a need of 'middle man's' involvement. Such transaction was possible due to smart use of peer-to-peer networking and proof-of-work systems, as well as cryptography. Bitcoin is based on the block chain, similar to PayPal's ledger. However, unlike ledger, Bitcoin is not controlled by central authority. It is a document, available to the public, and is distributed across nodes in Bitcoin network in a peer-to-peer fashion. Thanks to the Bitcoin's verifying the public ledger, it is possible to trace back any transactions that were made, even going as far as the creation of Bitcoin. This solution to double-spending brought another complication along the way and that is defrauding a block chain, as some malicious agents.

Since its inception Bitcoin has been split many times. This splitting is termed as Hard Fork technically. This splitting occurs when blochchain rules are changed and sharing of history of transaction history is done till a certain time. First notable hard fork occurred on 1st August 2017 splitting Bitcoin into two parts Bitcoin and Bitcoin cash. Other hard fork occurred on 24th October 2017 splitting each Bitcoin into 1 Bitcoin and 1 Bitcoin Gold.

### *A. Brief price history of Bitcoin*

Since its inception in 2009 Bitcoin has a very complex price action history. It is regarded as a highly volatile trading asset. In a very short span of time it has seen a lot of price action. Bitcoin has always remained the undisputed and most widely accepted leader in Crypto world. During the early days of adoption from January 2009 to March 2010 the price of Bitcoin was merely nothing as no buyers were found when a user named "SmokeTooMuch" auctioned 10,000 BTC for mere $50. First significant Milestone was achieved in March 2010 when BitcoinMarket.com (Now defunct) started operating as first Bitcoin exchange and the price was $0.003 for 1 BTC. In July 2010 Price of BTC skyrocketed from $0.008 to $0.08 in few days with almost 900% return. Another milestone was achieved on 9th February 2011 when Bitcoin took parity with US dollar. Since then high fluctuations have been seen in Bitcoin prices and it has never seen back $1 price again. Other significant milestone was achieved when first halving of Bitcoin rewads on 28th November 2012. The reward was halved to 25 Bitcoins from 50 Bitcoins. Bitcoin was gaining wider exposure throughout these years in both domains, good as well as bad. The first significant negative news impacting the Bitcoin directly was of shutting down of Silk Road website which dealt with black market transactions by Federal Authorities in October 2013. The federal Authorities seized over 26,000 Bitcoins. After this incident the price of Bitcoin crashed from $139 to $109 in a very short span of time. Between year 2011 and 2013 it has seen a steady growth with significant move coming in November 2013 when price rose from $350 to $1242. In February 2014, rumors of Mt.Gox being hacked began floating. Mt.Gox formally suspended Bitcoin trading that month after a series of large number of Bitcoin "thefts." In March 2014 Mt.Gox filed for bankruptcy citing with over $60 million of debts. It was declared that around 850,000 Bitcoins had been lost. After the debacle of Mt.Gox and controversy of Silk Road, another milestone was achieved on 11th December 2014 when Microsoft began accepting Bitcoin as a payment. Bitcoin appeared on the front page of renowned magazine The Economist on 31st October, 2015 marking another significant milestone. In the subsequent years the Bitcoin gained traction of Speculators and the price was trading in a range. On 9th July, 2016 the second halving of block rewards took place. The reward was halved to 12.5 Bitcoins from 25 Bitcoins. Beginning of the year 2017 marked the dawn of the biggest bull run for Bitcoin. The Price of the Bitcoin broke the previous high of $1242 in March 2017 and traded above $1250. Price of Bitcoin reached high of $3000 on 12th June 2017. On 2nd September 2017 price reached another milestone of $5000. Few weeks later China banned ICOs and cryptocurrency exchanges operations in the Mainland of China. Due to this the price of Bitcoin crashed down to $3000. After few weeks the Bitcoin started phenomenal Bull Run surpassing $10,000. The Bitcoin continued the bull run with launch of Bitcoin futures trading at the end of 2017. Two widely renowned future exchanges, the Chicago Board Options Exchange (Cboe) and the Chicago Mercantile Exchange (CME) started futures trading within a week of December 2017.The Price of Bitcoin reached all time high of $19783.06 on 17th December 2017. Since then the price of the Bitcoin

*ISSN: 2321-9653; IC Value: 45.98; SJ Impact Factor: 7.429*
*Volume 8 Issue III Mar 2020- Available at www.ijraset.com*

has been continuously decreasing with making a low of $3300 on 7th December 2018. On the contrary the volatility reached the record low in year 2018. Since then many debates are ongoing all throughout the world discussing about Bitcoin and other cryptocurrencies. The price of Bitcoin traded below $10,000 all throughout the year 2018 and 2019. Bitcoin regained the $10,000 mark on 8th February 2020. The closing price as of on 19th March 2020 is $5909.

