Block-chain: The Boon for Bitcoin

[1]Mr.Kandy Arora, [2]Mr.AshishVerma, [3]Mr.Aarush Sharma, [4]Prof.Neelu
[1,2,3]Student, [4]Associate Professor
[1,2,3]Department of Electronics and Communication Engineering,[4]Department of Computer science Engineering, Manav Rachna University, Faridabad,India
***Email:**[1]arorakandy16@gmail.com, [2]akv0116@gmail.com, [3]aarushshrm9@gmail.com, [5]neelu@mru.edu.in*

DOI:https://doi.org/10.5281/zenodo.1465684

Abstract

The research paper deals with Bitcoin ,its mining and how mining actually works how Bitcoins are made, uses of Bitcoin why we should use Bitco in. Digital wallets for storing Bitcoins It also covers some of the biggest issues associated with Bitcoin like adecentralized currency covering the vast problem of Doublespending ininitial days of Bitcoin trading.The uses of Block-chain in Bit coin'stransaction to solve the problem of Double spending of Bitcoin.Applications of Block-chain other than crypto currency like in healthcare sector,reale state, voting, cyber security,it also covers sections by which we can make block-chain faster especially while buying crypto currencies and why SSDs should be preferred for Bloch-chain operations.

***Keywords**: Block chain,Doublespending,Cryptocurrency.*

INTRODUCTION

Bitcoin is a virtual currency (Electronic cash) which was launched by *Satoshi Nakamoto*.Called an alias because till date it is a mystery, that Satoshi Nakamoto was a person, an organization or a group of people. The bitcoin is a virtual currency since it is a decentralized currency it does not need any one in the between like a bank or some financial brokers. The only thing needed here is the internet which is available across the world and is accessible by everyone on the planet. The bitcoin is now widely renowned across the world with which you can buy anything near you or in the different continent. It is not wrong to call Bitcoin as father of all cryptocurrencies as it is the first currency.

Bitcoins can be used to buy and sell stuff across the world. So what's so fascinating us about them since we already know bitcoin is used as a virtual currency but our credit card can do the same. Huh? Well' no, we can pay from our credit card but our bank company has all the information that where have we used it and if we want to use the money anonymously then it would not be the helping. So, here bitcoin plays its role. With the help of bitcoin we can use our money. If we want to hire an assassin to kill our work buddy, there. The bitcoin will play its role. Just kidding, don'tdothat!!

For getting the bitcoin there's the term coined "Bitcoin Exchanges". Simply they are called the market placewhich helps people to find the stocks and other information that may help them to buy the bitcoin using different currencies. Currently the best among all and the biggest bitcoin exchange is Mt gox.[2]

The other method for getting the bitcoin is "Mining". First of all for mining you'll be needing a high end computer withall the high tech graphics and CPUs installed in it. Mining is generally, people use their computers to solve the math puzzles and they are in return awarded with the bitcoins. The current rate of the mining reward is 25 bitcoins in around 10 minutes.

The introduction, logic behind and the origin is done. So, technically it's the round that says where can we store it. It is impossible to store it in your wallet. So to keep the environment friendly they had named it "Digital Wallet". These digital wallets are either there in the cloud or in the user's computer. Yes there is one problem in that.

You don't have the encryptionfor your data. Unlike your bank the digital wallets are not secured by any kind of the FDIC security patterns. But not need to worry these data storages are not made to be hacked. If there was any kind of security then there will not be anonymity.

Yes, the digital wallets keeps your info completely anonymous although you will be needing a name and a general stuff for identification for the process for which you are using the bitcoin. But it would be completely impossible to trace a person. Therefore the bitcoin has become the new way for buying illegal items like drugs and ammunations.

HOW BITCOINS ARE MADE (IN DETAIL)

The methods of creating the bitcoins is the mining which are elaborated briefly now let's see how technically the bitcoins are made.

The mining purpose

Mining is creating the bitcoins while you are sitting in your house. But that holds the topic to be covered afterwards, first purpose of the bitcoin mining is to ensure that all the participants are getting enough view of their bitcoin data.

The bitcoins were made in this way that any person or the company in specific can not avail the benefit from the people who have invested their money in the bitcoin it does not involve any kind of the taxes or any other charges that may be out of the bitcoin prices. Since bitcoin is made for the peer to peer network, it has no central database that may have the information of the people having how many bitcoins. So to provide the real time access of the bitcoin data to it's user is the first priority of the bitcoin mining. So we have talked about the theoretical benefits of the bitcoin mining.

How mining works

So let's say you want the different hash value, but the hash function you are using, is limited to some extent, then you will not get the hash valuesof your own choices if you do, then you would have also written all the inputs again and would have waited for all the values, this task is very much difficult but once you find the value of the required hash function then it is very easy to verify the function.So to mine a bitcoin, first you need to collect the new transactions in a block, then you hash the block to form the256 bit block hash value in the up listed function. If the hash function starts with zeroes the block has mined and then it automatically get sent to the bitcoin network and that hash becomes the identifier for the block you have mined.

