What is Blockchain Mining?

What is Mining?

- Mining is the process of creating new blocks on the blockchain ledger to record transactions.
- Miners are the people who mine the blocks.
- Miners solve hashing functions to find a target hash for a given block by changing the nonce in the header.
- The winning miner receives a reward for adding a new block to the chain.
- Miners pick up transactions from the transaction pool and gather them to create a block. The miners then run the block through a hashing algorithm with different nonce values to reach the target hash value.

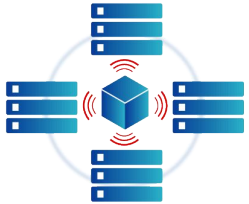
How mining is performed?

Alice wants to buy a product from Bob using Bitcoin.

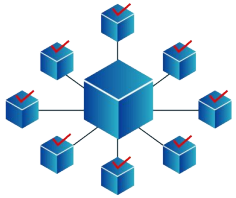
Transaction is created, with amount of bitcoins and Bob's address.

Alice uses her private key and sign the Transaction.

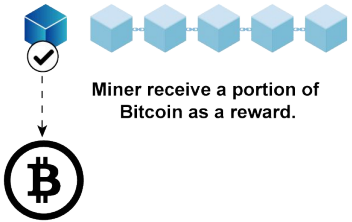
Transaction is bundled into a block with other transactions.



Block is broadcasted to all mining nodes in the network.



Transaction is validated by other nodes in the network.



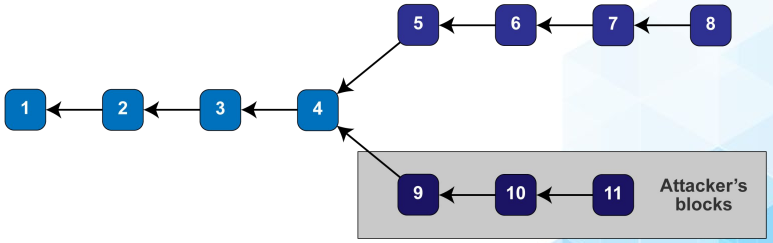
Miner receive a portion of Bitcoin as a reward.

Transaction is completed, new block is added to the blockchain.

Bob received his bitcoins from Alice.

Longest Chain Rule

- Longest Chain Rule defines the rules by which miners decide which chain to follow on the blockchain.
- This issues arises when 2 miners mine blocks at the same time and publish them to the network. The network accepts both the blocks and moves on to mining the next block on top of the previous block, resulting in a fork in the chain. To remedy this issue, the miners mine for blocks for the longest chain, and the other fork is abandoned.
- The longest chain is evaluated using chainwork. Chain work calculates the total number of hashes required to produce the chain from the genesis block.
- In order to alter a transaction in the blockchain, an actor would need to change the block hash and alter the subsequent blocks to build a new longest chain to supplant the current one.



CPU vs. GPU vs. ASIC Mining

- Mining is the process of allocating computer resources to the network, Users use their CPU, or GPU, or special hardware to mine.
- Using a CPU to mine cryptocurrency was the first solution that came with Bitcoin, but as the difficulty of calculating the desired hash increased, the CPU performance could not achieve the result in the desired time.
- GPU is used in mining in place of CPU to provide greater processing power.
- GPU mining was actively adopted in 2010-2011 when new coins became available and miners found more options for their hardware to mine.
- ASIC or Application Specific Integrated Circuits, are custom built processors used for specific functions like environmental monitoring, personal assistance, or in this case, mining.
- ASICs provide higher hash rates for the specific protocol. ASICs are very energy efficient as compared to GPUs or CPUs with high performance and provide higher profit margins.
- ASICs have upgradeability problems as they cannot be updated for different coins, being protocol specific. If there is any change in the algorithm, the miner becomes obsolete.

Blockchain Council

THANK YOU!

Any Questions?

Visit

community.blockchain-council.org

Mail Us

hello@blockchain-council.org