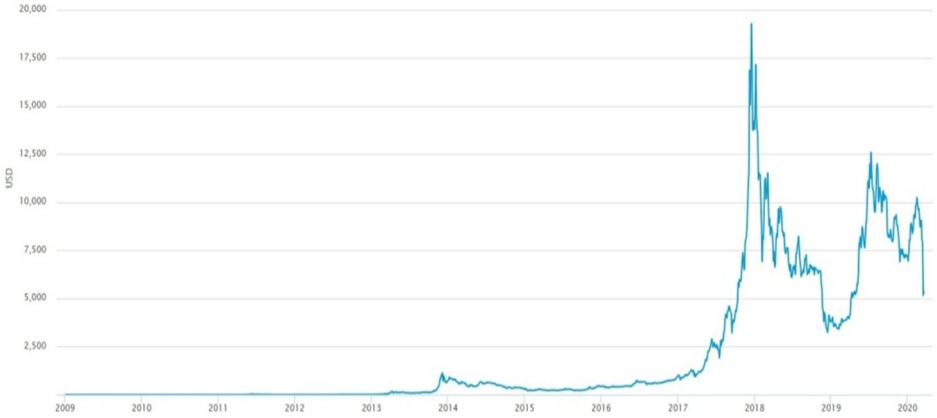



Figure1: Average USD market price across major Bitcoin exchanges.
Source: blockchain.com

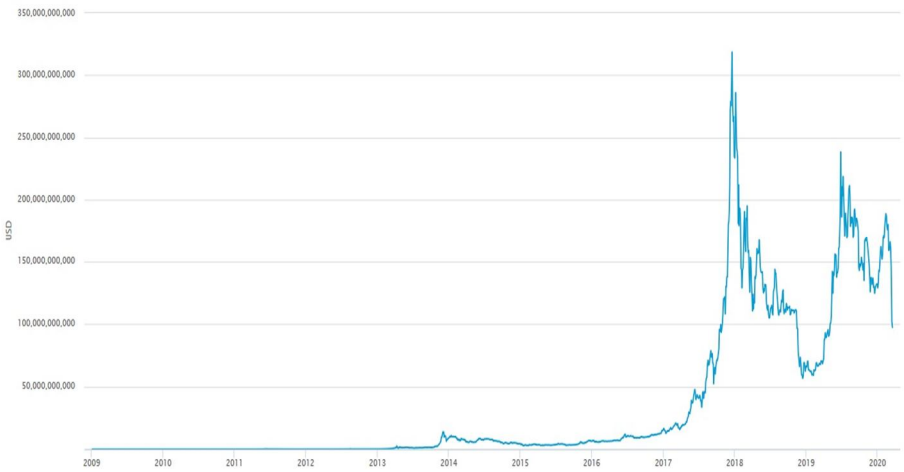



Figure2: Market Capitalization (The total USD value of bit coin supply in circulation, as calculated by the daily average market price across major exchanges).
Source: blockchain.com

*B. Technical Details behind Bitcoin*

Satoshi Nakamoto built Bitcoin on a blockchain that is also used by other cryptocurrencies. This technology is a list, which acts as an archive of all the records. These records are private, hard to hack and decentralized in nature. All users of the system have a copy of the blockchain that aid them to verify transactions that they made. Minors are the essential parties in the whole blockchain ecosystem. They can act as regular users as well as have a more specific function. They are users that play a key role in keeping the transactions operating well. The minor is responsible for building the blockchain of records which form the Bitcoin ledgers, which are called blocks. Each block contains various transactions that occurred over a specific period of time. Every 10 minutes a new block is added right after the transaction took place. What is worth noting is that the blockchain is transparent, meaning it is visible to the public, which in turn ensures the fair use of the system and secure transactions. Minors use a proof-of-work technology, while grouping the transactions in blocks. The PoW (Proof-of-Work) helps with confirming that the transaction is valid. Each block is linked to its predecessor by directing to a hash of the last block. A hash is said to be a function of converting an input of letters and numbers into an encrypted output of fixed length. In Bitcoin transactions, it is accepted to consider the longest chain to be the main chain.

