International Journal for Research in Applied Science & Engineering Technology (IJRASET)
ISSN: 2321-9653; IC Value: 45.98; SJ Impact Factor: 6.887
Volume 6 Issue III, March 2018- Available at www.ijraset.com

Technology Behind the Success of Bitcoin

Sumitra Samal[1], Astha Tiwari[2], Shweta Sachdev[3]
[1]*Asst. Professor , Department of Computer Science & Engineering SSIPMT, CSVTU, Raipur, INDIA*
[2 3,] *B.E 8th Semester, Dept. of Computer Science & Engineering , Chhattisgarh, India.*

Abstract: ***Bit coin is a type of crypto currency and worldwide payment system. It allows system to work without a central bank or single administrator and the first decentralized digital currency. Bit coin was invented by an unknown person or group of people under the name Satoshi Nakamoto. The network is peer-to-peer and transactions between the users are direct which are verified by network nodes through the use of cryptography and recorded in a public distributed ledger which is replicated, shared and synchronized digital data called a block chain. Block chain is used as the core technology for the transaction of bit currency, as block chain uses the concept of public and private key. People might think that the lack of control could mean chaos, but this is not true at all because the technology (block chain) behind bit coin is one of the most accurate and secured ever created.***
Keywords: ***Block chain, decentralized digital currency, distributed ledger***

I. INTRODUCTION

The concept of bit coin was proposed by an unknown developer who identified himself as Satoshi Nakamoto. In 2009 paper that he put on his cryptography mailing list, Nakamoto[1] specified the concept and proof. He left the project in 2010 but the community grew exponentially thereafter. Bit coin owners use various websites to trade and buy goods or exchange it with other physical currencies. Bit coin is the most popular virtual currency in the world and it has grown in value in recent years. It was created in 2009 as a new of paying for

things that would not be subject to central banks that are capable of devaluing currency. The sustainability concerns about bit coin voiced by economists and environmentalists, stem from the process of "mining" that is central to its existence. To make complex calculations that verify transactions in bit coin, the miners use computers. This uses tremendous amount of energy via computers.

II. WORKING OF BITCOIN

Bit coin is one of the first digital currencies to facilitate instant payments using peer-to-peer[2] technology. They are virtual coins which are designed to be self-contained; for their value, with no need for banks to move and store the money. They behave like physical gold coins, once you own them: they possess value and trade just as if they were nuggets of gold in your pocket. You can use your bit coins to purchase goods and services online, or you can tuck them away and hope that their value increases over the years. "Miners" are the independent individuals and companies who own the governing computing power and participate in the Bit coin network. Miners are motivated as they are rewarded and transaction fees paid in bit coin. The decentralized authority (miners) enforcing the reliability of the Bit coin network. To maintain total supply of bit coins to approximately 21 million, new bit coins are being released to the miners at a fixed, but periodically declining rate. One bit coin is divisible to eight decimal places (100 millionth of one bit coin), and this smallest unit is referred to as a Satoshi. Bit coin could eventually be made divisible to even more decimal places, If necessary, and if the participating miners accept the change.

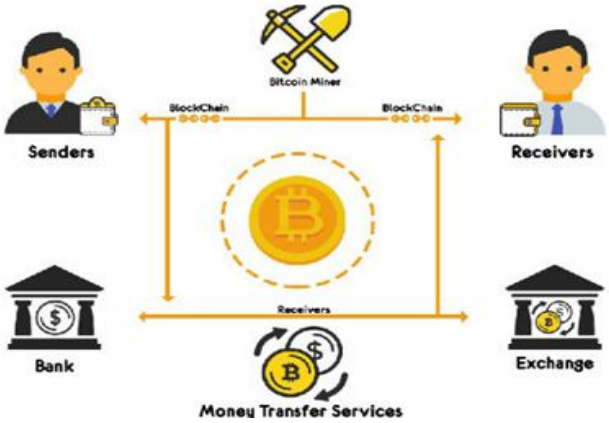

Figure 1: Working of bit coins source: https://bitcoinguider.in/what-bitcoin-how-generated-online/

