CONSENSUS ALGORITHMS:

BLOCKCHAIN STATE OF THE LEDGER

DISTRIBUTED PEER-TO-PEER NETWORK

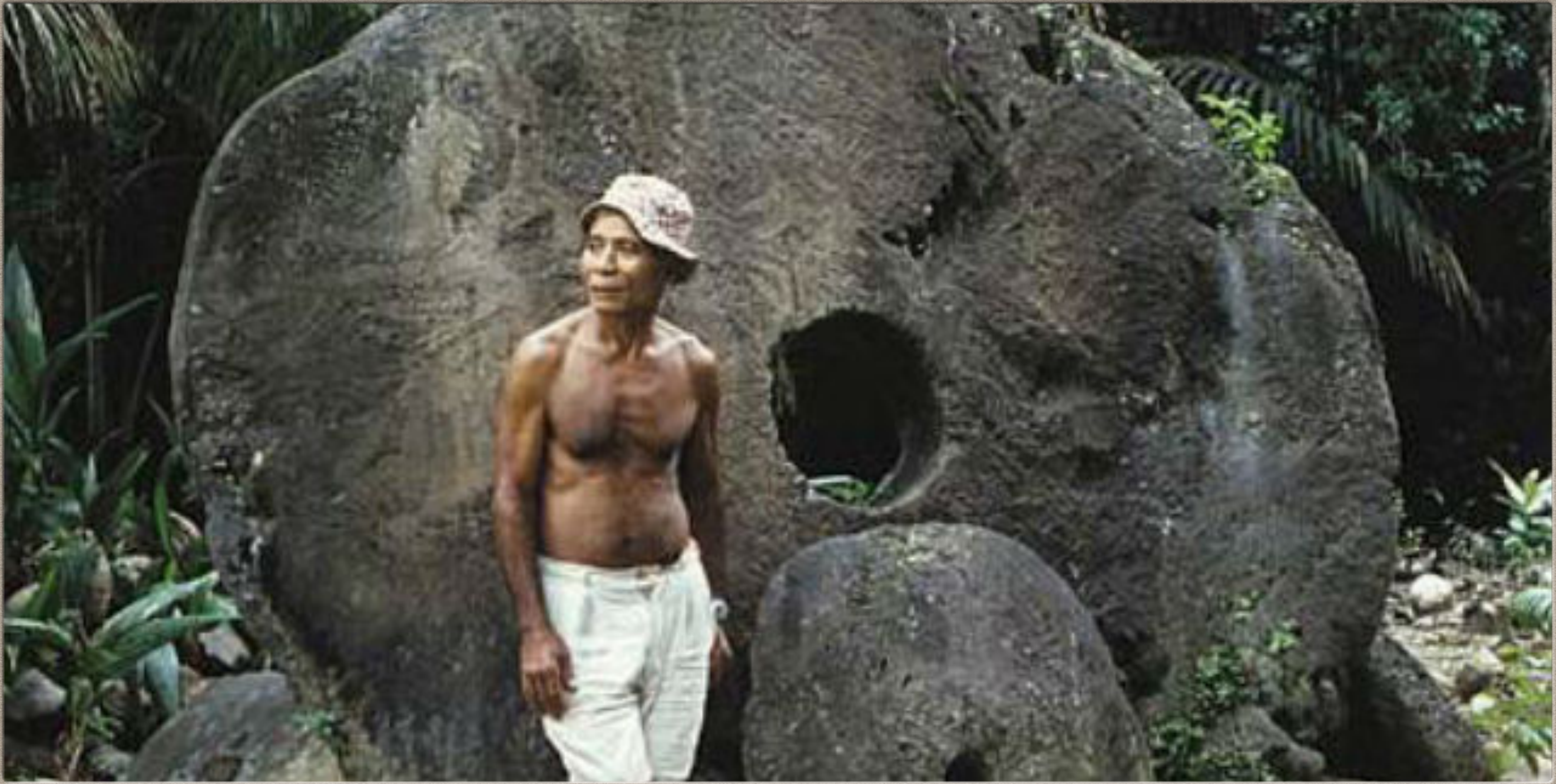
EACH NODE HAS A COPY OF THE LEDGER

WHEN A TRANSACTION IS ADDED TO THE LEDGER, TWO THINGS MUST HAPPEN:

- Is the transaction valid? The transaction must be approved.
- All nodes must add the transaction in the same manner so the ledger is the same on all nodes.