*ISSN: 2321-9653; IC Value: 45.98; SJ Impact Factor: 7.429*
*Volume 8 Issue III Mar 2020- Available at www.ijraset.com*

The next crucial aspect of the technology behind Bitcoin operation is Bitcoin nodes, which built on a peer-to-peer basis. Generally speaking, the nodes are the people, the regular users of Bitcoin, who are connected in a form of net in the network. They are known as miners as they are solely responsible for validating the process of transaction in a blockchain. All of the nodes are equally important, however not all of them have the same function. For instance, a peer node can spend the Bitcoins by designing transactions and authenticate that other user's transactions are legitimate. Users that operate as full nodes need no less than 200GB to store the entire blockchain, starting from the first block to the most recent one. A full node is a channel, an agent that consolidates lightweight nodes and the Bitcoin Network. They are vital parties that help the decentralized system of Bitcoin keep going and working properly. In order to be transaction to be completely valid, every block should refer to the preceding block hash. The transaction can only take place when the hash is correct. If ever a hacker tries to attack the network and change information of any specific block, the hash of the block will also get changed or modified. The breach will be detected as there will be considerable difference between the modified hash and the original hash. This makes sure that the blockchain is immutable and unalterable. If any modifications or changes which are made to the chain of blocks will be noticed throughout the entire network and they can easily be detected.

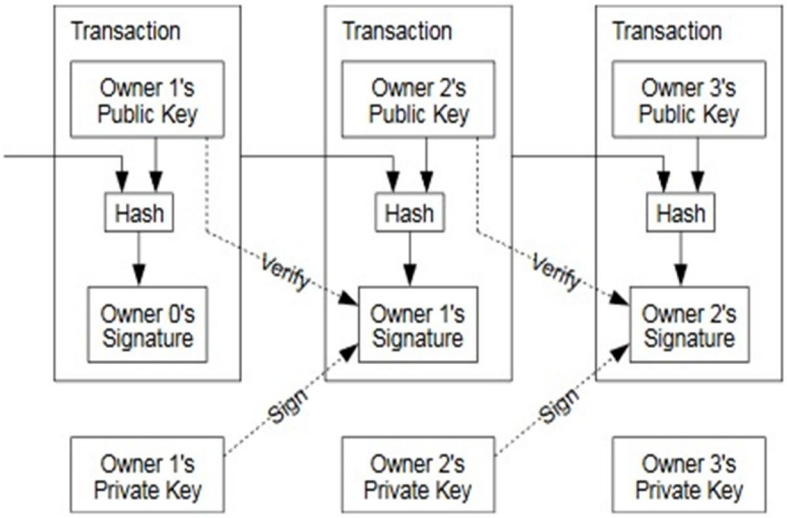



Figure3: Ownership Chain
Source: https://Bitcoin.org/Bitcoin.pdf

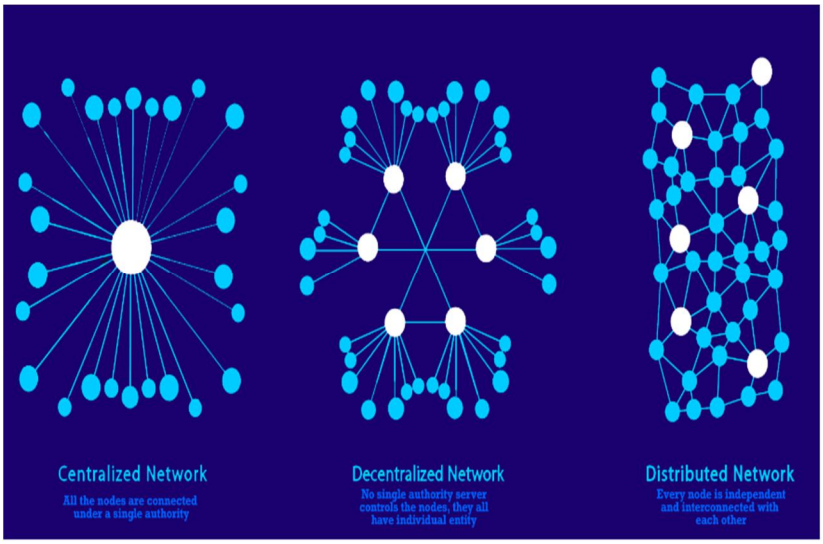



Figure4: Centralized vs. Decentralized vs. Distributed
Source: https://medium.com/@juliomacr/centralized-vs-decentralized-vs-distributed-a-quick-overview-1f3bd17b8468

