The underlying logic and basic applications of blockchain

Michael Wu

With the popularity of electronic cryptocurrencies such as Bitcoin and the development of emerging Internet ecosystems such as web3, the discussion behind blockchain has become increasingly popular. This article integrates information from various sources from a beginner's perspective. You can learn about the underlying logic of blockchain through this article and better understand how blockchain profoundly affects the development of our society today.

A blockchain is a distributed database or ledger shared among a computer network's nodes. They are best known for their crucial role in cryptocurrency systems for maintaining a secure and decentralized record of transactions, but they are not limited to cryptocurrency uses.

Blockchain is a type of shared database that differs from a typical database in the way it stores information; blockchains store data in blocks linked together via cryptography.Different types of information can be stored on a blockchain, but the most common use for transactions has been as a ledger. In Bitcoin’s case, blockchain is decentralized so that no single person or group has control—instead, all users collectively retain control.

You might be familiar with spreadsheets or databases. A blockchain is somewhat similar because it is a database where information is entered and stored. But the key difference between a traditional database or spreadsheet and a blockchain is how the data is structured and accessed.(Vigna, P., & Casey, M. J. (2016)page3)

You might be familiar with spreadsheets or databases. A blockchain is somewhat similar because it is a database where information is entered and stored. But the key difference

between a traditional database or spreadsheet and a blockchain is how the data is structured and accessed.

The blockchain collects transaction information and enters it into a block, like a cell in a spreadsheet containing information. Once it is full, the information is run through an encryption algorithm, which creates a hexadecimal number called the hash.The hash is then entered into the following block header and encrypted with the other information in the block.

A blockchain allows the data in a database to be spread out among several network nodes—computers or devices running software for the blockchain—at various locations. This not only creates redundancy but maintains the fidelity of the data. For example, if someone tries to alter a record at one instance of the database, the other nodes would prevent it from happening.

A change in any data changes the hash of the block it was in. Because each block contains the previous block's hash, a change in one would change the following blocks. The network would reject an altered block because the hashes would not match.

At its core, blockchain technology represents not just a technological advancement, but a paradigm shift in how we conceive trust, transparency, and decentralization in the digital age. Thus, blockchain stands not only as a testament to human ingenuity but also as a beacon guiding us towards a more inclusive and empowered global society.

Reference

1. Drescher, D. (2017). Blockchain basics: A non-technical introduction in 25 steps. Apress.
2. Tapscott, D., & Tapscott, A. (2016). Blockchain revolution: How the technology behind bitcoin and other cryptocurrencies is changing the world. Portfolio/Penguin.
3. Antonopoulos, A. M. (2017). Mastering bitcoin: Unlocking digital cryptocurrencies. O'Reilly Media.
4. Vigna, P., & Casey, M. J. (2016). The age of cryptocurrency: How bitcoin and digital money are challenging the global economic order. Picador.

Instructor

Mr.Chu Han