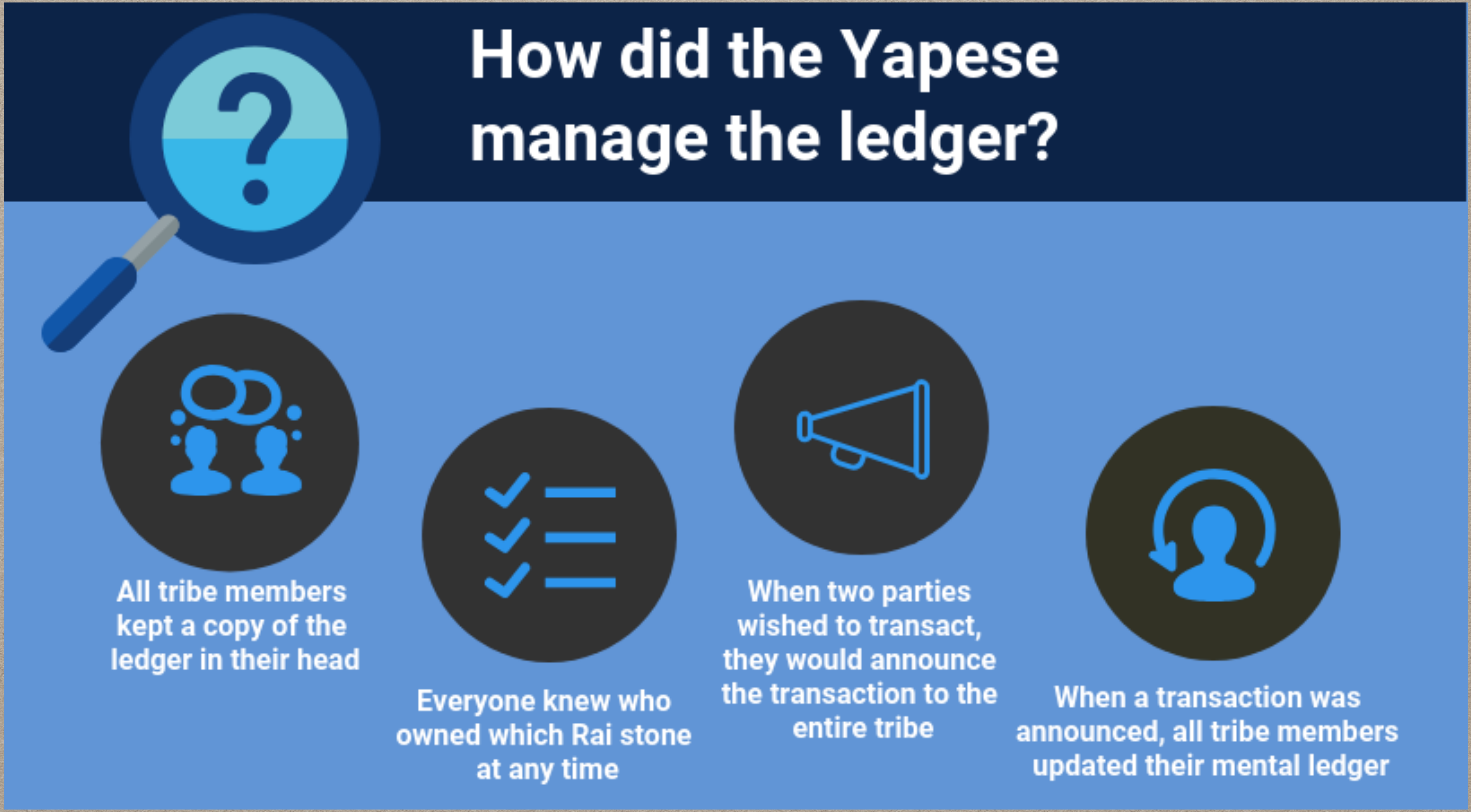
HOW DO YOU DO THIS?

CONSENSUS ALGORITHMS!



DISTRIBUTED LEDGER & CONSENSUS ALGORITHMS ARE NOT NEW

ISLAND OF YAP



How did the Yapese manage the ledger?