Bit coin mining is the process through which bit coins are released to come into circulation. Basically, it involves solving a computationally difficult puzzle to discover a new block, which is added to the block chain, and receiving a reward in the form of few bit coins. The block reward was 50 new bit coins in 2009; it decreases every four years. As more and more bit coins are created, the difficulty of the mining process – that is, the amount of computing power involved – increases. The mining difficulty began at 1.0 with Bit coin's debut back in 2009; at the end of the year, it was only 1.18. The mining struggle began at 1.0 with Bit coin's premiere, which happens to be in 2009; at the end of the year, value was found to be only 1.18. Under the well know source, by April 2017, the mining struggle was beyond 4.24 billion.

III. TECHNOLOGY BEHIND BIT COIN

[3]The technology masking bit coin and other crypto currencies— Block chain - is a continually updated list of all transactions or a shared digital ledger. It is a de-centralized ledger which keeps a record of each transaction that occurs across a fully distributed or peer-to-peer network, which can be either public or private. Cryptography is the strength of block chain which helps in validating and chaining together blocks of transactions, making it nearly impossible to interfere with any individual transaction record without getting detected. Block -chain gives the guarantee of validation of a transaction as it records the transactions not only on a main register but on a connected distributed system of registers, all of which are connected through a secure validation mechanism. There is a constant growth as 'completed' blocks are added to it with a new set of recordings. These blocks are continuously added to the block chain in a linear and chronological order. Each node (computer connected to the Bit coin network using a client that performs the task of validating and transferring transactions) gets a copy of the block chain, which further gets downloaded automatically upon joining the bit coin network. The complete information about the addresses and their balances right from the source block to the most recently completed block are contained in the block chain. Once the transactions are completed, the block goes into the block chain as permanent database. A new block is generated, each time a block gets completed. There are countless number of such blocks in the block chain.

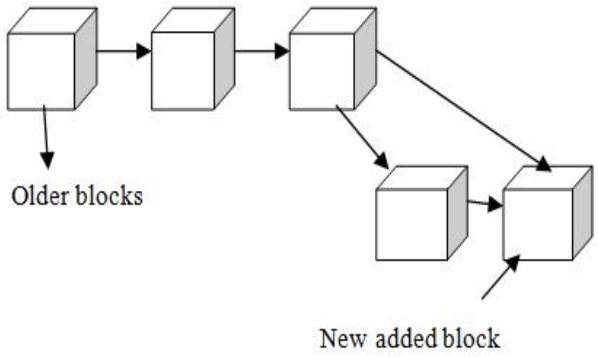

Figure 2: Represent Chain of Blocks in the Block chain source: http://www.jardcs.org/abstract.php?archiveid=2198

IV. WORKING OF BLOCK CHAIN

Bit coin solved the problem of double spending in transaction and later the concept of bit coin known as block chain. Block chain uses cryptographic concepts instead of the trusted of the third party for two willing parties to execute transaction s over the internet. Each transaction is equipped with digital signature. Each transaction is sent to the "public key" of the receiver digitally signed using the "private key" of the sender. In order to spend money, owner of the crypto currency needs to prove the ownership of the "private key". The digital signature is verified by the entity which received the digital currency on the transaction using the "public key" of the sender. To every node in the network, each transaction is broadcasted and then recorded in the public ledger after verification. Every single transaction has to through the verification for its validity before it is recorded in public ledger. Verification process should ensure two things before recording of any verified transaction. First spender should own the crypto currency- digital signature verification on the transaction. There should be sufficient crypto currency in second spender's account. The transactions are done in blocks which consists the information of the transaction including the hash code of the previous transactions, which is to be replicated in every node after verification. The transactions in one block are considered to have happened at the same time. In a

proper linear, chronological order with every block containing the hash of the previous block, these blocks are linked to each-other (like a chain). Unconfirmed transactions can be collected by any node in the network and these nodes can also create a block and then broadcast it to rest of the network as a suggestion as to which block should be the next one in the block chain. How does the network decide which block should be next in the block chain? At the same time, there can be multiple blocks created by different nodes. Since blocks can arrive at different orders at different points in the network, one can't rely on the order.

