History of block chain

Block chain was invented back in 2008 to serve as the public transaction ledger of the crypto currency bitcoin by a person using the name Satoshi Nakamoto whose identity is still unknown.

In 1991 (Haber & Stornetta, 1991) worked on a cryptographically secured chain of blocks, where they wanted to implement a system where documents timestamps could not be tampered with. An year later they incorporated merkle trees to the design, which improved its efficiency by allowing several document certificates to be collected in one block.

"A hash tree or Merkle tree is a tree in which every leaf node is labelled with the hash of a data block, and every non-leaf node is labelled with the cryptographic hash of the labels of its child nodes."

Introduction

If you have been following banking, investing, or crypto currency for the last ten years, then you must be familiars with "block chain". Basically, it is a record keeping technology (Fortney, 2019). Block chain is an incorruptible digital ledger of economic transactions that can be programmed to record both financial transactions and everything of value (Don & Alex, 2016). In simple terms, it is a time-stamped series of immutable record of data that is managed by cluster of computers not owed by a single entity. Each block of data is secured and bound to each other using a cryptographic principles.

When we say these words "block" and "chain" in these context it actually means that digital information which is the block stored in a public database which is the chain. Blocks on the block chain are made up of digital pieces of information. A single block can store up to 1MB of data. Therefore, a single block can house a few thousand transactions under one roof (Fortney, 2019). They are specifically have three parts:

1. Blocks store information about transactions. It stores the date, time and amount you have used for purchase.
2. Blocks stores information about individuals who take part in transactions. You can opt not to use your actual name, but your purchase is recorded using a unique digital signature such as a user name.

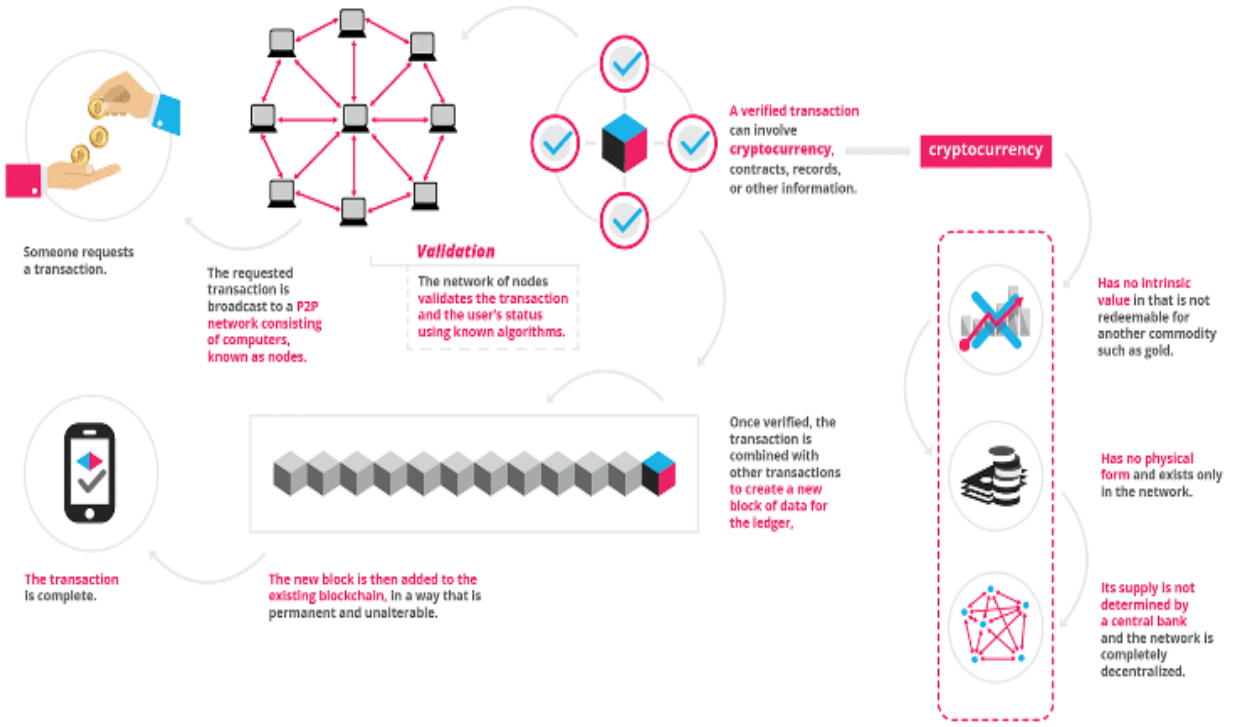
3. Blocks store information that differentiates then from other blocks. As people have names to distinguish us from each other, each block stores a unique code called “hash” that allows us to note it apart from every other block. This unique code gives the difference of different transactions.

Understanding the block chain technology

When a block stores new data it is stored into a block chain. As the name suggests, block chain consists of many blocks strung together. However, for a block to be added to the block chain four things must happen. They are:

I. A transaction must occur. An example is when you want to impulsively purchase goods. After hastily clicking through multiple checkout prompts, you will go against your better judgment and make a purchase.
II. The transaction must be verified. After making the purchase, the transaction must be verified. In public records of information, there is someone in charge of verifying data entries. However, with block chain that job is left up to a network of computers. These computers confirm the details of the purchase, including the transaction’s time, amount, and participants.
III. The transaction must be stored in a block. After your transaction has been verified, it gets a green light. The transaction’s amount and your digital signature are all stored in a block. There, it will join other transactions that are almost the same.
IV. That block must be given a hash. Once all of block’s transactions have been verified, it must be given a unique identifying code called a hash. The block is also given the hash of the most recent block added to the block chain. Once the block is hashed, it can be added to the block chain.

