What Makes A Blockchain Secure?

What Makes A Blockchain Secure?

A Blockchain is defined as a system in which a record of transactions made in Bitcoin or another cryptocurrency is maintained across several computers that are linked in a peer-to-peer network. One key difference between a typical database and a Blockchain is the way the data is structured.

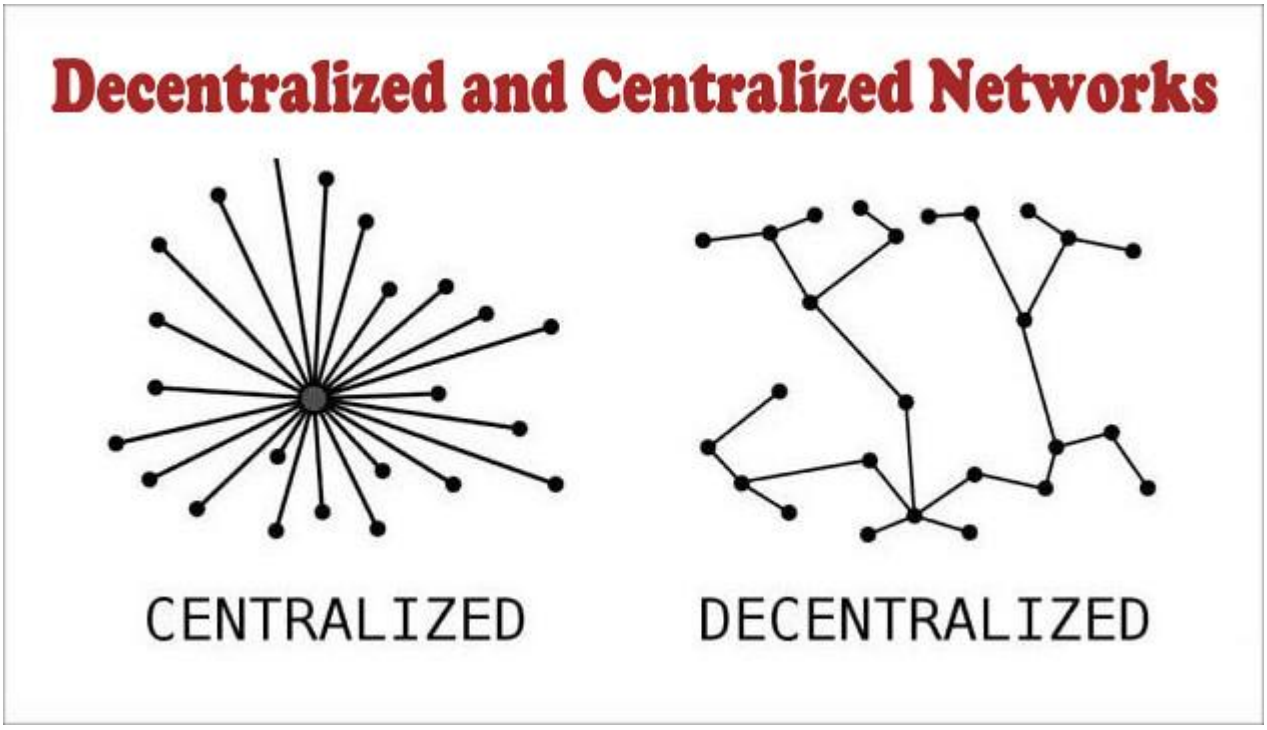
In a Blockchain, information is stored together in groups, also known as blocks. Each block has a finite capacity, and when filled, is 'chained' to the previous block, thereby giving rise to its unique name. Through this chain, each block is connected to every other block ahead of and behind it.

Blockchain's unprecedented integrity is dependent on the principles of cryptography, consensus, and decentralization, which deepen trust in transactions. The integrity in the transactions of Blockchain technology has attracted companies and governments to it, especially in spaces where security and immutability are of the utmost importance.

Here are 4 features that makes a Blockchain secure:

Decentralized Network

What Makes A Blockchain Secure?



This is a unique feature of Blockchain. Blockchain is not contained or controlled in one central location. Hence, they don't have a single source of vulnerability and are unalterable from one computer. With the requirement of a vast amount of computing capacity to reach all instances of a particular Blockchain and change them all at once, its decentralized nature makes attacks highly improbable.

Cryptography Effect

Cryptography is a system of transmitting and storing data in a specific form so that only the target recipients can process and read it. It not only prevents data alteration or theft, but is also be useful in user authentication. Cryptography is the bedrock of the security of Blockchain technology.

The hashing functions of cryptography are of primary significance. Hashing is known in the cryptocurrency world as a system where an algorithm (known as hash function) receives a data input of any size and returns output (known as a hash) containing a fixed and predictable size.

The hash (the output) always presents a similar length irrespective of the input size. The content of the output will be different if the input changes. Conversely, where the input is unchanged, the output (hash) remains unchanged as well, regardless of how many times the hash function is run. The hash (output) is sorely dependent on the input.

What Makes A Blockchain Secure?

Hashes are applied as peculiar identifiers in data blocks within Blockchains. A block's hash is developed in relation to a previous block's hash, thereby creating a chain of connected blocks. The data in a block determines the block hash, which implies that any alteration of the data will alter the same block hash.

Furthermore, a block's hash is developed based on the data of the block and the previous block's hash. It is these hash identifiers that play a significant role in guaranteeing Blockchain security and validating transactions.

Consensus

A consensus mechanism is a fault-tolerant mechanism that is used in computer and Blockchain systems to approve of the actual condition of a network, such as with cryptocurrencies. Since public Blockchains operate without the oversight of a centralized authority, they are required to be self-regulating systems that involves contribution from a large number of participants working on verification and authentication of any transaction occurring on the network.

To ensure the security of the network, these participants need to agree on a 'consensus' on the status of the network. This is achieved through a consensus mechanism, which defines a set of rules that decides on how the Blockchain should operate. There are different kinds of consensus mechanism algorithms which work on different principles, with varying advantages and disadvantages.

Immutability

Immutability is a feature of Blockchain which makes it possible for it to prevent changes to confirmed transactions. These transactions are not only cryptocurrency-related; non-financial digital data transactions are also included.

Immutability ensures the veracity of transaction records and data after a new data block is confirmed valid, as each block of information proceed using a cryptographic principle or a hash value. Changing the content within each block would alter the hash value, which makes it very obvious to the network's participants that an error or attack has occurred. Such a feature ensures that the data within the Blockchain network cannot be easily changed without detection.

What Makes A Blockchain Secure?

Conclusion

Blockchain has been observed to safely conduct and hold transaction records with an astonishing level of integrity and security. Exclusive features of decentralization, cryptography base, consensus, and immutability, among others, have definitely defined and concretized the security of Blockchain.