V. ADVANTAGES OF BLOCK CHAIN TECHNOLOGY

A. Transparency

Block chain technology is almost always open source this is one of the prime reasons block chain[5] is intriguing to businesses. There is an opportunity for other developers or users to modify it as they see fit. Alteration of logged data within a block chain is incredibly difficult, this is most important about it being open source. With countless eyes on the network, someone is probably going to see that logged data has been altered. This makes block chain a particularly secure technology.

B. Reduced transaction costs

Without the need for a third party, block chain allows peer-to-peer and business-to-business transactions to be completed, which is often a bank. They can actually reduce costs to the user or businesses over time, since there's no middleman involvement tied to block chain transactions.

C. Decentralization

Another central reason why block chain is exciting is that it doesn't have a central data hub. Block chain allows individual transactions to have their own proof of validity and the authorization to enforce those constraints, instead of running a massive data center and verifying transactions through that hub. With information on a particular block chain kept in pieces throughout the world on individual servers, it ensures that if this information fell into unwanted hands.

D. User-controlled networks

By the control aspect of block chain, crypto currency investors seem to be really encouraged., users and developers are the ones who get to call the shots, rather than having a third party run the show. For instance, an inability to reach an 80% consensus on an upgrade tied to bit coin's block chain is what necessitated a fork into two separate currencies more than four months ago.

VI. UPLIFTING FEATURES OF BIT-COIN

[4]Bit coins are not regulated by any government, nor created by any central bank - Accordingly, there are no bank keeping record of your money movement, government tax agencies and police cannot track your money. This is bound to change eventually, as unsupervised money is a real threat to government control, taxation, and policing. Indeed, bit coins have become a tool for illegal trade and money laundering, precisely because of the lack of government supervision. Large volumes of bit coins were being purchased by criminals, so the value of bit coins sky-rocketed in the past. Because there is no regulation, however, you can lose out immensely as a miner or investor.

Bit coins completely bypass banks - With no middleman bank to take a slice, bit coins are transferred via a peer-to-peer network between individuals. Banks and law enforcement cannot seize or freeze or audit bit coins. There is no spending and withdrawal limits imposed on bit coin wallets. Only and only bit coin wallet owner can decide how their wealth will be managed. This is really threatening to banks.

coins are changing how we store and spend our personal wealth - Since the advent of printed (and eventually virtual) money, the world has handed over the power of currency to a central government and various banks. Virtual money is printed by these banks, store our virtual money[6], move our virtual money, and charge us for their middleman services. By simply printing or conjuring more digits in their electronic ledgers, banks can satisfy there need of more currency. This system is easily abused and gamed by banks because paper money is essentially paper checks with a promise to have value, with no actual physical gold behind the scenes to back those promises. To put the control of personal wealth back into the hands of the individual, bit coins are designed. Instead of paper or virtual bank balances that promise to have value, Bit coins are actual packages of complex data that have value in themselves.

Bit coin transactions are irreversible - There are certain benefits when banks are involved like insurance and reversibility while using conventional payment methods such as credit card charge, bank draft, personal checks, or wire transfer. In the case of bit coins, the result is final, every time bit coins change hands and change wallets. Simultaneously, there is no insurance protection of your bit coin wallet: If you lose your wallet's hard drive data or even your wallet password, remember: your wallet's contents are gone forever.

VII. CONCLUSION

Bit coin is one of the first digital currencies. It is a crypto currency which was developed by Satoshi Nakamoto in 2009 as a new of paying for things that would not be subject to central banks that are capable of devaluing currency and the technology used in bit coin is block chain which is a distributed or peer-to-peer network keeping records of each transaction. Transactions between the users are direct which are verified through cryptography.

REFERENCES

[1] https://247cryptonews.com/bitcoin-news/
[2] https://www.investopedia.com/terms/b/bitcoin.asp
[3] http://www.jardcs.org/abstract.php?archiveid=2198
[4] https://sites.psu.edu/szpassion/2017/11/10/what-is-bitcoin- and-why-it-matters/
[5] https://www.lifewire.com/what-are-bitcoins-2483146
[6] https://en.wikipedia.org/wiki/Bitcoin