BlockChain

Farid Dehgan

Tabriz Open Software Talks
March 2018

Outline

- Blockchain
- Why?
- Applications
- Smart Contract
- Proof of work
- Proof of Stake
- Proof of Importance
- Proof of Capacity
- Tools

BlockChain

WHAT IS BLOCKCHAIN TECHNOLOGY?

A digital ledger that keeps a record of all transactions taking place on a peer-to-peer network

All information transferred via blockchain is encrypted and every occurrence recorded, meaning it cannot be altered

It is decentralised, so there's no need for any central, certifying authority

It can be used for much more than the transfer of currency; contracts, records and other kinds of data can be shared

Encrypted information can be shared across multiple providers without risk of a privacy breach

Source: *IoT World News*

7 WAYS THE BLOCKCHAIN CAN HELP THE ENVIRONMENT

ENVIRONMENTAL TREATIES

TRACK REAL IMPACT AND COMPLIANCE OF ENVIRONMENTAL TREATIES
DECREASE FRAUD AND MANIPULATION

ENERGY

INCREASE EFFICIENCY WITH P2P ELECTRICAL GRIDS
IMPROVE ACCESS TO POWER IN AREAS WITH POVERTY OR NATURAL DISASTERS

NON-PROFITS

TRACK WHERE DONATIONS ARE GOING
DECREASE INEFFICIENCY AND BUREAUCRACY IN CHARITIES

RECYCLING

ENCOURAGE RECYCLING BY PROVIDING TOKENIZED REWARD
TRACK AND EVALUATE EFFICACY OF RECYCLING PROGRAMS

CARBON TAX

CALCULATE TAX FOR PRODUCTS BASED ON CARBON FOOTPRINT
CREATE A REPUTATION SYSTEM FOR COMPANIES BASED ON EMISSIONS

SUPPLY CHAINS

TRANSPARENTLY TRACK PRODUCTS FROM ORIGIN TO STORE SHELF
REDUCE CARBON FOOTPRINT AND UNSUSTAINABLE PRACTICES

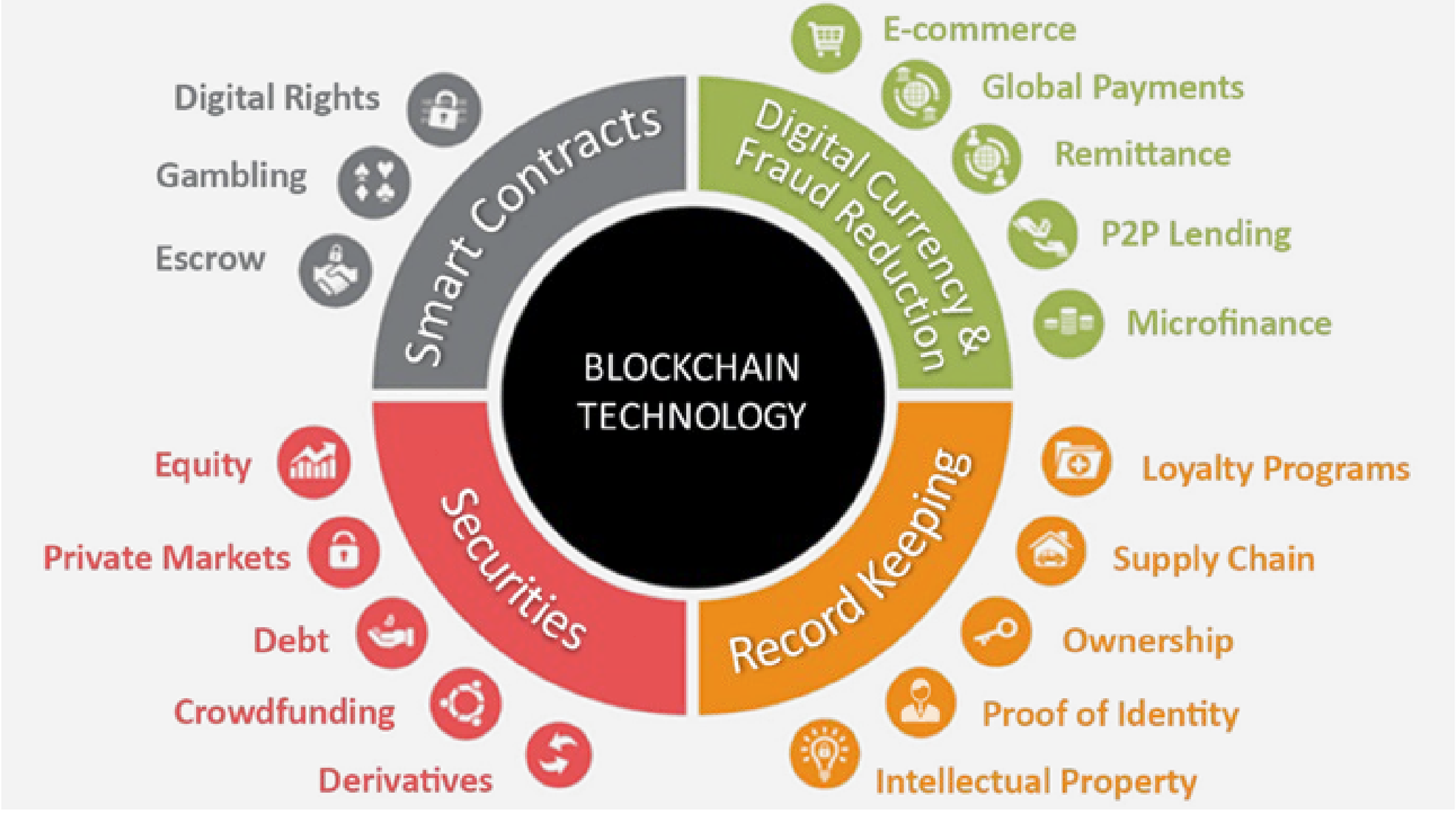
CHANGING INCENTIVES

ALIGN INCENTIVES WITH SUSTAINABLE PRACTICES
CREATE INCENTIVES FOR PEOPLE TO ACT IN SUSTAINABLE WAYS

CREATED BY
FUTURETHINKERS.ORG

INFORMATION BY
BCDC.ONLINE

Applications



Blockgee

1

An option contact between parties is written as code into the blockchain. The individuals involved are anonymous, but the contact is the public ledger.

