



Paul Pinault

Blog/contact : www.disk91.com

Twitter : @disk_91

YouTube: <https://www.youtube.com/c/PaulPinault>

BlockChain Technology

Introduction to Blockchain Technology and associated application

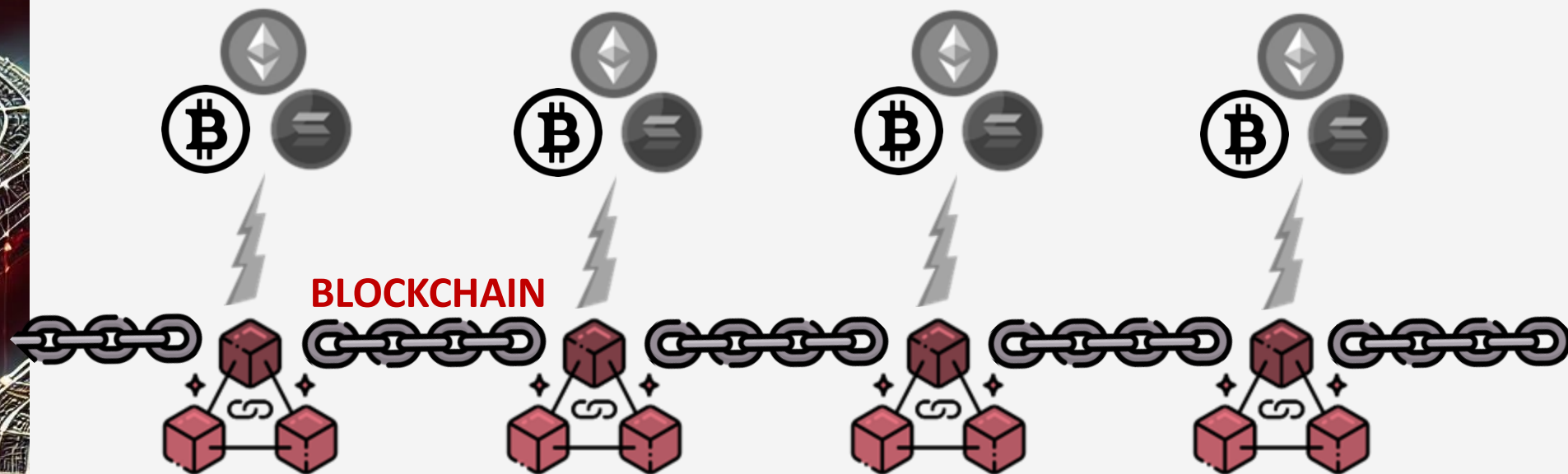


Crypto is not ...

Blockchain

A CRYPTO ASSET is a product and a fuel of the blockchain execution

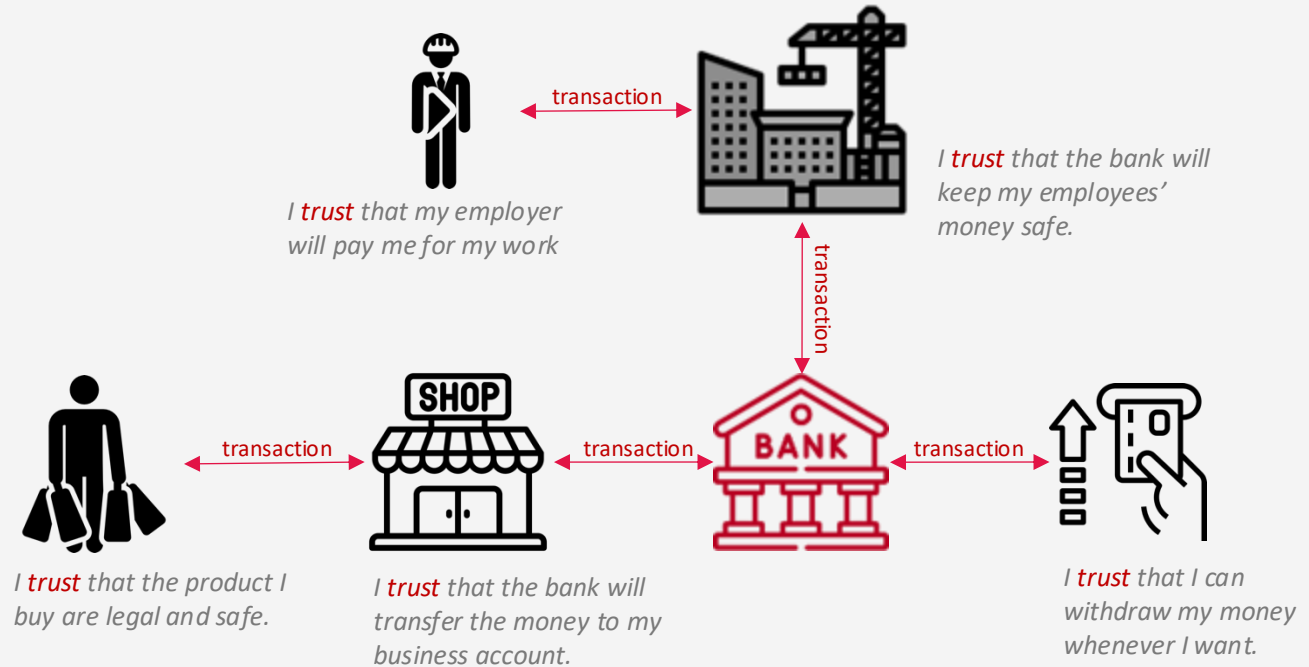
CRYPTO ASSETS



- A BLOCKCHAIN is a technology
- It stores transactions, contracts
 - It creates trust with math & algorithm

Blockchain is a ...

Trust solution



The **trusted third party** is the one who will guarantee the proper execution of the transaction through its statutory position and a legal framework.

Common ...

Trusted third parties



I **trust** companies for

- Salary
- Product conformity
- ...



I **trust** notary for

- Recording real estate transactions
- Secure my will
- ...



I **trust** bank for

- Keeping my money safe
- Execute payments
- ...



I **trust** accountant for

- Delivering accurate financial statements
- ...



I **trust** state for

- Creating money
- Have stable laws
- ...



I **trust** shop for

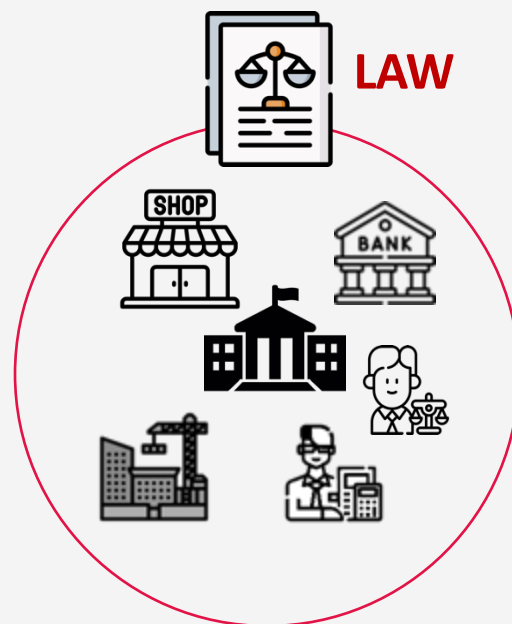
- Delivering goods
- Ensure the guarantee
- ...



The **law** secures trust by imposing deterrent penalties on those who would break it.

Trust ...

Systemic vs Algorithmic



A *trust system* built around a state (or cross-state organization) and laws is interdependent and strengthens as it grows, yet remains fragile



An *algorithmic trust* will autonomously create trust based on its own set of rules (smart contract) that are mathematically verifiable, without human intervention.

What builds trust ?

3 Trust keys



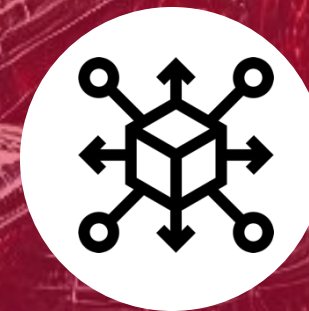
Smart Contract

Defines the rules applicable to transaction, only these rules apply



Transparency

Smart Contracts and transactions are accessible to anyone



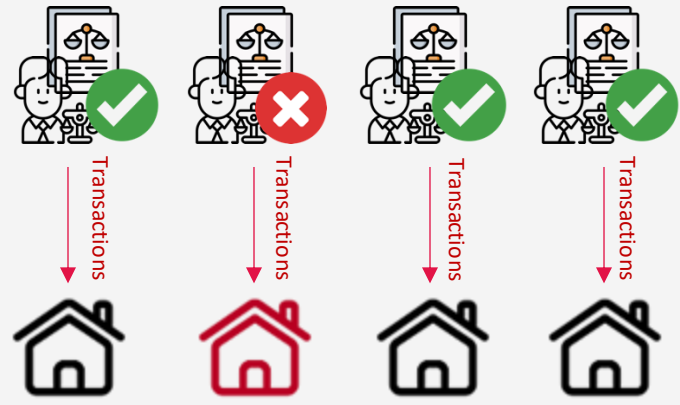
Distribution

Execution of smart contract, audit, validation of blocs is made "randomly" by any member of the blockchain

Trust ...

