**Scenario: Alice Sends 5 BTC to Bob**

Alice wants to send **5 BTC** to Bob. The network consists of **six miners** competing to mine the next block.

**Step 1: Alice Creates a Transaction**

* Alice constructs a transaction:
  + **Sender:** Alice
  + **Receiver:** Bob
  + **Amount:** 5 BTC
  + **Digital Signature:** Signed with Alice’s private key
* Alice broadcasts this transaction to the Bitcoin network.

**Step 2: Transaction Propagation**

* The transaction enters the **mempool** (a waiting area where unconfirmed transactions are stored).
* The six miners in the network pick up this transaction and include it in their candidate block.

**Step 3: Miners Compete to Solve PoW**

* Each miner starts working on the Proof-of-Work puzzle:
  + They construct a block containing Alice’s transaction.
  + They compute the block hash by finding a **valid nonce** (i.e., a number that, when hashed with the block data, produces a hash below the target difficulty).
  + Example:

Block Hash = SHA-256(Block Header + Nonce) < Difficulty Target

* Suppose the six miners working on this block are:
  + Miner A
  + Miner B
  + Miner C
  + Miner D
  + Miner E
  + Miner F
* Each miner is **guessing different nonce values** to find the correct hash.

**Step 4: Miner E Finds a Valid Nonce**

* Miner E finds a valid nonce that meets the difficulty target:

SHA-256(Block Header + Nonce) < Target

* This means Miner E has successfully **solved the PoW challenge** before the other miners.

**Step 5: Block Propagation**

* Miner E **broadcasts the newly mined block** (which includes Alice’s transaction) to the network.
* Other miners (A, B, C, D, F) receive this block and **verify**:
  + If the nonce is correct.
  + If all transactions (including Alice’s) are valid.
* Since the nonce is correct, the **majority of nodes accept this block**.

**Step 6: Block Finalization**

* Alice’s transaction (5 BTC to Bob) is now confirmed in the blockchain.
* Miner E gets the **block reward** (e.g., 6.25 BTC in Bitcoin) + transaction fees.

**Assume that Miner E finds a block and broadcasts it to the network. However, instead of a valid nonce, Miner E includes a wrong or manipulated nonce. Here’s what happens step by step:**

**Step 1: Miner E Finds a Block (But Uses a Wrong Nonce)**

* **Miner E constructs a block containing Alice’s transaction.**
* **Instead of calculating a valid nonce that satisfies the difficulty target, Miner E modifies the nonce and broadcasts the block.**

**Step 2: Other Miners Validate the Block**

**Once Miner E sends the block to the network, other miners (A, B, C, D, F) receive it and perform verification checks:**

1. **Nonce Verification**
   * **Each miner independently calculates:**

**SHA-256(Block Header + Nonce) < Difficulty Target**

* + **If the nonce is incorrect, the hash will not meet the difficulty target.**
  + **The majority of the network rejects this block.**

1. **Block Hash Check**
   * **The block hash must be below the network’s difficulty target.**
   * **If Miner E sent a wrong nonce, the block hash would be invalid.**
2. **Transaction Validity Check**
   * **Even if Alice’s transaction is correct, the invalid nonce makes the whole block invalid.**

**Step 3: Block Rejection**

* **Since the block does not meet the required PoW condition, the network rejects it.**
* **The blockchain remains unchanged, and the mining process continues.**
* **Miner E wasted computing power but does not get any rewards.**

**Step 4: Other Miners Continue Mining**

* **The other miners (A, B, C, D, F) ignore the invalid block and continue mining.**
* **Eventually, another miner (say, Miner A) finds a valid block and broadcasts it.**
* **The network verifies and accepts Miner A's block, officially adding it to the blockchain.**

**Can a Miner Fake a Valid Nonce?**

**No, a miner cannot fake a valid nonce because:**

1. **The network independently verifies the nonce by hashing the block.**
2. **PoW requires that the nonce produces a valid hash below the target.**
3. **If the nonce is wrong, the hash will not match, and nodes will reject the block.**

**Conclusion**

* **If Miner E sends a wrong nonce, the network rejects the block.**
* **The blockchain ensures that only blocks with valid nonces are accepted.**
* **The mining process continues until a valid block is found.**

**This is why PoW is secure—it prevents miners from inserting fake or invalid blocks. 🚀**