ICANN 78 ANNUAL GENERAL MEETING

ICANN 1998–2023

IANA Stewardship Transition 2016–2023

BlockchainS in 12 Easy Steps

Alain Durand, Distinguished Technologist, OCTO

ICANN 78
22 October 2023

Introduction

- **There is no such thing as THE blockchain.**

- There are many blockchains, all different in their purpose, technology, and governance.
- At their core, all blockchains are based on similar data structure: a cryptographically verifiable chain of blocks. What data is in each block and how they are added is what differentiates them at a technical level.

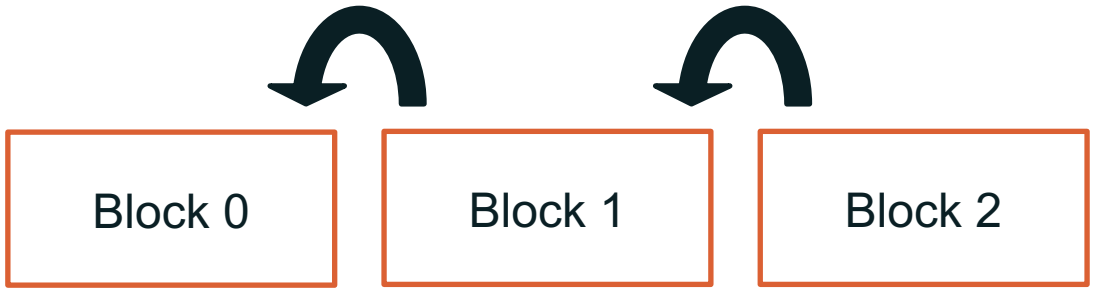
Caveats:

- The 12 steps described in this presentation are generic and are not descriptive of any specific blockchain implementation.
- Thus, the list of steps is neither fully accurate nor fully complete.
- Some steps reflect the Bitcoin model, some don’t.

Step 1: A Block

Blocks can contain arbitrary data. All block are cryptographically signed.

Step 2: A Blockchain



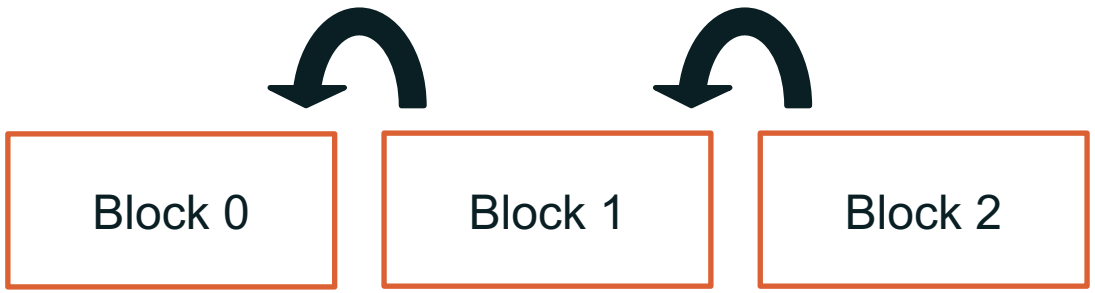
Blockchain

A Blockchain is a list of blocks that are chained back to each other.

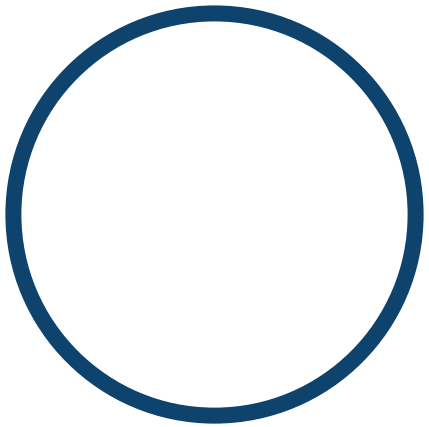
Each block contains a cryptographic hash of the entire chain up to it.
Thus, any observer can verify the integrity of the blockchain.

New data can be added in new blocks, but existing blocks can never be changed.