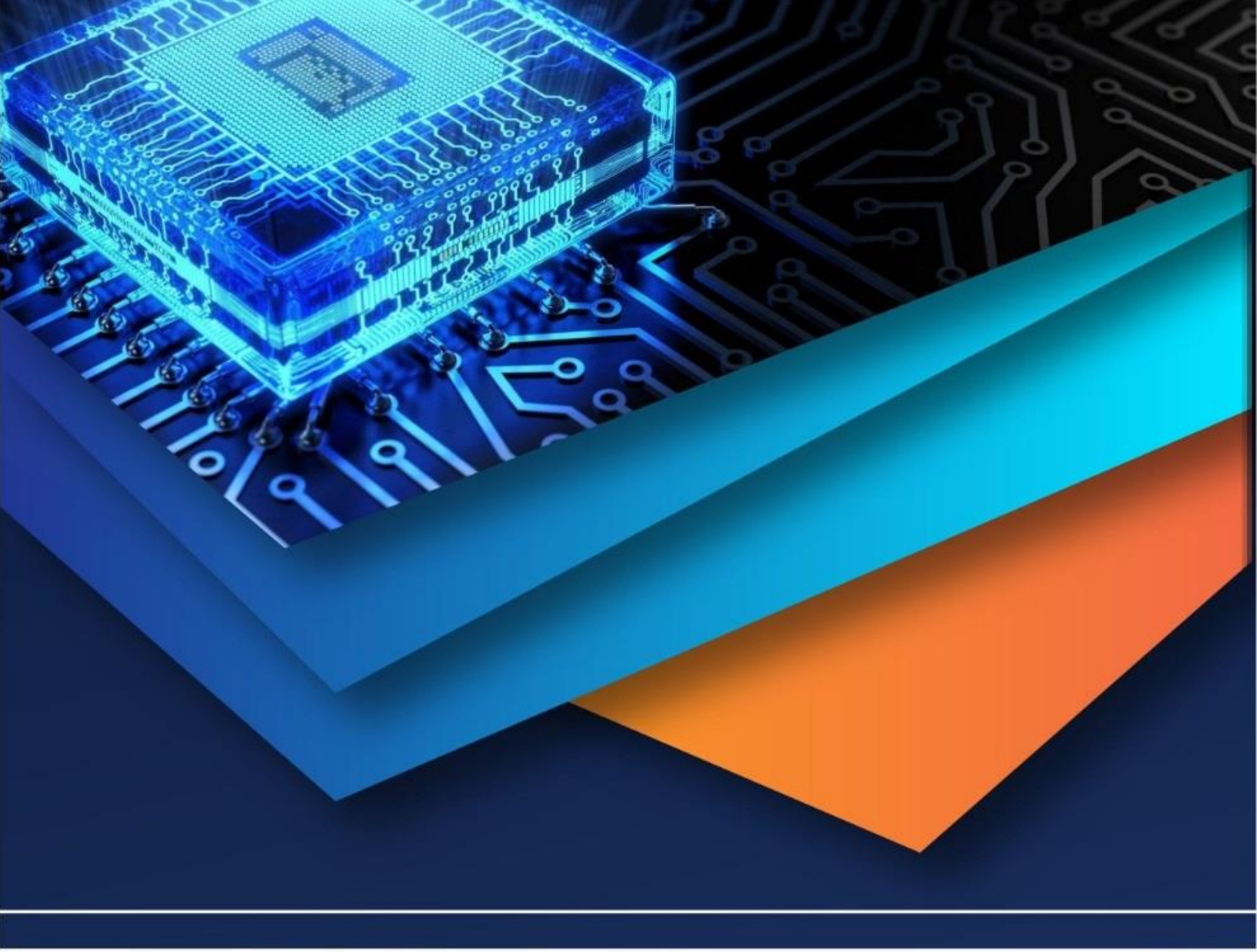
Bitcoin transactions are designed to facilitate the transfer of Bitcoin to a Bitcoin address. This address is a hash. Every user is a holder of a specific address that matches a matching private key. The address allows the user to transfer Bitcoins using a public key, thanks to the hash technology. Even though the public key can be visible to anyone, it is better to limit the exposure as much as possible for the one's safety. The private key should remain secret, as the Bitcoins with this type of key can be hacked and stolen.
The next three concepts that are vital to understand are wallet, digital signature and protocols. A wallet is a string of letters and number that form an address. The address appears in different blocks whenever a transaction occurs. This address is needed to conceal the identity of the sender/receiver. The only thing that is visible is the number of wallet that belongs to the corresponding person. Such address can also be called a public key. Digital signature is an essential part in performing a transaction. For carrying out the transaction, a person needs an address and a private key, which as previously mentioned, should be kept in secret. Whenever a sender wishes to send Bitcoins, make a transaction, he or she must sign with their private key. After a person signs a transaction, it is then sent to a blockchain network. Consequently the nodes do their work by checking the validity of the transaction. Cryptographic keys, the private and the public keys, are strings of bits that are used by an algorithm to transform text into cipher text. The keys use advanced mathematics that deals with prime numbers to design keys. Protocols are a large set of rules that are a central part to how a blockchain operates as a peer-to-peer, distributed information database. Such protocols work autonomously and make sure that the technology behind blockchain runs smoothly. In a nutshell, Blockchain allows nodes of the network to perform mathematical verification and consequently reach a consensus to agree on any particular value. Once the majority of the nodes reaches to a consensus, the block is time stamped and added to the exiting blockchain.