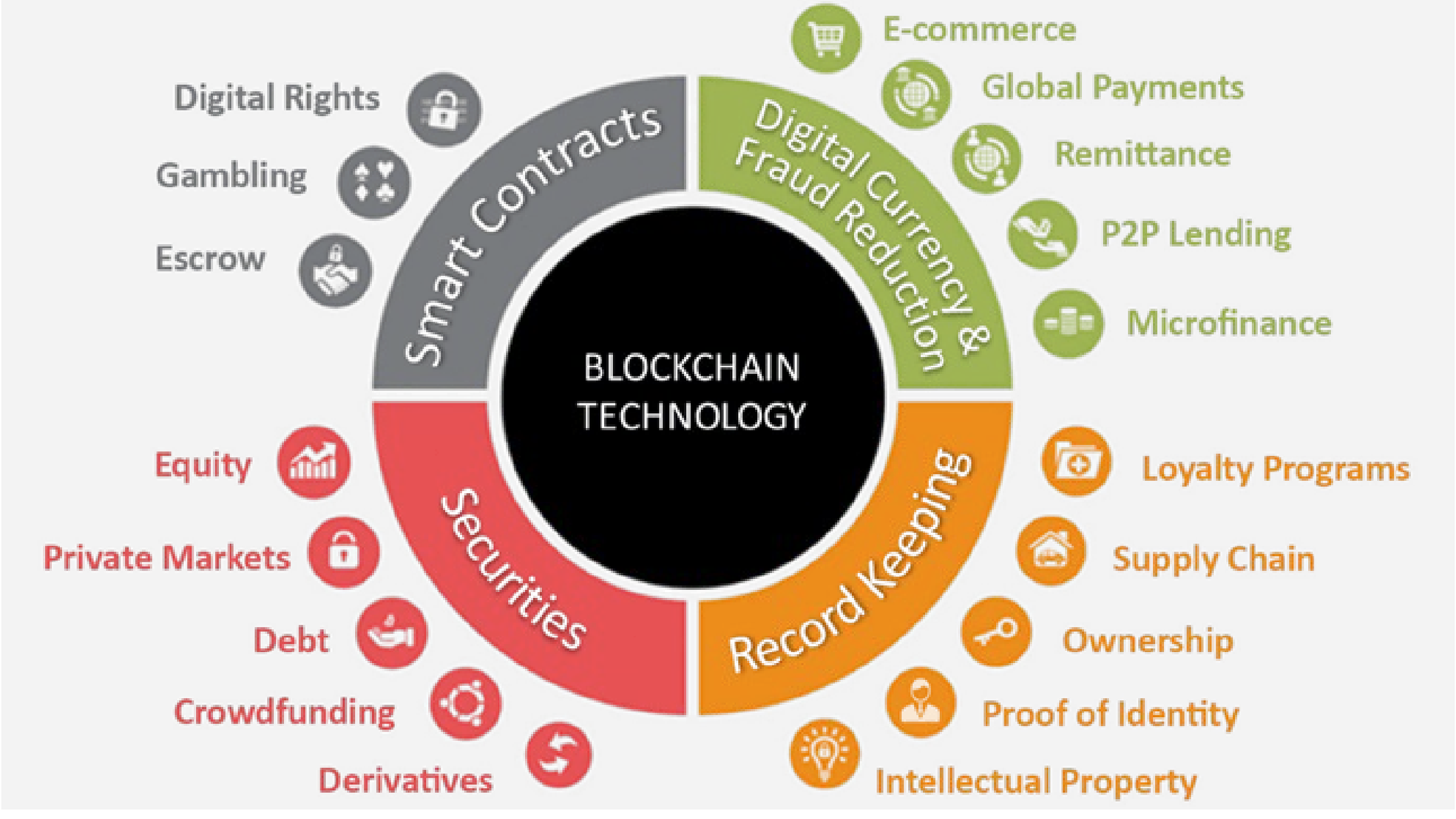
2

A triggering event like an expiration date and strike price is hit and the contract executes itself according to the coded terms.