Step 3: Miners



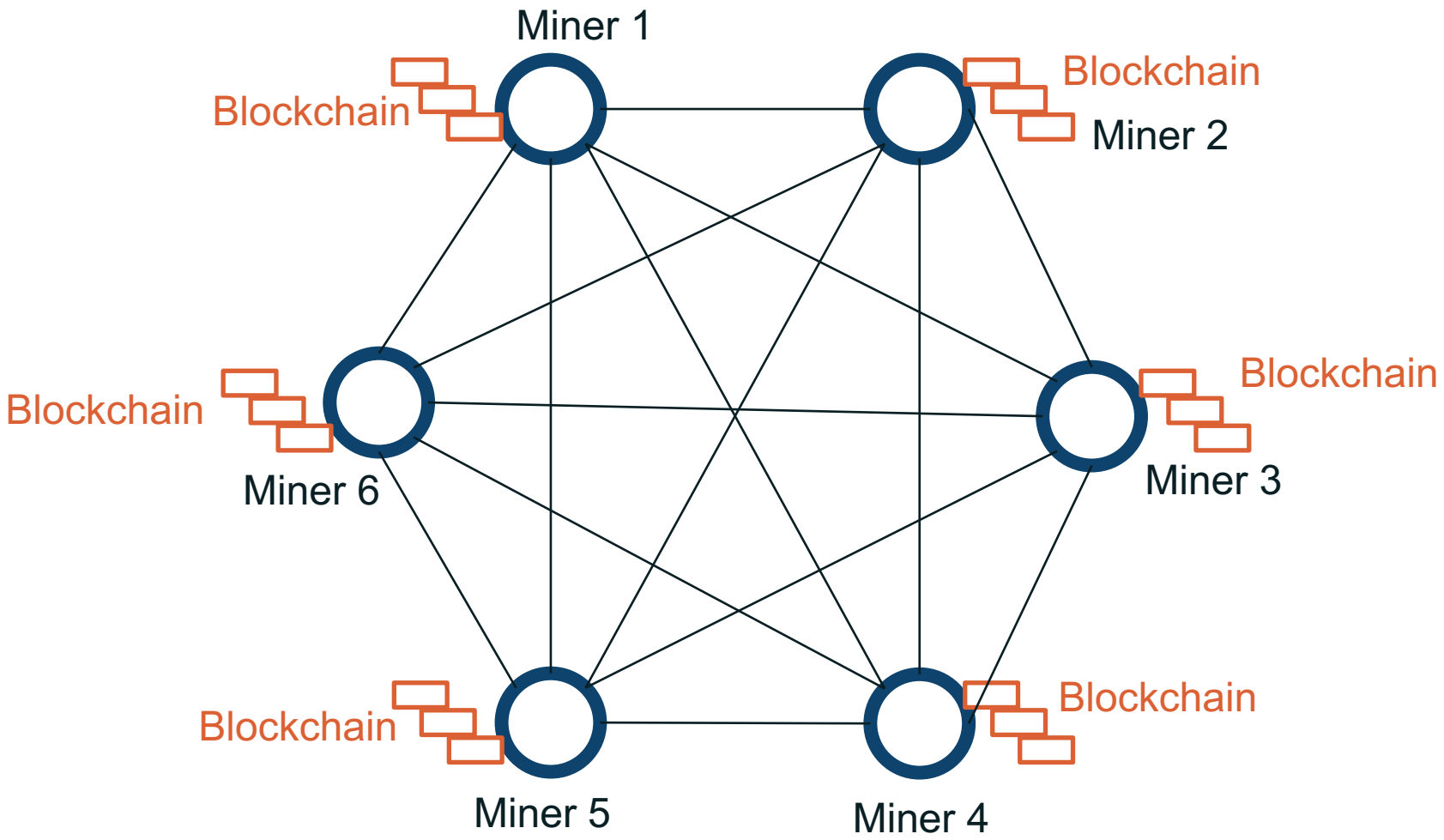
Blockchain



Miner

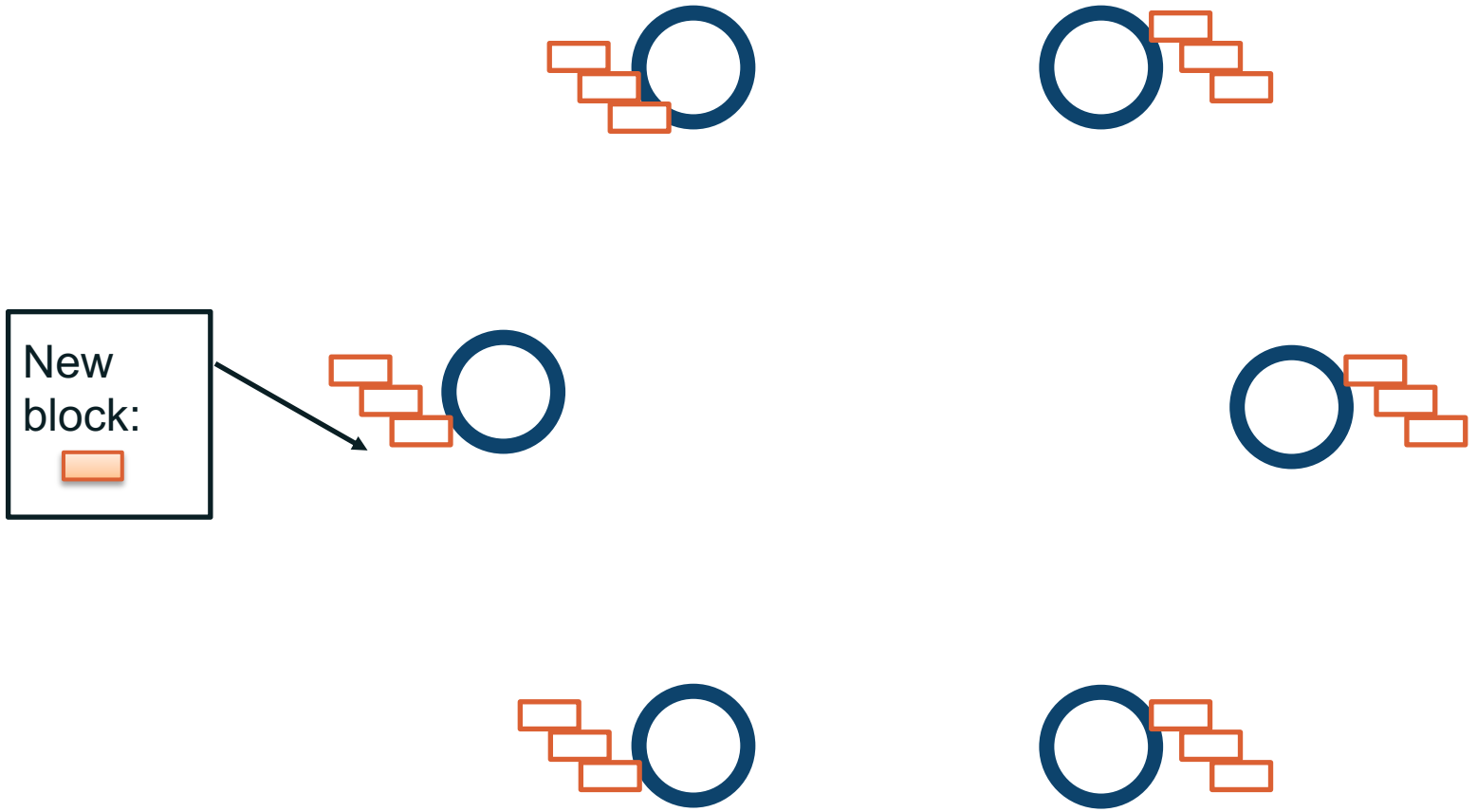
Anybody can maintain a local copy of the blockchain.
Some nodes participate in a competition to have the right to add a new block to the blockchain.
They are called “miners”.

