International Research Journal of Engineering and Technology (IRJET) e-ISSN: 2395 -0056
Volume: 04 Issue: 06 | June -2017 www.irjet.net p-ISSN: 2395-0072

INTRODUCTION OF BITCOIN WITH COMPARISON TO OTHER ALTERNATIVE COINS CALLED ALTCOIN

Rajeshwari Rawat[1], Nishi Tiku[2]

[1]Student, Dept. of Master of Computer Application, Vivekanand Education Society's Institute of Technology, Maharashtra, India
[2] Professor, Dept. of Master of Computer Application, Vivekanand Education Society's Institute of Technology, Maharashtra, India

---

Abstract - *"Bitcoin is the most important invention in the history of the world since the Internet" once said by Roger Ver a former politician and an early investor in Bitcoin related startups. A whole new economy is said be built on top of cryptocurrencies, and a whole new asset class is being born with these Bitcoins. One which no state government or bank can stop. These Bitcoin isn't attached to any state or government, so doesn't have a central issuing authority, which makes it more popular, fair and transparent thus easily available for everyone to use. All the transactions are tacked in a global database or ledger called blockchain. Apart from these Bitcoins there are various other alternative currencies called Altcoin that describes every single cryptocurrencies except for the Bitcoins. These coins attempt to improve on the ideas of what Bitcoin represents. Developer who wants to explore the boundaries of underlying blockchain technology goes for the development of Altcoin.*

Key Words: **Cryptocurrency, Blockchain, Bitcoin, Altcoin, Mining, Miners, Proof-of-work, Hash algorithm**

1. INTRODUCTION

Bitcoin was introduced in 2009, developed by Santoshi Nakamoto, who published the invention on 31st October 2008 in a research paper called "Bitcoin: A Peer-to-Peer Electronic Cash System" showcasing his thought of a very new cryptocurrency. Not very successful in early days, is currently the most widely used and known type of digital currency. Its market capitalization could grow to $1.75 trillion which would make each bitcoin worth $100,000 in next 10 years, according to Saxo Bank analyst Kay Van Petersen. Bitcoin is a digital asset outlined to work as a mode of exchange using cryptography to control its creation and management with no central issuing authority. There is no organization that decides when to make more bitcoin, figuring out how many to produce, or keeping track of where Bitcoins are. In 1999, Professor Milton Friedman, a Nobel Prize winner in economics stated "I think the internet is going to be one of the major forces for reducing the role of government. The one thing that's missing but will soon be developed is a reliable e-cash" nine years later, Bitcoin was born. Bitcoin is definitely the most well-known cryptocurrency but there are over 700 other cryptocurrencies termed as Altcoin, of these some are considered to be potential challengers to Bitcoins.

2. OBJECTIVE

[1] Introduction to the Bitcoin and how they actually work.

[2] Advantages of these Bitcoin available

[3] Introducing to the Altcoin available with few examples

[4]Comparing Bitcoin to the Altcoin

3. HOW BITCOIN WORK

3.1 Bitcoin Blockchain

This fully digital currency allows performing exchange between computers in a world-wide peer-to-peer network. Bitcoin is not just a string of data that can be duplicated; it is actually an entry on a huge global ledger called Blockchain. Thus, instead of a central authority a public ledger called Blockchain is used keeping record of every bitcoin transaction that has ever happened, as of 2016 complete ledger is about 107 GBs of data. So, each time we do bitcoin transaction, we are not sending a bunch of file instead writing exchange on the big ledger. Regardless of blockchain being a central record, there is no official group of people who update ledger. Anybody can volunteer to keep blockchain updated with new transaction. To add a block of transaction to chain, each person maintaining a ledger has to solve a special kind of math problem created by cryptographic hash function. This hash function is an algorithm that takes input of any size giving an output of fixed fix. Whoever is first to solve this hash function gets to

add next block of transaction to the blockchain, which then generates a new math hash function that needs to be solved.

Bitcoin uses SHA (Secure Hash Algorithm) 256 bit hash function. It is said to be one of the strongest hash function available, originally developed by United States national security agency. If multiple people make block at roughly the same time, the network picks one to keep building upon which, becomes longest and most trusted chain. A complete copy of a currency's Blockchain contains every transaction that is ever executed in the currency. With this detail, one can find out how much value belonged to each address at any point in history thus maintain record.

