PUBLIC VS PRIVATE BLOCKCHAINS: WHAT'S THE DIFFERENCE?

Blockchain, the underlying technology behind cryptocurrencies like Bitcoin, is quickly gaining popularity in the digital space. More and more companies are recognizing its revolutionary potential and are choosing to adopt this new technology for their daily operations, making blockchain less of a buzzword and more of a forward-thinking mantra.

In short, a blockchain is a continuously growing list of public records broken up into "blocks" based on specific windows of time. A community of users controls how this information is edited and updated, and all blocks are chained together chronologically.

While more organizations are becoming aware of the applications for blockchain in the enterprise, there is less familiarity with the differences between public and private blockchains.

The Similarities of Public and Private Blockchains

Before we touch on the differences, it is important to understand the similarities between public and private blockchains. Both of them:

- Are decentralized peer-to-peer networks built on a community of users, meaning that no one entity (like a bank or broker) is in charge of authorizing transactions
- Rely on numerous users to authenticate edits to the distributed ledger, thereby creating a new master copy that is accessible to everyone at all times
- Are completely immutable, meaning the verified block can never be erased or modified once it is authenticated by users

So, how are they different?

Public Blockchain

Public blockchain is the model of Bitcoin, Ethereum, and Litecoin and is essentially considered to be the original distributed ledger structure.

This type of blockchain is completely open and anyone can join and participate in the network. It can receive and send transactions from anybody in the world, and can also be audited by anyone who is in the system.

Each node (a computer connected to the network) has as much transmission and power as any other, making public blockchains not only decentralized, but fully distributed, as well.

In order for a transaction to be considered valid, it must be authorized by each of its constituent nodes through the consensus process. Once this authorization takes place, the record is added to the chain. Public blockchains typically have incentives to encourage people to join the network as well as to authenticate transactions.

One of the biggest disadvantages of a public blockchain is its complete openness. This type of transparency implies little to no privacy for transactions and supports a weak concept of security. Another drawback is the substantial amount of computing power that is necessary for the maintenance of the ledger. With so many nodes and transactions as part of the network, this type of scale requires extensive effort to achieve consensus.

Private Blockchain

Private blockchains, on the other hand, are essentially forks of the originator but are deployed in what is called a permissioned manner.

In order to gain access to a private blockchain network, one must be invited and then validated by either the network starter or by specific rules that were put into place by the network starter. Once the invitation is accepted, the new entity can contribute to the maintenance of the blockchain in the customary manner. Due to the fact that the blockchain is on a closed network, it offers the benefits of the technology but not necessarily the distributed characteristics of the public blockchain. The extent to which the entity can view or validate transactions is up to the network starter to determine.

A typical way for enterprises to use private blockchains is intrabusiness, ensuring that only company members have access. This is a useful business solution if there is no reason anyone outside of the company should be part of the chain as data can be restricted to certain individuals on a need-to-know basis. With fewer people as part of the chain, they are typically quicker and more efficient with an easier consensus process.

While this sort of structure may not be entirely different from older digital structures as the public blockchain is, the technology is still highly powerful and the strong cryptography and auditability offers more security than traditional protocols.

Public vs Private Blockchain- What to Choose?

Whether organizations choose to turn to the more established public blockchains, or rest assured with higher security measures for private ones, the potential of blockchain technology for

enterprises is still wildly untapped.

As security measures for public blockchains become stronger, their value will further increase, making the use of private blockchains less essential. However, when it comes to having more control and the ability to restrict access to specific individuals, private blockchains can't be beat. In the end, the choice of whether to use a public or private blockchain for business lies with each organization that utilizes it.