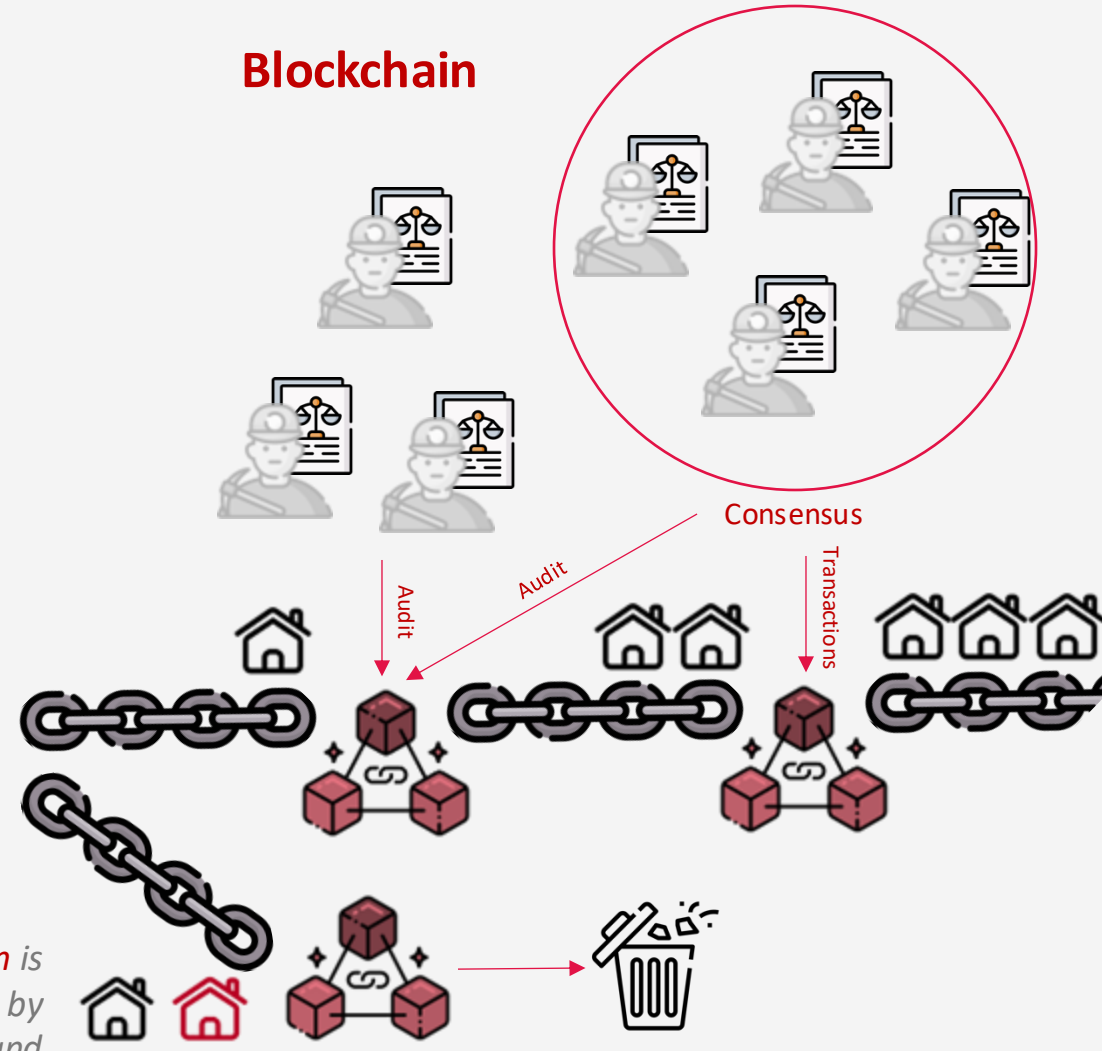
Mechanism

Traditional



A *malicious transaction* has been added by a single person (a trusted third party) into the transaction list.

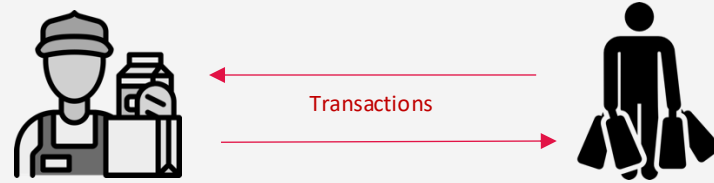
Blockchain



A *malicious transaction* is immediately identified by most of the members and rejected

Blockchain is recording ...

Transactions



A *transaction* involved, in general, 2 entities and can be composed by multiple operations

TRANSACTION

FROM
TO
DATE
AMOUNT



Blockchain is recording ...

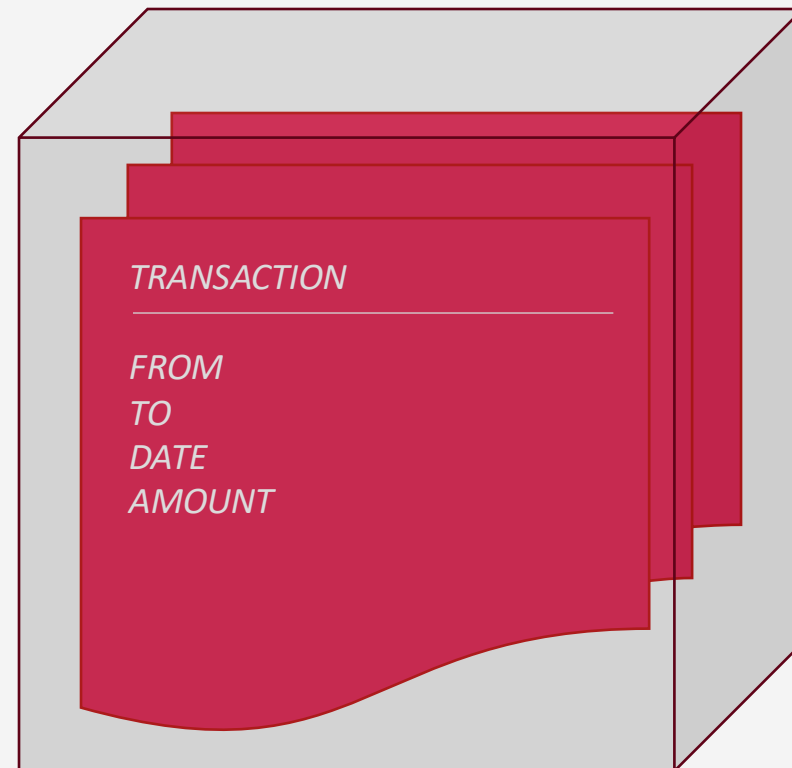
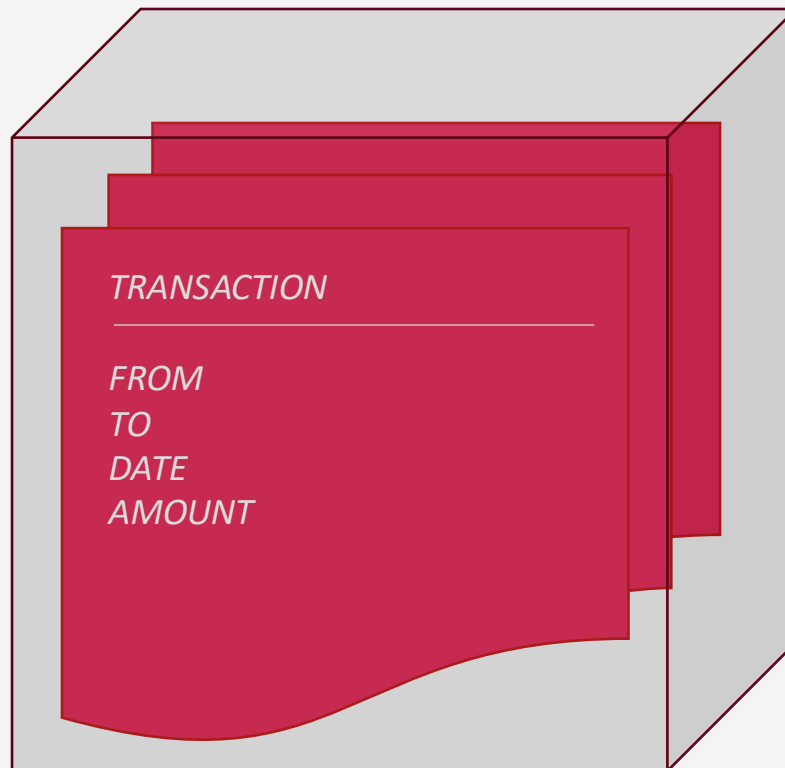
Transactions into blocks

A *block* is a group of transactions processed at a single moment.

Periodic *block* creation makes the blockchain pace predictable and scalable.

T

T+X



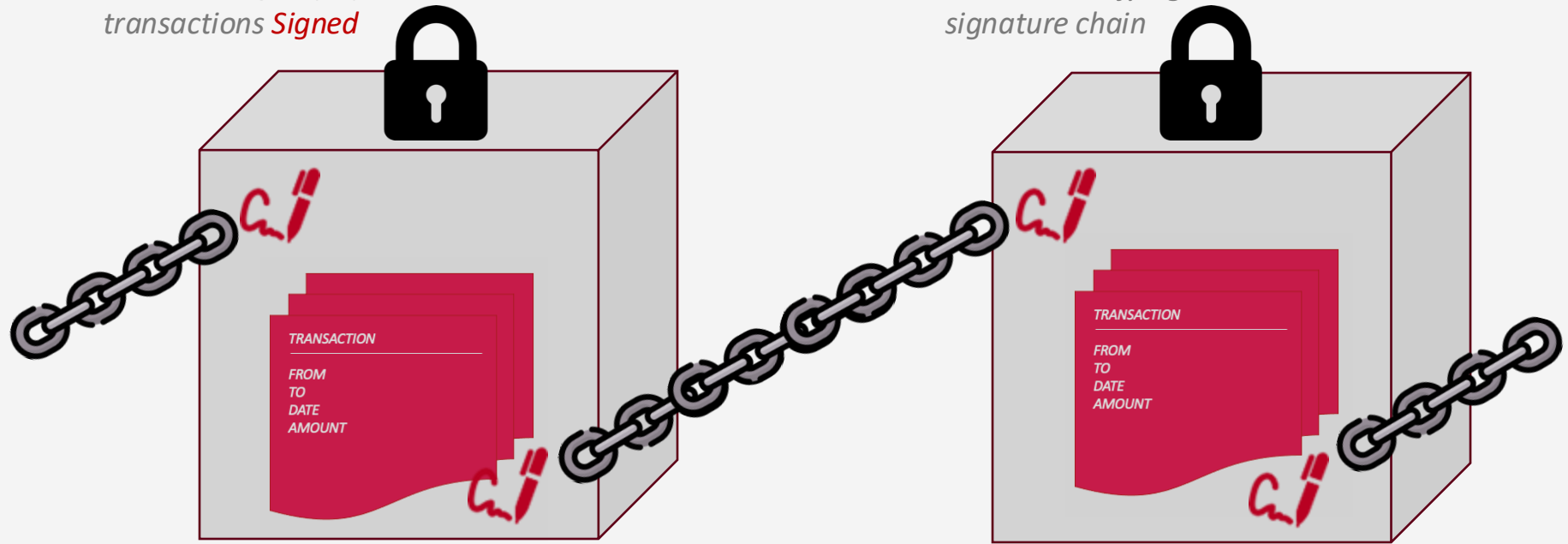
Blockchain is recording ...

