Block Validation

One of the key mechanisms enabling blockchain functionality is the block validation process. The two main types of blockchain, Proof of Work (PoW) and Proof of Stake (PoS), have a distinctively different block validation process.

Who Is a Blockchain Validator?

- A blockchain validator is **a network node** that helps process and validate transaction blocks on the platform so that they can be added to the permanent ledger of the blockchain. When using the term "validator," some people presume the nodes validating transactions on PoS blockchains. They contrast it with the term "**miner**," used on PoW blockchain platforms.
- However, block validation is a process equally applicable to both of these blockchain varieties. The more correct synonym for mining, applicable to PoS blockchains, would be **staking**, the process of block validation used on this type of platform.
- As transactions on the blockchain are initiated by users, they are queued on the network for subsequent validation. Validator nodes then batch individual transactions into a block to verify it. Each blockchain has its own rules pertaining to the number of transactions per block. When the block has been completed, validators process it to add it to the blockchain as a permanent record.
- On some blockchains, validators may choose which transactions to batch into a block. This selection is not necessarily in chronological order, but is driven by the validator's preferences, typically based on **transaction fees** involved.
- The fees are added to each blockchain transaction by the sender of crypto assets as an incentive for validators. Senders may choose the fee amount, and could even send a transaction without any fees at all.
- However, transactions with very low or no fees are more likely to be ignored by validators and, thus, might remain in an unconfirmed state for long periods of time. If, after a while, the transaction is not added to a block for validation, it is normally dropped from the network.
- The actual process of validating a block differs between PoW-based blockchains, such as Bitcoin (BTC) or Ethereum (ETH), and PoS blockchains, such as Solana (SOL) or Ethereum 2.0.

Blockchain Validation:

Introduction

- For a decentralized network like Blockchain, it’s essential to keep all the network participants synchronized. However, it seems far-fetched to make everyone agree on one thing. Blockchain uses a consensus mechanism to establish governance among all the network participants. In this article, we’ll go through one of the most popular and foundational consensus protocols, i.e., Proof-of-Work (PoW) in the blockchain.

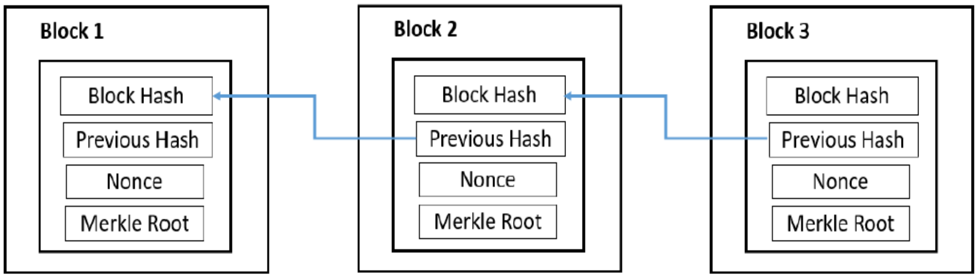
First, Let’s begin by understanding the consensus mechanism.

What is the Consensus Mechanism?

- In simple terms, **Consensus** means achieving a decision state with which all network participants agree. For instance, a group of friends agrees to play football without conflicts.
- Here, to reach a decision to play football together is a state of consensus or mutual agreement.
- “The **purpose of the Consensus mechanism in a blockchain** is to allow a group of separate nodes to distribute the right to update the network or system. However, the update will happen according to a few established rules among the set of participants in a secure way.”

What is Proof-of-Work (PoW)?

- Proof-of-Work (PoW) consensus mechanism is the oldest yet most popular. The idea first popped in 1993 when **Moni Naor and Cynthia Dowrk** published an article exploring the potential of algorithms to prevent fraud. Later, **Satoshi Nakamoto** coined the algorithm (an anonymous figure behind the discovery of Bitcoin) in his whitepaper on “Bitcoin: A peer-to peer E-Cash system” in 2008.
- PoW plays a significant role in the evolution of Blockchain Technology. **The idea is to create a verification system that is hard to crack**.
- The decentralized network works on a principle of not trusting but staying cooperative. Blockchain (a decentralized network) chain of linearly connected information-contained blocks secured using cryptography. Here, each block contains the hash of its previous block to keep connected.



