[PDF Database Document] - BTCC Cryptocurrency Exchange

Original:
https://www.btcc.com/en-US/academy/crypto-basics/how-does-blockchain-work?_guides-for-blockchain

How Does Blockchain Work? Guides for Blockchain

Working Process of Blockchain

Blockchain is a combination of three important technologies – encryption key, point-to-point network and digital ledger. There are two types of encryption keys — private key and public key. Each person has these two keys, which are used to create a digital signature. This digital signature is a unique and secure digital identity reference, and it is also the most important aspect of blockchain technology. Each transaction is authorized by the owner's digital signature.

A transaction is authorized by mathematical verification in a peer-to-peer network. This peer-to-peer network is a huge group. As an authority, they reach a consensus on transactions and other issues.All these transactions are stored in a structure called a digital ledger. Generally speaking, the working principle of digital ledger is like a spreadsheet, which contains all the nodes in the network and has all the purchase history of each node. The information contained in the digital ledger is highly secure, and the digital signature ensures that it will not be tampered with. The most interesting thing about this ledger is that anyone can see the data, but no one can destroy it.

What is Public Distributed Ledger

Public distributed ledger is a collection of digital data, which is shared, synchronized around the multiple websites, countries and institutions. Now let's think that a blockchain that can be accessed by anyone in networks. If someone tries to change the data of one of the blocks, everyone in the network can see the change, because everyone in the network has a copy of the ledger. In this way, the data can be prevented from being tampered with.

Hash Encryption

The blockchain uses Cryptography to ensure that all data in the block is not accessed or changed without authorization. The blockchain uses SHA-256 for encryption,which is one of the strongest hash functions at present. This encrypted hash algorithm generates an almost unique 256 bit signature for a text. Blockchain also uses digital signatures to authenticate users.

Each user has a public and private key. The public key is used to uniquely identify the user, while the private key enables the user to access everything in the account. In the process of the sender,

the sender’s information passes through a hash function; Then, the output is passed through a signature algorithm , and the user’s digital signature is obtained. The user’s information, digital signature and public key are transmitted.

From receiver, the information are passes through an encryption function to get a hash value. The hash value is compared with the hash output obtained by bypassing the digital signature and public key by the verification function.

Structure of Each Block

As mentioned earlier, each block in the blockchain is encrypted with SHA-256 to ensure the security of data. Each block has four structure .

- Previous hash value – this field stores the hash value of the previous block in the blockchain
- Transaction details – this field includes information about several transactions
- Nonce – this field contains a random value (nonce value) whose sole purpose is to be a variable of hash value.
- Hash address – this field contains the unique identification of the block; It is a hexadecimal value composed of 64 characters, including letters and numbers, obtained by using SHA-256 algorithm.