Transactions into blocks



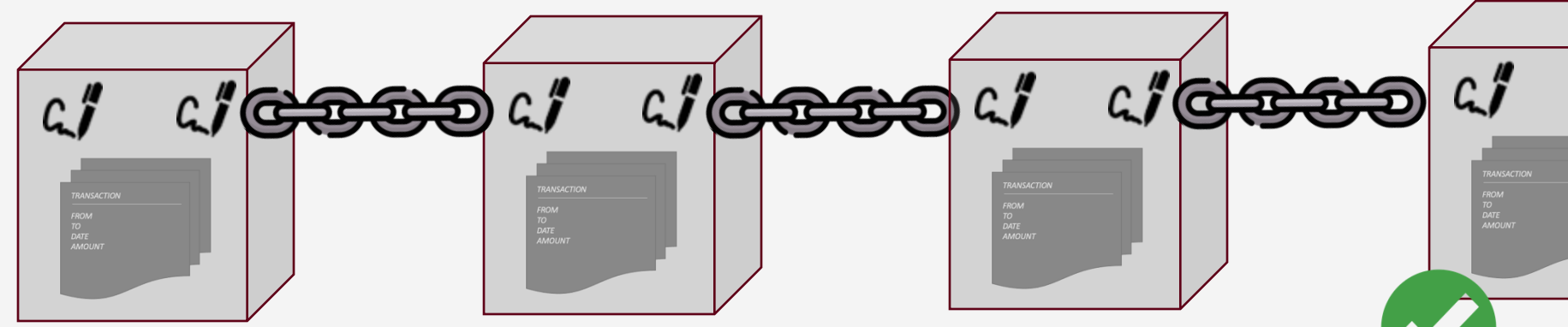
A *block* is a group of transactions *Signed*

A block contains the *previous signature* so it's impossible to modify a previous block without modifying the whole signature chain

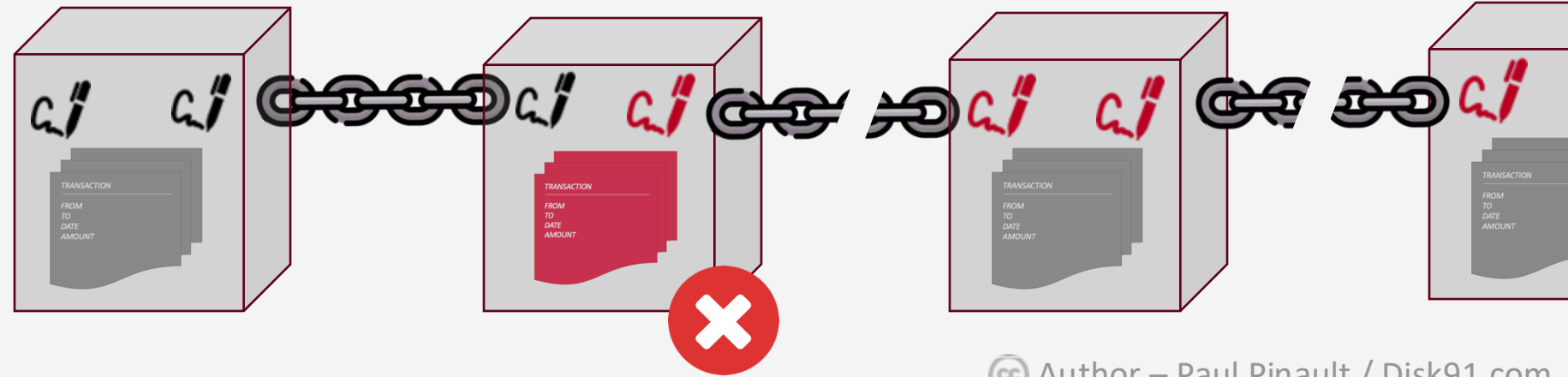


Blockchain is recording ...

Transactions into blocks



If a **malicious transaction** modify a block, the signature will change and not match the following signature. Chain is broken, this malicious block will be **rejected**



BlockChain manage smart contract and ...

Wallets

A *wallet* is a virtual representation of the transaction sequence like a bank account.

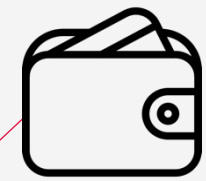
TRANSACTION

FROM
TO
DATE
AMOUNT



- CREATE TRANSFERT,
CONSUME TOKEN

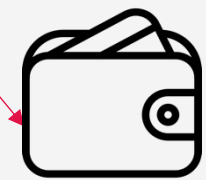
Rules



Own



Transactions



Own



Blockchain manage dynamic...

Smart Contract Execution


A *wallet* is a virtual representation of the transaction sequence like a bank account.




