Java Blockchains

EFTHIMIOS ALEPIS

Blockchain: a decentralized ledger of information

Blocks of data connected through the use of cryptography

Belongs to a network of nodes connected over the public network

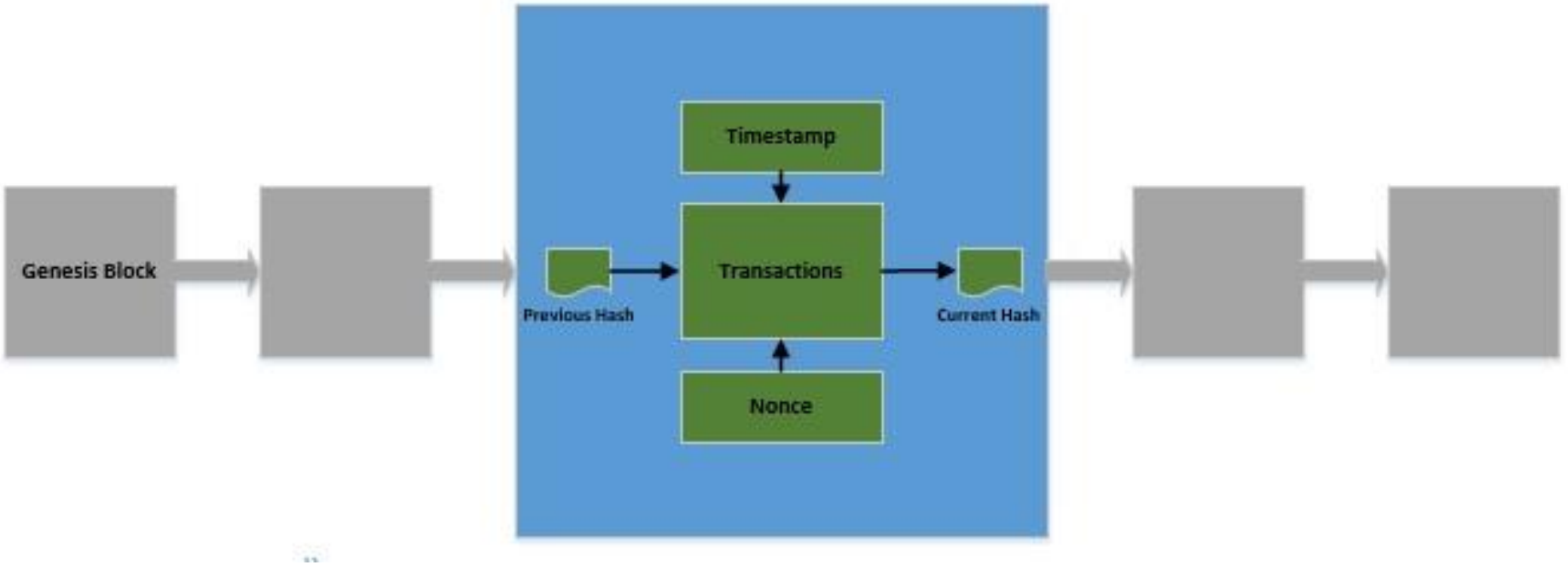
Blockchain important attributes

Data as part of a block is tamper-proof. Every block is referenced by a cryptographic digest, commonly known as a hash, making the block tamper-proof.

Blockchain is completely decentralized across the network. This means that there is no master node, and every node in the network has the same copy.

Offers **transparency** since every node participating in the network validates and adds a new block to its chain through consensus with other nodes. Hence, every node has complete visibility of the data.