## II. CONCLUSION

The Bitcoin and the revolutionary technology of Blockchain holds a high potential of applications in diverse industries and sectors like Intellectual Property Protection, Identity Management, Government Elections, Smart Contracts, Remittances etc. Although few industries have already started adopting blockchain in their businesses, while many are still exploring the possible ways through which they can use the Blockchain. Bitcoin is gaining popularity among common masses. Bitcoin and Blockchain are not same. Cryptocurrencies are made using the Blockchain technology. In a nutshell Bitcoin is a form of electronic cash. In simple words Bicoin is a decentralized digital currency. It does not have a interference of Central Bank or Single administrator. Bitcoin can easily be send from one user to the another user using peer to peer Bitcoin blockchain network without a middleman. Bitcoin is a innovative way to transfer money with many key features like Reliability, Immutability, Irreversibility, Peer to Peer Network, Privacy, Divisibility, Pseudonymity and Limited supply etc. There are some problems which were highlighted from time to time are Hacking Accounts, High Volatility, and Transaction delays etc. On the contrary, Bitcoin is one of the most reliable and fast way of sending and receiving money. Although Regulatory bodies all around the world have not accepted Bitcoin as the legal currency while common masses are trading it widely for monetary gains as well as transfer of money.

## REFERENCES

[1] L. P. Nian and D. L. K. Chuen, "Handbook of digital currency," Academic Press, edition 1, 2015.
[2] Z. Zheng, S. Xie, H. Dai and H. Wang, "An overview of blockchain technology: Architecture, consensus, and future trends," IEEE International Congress on Big Data, 2017.
[3] S. Chen, H. Xu, D. Liu, B. Hu, and H. Wang, "The ABCs of Bitcoin," Research and Insights, Wilmington Trust, 2019.
[4] B. Albuquerque and M. Callado, "Understanding Bitcoins: Facts and Questions," Revista Brasileira de Economia, 2015.
[5] E. Dourado and J. Brito, "Cryptocurrency," The New Palgrave Dictionary of Economics, 2014.
[6] D. Graeber, "Debt: The First 5,000 Years," Melville House, 2012.
[7] Nakamoto, S., 2008. Bitcoin: a peer-to-peer electronic cash system. Retrieved from https://Bitcoin.org/Bitcoin.pdf
[8] Noelle Acheson, 26th January, 2018. Retrieved from https://www.coindesk.com/learn/Bitcoin-101/what-is-Bitcoin
[9] Gareth Jenkinson, 31st October, 2018, A Brief History of Bitcoin: 10 Years of Highs and Lows. Retrieved from https://cointelegraph.com/news/a-brief-history-of-Bitcoin-10-years-of-highs-and-lows
[10] Julio Marín, 31st January, 2019. Retrieved from https://medium.com/@juliomacr/centralized-vs-decentralized-vs-distributed-a-quick-overview-1f3bd17b8468
[11] Cointelegraph guides. Retrieved from https://cointelegraph.com/Bitcoin-for-beginners/how-blockchain-technology-works-guide-for-beginners
[12] Closing Price of 19th March, 2020. Retrived from https://cointelegraph.com/Bitcoin-price-index



10.22214/IJRASET

45.98

IMPACT FACTOR: 7.129

IMPACT FACTOR: 7.429

# INTERNATIONAL JOURNAL FOR RESEARCH

IN APPLIED SCIENCE & ENGINEERING TECHNOLOGY