Generic Smart Contract Rules


- ADD, REMOVE, MODIFY, EXECUTE SMART CONTRACTS
- CREATE TRANSFERT, CONSUME NAATIVE TOKEN

TRANSACTION

DATA IN 

DATA OUT 

DATE

 Specific Smart Contract

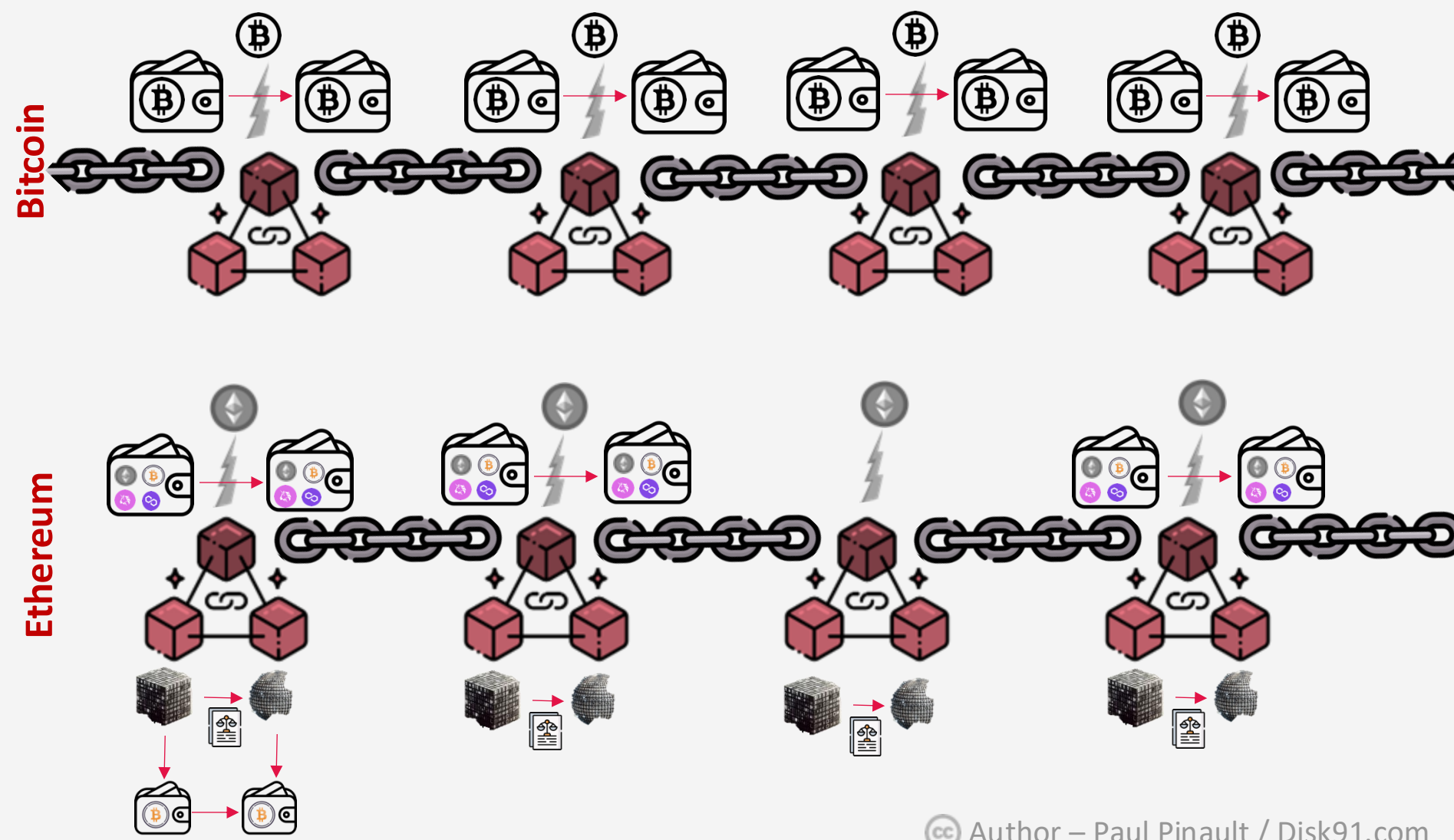


DATA TRANSFORMATION



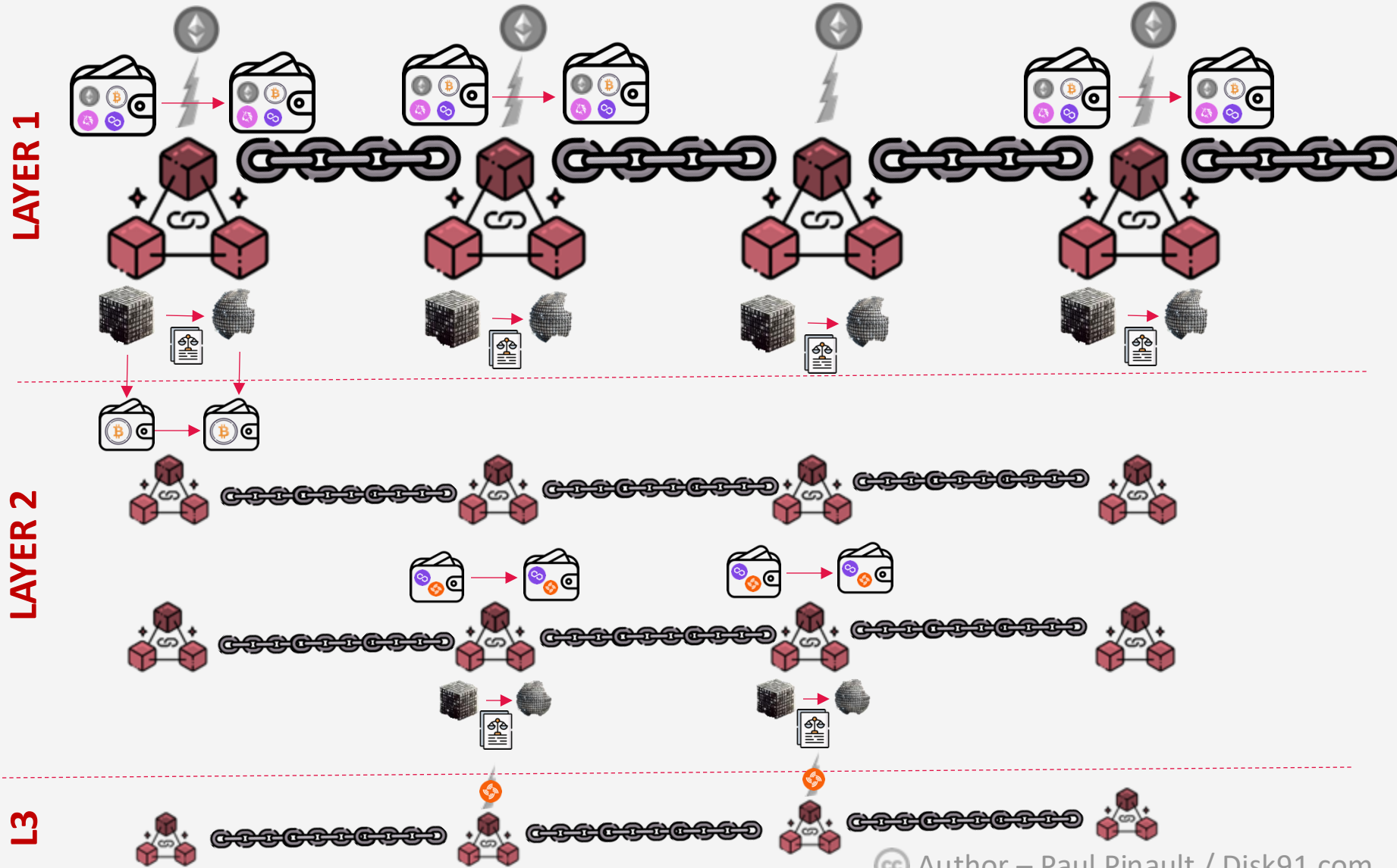
Two type of blockchains...

Bitcoin vs Ethereum



Smart Contracts allows ..

Multi-Layer Blockchains





BlockChain is also...

NFT (Non-Fungible Token)

An **NFT** is a digital ownership title that can be exchanged with predefined and unique rules.

NFT

SIGNATURE

CREATOR

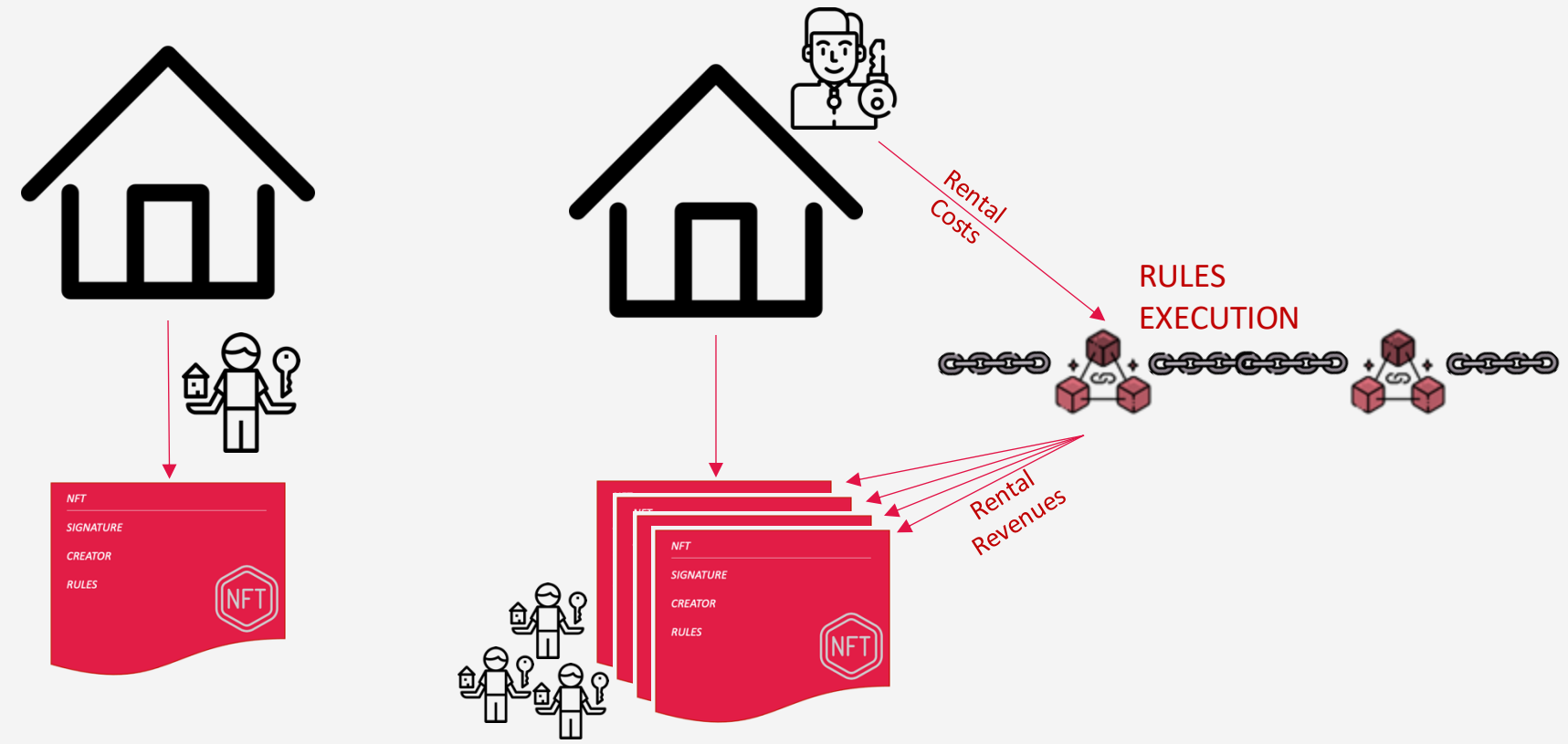
RULES



- IT CAN BE ART BUT **IT'S NOT ART**
- IT CAN BE
 - House
 - Art
 - Music rights
 - Physical Equipment
 - Vote rights
 - Car ownership
 - Identity
 - Membership
 - ...
- IT CAN BE
 - An entire property
 - A shared of a property

NFT is for a property or ...

Shared Property

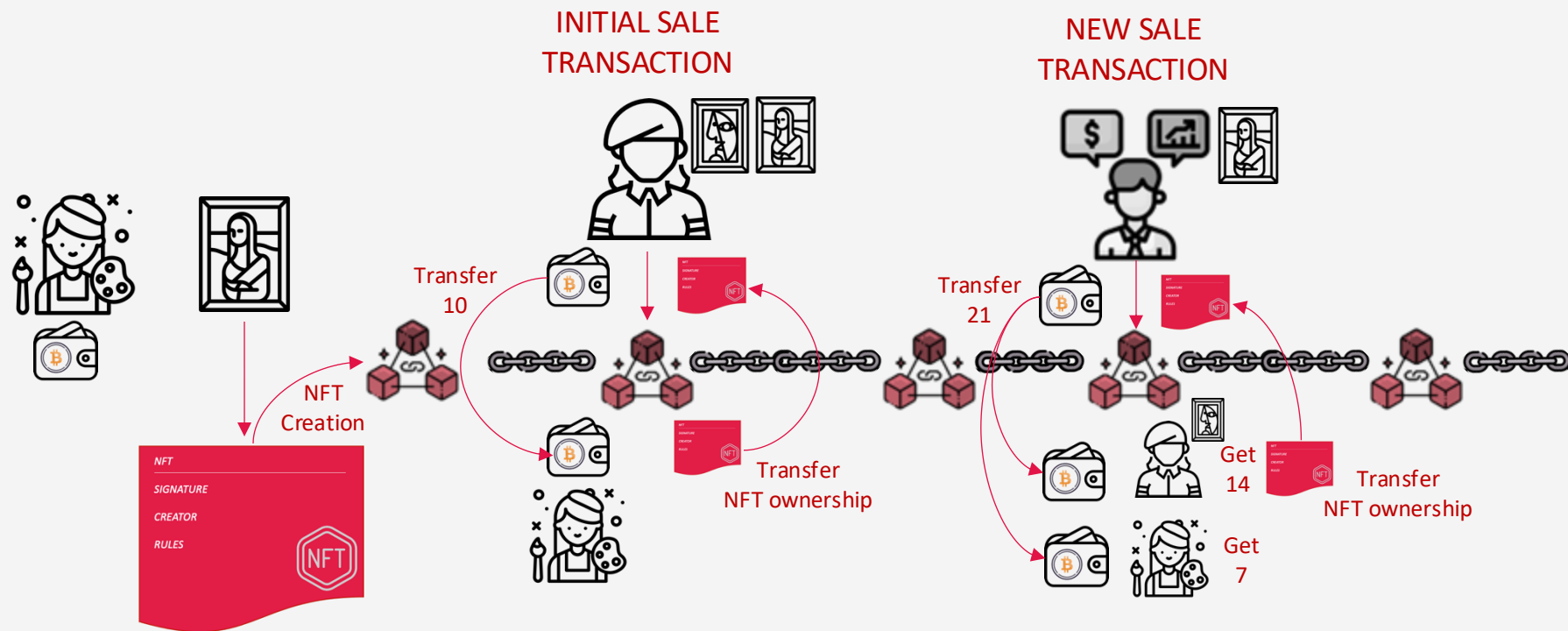


An **NFT** can be a single entity corresponding a physical or digital good / right

An **NFT** can also be a shared of a good / right. With the whole NFTs you can pretend owning the good. You can also get the equivalent shared of good's revenues

NFT provides ...