The thing here is that you cannot easily mine a block, most of the chances are that it won't work and you do it again and again for thousands of times. But for every ten minutes one has to do it and that block get sent to the bitcoin network and is successfully gets accepted.

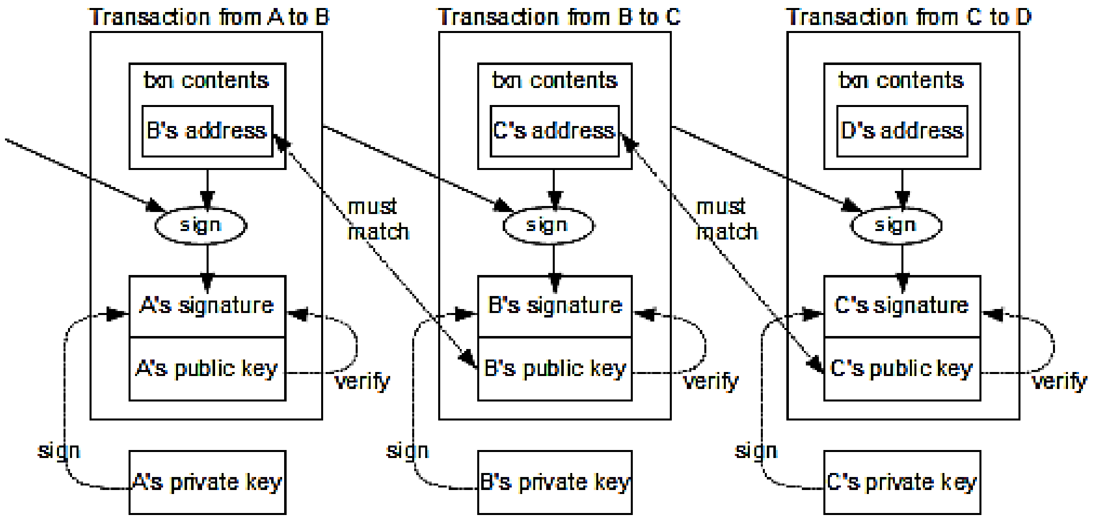

Fig: 1.*Bitcoin(Electronic Cash) Mining*

Block-chain

Block-chain is a decentralised system. It is a list of several records which is continuous The Block-chain are secured by using cryptography technique each mini block of aBlock-chain is an combination of three head ,first head contains a cryptographic hash of previous blockSecond head contains the data part whereas the head of Block-chain contains a timestamp. In 2008 Satoshi Nakamoto invented Block-chain to use in its Bitcoin cryptocurrency, Block-chain solved the problem of double- spending in bitcoin.

Double-spending problem

the value of currency decreases with relative to other monetary units in 2007 a number of ways were suggested to control problem of Double- spending .In 2009 the Bitcoin solves the problem of Double spending. Each transaction will be called valid if and only if it would be included in Block-chain this makes Double-spending almost difficult.

COMPARATIVE STUDY

Bitcoin is the first decentralised peer-to-peer and the most important cryptocurrency. Bitcoin purchases are different. User's purchases are not associated with its personal identity unless the user himself/herself publishes his/her transaction like cash purchases & can't be tracked back to him. In bitcoin the address which is generated for the user purchase changes with each transaction.

There are no sale taxes applied on any purchases. The foreign purchases involve fees and exchange cost. As bitcoin transactions are not done underany government involvement, so the cost of transaction is very low.

Application of block chain

CYBER SECURITY

By using Block-chain and cryptographic techniques the data can be sent across a network securely. If this technology is used around the world thenthe probability of hacking can be decreased. So, in the end the block chain network diminishes the digital theft problems by simply eliminating the human interference.

VOTING

During elections sanctioning of voter's identity is important. It requires highly secure network for keeping records of votes and to certify the winner.This technology can't be hacked so votes can't bechanged or removed.