Step 4: “Miner" Form A Peer-to-Peer Network



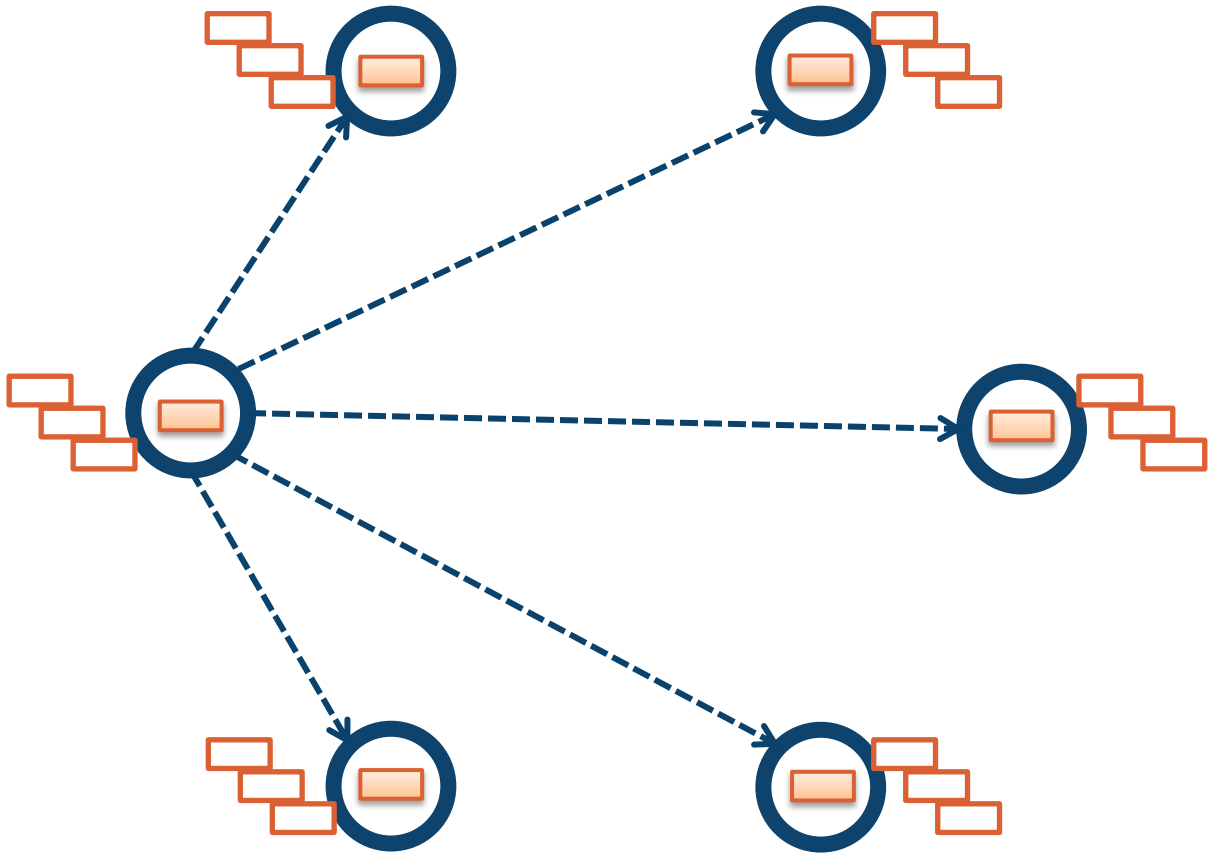
Miners have identical copies of the blockchain.

Step 5: A New Block Needs To Be Added To The Blockchain



New block will be added at the end of the blockchain.