Once a block is added to the block chain, it becomes publicly available for anyone to view. You have access to transaction data, along with information about when, where, and by who the block was added to the block chain.

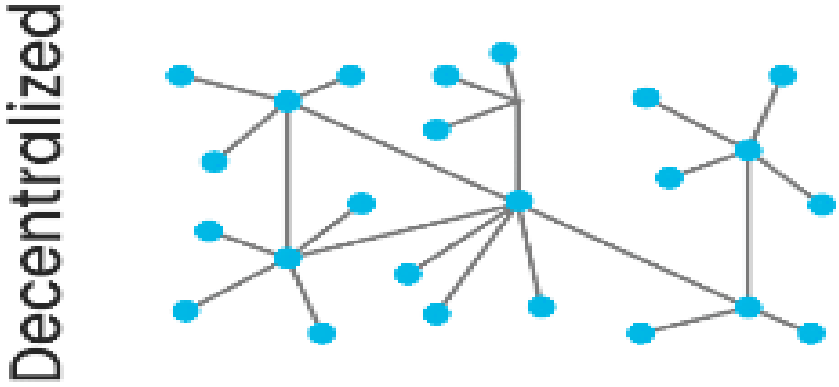


Pillars of Block chain Technology

There are three main properties of the block chain technology which has helped it gain a huge widespread. They are:

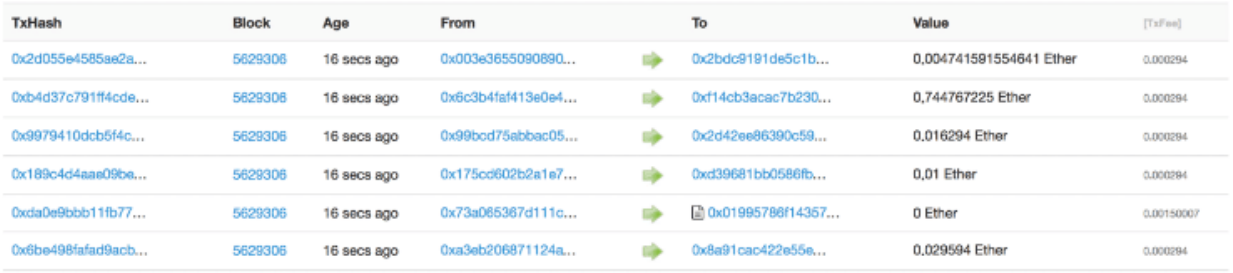
1. Decentralization

   A decentralized network gives you an opportunity to interact with your friend directly without going through a third party. This is the main ideology in block chain. A decentralized system's information is not stored by one single entity. Everyone in the network owns the information (Don & Alex, 2019).



2. Transparency

   A person's identity is hidden using complex cryptography and represented only by their public address. While the person's real identity is secure, you will still see all the transactions that were done by their public address.



TxHash	Block	Age	From		To	Value	[TxFee]
0x2d055e4585ae2a...	5629306	16 secs ago	0x003e3655090890...		0x2bdc9191de5c1b...	0.004741591554641 Ether	0.000294
0xb4d37c791ff4cde...	5629306	16 secs ago	0x6c3b4faf413e0e4...		0xf14cb3acac7b230...	0.744767225 Ether	0.000294
0x9979410dcb5f4c...	5629306	16 secs ago	0x99bcd75abbac05...		0x2d42ee86390c59...	0.016294 Ether	0.000294
0x189c4d4aae09be...	5629306	16 secs ago	0x175cd602b2a1e7...		0xd39681bb0586fb...	0.01 Ether	0.000294
0xda0e9bbb11fb77...	5629306	16 secs ago	0x73a065367d111c...		0x01995786f14357...	0 Ether	0.00150007
0x6be498fafad9acb...	5629306	16 secs ago	0xa3eb206871124a...		0x8a91cac422e55e...	0.029594 Ether	0.000294

3. Immutability

   In the context of the block chain, immutability means that once something has been entered into the block chain, it cannot be tampered with. Hashing means taking an input string of any length and giving out an output of a fixed length.

INPUT	HASH
Hi	3639EFCD08ABB273B1619E82E78C29A7DF02C1051B1820E99FC395DCAA3326B8
Welcome to blockgeeks. Glad to have you here.	53A53FC9E2A03F9B6E66D84BA701574CD9CF5F01FB498C41731881BCDC68A7C8

Advantages of block chain

- It is not owned by a single entity, hence it is decentralized
- The data is cryptographically stored inside
- The block chain is immutable, so no one can tamper with the data that is inside the block chain
- The block chain is transparent so one can track the data if they want

References

Don & Alex. (2016).What is block chain Technology? A Step-by-step guide for beginners. Retrieved from https://blockgeeks.com/guides/what-is-blockchain-technology/

Fortney, L. (2019). Block chain, Explained. Retrieved from https://www.investopedia.com/terms/b/blockchain.asp