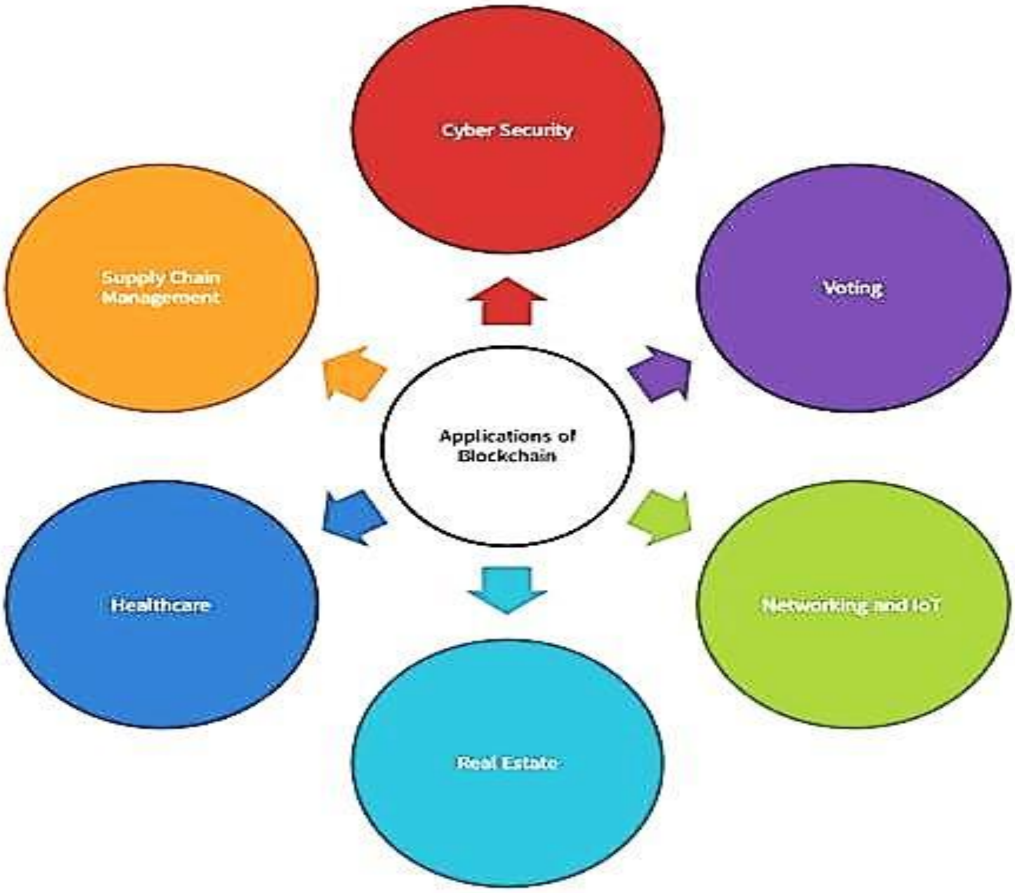

Fig: 2.*Application of Block chain*

NETWORKING & IOT

Block chain generation can be used as a medium for gadgets, which doesn't require any valuable hub for verbal exchange. By using the use of this we are able to talk variety of devices & manage software updates, insects without crucial manage gadget to discover each other.

REAL ESTATE

If there may be a distribution of real estate investment then the generated return budget will be moved from financial institution account to an account with the aid of account clearing house.

HEALTHCARE

There are so many healthcare establishments which are not capable of proportion records on-line throughout distinct structures. Block chains provide stepped forward facts cooperation between the providers. With the aid of using this we get more accurate diagnoses. This era is used by way of hospitals & worried healthcare companies to percentage the records on-line with none problem regarding integrity & information safety.

SUPPLY CHAIN MANAGEMENT

Supply chains are truly very complex nowadays. It needs for a charge between producer and customer. Contracts have to be held by using bankers and lawyer so it require a large amount of cash and time but Block-chain can remedy a variety of such problems because block-chain can be used for any sort of crypto change.

PROPOSED WORK/METHODOLOGY

So far we have discussed that Block-chain is a wonderful concept in every field but do we even realised that it also have some bad things which could be changed very easily example whenever we buy a bitcoin we gather all transaction information associated with that Bitcoin earlier from where its exchanges started it need a lot of disk space so here the data writing speed of our disk plays a major role so we should use SSD[5]disks for such purpose instead of traditional spinning disk as they are faster we can also make it much better by just increasing container density.

By using an IO profile which is most suited for our application in case storage provider provides this facility.

CONCLUSION

So here, it is the right stage to conclude,the increasing hype in the running stage of the block chain have many conditions that are required necessarily to proceed , so that the block chain methods are performed without any glitches. Whenever any good ideas are pressed into the business world like finance, energy and other sectors. Block-chain give them the boost which ultimately lead to the perfect performances by these business ventures. The data which is associated with the Block-chain is embedded inside the network as a complete part of itself, if we want to prioritize then we need to say it as an public the motive behind saying it as an persistent is that it is impossible to get it corrupted and working on it without the flaws, the altering of any particle of the information in the Block-chain world would mean consuming the massive amount of the digital power to revoke the complete network.

It is necessary to keep in mind that if we want the Block- chain to work perfectly, we need the node to node network or the nodule connections, This practice should be motivated and with the following mind-sets and those ethical standards, only after achieving these we are able to make Block-chain a powerful tool for improving all the uplisted bullet points that are business models, personal digital ventures and all the trade and the practices.

Block-Chain as the Boon for the Bitcoin

After this only the Block-chain can become the great tool to provide the best of the best facilities to the countries and it can also help us to get avenue to the people minds and making it the best and most used tool in the world for the betterment of the people and the planet.

REFERENCES

1. Satoshi Nakamoto, Bitcoin a peer to peer electronic cash system
2. www.BitcoinExchangeGuide.com
3. W. Feller, “An introduction to probability theory andapplications”,1957
4. Wikipedia
5. www.portworx.com, April 2018

Cite as:
Mr.Kandy Arora, Mr.Ashish Verma, Mr.Aarush Sharma, & Prof.Neelu. (2018). Block-chain: The Boon for Bitcoin. Journal of Embedded Systems and Processing, 3(3), 6–10. http://doi.org/10.5281/zenodo.1465684