Step 6: Distributing Candidate Block To All Miners



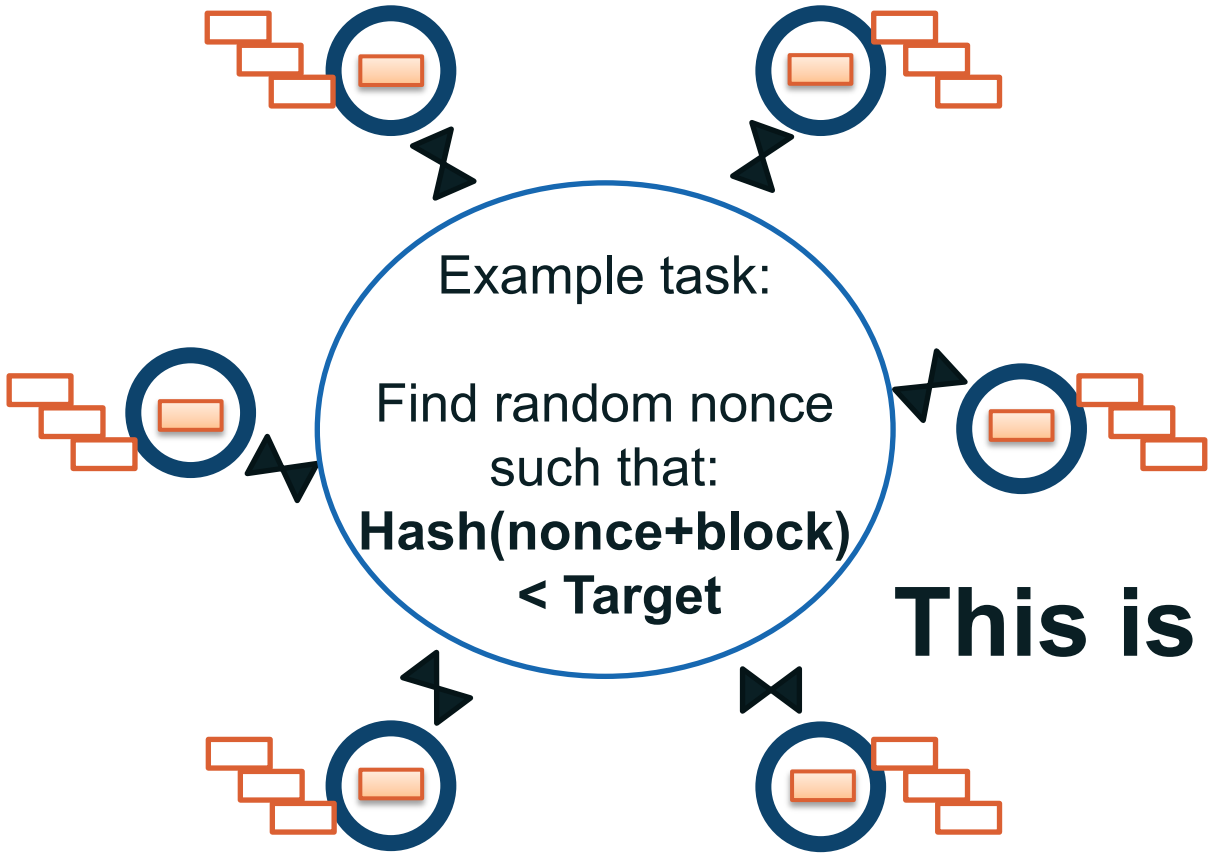
The requesting miner sends the new block to all participating miners.

Step 7: All Miners Perform The Same Compute Intensive Task

This phase is consuming a huge amount of energy.

