MimbleWimble Blockchain: Everything You Need to Know

Original: https://www.btcc.com/en-US/academy/crypto-basics/mimblewimble-blockchain-everything-you-need-to-know

What is the Mimblewimble Blockchain?

Have you heard of mimblewimble? It is a new blockchain technology, which is sweeping the world. What on earth is it? Why is everyone so excited about it? In this guide, we will discuss everything about mimblewimble.

The mimblewimble blockchain is a new and upcoming blockchain technology with many exciting functions. It is designed to be extensible and privacy oriented. One of the main features of mimblewimble is its scalability. The blockchain can handle a large number of transactions without any problems. This makes it very suitable for commercial applications.

Mimblewimble has other features that make it a promising technology. It may completely change the way we use blockchain technology. We can expect to see more applications of mimblewimble in the future.

The History of Mimblewimble

The history of mimblewimble can be traced back to july2016, when an anonymous author published a paper proposing the protocol. The author is a Cryptologist or Bitcoin expert. His name is “Tom Elvis jedusor”, which is the French name of Voldemort in Harry Potter.

Although it is not confirmed that Tom Elvis jedusor is indeed the creator of mimblewimble, the proposal has the same characteristics as the villains in the Harry Potter series. For example, both have incredible privacy and both have the ability to avoid detection. Maybe jedusor is just a fan of the Harry Potter series. So he decided to name his proposal after one of the villains, but there was no way to be sure.

In December 2016, there was growing interest in mimblewimble, when a new cryptocurrency grin (GRIN) using the protocol was being developed. Since then, developers have been studying proposals to support smart contracts to the protocol.

In August 2017, blockstream released a white paper detailing how mimblewimble was used to create a new blockchain called "bullet proof". Bulletproofs is a new type of cryptography, which can improve the privacy and security of Bitcoin (BTC).

In October 2017, blockstream launched an experimental grin network using the mimblewimble protocol. Grin is a completely decentralized cryptocurrency without any central authority. In February 2018, Peter Todd, the famous Bitcoin developer, released a proposal on adding support for smart contracts in mimblewimble. The proposal calls for a scripting language called "elixir".

In may2018, Andrew poelstra, a mathematician of blockstream, delivered a speech on mimblewimble at the scaling Bitcoin conference of Stanford University. The speech discussed how mimblewimble created a new blockchain called "confidential transaction", which is a new encryption technology that can improve the privacy of Bitcoin transactions.

In November2018, green announced that it would launch the second test network in january2019 to test a new transaction type – confidential transaction. This new encryption technology improves the privacy of Bitcoin transactions.

Comparison Between Mimblewimble and Bitcoin

There are several features that make mimblewimble stand out from Bitcoin. First, its blockchain is much smaller. The mimblewimble transaction is more effective than the TCD transaction, so the blockchain does not need to store so much data. This makes it faster and more scalable.

Second, mimblewimble is safer. It uses a different hash algorithm, called Elliptic Curve Cryptography (ECC), which is more difficult to crack than the hash algorithm used in Bitcoin. Finally, mimblewimble provides privacy features that Bitcoin does not have. All transaction data is hidden, so people can't see where your money is spent. This may make it attractive to criminals or people who want to keep their financial transactions private.

Despite these advantages, mimblewimble has some potential disadvantages. For example, it is not as well known as Bitcoin, so it may not be adopted by merchants and users. In addition, since all transaction data are hidden, it may be difficult to trace criminals who use mimblewimble for illegal activities.

In general, mimblewimble is a promising cryptocurrency with several advantages over Bitcoin. With its smaller blockchain scale, faster speed and stronger security, it can become a major role in the digital currency world.

Merits and Demerits

Mimblewimble has both advantages and disadvantages. Some of these advantages include privacy, scalability, and replaceability. In terms of privacy, it is difficult to track transactions on the blockchain because they are hidden in confidential transactions. Scalability is another advantage because the mimblewimble can process many transactions per second. Variability is an important feature of digital currency, because it means that all coins are equal and interchangeable. This is important because it prevents some coins from being blacklisted.

Some of the disadvantages of mimblewimble include that it is still under development and has not yet been implemented. People also lack understanding of its working principle, which makes it difficult for people and enterprises to adopt it.

Mimblewimble is still under development, so it is too early to say whether its advantages outweigh its disadvantages. However, its privacy, scalability and replaceability are very important, and may have a great impact in the field of digital currency. It will be interesting to see how mimblewimble has developed and whether it can realize its potential.

Conclusion

Mimblewimble is a new cryptocurrency protocol. Compared with traditional blockchain, it has many advantages, including increased privacy and security, fast transaction and low cost. Although it is still under development, there is no doubt that this technology has the potential to change the way we use cryptocurrency.