Moreover, every block contains several other pieces of information like timestamp, block height, transaction records, Merkle Root Hash, block hash, previous block hash, difficulty level, and many more in the block header. The other section contains a set of financial transactions whose hashes will convert into the Merkle root eventually. Hence, a blockchain is a chain of blocks of transactions.

Mining a Block

- When it comes to **adding a new block to the chain**, it's seen as a new update to the current system. Therefore, it requires network participants' permission. In order to make a decision to add a new block or not, **Proof-of-Work (PoW)**, a consensus mechanism, is used. Only verified transactions get added to the network.
- In contrast, not all blocks are valid. In fact, most proposed blocks are considered invalid by the network. The **Block validity** is defined by the Blockchain protocol. A Blockchain network has an arbitrary "**Difficulty**" setting managed by the protocol, which changes how hard it is to mine a block. Here, **mining** means adding a new block.
- **Miners** propose the new blocks in the chain. They are externals who wish to add their block to the network. The **work required to create a valid block** is where the value comes from. Miners receive rewards in proportion to their share of the computation power they spend to mine a new block. **By mining a valid block, the miner proves the work done**. In Blockchains like the Bitcoin network or Ethereum, the difficulty level can change to ensure that blocks are created at regular intervals.

How does the PoW Algorithm work?

A **Proof-of-Work (PoW) consensus algorithm** works in such a way that each miner needs to cross the **level of difficulty** to prove the block valid. A block is only marked as "**valid**" if the hash value of the entire block is below the difficulty hash.

Block Hash < Difficulty Hash

A block contains crucial transaction information that can't be changed. So, the Miners change the **nonce** to get the hash lower than the difficulty threshold. The nonce is a component of a block that can be altered to achieve the difficulty level restrictions.

Let's take an example to understand how it works.

Harry is a bitcoin miner who wishes to add his block of bitcoin (a digital currency) transactions to the network. However, to make his block valid. First, he has to change the block nonce until the hash of his block gets lower to the difficulty threshold.

Let's say,

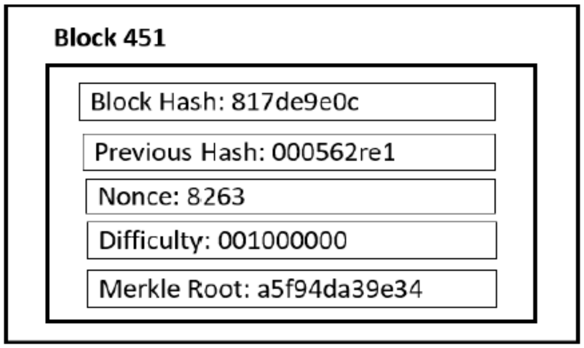
Harry's block Hash: 817de9e0c

Difficulty Hash: 001000000

Nonce: 8263

For, this, Block Hash > Difficulty Hash, which is considered invalid.

817de9e0c1 > 001000000



Block 451

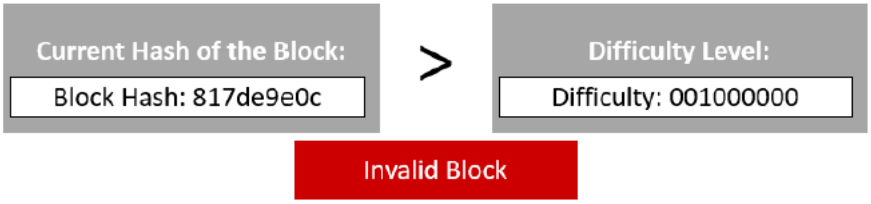
Block Hash: 817de9e0c

Previous Hash: 000562re1

Nonce: 8263

Difficulty: 001000000

Merkle Root: a5f94da39e34



Current Hash of the Block:

Block Hash: 817de9e0c

>

Difficulty Level:

Difficulty: 001000000

Invalid Block

Harry will change the nonce until he gets the first 3 digits as zeroes.