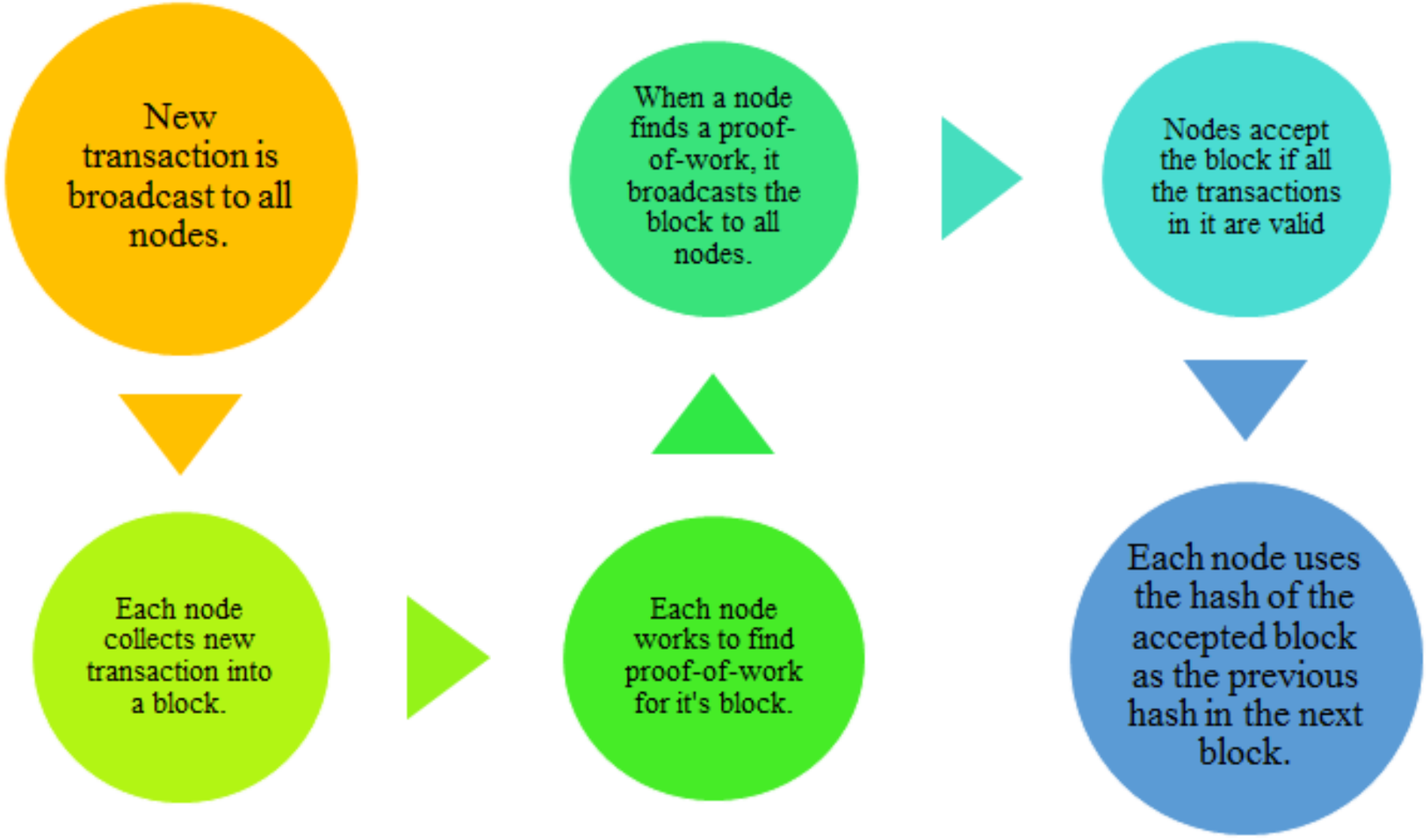
3

Regulators can use the blockchain to understand the activity in the market while maintaining the privacy of individual actors' positions