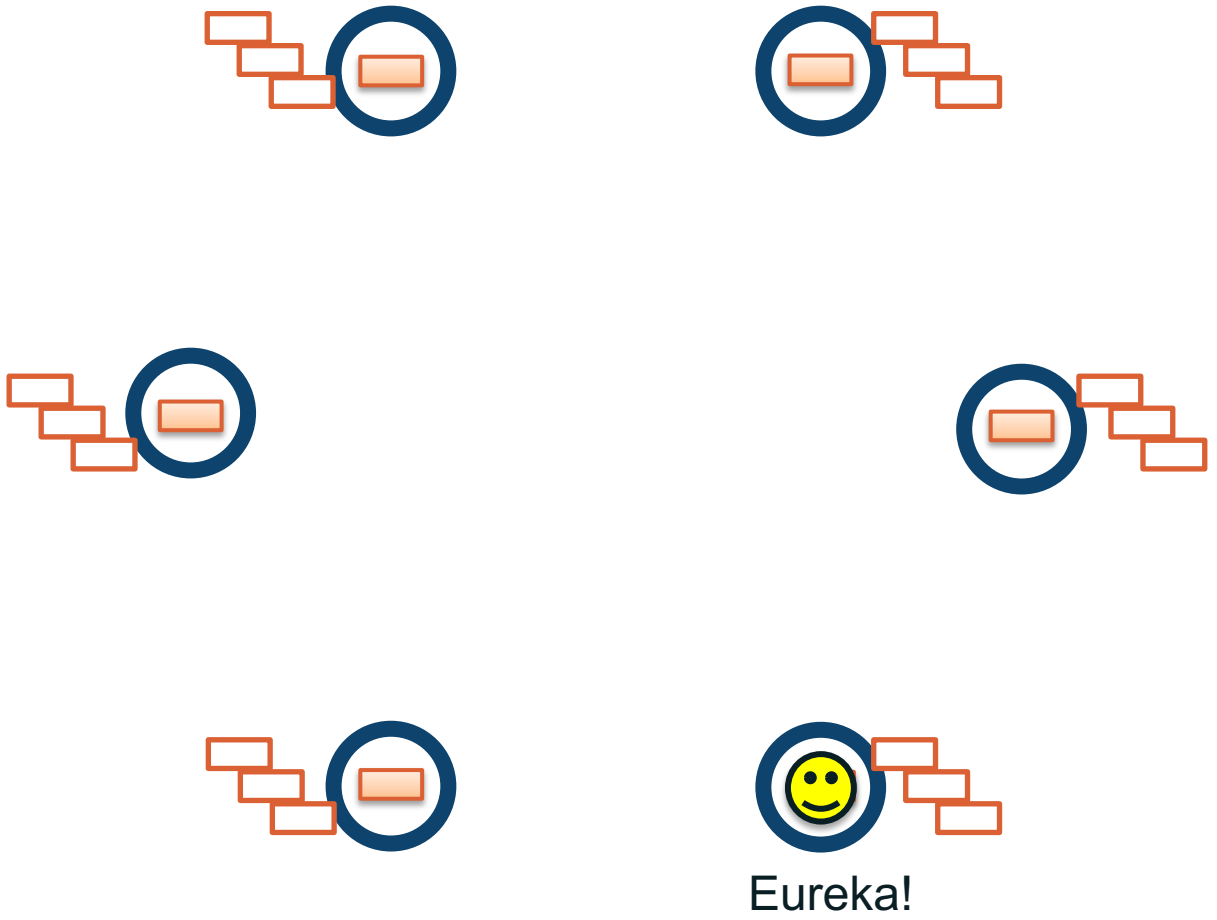
Proof of Work

There is an alterative approach: **Proof of Stake**

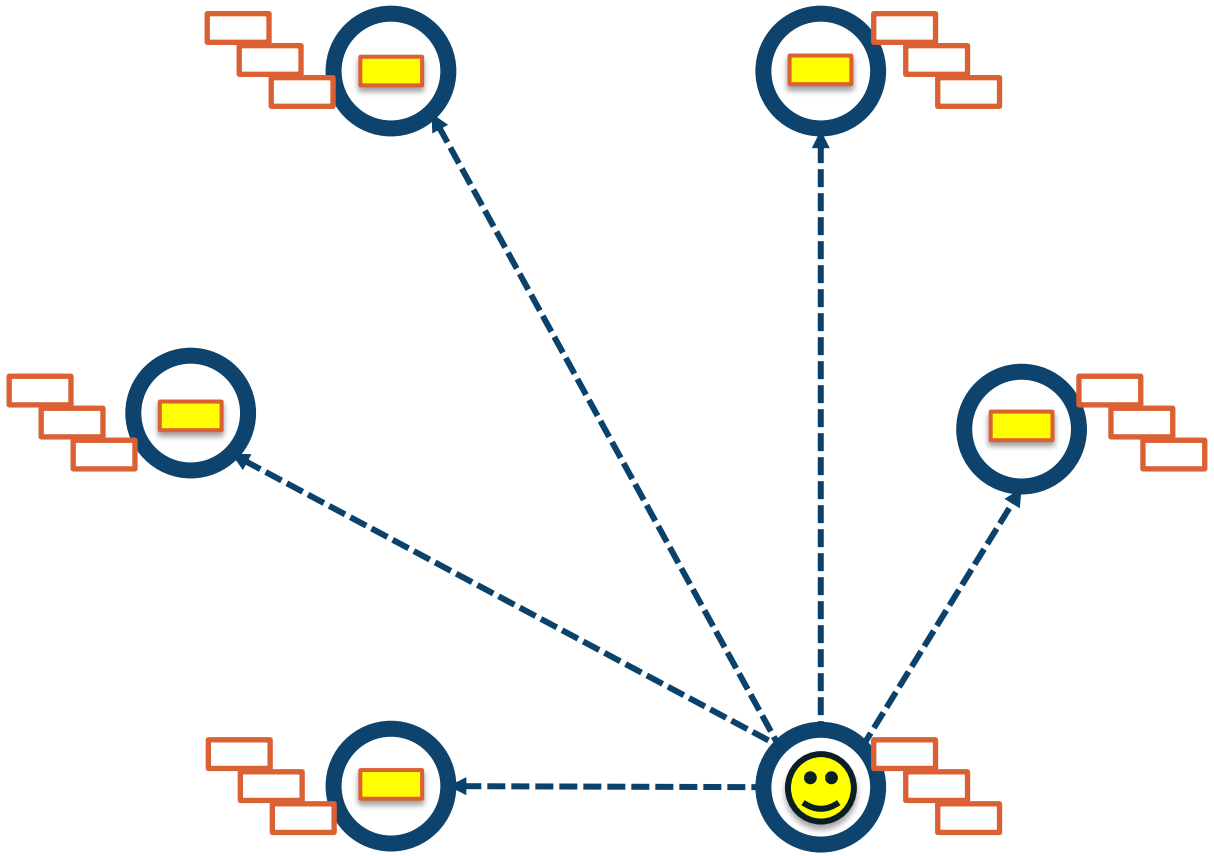


This is a race!