Rules



An **NFT** is emitted with rule like 33% of any later sale will be given for NFR creator.

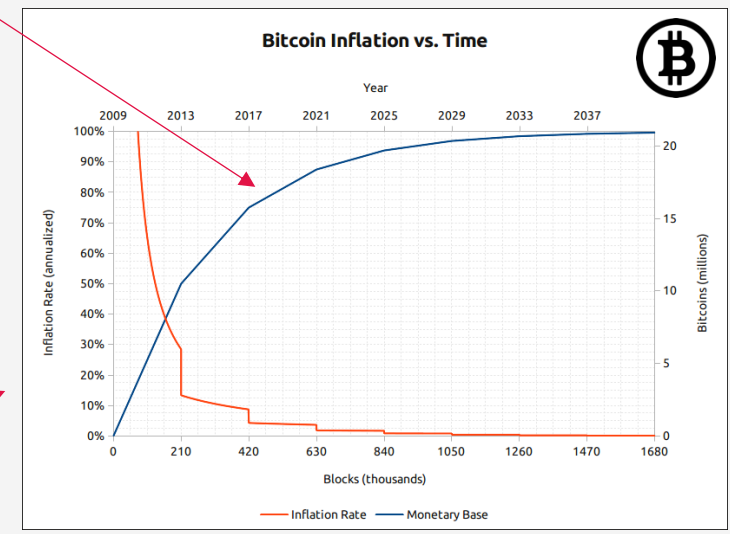
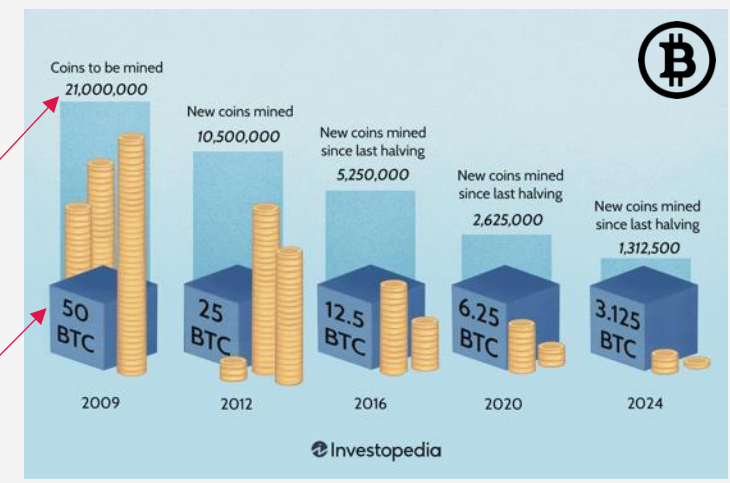
An **NFT** contains rules, there is no definition of the rules by defaults, the blockchain can execute certain type of rules. NFT contains rules selection and parameters.

Blockchains generate...

Tokens



- Have a Market Value
- Can be exchanged
- Represent a voting power
- Have a finite quantity
- Have a scheduled distribution
- Can be destroyed



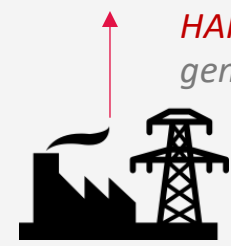
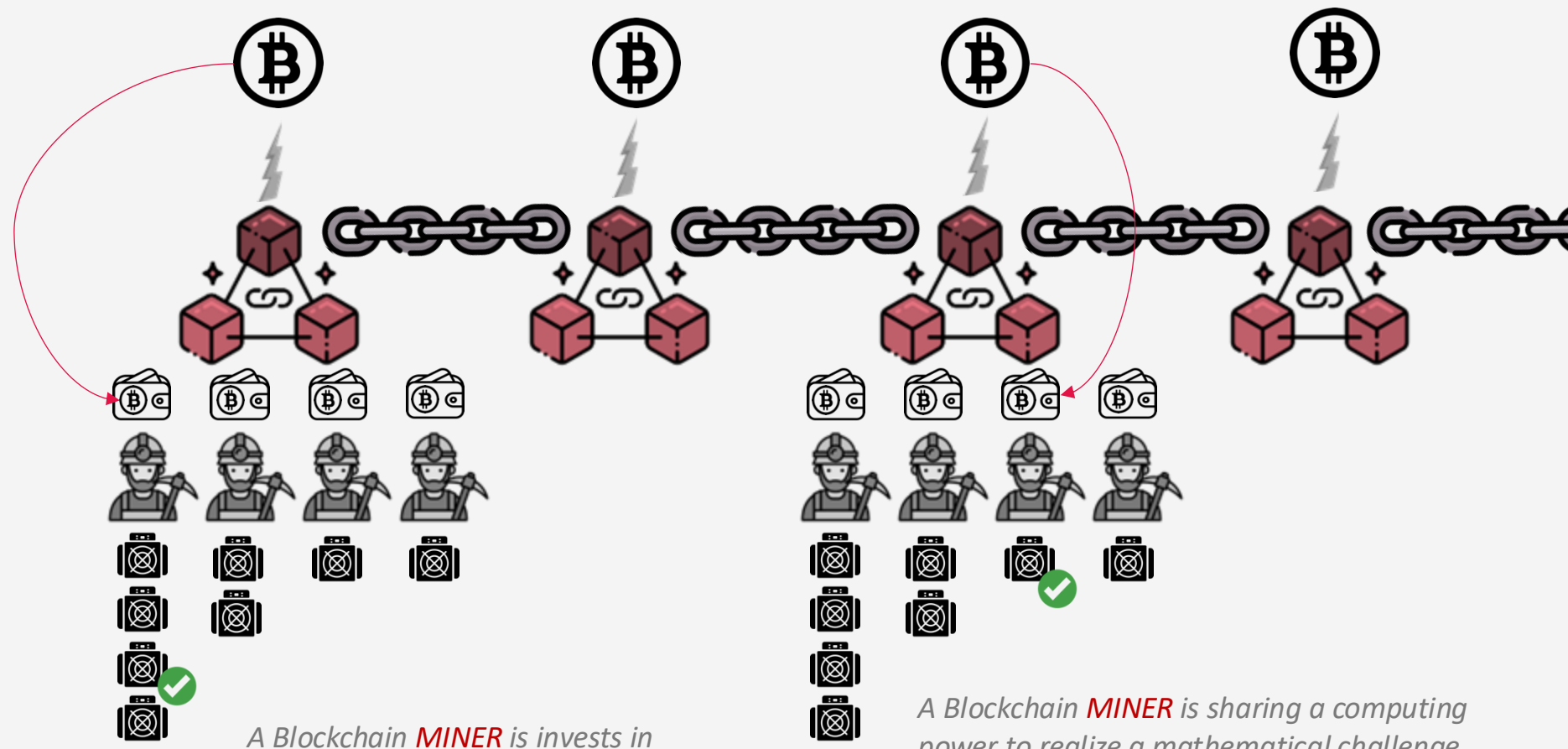
A Blockchain **TOKEN** is closer to **stock** than a currency. Stocks are distributed to worker in relation to their work (Scop – cooperative production company / worker cooperative)

A Blockchain **WHITE PAPER** defines the **TOKEN's** creation rules, distribution rules, total quantity, halving schedules...



Token are mint by...

Miners



A Blockchain **MINER** invests in **HARDWARE** (dedicated like ASIC or generic like GPU), hosting and **POWER**

A Blockchain **MINER** is sharing a computing power to realize a mathematical challenge (Proof of Work - PoW). The first one to successfully realize the mathematical challenges get Tokens as reward.



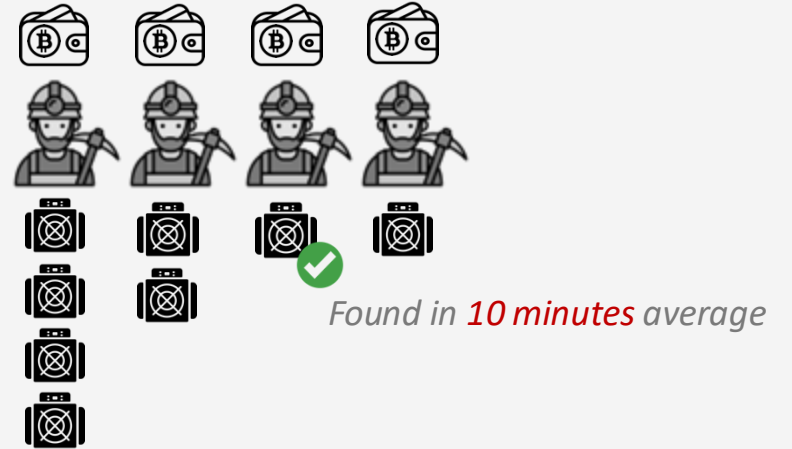
Mining can be achieved different ways like ...


Proof of Work (PoW)

For the value 123456789123456789, find a new value giving a hash result ending with xxxxxxxxxxxx0



For the value 123456789123456789, find a new value giving a hash result ending with xxxxxxxxxxxx000



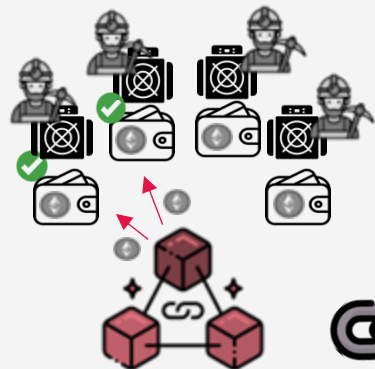
Token **value creation** is linked to **adoption**, adoption linked to **complexity**, complexity linked to **cost**, cost is link value creation. 