Blockchain blocks



Mining a block

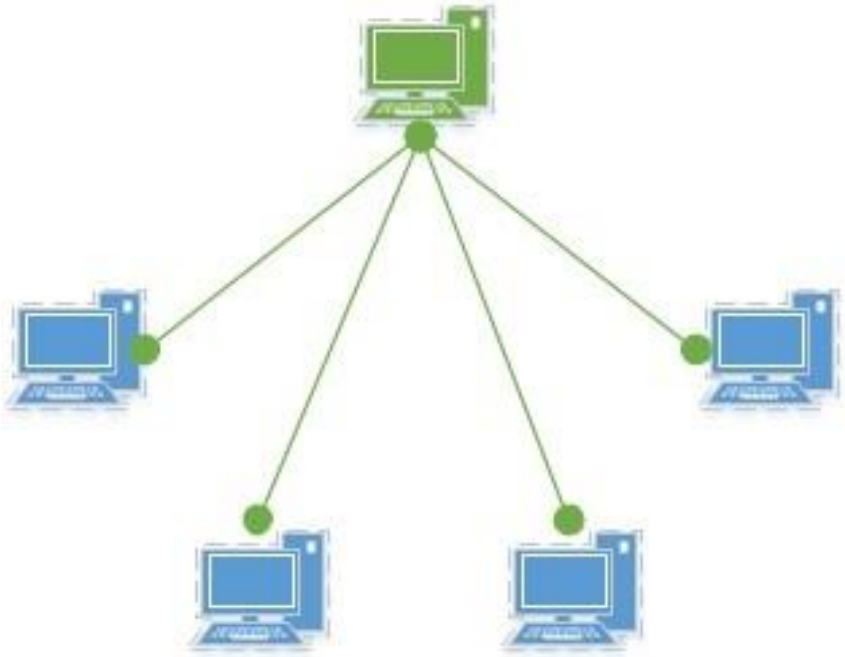
Generating the hash value of a block is called "mining" the block.

Mining a block is typically computationally expensive to do as it serves as the "proof of work".

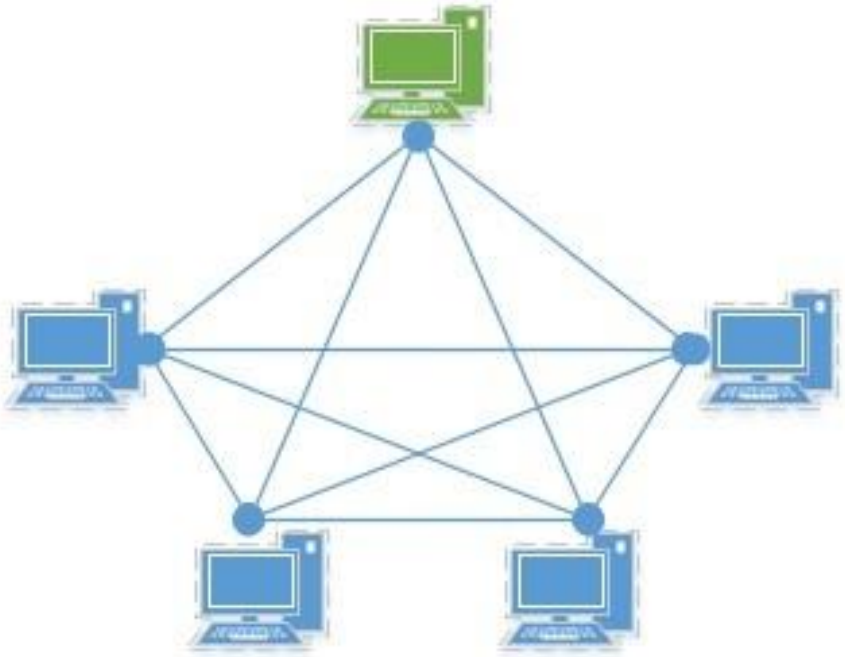
The hash of a block typically consists of the following data:

- Primarily, the hash of a block consists of the transactions it encapsulates
- The hash also consists of the timestamp of the block's creation
- It also includes a nonce, an arbitrary number used in cryptography
- Finally, the hash of the current block also includes the hash of the previous block

Adding a block



A Node Broadcasts a Mined Block



Other Nodes Broadcast Acceptance