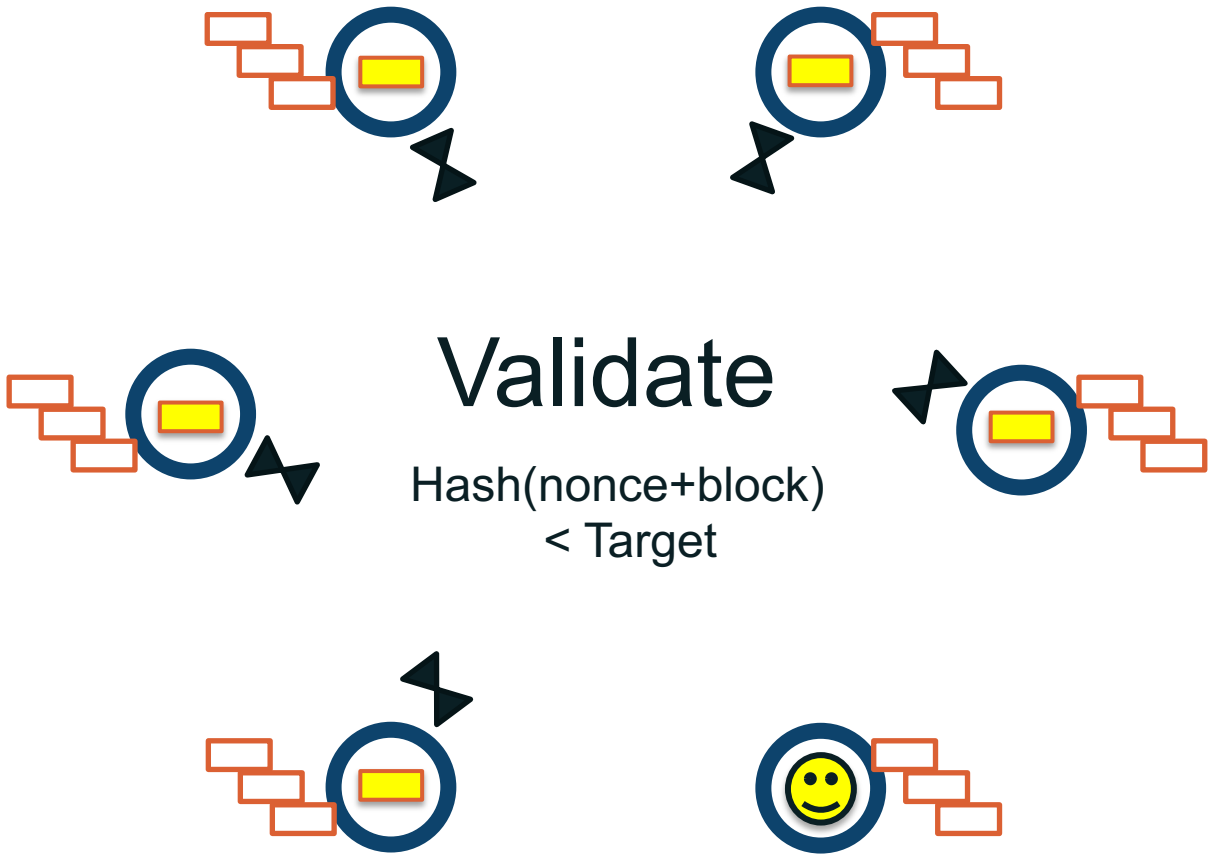
Step 8: A Miner Finds The Answer First



Step 9: Winner Propagates Solution To All Miners

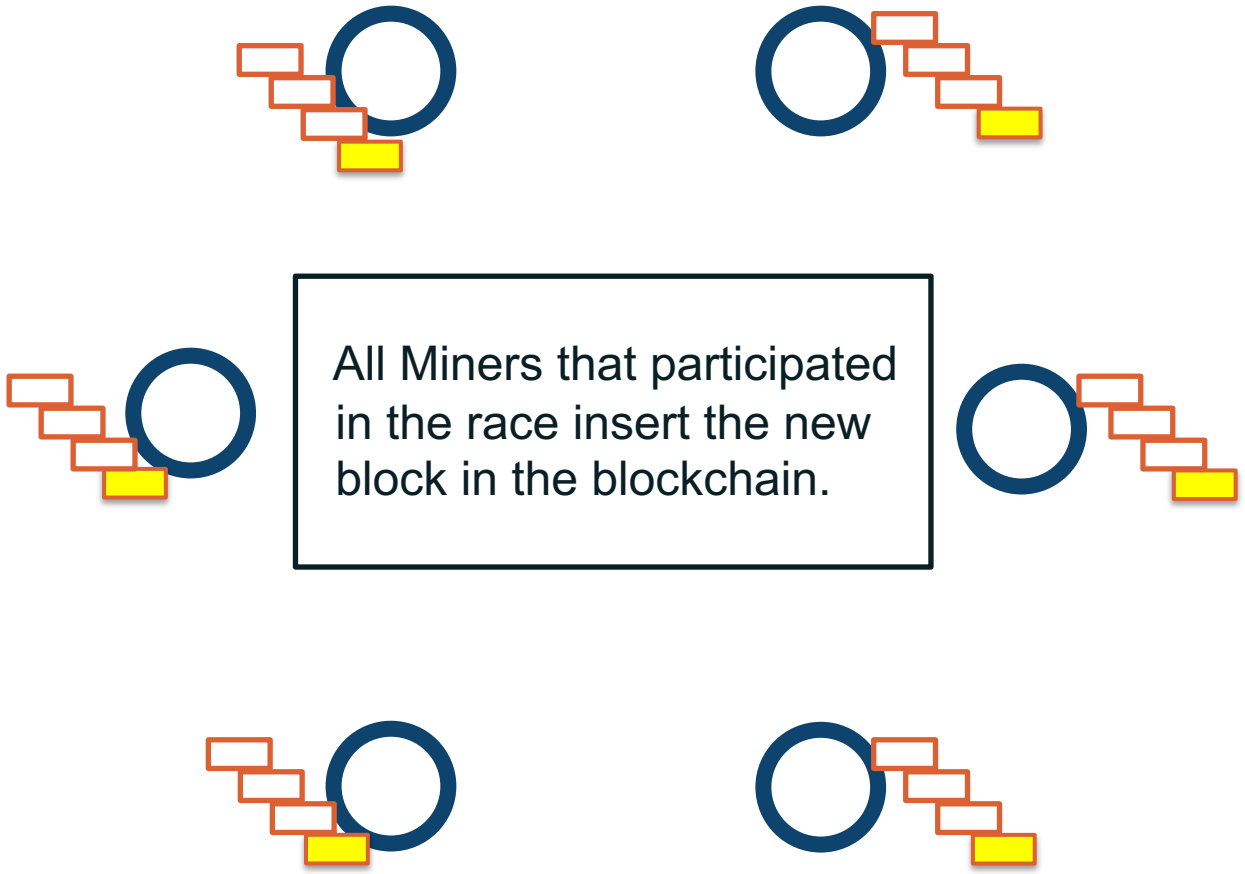


Step 10: All Miners Validate The Proposed Solution