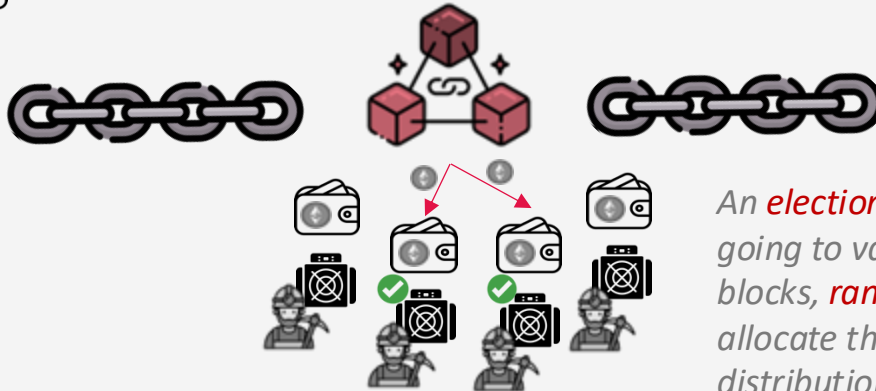


Mining can be achieved different ways like ...

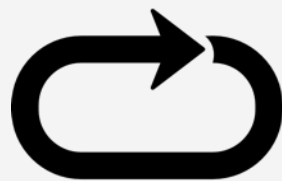
Proof of Stake (PoS)



A stable pool of *Oracle* or *Master Node* or *Validators* locks Tokens for getting a chance to validate blocks, equivalent or related to the amount locked.



An *election* decide who's going to validate the next blocks, *randomly*, and allocate the token distribution to them



Stacking reduce the Token *availability* on the market, availability impacts *token value*, value impact *return on invest*, return on invest impact *stacking* quantities.

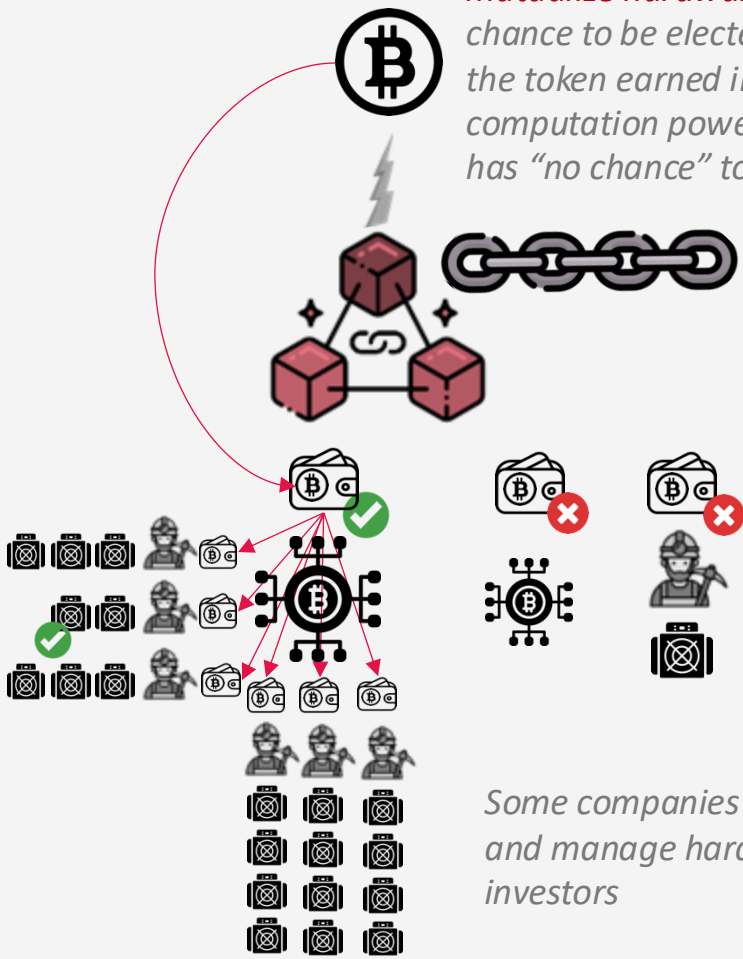
More miner Stacks, less tokens every of them get : the chance to be elected decrease.



Miner can be organized as a ...

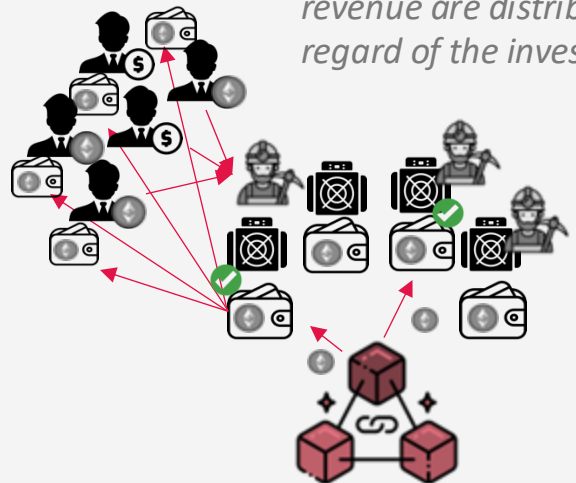
Pool

PoW Blockchain have *Pool* to *mutualize hardware* and get better chance to be elected, then they *share* the token earned in regard of computation power. A single miner has "no chance" to be elected.



Some companies also rent and manage hardware for investors

PoS Blockchain have *Pool* to *mutualize token* investment and create Nodes. The revenue are distributed in regard of the investment



The purpose is to propose a *simplified access to mining* with a recurrent revenue in token (can be a *loss*)



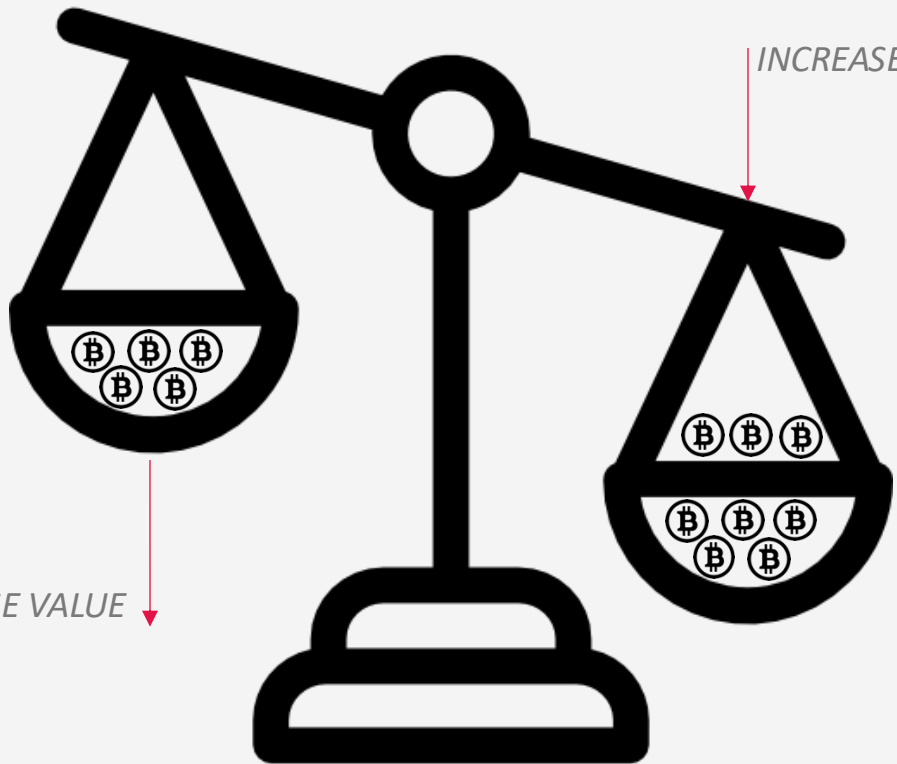
Miner incentive is related to ...

Token Value

OFFER

Comes from:

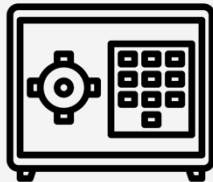
- Mining activity
- Stacking period ending
- Profit taking
- Market Panic
- ...



DEMAND

Comes from:

- Project ambition / traction / FoMo
- Blockchain Transactions
- Stacking
- Entry Fees



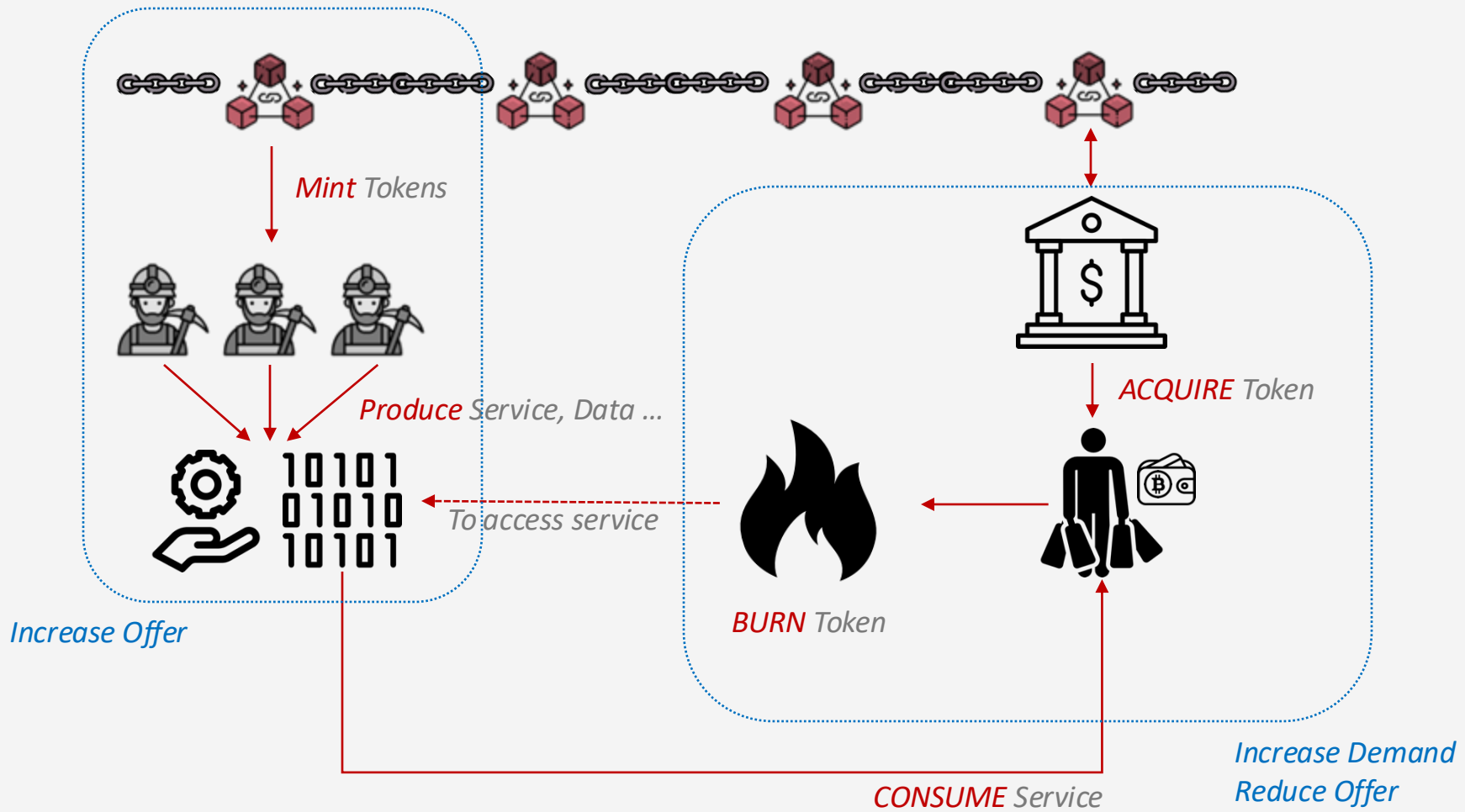
LOCKED (Offer reduction)