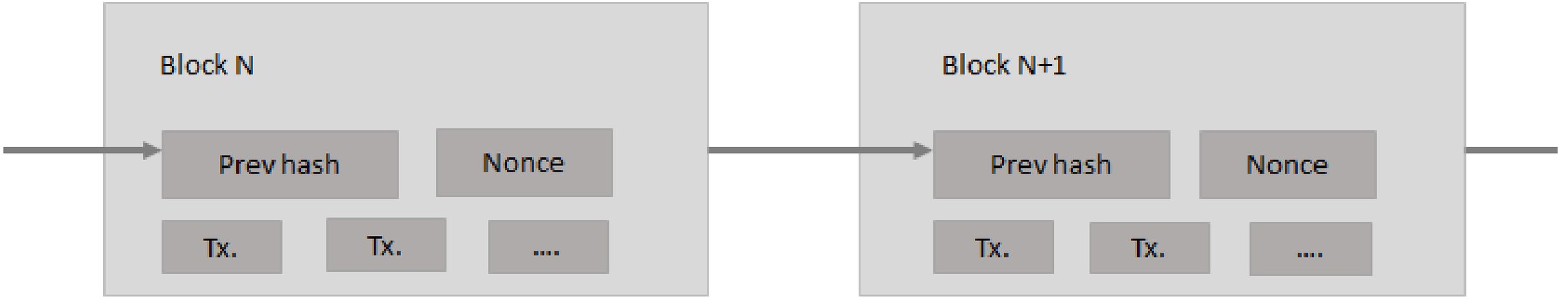
Applications



Proof of Work



Proof of Work



ETHEREUM'S PROOF OF STAKE

SMART CONTRACT: CASPER

VALIDATORS TRANSFER THEIR STAKE TO CASPER

CASPER WILL IMPLEMENT 2 ROUNDS OF VOTING

CASPER WILL SLASH ANY BAD VALIDATORS

VALIDATORS

HAVE 2 VOTING FUNCTIONS:

-PREPARE - COMMIT

THESE VOTES ARE WEIGHTED BY AMOUNT STAKED

VALIDATORS CAN ONLY VOTE ONCE PER POSITION ON THE BLOCK CHAIN

THE 2 ROUNDS OF VALIDATOR VOTES BUILDS CONSENSUS

MIJIN
PRIVATE CHAIN

XEM
PUBLIC CHAIN

BUILT WITH

@ontofractal

NEM
BLOCKCHAIN SOFTWARE

USES

PoI
CONSENSUS ALGORITHM

BASED ON

EIGENTRUST++

EVOLUTION OF

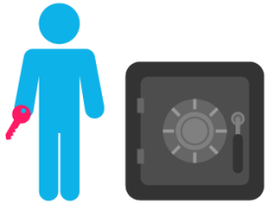
EIGENTRUST

Proof of Capacity

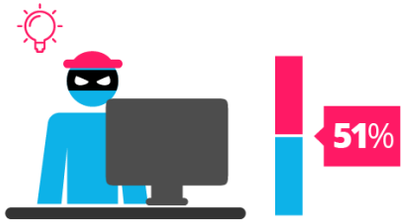
Blockgeeks

Proof of Work vs Proof of Stake

proof of work is a requirement to define an expensive computer calculation, also called mining

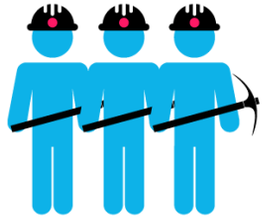


Proof of stake, the creator of a new block is chosen in a deterministic way, depending on its wealth, also defined as stake.



A reward is given to the first miner who solves each blocks problem.

The PoS system there is no block reward, so, the miners take the transaction fees.



Network miners compete to be the first to find a solution for the mathematical problem

Proof of Stake currencies can be several thousand times more cost effective.