3.2 Processing: Bitcoin mining

It is a decentralized computational process that serves basically two purposes. Firstly, to confirms the transaction is processed in a trustful manner when enough computational power is devoted to blockchain, secondly, to create or issue new bitcoins into the blockchain. When a block of transaction is created, miners put it through a process. The process goes like this, they first validate the transactions are valid, and then bundles the transaction in a block. They then select the header of the most recent block and insert it into the new block as hash. The miners then solve the proof of work problem, after successful solution of proof of work is found, the new block is added to local blockchain and propagated to the network. This, is how the block is been added to the blockchain, adding transaction records to Bitcoin's public ledger of past transactions.

Primary purpose of mining is to allow Bitcoin nodes to reach a secure transaction of bitcoin, also a mechanism used to introduce Bitcoins into System. These miners are transactional fees as well as "subsidy" of newly created coins. When a new block is discovered, the discoverer or the miner is awarded with certain number of bitcoin, agreed upon everyone in the network.

There are some difficulties to these mining such as computationally-difficult problem because SHA-256 hash states that a block must start with zeroes, probability of calculating a hash that starts with many zeros is very low thus many attempts must be made to generate a new hash each round. Next is difficulty metric that is the measure of how difficult it is to find a new block. As, more miners join to mine the block, the rate of block creation will go up, as the rate of block generation goes up, the difficulty rises that will lead to pushing the rate of block creation back down.

3.3 Proof-Of-Work

It is usually very easy to produce a hash from a collection of data. Computers are really good at this. In order to make it difficult to avoid hashing of transaction blocks each second and bitcoins mined in minutes, bitcoin protocol deliberately makes it more difficult by introducing something called 'proof-of-work'. Proof of work demands that a block's hash has to look a certain way, won't just accept any old hash. As soon as a new piece of data is included, the hash generated will be totally different. It must have a certain number of zeroes at the start.

Thus, proof of work can be defined as the method to ensure that the information (new block) was difficult (costly, time consuming) to be made. More specifically as defined in Wikipedia A proof-of-work (POW) system (or protocol, or function) is an economic measure to deter denial of service attacks and other service such as spam on network by requiring some work from the service requester, usually meaning the processing time by a computer.

Thus, the overall process and the step that the bitcoin goes though as explained in [3] by the author is as follows:

1) Firstly new transactions are broadcasted to all the nodes.
2) Each node collects the new transactions into a block of blockchain
3) Each node works on finding a difficult proof-of-work for its block by solving the hash algorithm
4) After finding a proof-of-work, it broadcasts the block to all the available nodes
5) Only if all the transactions are valid and not already spend the nodes then accepts the block
6) A next block is the created into the blockchain, as the result of previous step this means the nodes has accepts the block, using the hash of the accepted block as the previous hash.

4. Security

Bitcoin would not exist without a little thing called cryptography, is also sometimes referred to as world's first cryptocurrency. Bitcoin are kept safe thanks to cryptography, consisting of keys, which are basically chunk of information that can be used to make mathematical guarantee about message indicating that it is actually from

the intended person. Bitcoin transaction is the transfer of value between Bitcoin wallets that gets included in blockchain, when we create an account on wallet, that account is linked to two unique keys – private key and public key.

Private Key takes some data and marks it by signing, providing a mathematical proof that they have come from owner of the wallet. The signature also prevents the transaction from being altered by some intruder once been issued. The signed private key is then send out to the bitcoin network and everyone can use of the public key to make sure sign checks out. This way all those keeping track of Bitcoins trading knows to add transaction to their copy of blockchain. In other words, if public key works that's a proof that data was signed by owner's private key. This proof of identity isn't something that can be faked. Thus, cryptography helps to achieve fundamental security concepts:

[1] **Confidentiality:** the information can be read or accessed by only intended receiver, avoiding the information to be understood by someone for whom it was unintended.

[2] Integrity: Information cannot be altered between the owner and the intended receipt of the data.

[3] **Authentication:** The owner and the receiver can confirm each other's identity thus, achieving authenticity on the identity.

5. Who controls the Bitcoin network?

Bitcoin is not controlled by any central authority or government, instead is controlled by all Bitcoin users all around the world. This makes it very powerful and more willing to use. Thus once quoted "Bitcoin will do to banks what email did to the postal industry" by Rick Falkvinge. Bitcoin has the appearance of being decentralized; these are controlled by the miners. As of June 1st, 2017 there are 16,366,257 BTC out of a total 21,000,000 BTC in theoretical supply, which has yet to be mined.