Comes from:

- Stacked
- Sleeping wallets (saving)

Demand is driven, long term, based on

Burn & Mint equilibrium

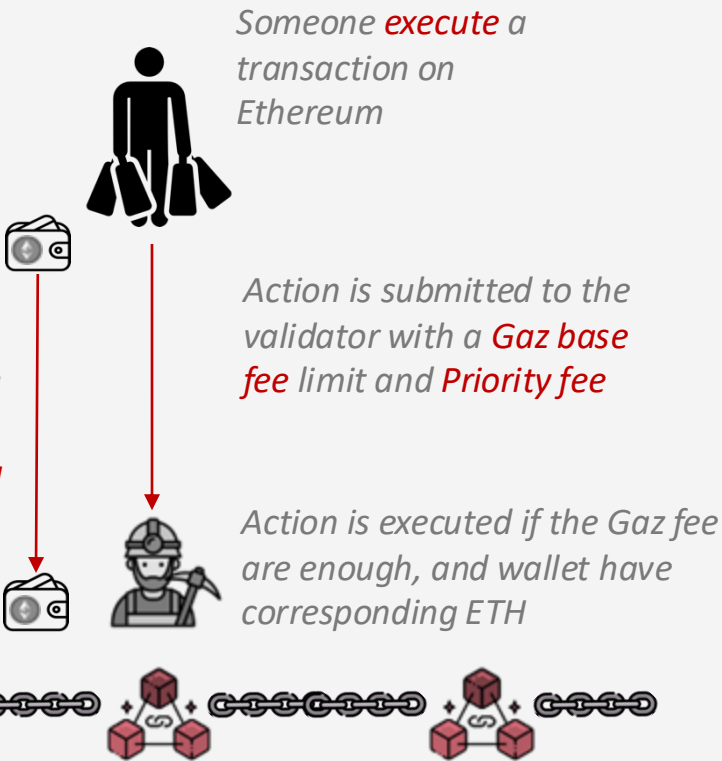


Demand is driven, long term, based on

Ethereum Gaz Fee



Gaz fee pays the **computing power** and depends on transaction **load**



Any action has a cost in unit of gaz (**gwei**)

- ERC20 transfer like 65k
- SWAP like 185k

This is multiplied by the **base fee** (based on load) + **priority fee**.

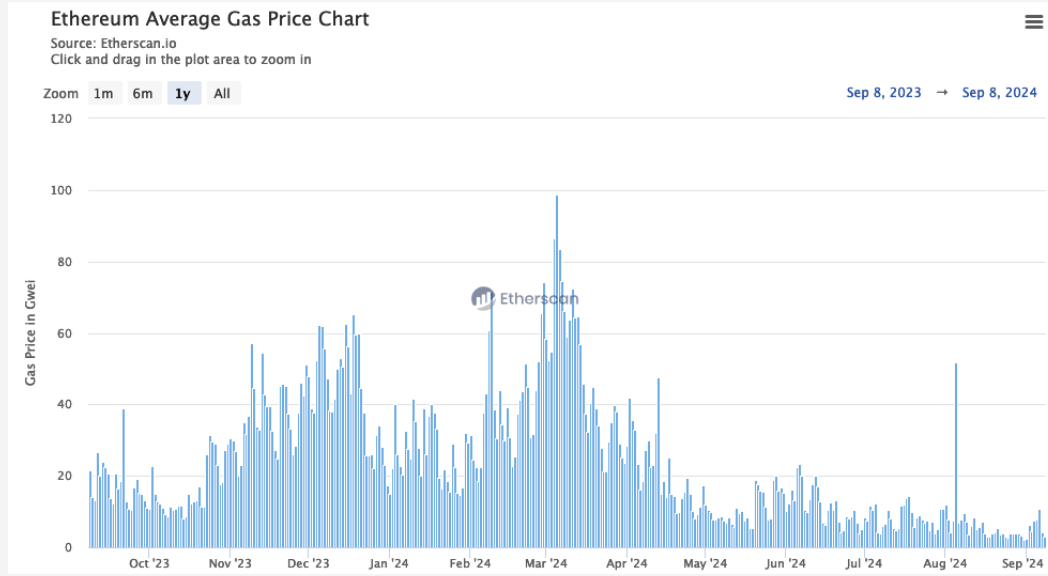
Let's consider 4 gwei for base and 1 for priority

ERC20 transfer like:
Fee (\$) = (65k * (4+1) * ETH cost in \$) / 10^9

Today = \$0,76

Demand is driven, long term, based on

Ethereum Gas Fee



ERC20 transfer like:
 $Fee (\$) = (65k * (98) * \$3346) / 10^9$

ERC20 transfer like:
 $Fee (\$) = (65k * (3) * \$2272) / 10^9$

March 5th = \$21

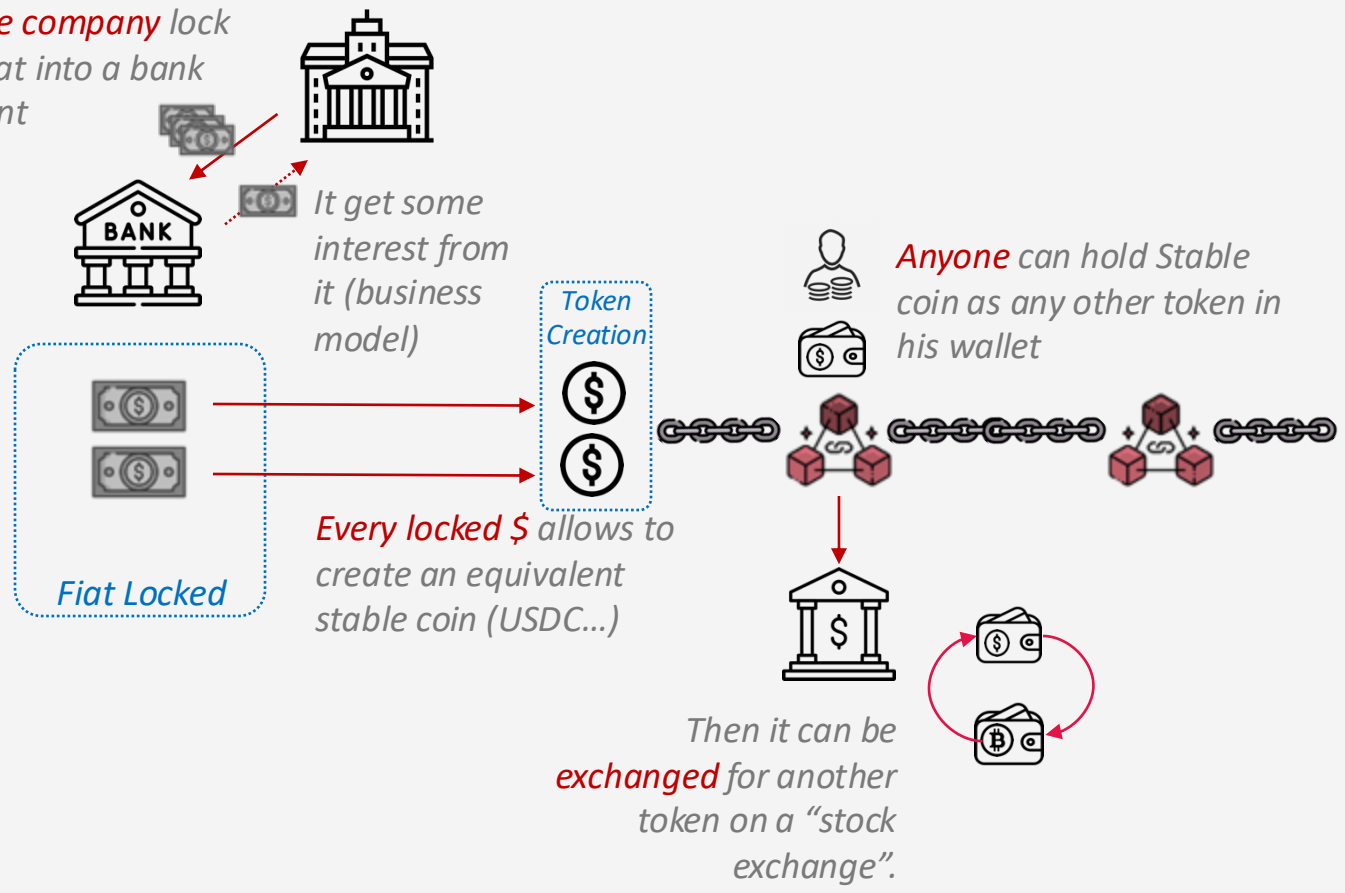
x47
(average)