All tribe members kept a copy of the ledger in their head

Everyone knew who owned which Rai stone at any time

When two parties wished to transact, they would announce the transaction to the entire tribe

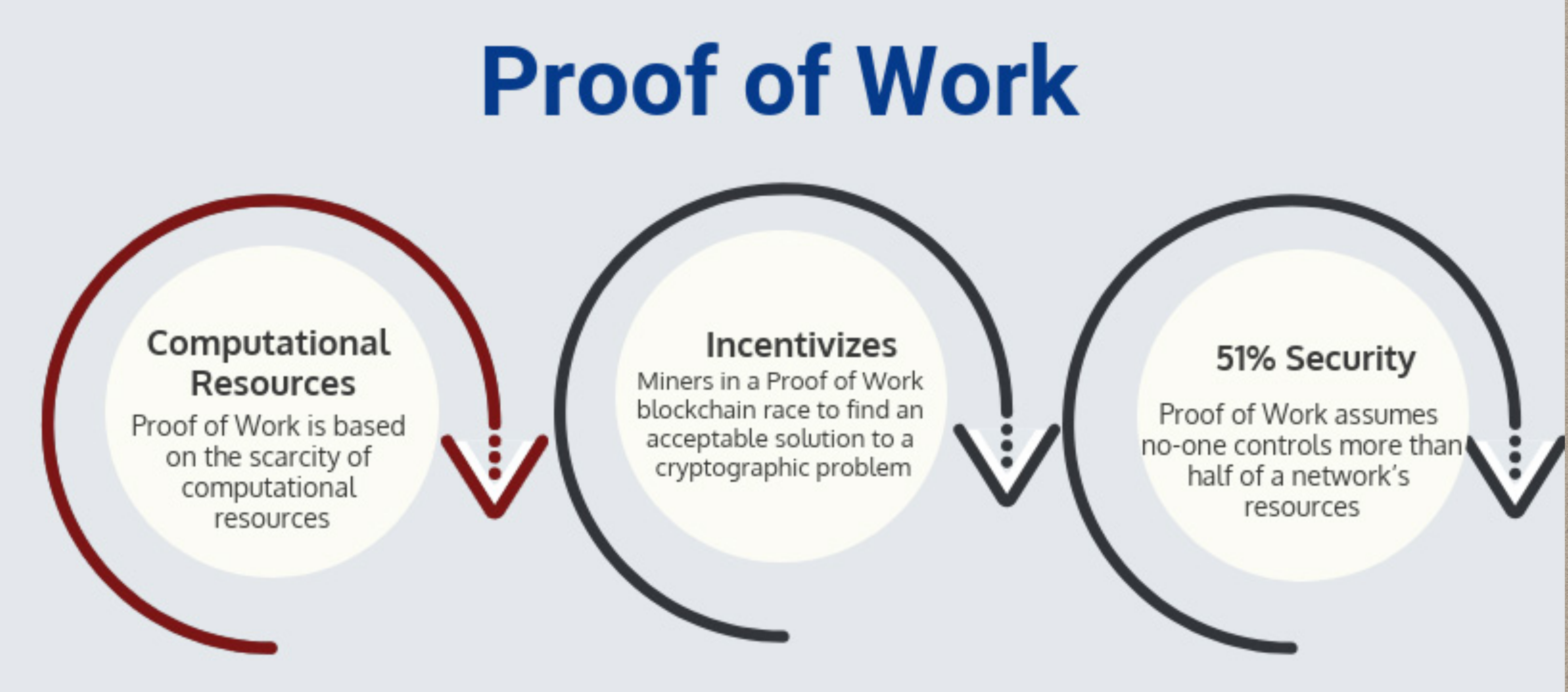
When a transaction was announced, all tribe members updated their mental ledger

BLOCKCHAIN CONSENSUS

- **Satoshi Nakamoto**, the creator of blockchain, invented a method to achieve consensus based on **scarcity**.
- Blockchain consensus algorithms boil down to a vote tied to a limited resource, such as CPU cycles.
- Law of Supply and Demand: Collecting enough of an asset to have a controlling share will drive up the price of the asset enough to make achieving that level of control unfeasibly expensive.