The limit of 21 million bitcoins is inherent in to the protocol, and there will never be more bitcoins than this. A block introduces 50 new coins into the bitcoin ecosystem. This quantity mined halves every 210,000 blocks. As of recent new the reward for mining a block was recently cut in half on July 9th, 2016 from 25 bitcoins to 12.5 bitcoins as reward for solving the problem. This halving event occurs every four years with the next one for 2020 with a block reward amount of 6.25 Bitcoins. We can observe the limit of coins mathematically as the summation of this geometric series as given below:

$$\sum_{n=0}^{\infty} \frac{210000 \times 50}{2^n} = 210000 \times 50 \times \frac{1}{1-\frac{1}{2}} = 21000000$$

Bitcoin has the property of volatility mainly due to the fact that there is a limited amount of coins and the demand for them increases by each passing day.

6. Bitcoin advantages

Following are listed some of the advantages that is observed in a bitcoin. These advantages are a good reason for the investors or anyone who would like to buy or sell Bitcoins.

It is decentralized. Most important feature of Bitcoin is decentralization meaning no one can take your Bitcoins away from you or freeze your account, due to the absence of body called a central regulating authority system. You own your money completely and have control on your transactions.

Your purchases are not taxed. Owing to absence of single central authority that would regulate Bitcoin transactions, there is absence of any tax on any Bitcoin transaction.

It is secure. Your payment information cannot be stolen away from you in any case. A Bitcoin transaction does not require any personal data to be submitted, thus protecting you from any kind identity theft. Sender cannot reverse his transaction which means fewer risks for merchants as well. General ledger called blockchain keeps all record of transaction securely also helping keeping track of all transaction performed.

It gives you privacy. Since no personal information is attached to your Bitcoin wallet, people do not know who purchased what achieving privacy. Also it is transparent, meaning that anyone can find information on addresses and their balances in a public ledger.

It is time-saving. It does not matter where you are and where you want to transfer your coins, with Bitcoin such transfer becomes close to instantaneous thus time consuming.

Zero or low transaction fees. Since there are no intermediate in Bitcoin network, no one will charge you for anything. There might be some fees for faster processing of transactions or conversion of bitcoins into fiat currency. Still, the costs are kept very low.

It is not subject to inflation. Bitcoin volume growth is predictable and number of Bitcoins to be ever issued is fixed limited to 21 million, so they cannot be churned out like fiat currencies and poured into economy.

7. Altcoin introduction

Altcoin as the name says are alternative currencies. It can be said that these are Bitcoin clones or alternative to Bitcoins. As of 11 July 2016 there were more than 710 cryptocurrencies available for trade in online markets and more than 740 in total but only a few dozen of them are successful to reach a market capitalization of above $10 million above as of early 2017. Altcoin seeks to improve on the idea Bitcoin represents, giving an option to trade or speculate if not on Bitcoin against fiat currency markets. The basic ideas behind development of Altcoin as researched through mainly are firstly, some developer want to explore the boundaries of underlying Blockchain technology, so rather than submitting their ideas to the bitcoin developers, they use the bitcoin code, change the name make some minor tweaks and then launch it as a brand new digital currency with their new add-on features thus introducing a brand new Altcoin into the market. Secondly, Bitcoin has a huge market capitalization in billions, and many businesses now rely on it, making too many changes could create problem for people making use of it thus in order to avoid this Altcoin are introduced.

There are many Altcoin introduced so far that have been able to make a better version of coin by incorporating feature such as anonymous transactions, turning completeness, better mining algorithms and many more. A special concern is concentrated on qualities such as stability, robustness and security which Bitcoin is able to achieve successfully. Further through this paper we introduce to some famous and successful Altcoin developed.

