Bitcoin: A Peer-to-Peer Electronic Cash System (Essay)

In this day and age of the digital era, most transactions are done via the Internet, these transactions or commerce are mostly established while depending upon other third-party institutions which are derived from the trust-based model. The system based upon the model otherwise works well but the model brings its innate infirmity which cannot be avoided at times. Other authentication methods like digital signature do provide a kind of relief to some extent but the principal problem like double spending which means to spend money more than once and hence the involvement of other financial institutions, making the authentication method like digital signature lose its main benefit. The urgency was to create an electronic payment method that does not depend upon trust but on cryptographic proof. This paper provides a resolution to the double-spending problem with the introduction of peer-to-peer distributed timestamp.

Bitcoin as we know is just the first implemented example of cryptocurrency, and this paper provides the details and description of what the computers are doing when it sends, receives, and creates cryptocurrencies. While understanding bitcoin it is essential to know how the transactions of the bitcoin works. Those transactions are put together in a collection called a block and the block forms one page of the ledger which is called the blockchain. The individual transactions that appear in a block are elucidated in this paper, but it is essential to know that bitcoins like cash or stocks do not exist. When we say we've got bitcoin (BTC) it means that the person's got a public key, and a unique private key that approves the bitcoin (BTC) previously sent to the above public key to be sent elsewhere. The private key must be kept secret and should not be shared with anyone unless sure. Bitcoins a little different in that sense because we never actually hold something like a token or a coin, instead we've got rights and the holder can transfer those rights. Unlike other transactions, in bitcoin we know who gave or sold those bitcoins; so, we could say there is always a connection before and when the payee wants to sell the bitcoins again. If we want to sell or send a specific number of bitcoins we must/have to be able to locate all the places and the blockchain is used as the record of the transactions between various bitcoin addresses. These transactions are upgraded and shared across the nodes as the increase or the decrease in balances goes on. To make it clear, we must understand that the total of the input transactions where, each input transaction could be in any amount not just one bitcoin (BTC) should be greater or equal to the output transactions. If not, then it is not a valid transaction and it would not be accepted by the blockchain

or peers evaluating the blockchain. The transaction fees which comes to place when any bitcoin is not accounted for explicitly are put into a block and whoever mines the block also gets hold of those rights to collect all the bitcoins in that block.

The blockchain was first intended to be used to securely order and validate but nowadays it is much more than that, being used to prove that a digital file existed at a certain point in time creating proof-of-existence. This is exactly the reason why and how the bitcoin (BTC) came to be used by many people as bitcoin is the most secure database available today. The miners altogether calculated over eighty billion SHA-256 hashes per second (the SHA-256 hashes are authentication and encryption protocols used for secured password hashing) and as the price is extremely high approximately fifty thousand dollars or more, to reverse a transaction with even confirmation would be really costly this ensures that the security is strong for transactions which are included in a block and are added to the toughest valid blockchain.

The creator of Bitcoin wanted to solve the problem of reversibility and that's when blockchain came to be and bitcoin came about when he wanted to solve the blockchain's incentive problem. The creator of bitcoin Nakamoto rendered an incentive to miners to protect the integrity of the chain and when even if the miners attempt to overthrow the integrity, they would also be overthrowing the value of the block reward throwing away the money and their investment. This is how the bitcoin makes sure that incentives line up between miners and users, the miners favor bitcoin cause of the high liquid digital assets and, implied promises of irreversibility are thus maintained. The paper also explains the calculations considering various scenarios of an attack, it explains the probability just in case an attacker catches up but honestly in my opinion it cannot just be explained in a few lines or words as it does include mathematical calculation and C code which is not that easy to grasp but all in all the creator Nakamoto explains in details about the decentralized cryptocurrency which he has delivered; in just a few pages through this paper.

In my opinion after reading the whitepaper and researching more about it through various sources the work done by the creator is astounding but it takes a lot of other aspects to understand how exactly bitcoin works thus making it an interesting but not an easy thing to learn. I have explained the basics, but it might still be difficult for a layman to understand from this essay cause not everything is explained detailly.

In conclusion, this paper explains how bitcoin ingeniously solves the problem of double-spending problem without being based on trust and the use of third parties or financial institutions. Bitcoin

cybersecurity branches from financial transactions being broken down into blocks that are almost impossible to infiltrate delivering bitcoins rights/funds from one place to another in a secure way. The way the nodes can include and exclude themselves at their will with the acceptance of proof-of-work chain as a proof of what happened while they were not there. The last line of the paper in the conclusion part tells us that there are more places for bitcoin to make it more future proof and since bitcoin has come this far even though as we know that new technology does suffer while being accepted into the mainstream the future for cryptocurrency looks better than ever.

References:

Paper: https://bitcoin.org/bitcoin.pdf

https://bitcoin.org/en/bitcoin-paper

Cited from:

Light, J. (2019, February 17). The problem bitcoin solves. Retrieved from https://medium.com/@lightcoin/the-problem-bitcoin-solves-8b3944ea77a7

The Cybersecurity for Cryptocurrency. (n.d.). Retrieved from https://www.business.att.com/learn/tech-advice/the-cybersecurity-side-of-cryptocurrency.html