CONSENSUS ALGORITHMS

- Proof of Work (PoW)
- Proof of Stake (PoS)
- Proof of Burn (PoB)
- Proof of Elapsed Time (PoET)
- And others…



Proof of Work

Computational Resources
Proof of Work is based on the scarcity of computational resources

Incentivizes
Miners in a Proof of Work blockchain race to find an acceptable solution to a cryptographic problem

51% Security
Proof of Work assumes no-one controls more than half of a network's resources

BITCOIN USES PROOF OF WORK

BASED ON SCARCITY OF CPU RESOURCES

CONCLUSION

REVIEW OF KEY TERMS

- Peer-to-peer network
- Distributed ledger
- Consensus algorithms based on scarcity

μου κροτηθέντος· τρέπονται ῥωμαῖοι καὶ πολὺς ἐγένετο φθόρος·
βούλγαροι
ῥωμαῖοι

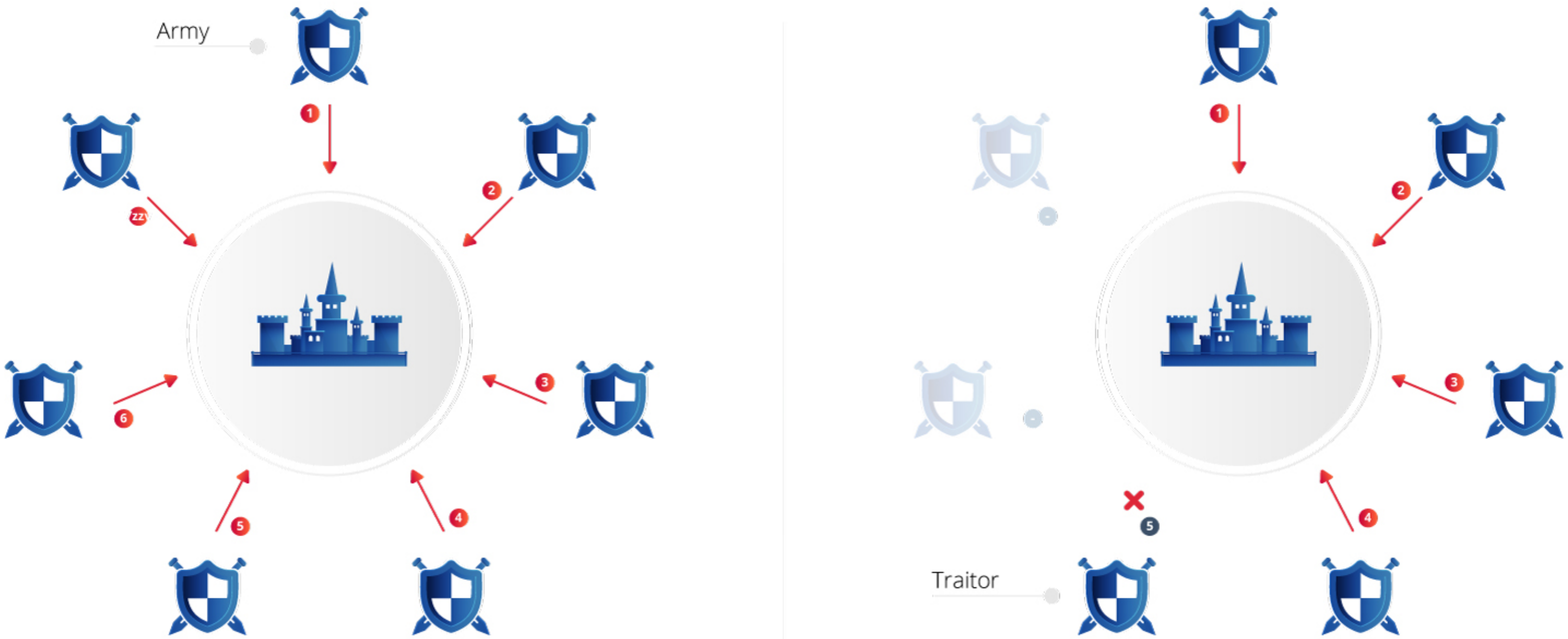
THE BYZANTINE GENERALS PROBLEM

IF ALL GENERALS ATTACK, THE ATTACKERS WIN.
IF ANY HOLD OUT, THE ATTACKERS LOSE.

Byzantine Fault Tolerance

Coordinated attack ✓

✗ **Uncoordinated attack**



Lisk ACADEMY