7.1 Litecoin

Most of these Altcoin do not survive for long duration with few exceptions. One of the exceptions is Litecoin, which was one of the first Altcoin developed. Apart from using a different hashing algorithm than Bitcoin, Litcoin is said to have a higher number of currency units. Litcoin announced in 2011 created by former Google engineer Charles Lee with a goal of being 'silver' to Bitcoin's 'gold'. The key difference for end-users being 2.5 minutes to generate a block as compared to Bitcoin's 10 minutes. Other important difference being Bitcoin using SHA-256 hashing algorithm over Litcoin using Scrypt algorithm, this algorithm incorporates the SHA-256 algorithm but with much more serialised calculations. Scrypt favours large amount of high-speed RAM thus known as 'memory hard problem'. When considered transaction, Litecoin handles a higher volume of transaction speed (or faster block time) and confirmation speed compared to Bitcoin because of its faster block generation. For instance in case of Litecoin a merchant who waited for a minimum of two confirmations would only need to wait five minutes as compared to ten minutes for just one confirmation in case of Bitcoin .

7.2 Ripple

Ripple is currently the third-largest cryptocurrency by market capitalization after Bitcoin and Ethereum. In many ways, Ripple as a currency is extremely similar to Bitcoin: a decentralised, maths-based currency with a finite number of units. One main difference in Ripple to Bitcoin is that they are not mined in the same way as Bitcoins. Instead, are created using a method called consensus, which requires "comparatively negligible computing power". 100 billion XRP or Ripple coins are expected to be created, but they are far cheaper than Bitcoins.

7.3 Namecoin

Namecoin is another Bitcoin that is created from modified Bitcoin software, and hence is quite similar to it. Like Bitcoin, it uses the SHA-256 algorithm; also it can be mined, up to a limit of 21 million like Bitcoin. However, it differs in one major aspect that they were not intended to be used as currency instead was developed as a decentralized DNS, right now, working as both a cryptocurrency and an alternative, decentralized DNS. Launched in 18th April 2011, Namecoin unlike Bitcoin can store data within its own blockchain transaction database. Namecoin is said to merge-mined with Bitcoin that is a node can mine for both Namecoin and Bitcoin simultaneously at the same rate that they would mine just one.

8. Comparison of the both

There are number of Altcoin all around each have their own individual characteristics and algorithms. These Altcoin are said to play a vital role in the cryptocurrency world, encouraging further decentralisation, innovation and competition apart from the available Bitcoins. Bitcoins are considered to be most well-known cryptocurrency with its developed infrastructure and growing fan base, where as different Altcoin trying to grow its popularity by incorporating new characteristics. Bitcoin and Litecoin is

limited in the amount of coins that will be produced, however there are other Altcoin such as Dogecoin and Peercoin that are inflationary with an indefinite creation of coins.

Market capitalization of Bitcoin is said to have the highest among all the cryptocurrency followed by other coins such as Ethereum, Ripple, Litecoin. All cryptocurrency are built on the protocol of being decentralized with difference being in the mining algorithm used to mine the block. Bitcoin are considered to take comparatively more transactional speed (block formation) than other Altcoins. Which means that transactions made using Altcoins such as Litecoin can be confirmed more quickly than in bitcoin. Some coins such as Peercoin distinguish itself from the Bitcoin by using "Proof-of-stake/ Proof-of-work" hybrid. Proof-of-stake requires less energy compared to Proof-of-work used in Bitcoin. Thus, is said to be sustainable and long-term environmental friendly as mining require less magnitude of power.

9. CONCLUSIONS

Having these Altcoin as an option along with Bitcoin would lead not just to innovation, but also ensure that it truly is best option out there. Otherwise, we end up with having only one cryptocurrency as an option. This would in result, give network too much power and if the core developers made changes that people didn't agree it would be more difficult. Having choice is freedom and allows people choose best option for the available cryptocurrencies and balance the power of this new internet money. All around the world, there are constantly new Altcoins being created, some are mere copies, but we sometimes see an Altcoin implement a completely unique and a revolutionary idea. These new ideas and innovations can then be sent upstream to more established coins such as Bitcoin and Litecoin. It can be said that Altcoins act as a test bed so that before these changes are implanted in more established coins the concept had already been proven to work without issues. It is important to have a proper understanding of Bitcoins well as the Altcoins available in order to buy, sell or perform any kind transactions with these cryptocurrency coins as pros and cons exists for all the coins.

REFERENCES

[1] http://www.coindesk.com/information/comparing-litecoin-bitcoin/
[2] https://www.linkedin.com/pulse/why-altcoins-just-important-bitcoin-derrick-alling
[3] https://bitcoin.org/bitcoin.pdf
[4] https://www.thebalance.com/altcoins-a-basic-guide-391206
[5] https://en.wikipedia.org/wiki/Bitcoin