Proof-of-Work: The Hash Puzzle

Hard to find (billions of tries) | Easy to verify (one hash)

Block Header

Prev Hash

Merkle Root

Timestamp

SHA-256

(twice)

256-bit output

Hash < Target?

`0000...xyz`

(leading zeros)

NONCE

Try: 0, 1, 2, ...

(random search)

NO -> Try another nonce

YES

Valid Block!