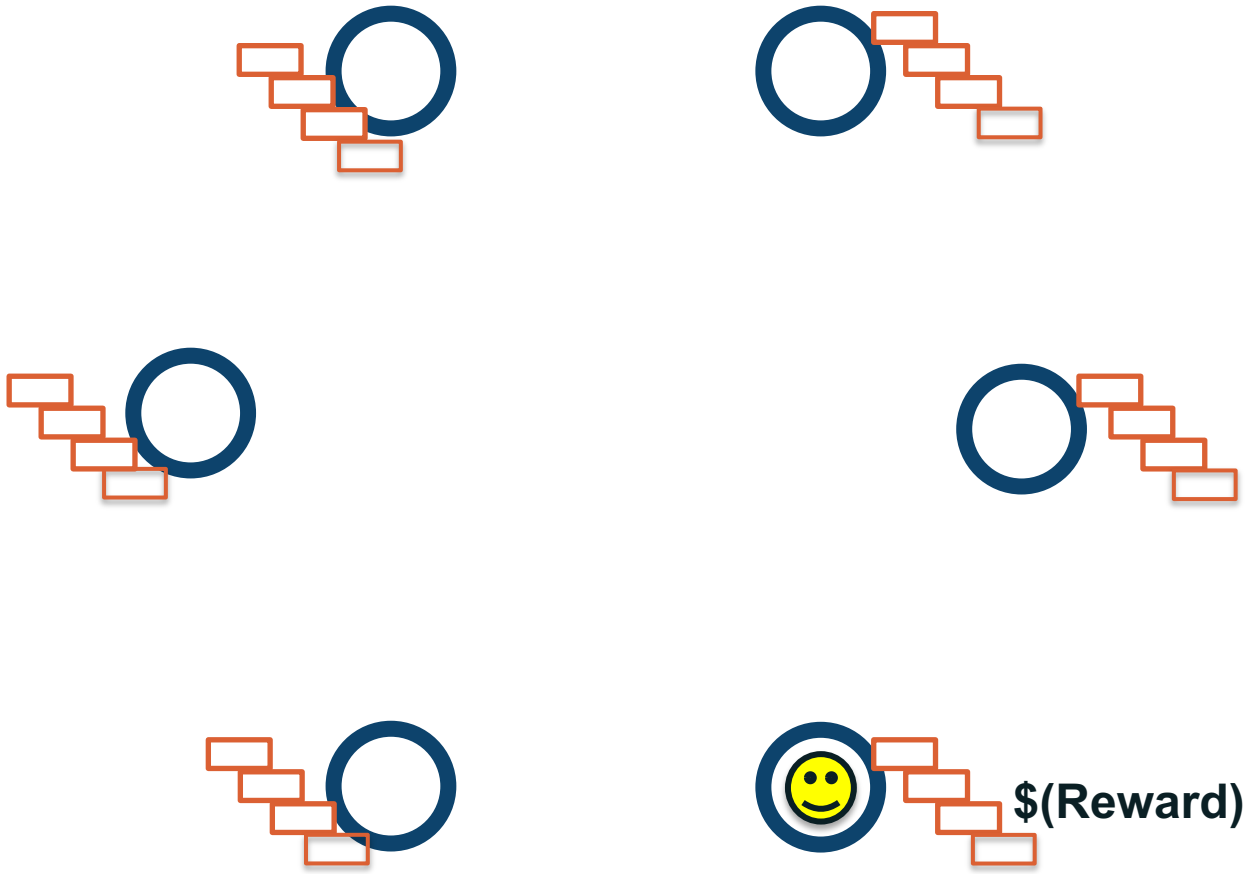
Note: The validation phase is very fast (a single hash calculation).

Step 11: New Block Is Inserted In The Blockchain By All Miners



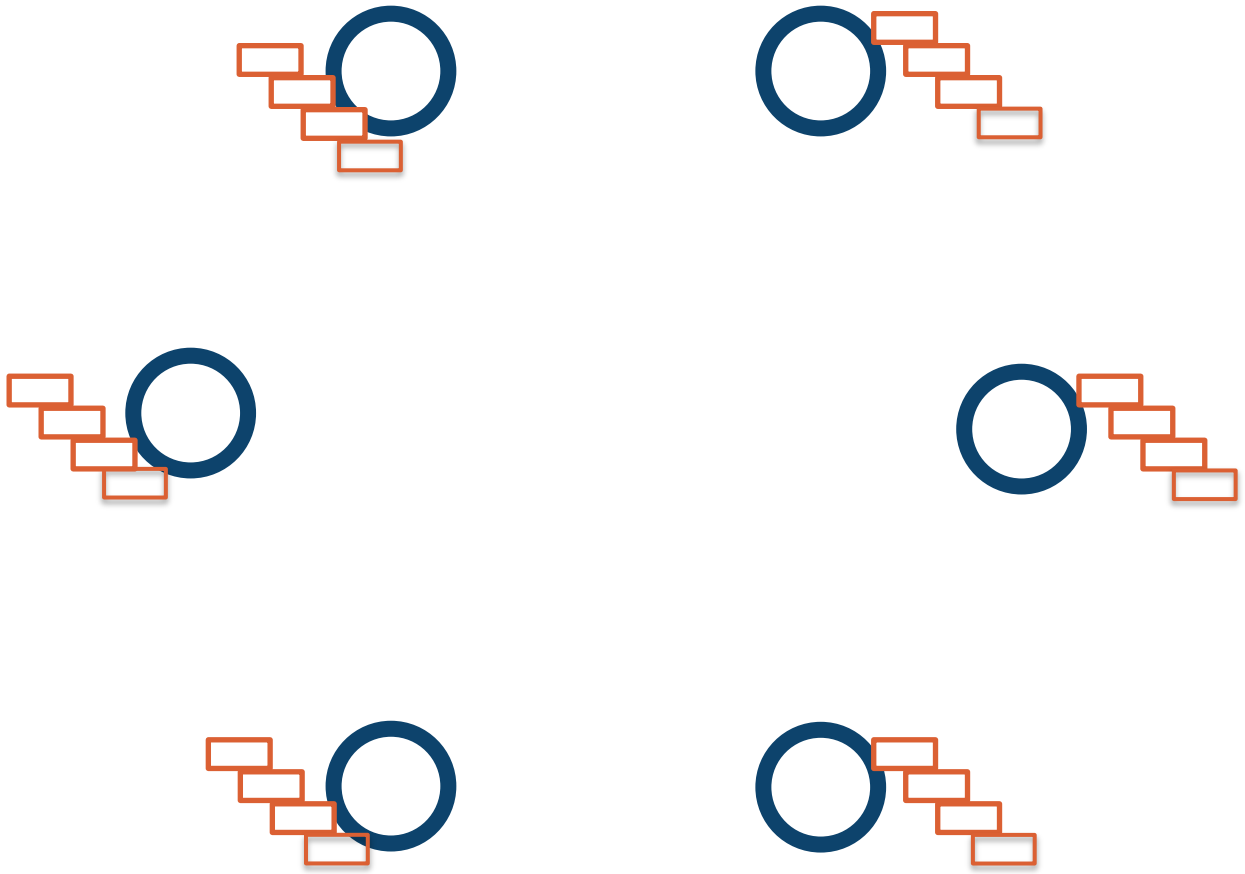
This phase is happening at a predefined clock time.

