What is Blockchain?

Author: Rohith Perumalla

Date: 9/4/17

Subject: Blockchain

Citations:

Mazonka, Oleg (2016-12-29). "Blockchain: Simple Explanation" (PDF). Journal of Reference.

Summary:

Blockchain is a new approach to a digital ledger that works by using hash chains and by following a strict set of guidelines. Hash chains are chunks of data that are connected using a hash function that ensures consistency between various data sizes. Each chunk carries a payload that cannot be changed unless the previous block’s payload is modified. Blockchain is the organization of these hash chains inside another hash chain. The main goal of Blockchain is to decentralize information and eliminate the chances of it being controlled or abused by a singular entity.

Analysis:

Blockchain is composed of 3 main core features: a distributed network architecture, hash functions, and public key cryptography.

Blockchain takes on a new approach to databases and digital ledgers by implementing a decentralized network which makes it more reliable and less prone to abuse. Traditionally networks and databases are set up in a centralized design. A centralized design has a central point which is prone to abuse by its owner and threatens the whole network's stability if attacked. A completely-decentralized network(distributed network) has the information distributed ensuring that no one entity can have more power than another. Distributed networks also have more redundant paths ensuring that information is always available in case a path is compromised.

Blockchain maintains the integrity of the information by implementing hash functions and combining them with public key cryptography. A hash function is a method of converting some data of a variable size to a predefined length called a hash. Hashes are put together to create hash functions, the fundamental building block of blockchains. Cryptographic hash functions are used to convert the data to secure hashes, some include MD5, SHA1, and SHA2. However cryptographic hashes are still created using some algorithm so if that algorithm is reversed the original data is revealed, so if these hash functions are cracked the integrity of the data is put at risk. To solve this issue blockchain uses public key cryptography.

Public key cryptography ensures that only one person can add information to the hash chain which combines with the cryptography of hash functions helps get the data to the point where it is theoretically impossible to crack. By using a public key and private key data is translated from point to point with a digital signature. The digital signature ensures that the previous owner was the one who made the addition to the chain maintaining the integrity of the chain. At any point, a new block is added to the chain but does not have the right digital signage it is automatically disregarded. Public key cryptography provides digital signage and combined with hash functions ensure the integrity of the whole chain of data.

For example, if there were 4 people: Adam, Rob, Steve, and Joe; all 4 of them were trading a pen and attached to the pen was a receipt showing previous transactions to make sure that apple isn't sold twice to different people. Adam starts off with the pen and sells it to Rob. At this moment in time on the receipt, there is Rob’s name saying he now owns it and also includes Adam’s signature indicating that Adam sold it to him. Then Rob goes to sell it to Steve; Steve checks the receipt and sees that Rob has it and Adam gave it to him because of the signature and knows that Rob is the rightful owner and has the right to resell it. Before the pen gets to Steve, Joe steals the pen and adds a receipt that says he now owns it. But under closer inspection, the authorities can see that Rob never signed the receipt handing it over to Joe so the receipt claiming Joe as the owner is invalidated. This whole scenario matches up with blockchain. The receipt has two parts: the current owner and the signature of the previous owner. The current owner is equivalent to the Public Key + Hash, and the signature of the previous owner is from the Private Key. The concept that only the owner can add to the block was demonstrated when Joe attempts to add his own information to the receipt when he didn't have the privileges and just as that part of the receipt is invalidated the blockchain disregards illegitimate additions to the chain.

What is Blockchain?

The blockchain is an innovative way to decentralize data eliminating the issues and concerns of centralized data while maintaining the integrity of data. By connecting hash chains within hash chains blockchain finds a balance between usability, simplicity, integrity, and authority. But even though these benefits are available it important to consider the negative effects of decentralizing data and using blockchain. Know your customer, anti-money laundering, and tax obligations may no longer be applicable. These negative effects apply to monetary tokens - tokens with other types of value will have different types of rules and regulations that will not be applicable. This lack of regulation may facilitate illegal activities and may pose many unforeseen issues. While blockchain is a new and innovative solution to keeping account of data, it is important to keep in sight the long and short term effects. Aside from that, blockchain seems as if it will successfully fulfill its purpose "to replace the central access point that can be controlled and possibly abused by a human."