PROOF OF CAPACITY VS PROOF OF STAKE

POC IS MORE DECENTRALIZED

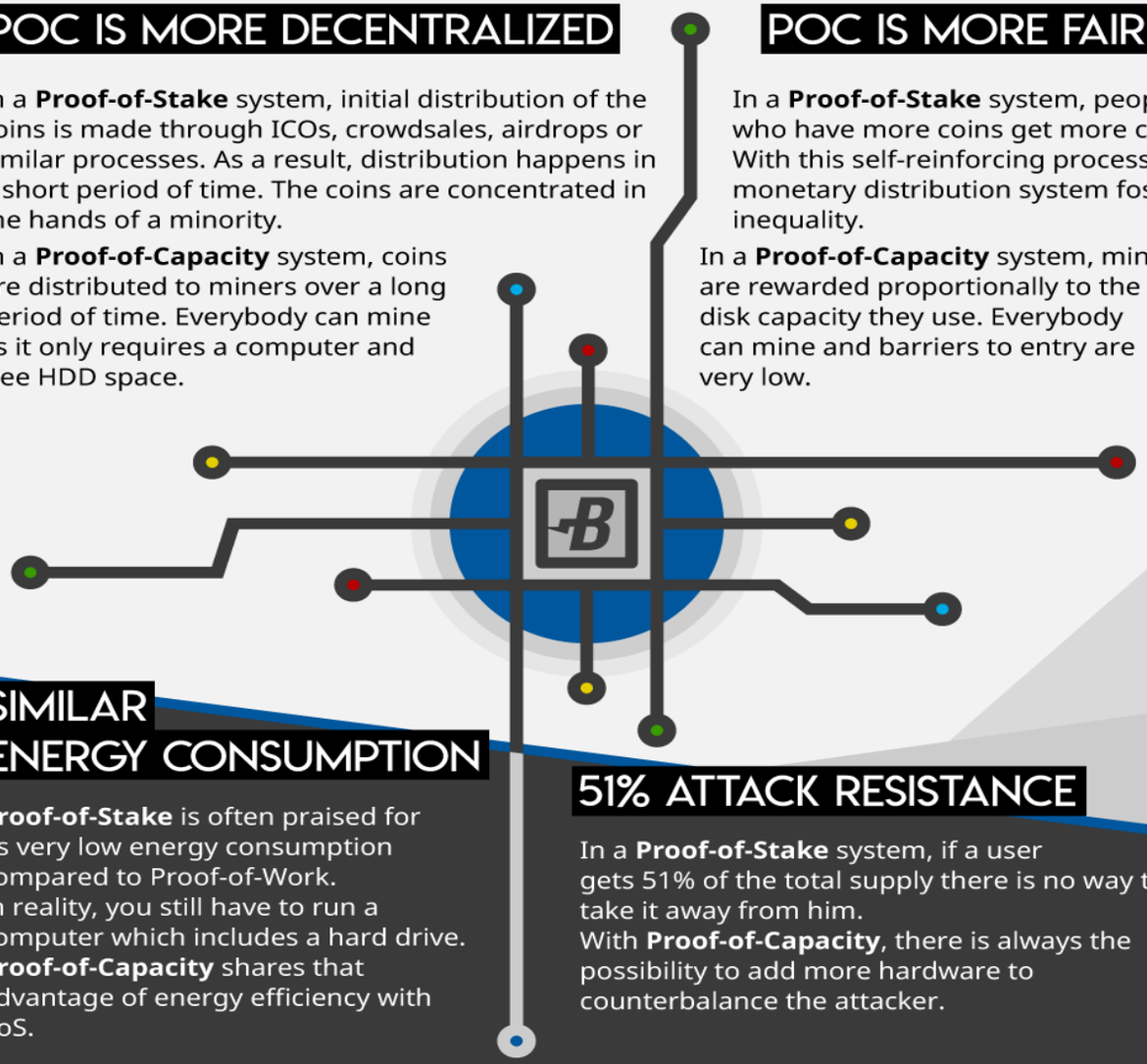
In a **Proof-of-Stake** system, initial distribution of the coins is made through ICOs, crowdsales, airdrops or similar processes. As a result, distribution happens in a short period of time. The coins are concentrated in the hands of a minority.

In a **Proof-of-Capacity** system, coins are distributed to miners over a long period of time. Everybody can mine as it only requires a computer and free HDD space.

POC IS MORE FAIR

In a **Proof-of-Stake** system, people who have more coins get more coins. With this self-reinforcing process this monetary distribution system fosters inequality.

In a **Proof-of-Capacity** system, miners are rewarded proportionally to the disk capacity they use. Everybody can mine and barriers to entry are very low.



SIMILAR ENERGY CONSUMPTION

Proof-of-Stake is often praised for its very low energy consumption compared to Proof-of-Work.
In reality, you still have to run a computer which includes a hard drive. **Proof-of-Capacity** shares that advantage of energy efficiency with PoS.

51% ATTACK RESISTANCE

In a **Proof-of-Stake** system, if a user gets 51% of the total supply there is no way to take it away from him.
With **Proof-of-Capacity**, there is always the possibility to add more hardware to counterbalance the attacker.

Platforms

- Solidity
- Truffle
- Embark
- Web3.js
- Meteor