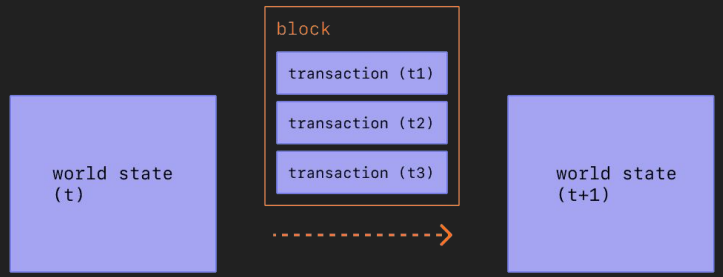
Blocks and hashes

Block are batches of transactions with a hash of the previous block in the chain. This links blocks together because hashes are cryptographically derived from the block data. This prevents fraud, because one change in any block in history would invalidate all the following blocks as all subsequent hashes would change and everyone running the blockchain would notice.



Blocks and hashes

To preserve the transaction history, blocks are strictly ordered (every block contains a reference to its parent block), and transactions within blocks are strictly ordered as well.

Once a block us put together (mined) by some miner on the network, it is propagated to the rest of the network. All nodes add this block to the end of their blockchain, and mining continues. The exact block-assembly (mining) process and commitment/consensus process is currently specified by Ethereum’s “proof-of-work” protocol.

Proof-Of-Work protocol

・Mining nodes have to spend a variable but substantial amount of energy, time and computational power to produce a “certificate of legitimacy” for a block they propose to the network.

・ Other miners who hear about a new block with a valid certificate of legitimacy must accept the new block as the canonical next block on the blockchain.

・The exact amount of time needed for any given miner to produce this certificate is a random variable with high variance. This ensures that it unlikely that two miners produce validations for a proposed next block simultaneously.

Blocks and hashes

- timestamp - the time when the block was mined
- blockNumber - the length of the blockchain in blocks
- baseFeePerGas - the minimum fee per gas required for a transaction to be included in the block
- difficulty - the effort required to mine the block
- mixHas - a unique identifier for that block
- parentHash - the unique identifier for the block that came before
- transactions - the transactions included in the block
- stateRoot - the entire state of the system; account balances, contract storages, contract code and account nonces are inside
- nonce - a hash that, when combined with mixHash, proves that the block has gone through Proof-Of-Work

Block time

Block time refers to the time it takes to mine a new block. In Ethereum, the average block time is between 12 to 14 seconds and is evaluated after each block. The expected block time is set as constant at the protocol level and is used to protect the network’s security when the miners add more computational power. The average block time get compared with expect block time, and if the average block time is higher, the difficulty is decrease in the block header. If the average block time is smaller, then the difficulty in the block header will be increased.

Block size

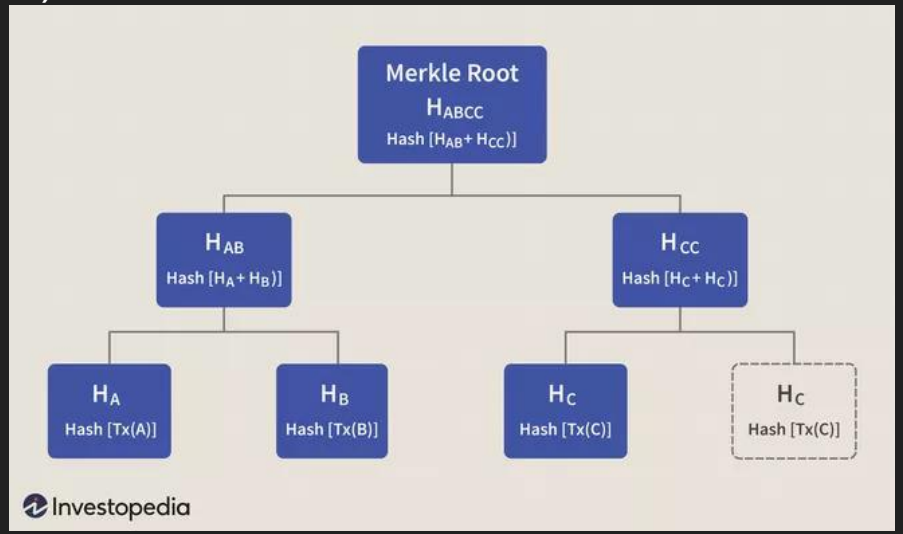
Blocks themselves are bounded in size. Each block has a target size of 15 million gas but size of the block will increase or decrease in accordance with network demands up until the block limit of 30 million gas.