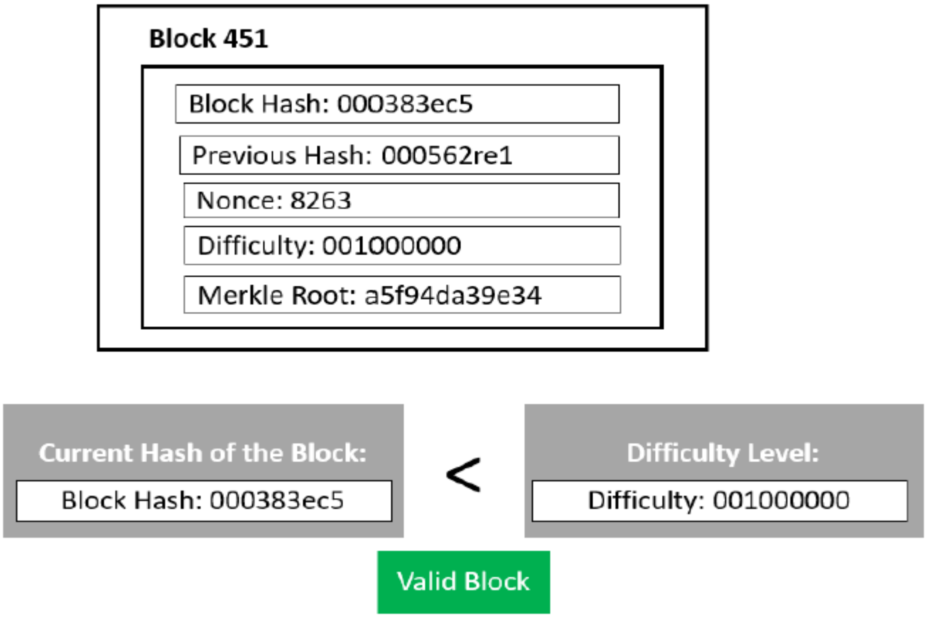
After continuously changing nonce for hours, he finally got the hash.

Harry's block Hash: 000383ec5

Difficulty Hash: 001000000

Nonce: 6778

Now, the difficulty threshold got achieved. **Block Hash < Difficulty Hash.**



Hence, Harry's block will be marked as valid and will get added to the blockchain. For mining a block in the bitcoin blockchain, Harry gets a few bitcoins as block **rewards** for spending the computation power to find the valid hash.

This process is entirely based on chance. Hence, the miner's job is to change the nonce value until the overall block hash reaches lower than the difficulty hash. There are other responsibilities of miners, but that's a topic for another article.

Benefits of PoW

Following are the advantages of the Proof-of-Work (PoW) mechanism:

- **A hard-to-find solution. Yet, easy verification.**
- **Initial consensus mechanism**, PoW doesn't need the initial staking of coins before mining. One can start with 0 coins, and it will go only positive.
- **Easy to implement** in comparison with other blockchain consensus mechanisms.
- It is **fault-tolerant.** It means the failure of one component will not shut the whole blockchain network.
- Give miners an **earning opportunity** for adding a block.
- PoW is the **oldest, trusted, and most popular** consensus protocol.

Limitations of PoW

Following are the disadvantages of the Proof-of-Work (PoW) mechanism:

- A lot of energy gets wasted as only one miner can eventually add its block.
- It requires heavy computation power hence massive resource and energy consumption.
- A 51% attack risk on the network. The controlling entity can acquire 51% to dominate the network.
- Spread environmental hazards using additional machinery.
- Pow is a time and energy-consuming process.
- It needed heavy expenses for hardware.
- Risk of denial of service attacks by intruders.