Sept 1st = \$0.44

Some of the token are a bit particular

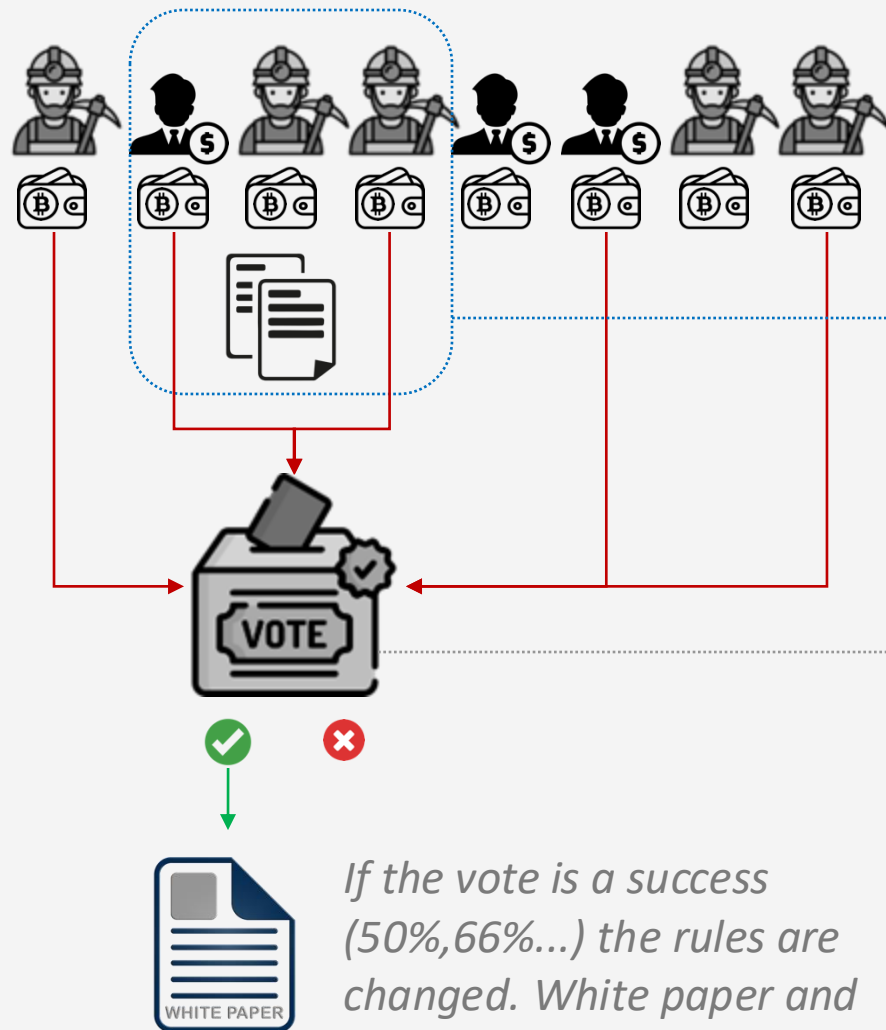
The Stable coins

Private company lock real fiat into a bank account



Blockchain rules are based on

Governance



Blockchain participants

Some of them propose, write a xIP (Improvement Proposal) to modify the Blockchain rules

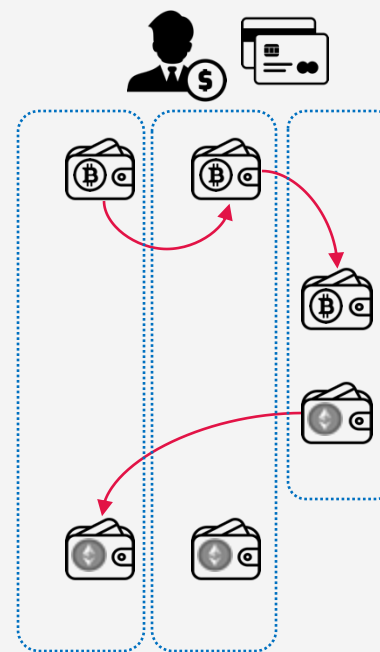
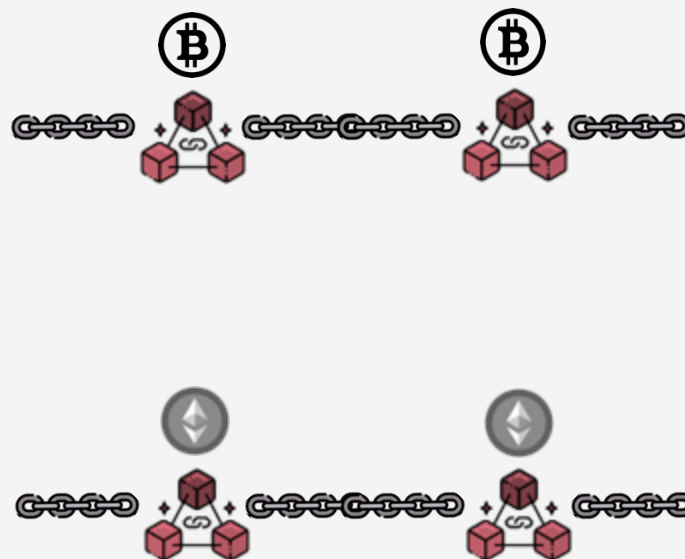
Participant Vote for the xIP based on their voting power. It can be wallet tokens, locked token, locked token with long term incentive...

If the vote is a success (50%,66%...) the rules are changed. White paper and code is updated. Miner may deploy the new rules or fork.

Token can be swapped on

Centralized Exchanges

Transaction on Blockchain are *slow* (like 1h to be confirmed) and *expensive*, they can't be performed from one chain to another (out of bridges)



Native Wallet owned by exchange, global, to avoid blockchain transactions



Virtual Wallet where to have dynamic & immediate exchange at low cost.

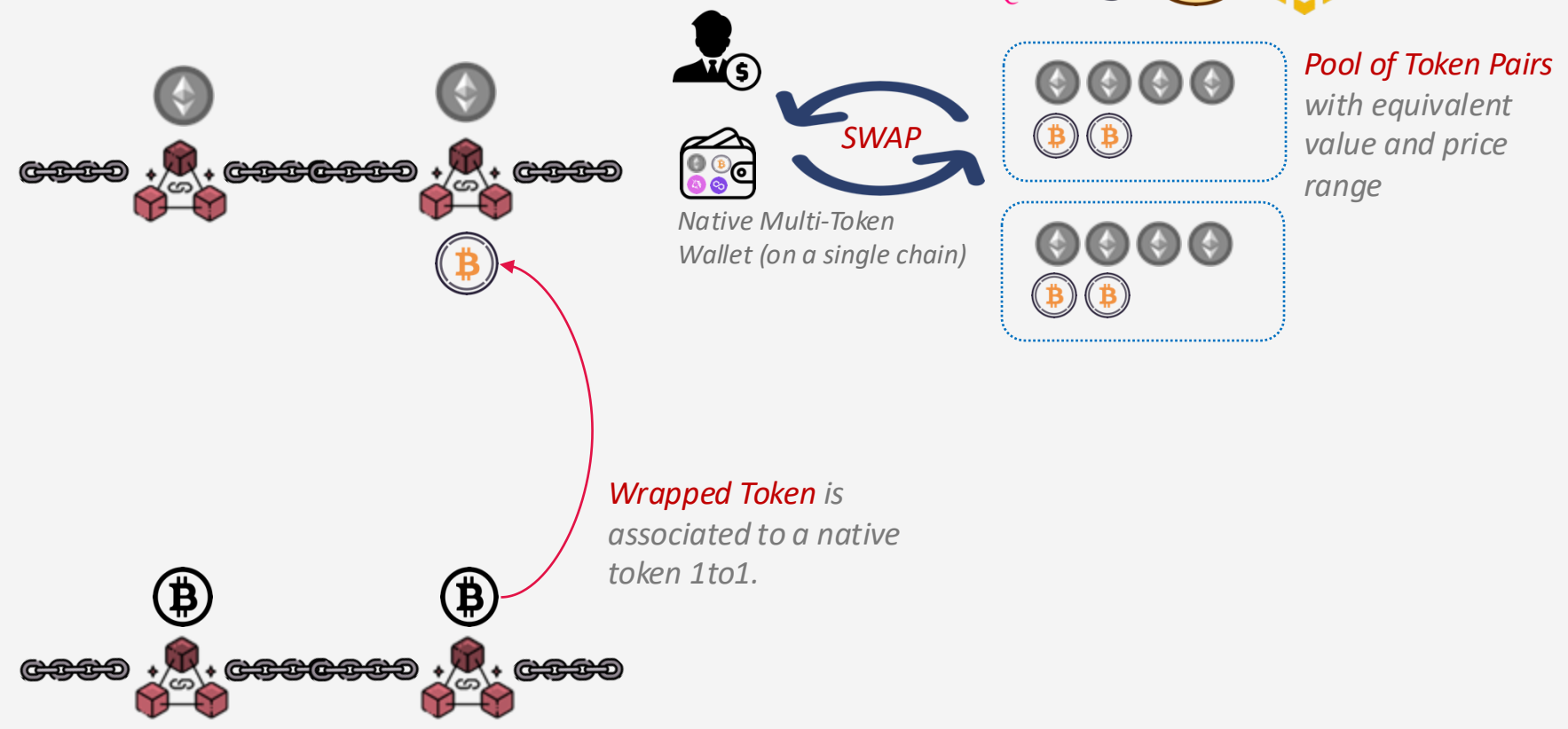
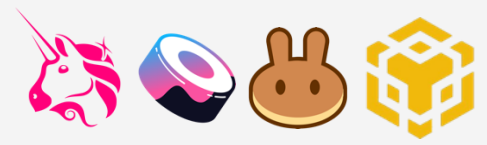
Native Wallet owned by user.

Native Wallet owned by exchange, dedicated to one user.

Token can be swapped on

Decentralized Exchange (Dex)

Dex are Distributed Exchanges with the ability to swap a token with another token.



You can also find

REWARDS

- Air DROP : free Tokens for early adopters
- Fixed or variable APY for locked tokens, 1h to x months
 - Real APY ex USDC
- APY for PoS (Proof of Stake)
 - Distributed token is a fixed quantity of per period, so the APY is variable. Usually locked.

You can also find

ETF

- A tracker of something:
 - CAC 40 ETF = actions of each of the 40 companies as a pool.
 - ETF BITCOIN: 1ETF \Leftrightarrow 1 BITCOIN
 - Available at blackrock.