Hashes, Markle tree

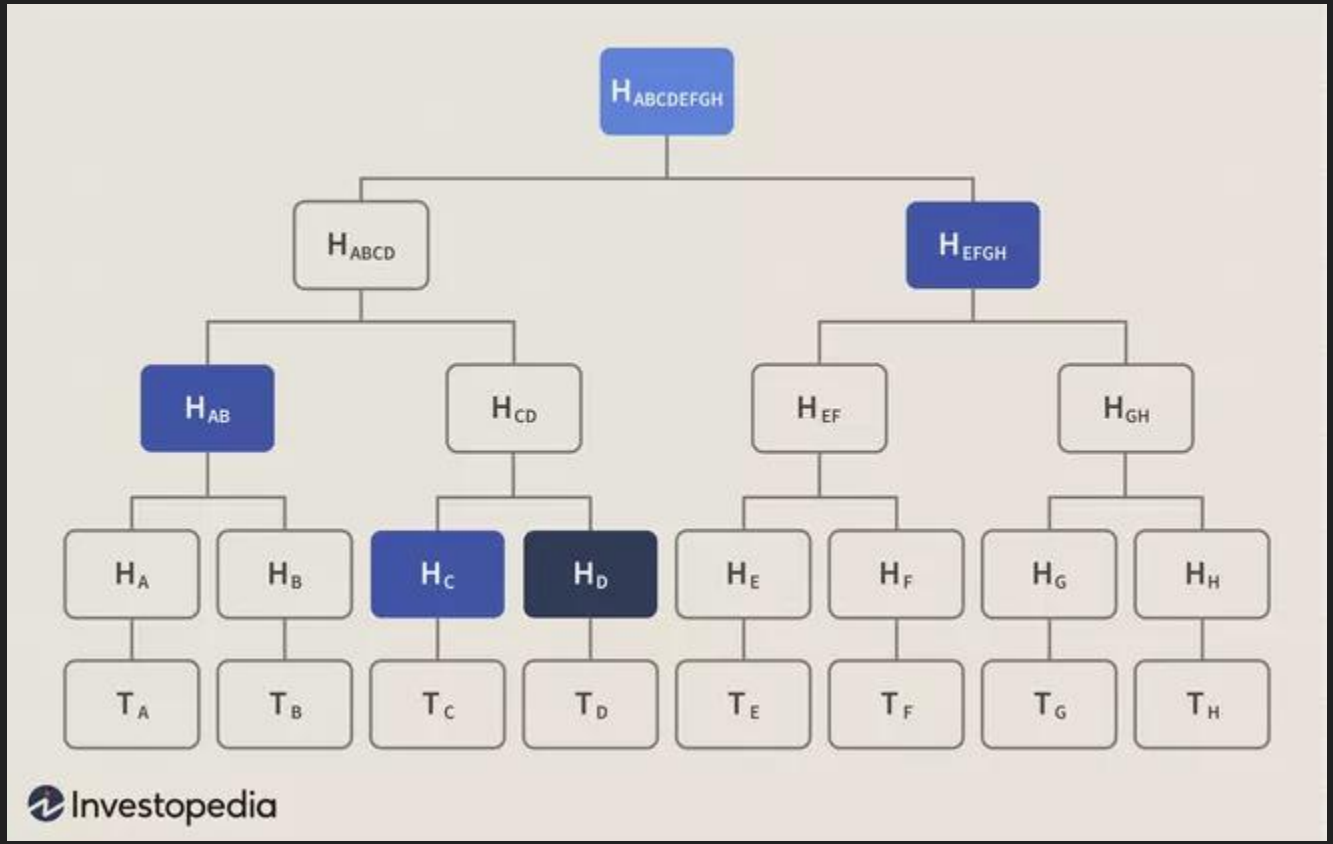
A hash tree, or the Merkel tree, encodes the blockchain data in an efficient and secure manner. It enables the quick verification of blockchain data, as well as quick movement of large amount of data from one computer node to other in the peer-to-peer blockchain network.
Every transaction occurring on the blockchain network has a hash associated with it. However, these hashes are not stored in a sequential order on the block, rather in the form of a tree-like structure that each hash is linked to its parent following a parent-child tree-like relation.

Hashes, Markle tree

For example, consider a seven-transaction block. At the lowest level (called the leaf-level), there will be four transaction hashes. At the level one above the leaf-level, there will be two transaction hashes, each of which will connect to two hashes that are below them at the leaf level. At the top (level two), there will be the last transaction hash called the root, and it will connect to the two hashes below it (at level one).



Hashes, Markle tree



Useful links

- Blocks | ethereum.org
- Merkle Root (Cryptocurrency) Definition
- MetaMask
- Networks | ethereum.org
- FaucETH
- Etherscan
- Solidity
- GitHub - ethereumbook/ethereumbook: Mastering Ethereum, by Andreas M. Antonopoulos, Gavin Wood