Step 12: Winner Gets A Reward



The “reward” is here to incentivize miners to participate to the system and provide compute resources for proof-of-work.

Repeat: The New Block Is Ready To Be Used

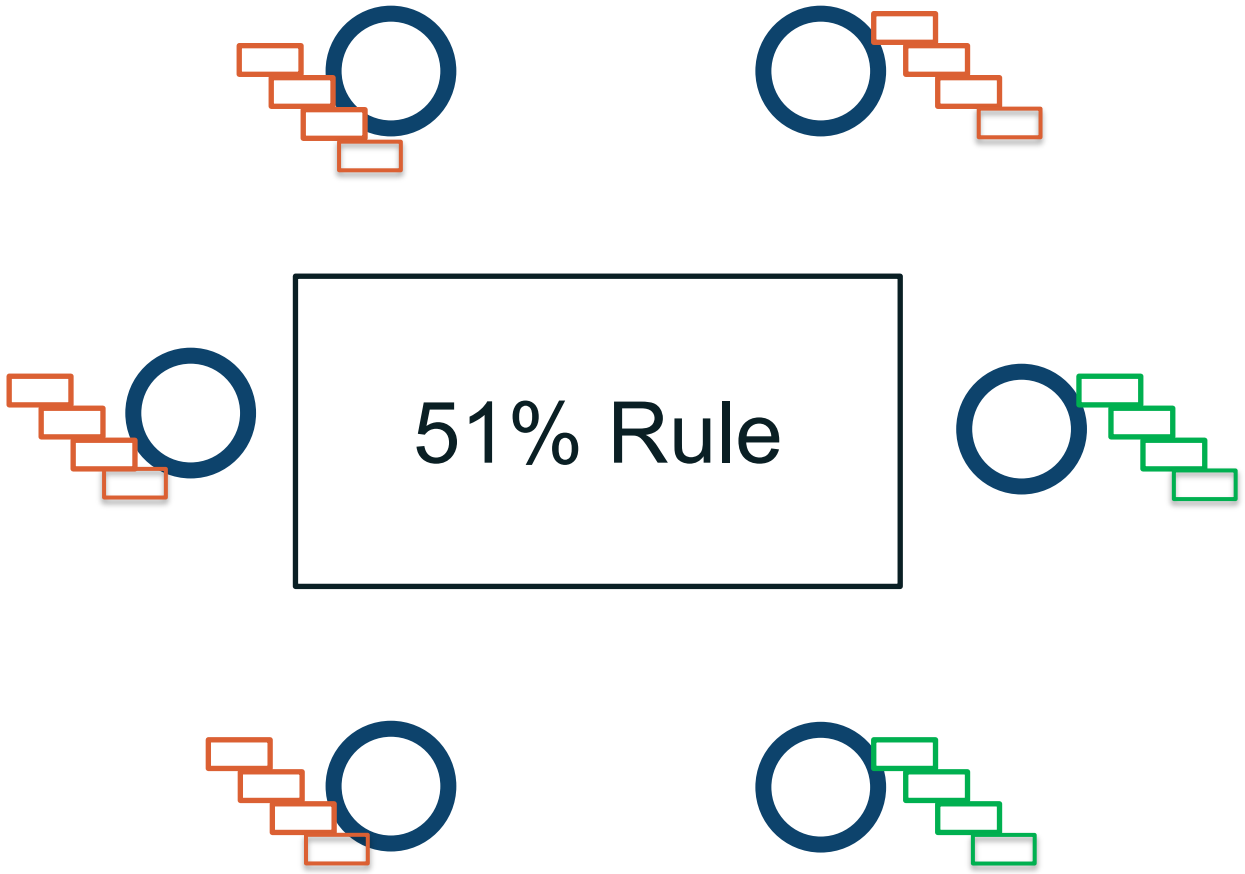


Repeat…!

Conflict Resolution

Nodes get copies of the blockchain from all the miners.

In case of conflict, nodes will “trust” the blockchain held by the majority of the miners.



The proof of work is solely to build a “voting poll tax” into the system.
Only miners willing to offer significant compute power can participate.
It protects against rogue miners joining the network to perform the 51% vote attack.

Engage with ICANN

Thank You and Questions

Visit us at **icann.org**
Email: email@icann.org

@icann

facebook.com/icannorg

youtube.com/icannnews

flickr.com/icann

linkedin/company/icann

soundcloud/icann

instagram.com/icannorg