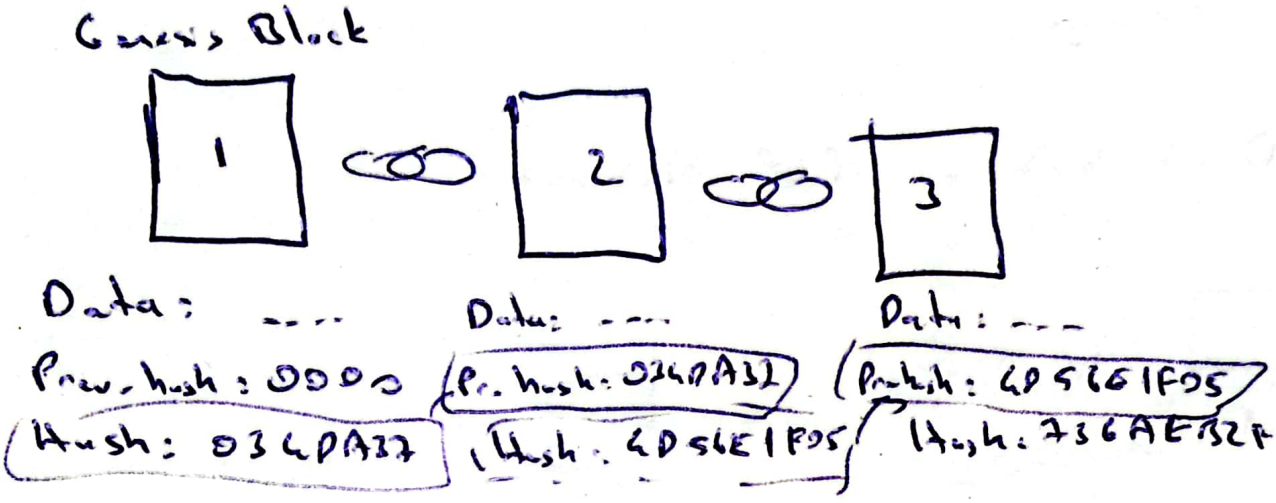
= Block - Chain =

A blockchain is a continously growing list of records, called block, which are linked and secured using cryptography.



- Mining
- Consensus Protocol
- Hash cryptograph
- Immutable Ledger
- Distributed P2P Network

= Hash Cryptography

Electronic Data $\xrightarrow{\text{Sha256}}$ 0A3457 6 9BC754 AB

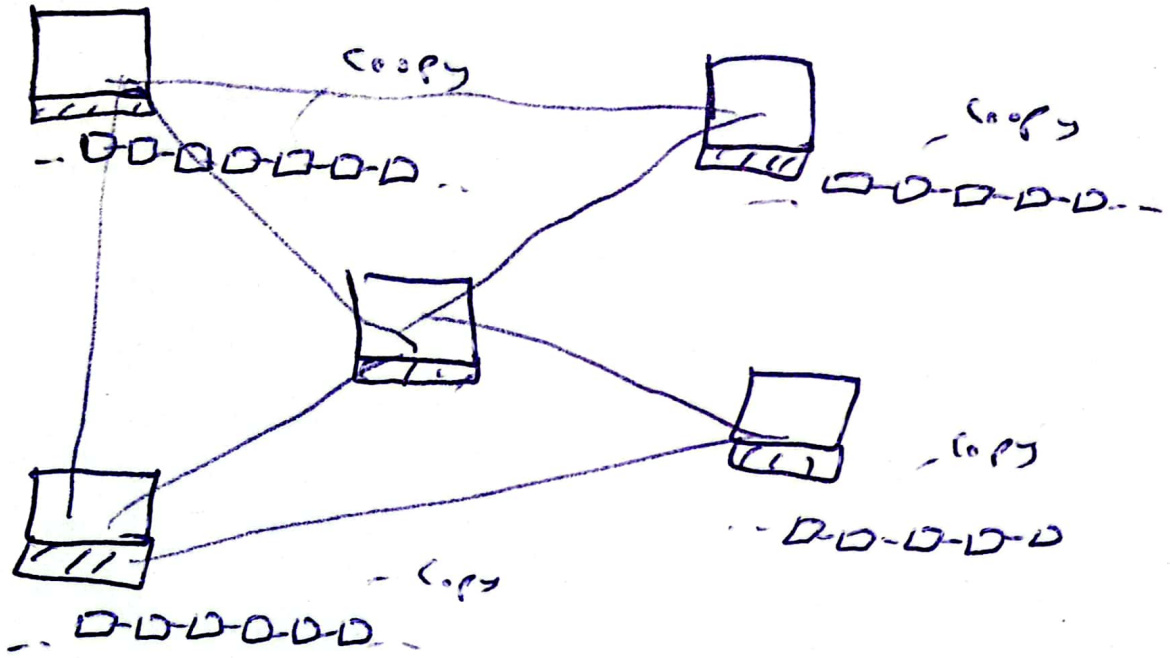
The 5 requirements for Hash algorithm.

1. One-way
2. Deterministic
3. Fast Computation
4. Avalanche Effect
5. Must withstand collisions

= Immutable Ledger =

Since a block changes, all the data in the next block is corrupted. Because pre-hash values changes. Therefore, the more blocks there are, the harder it is for the ledger to change.

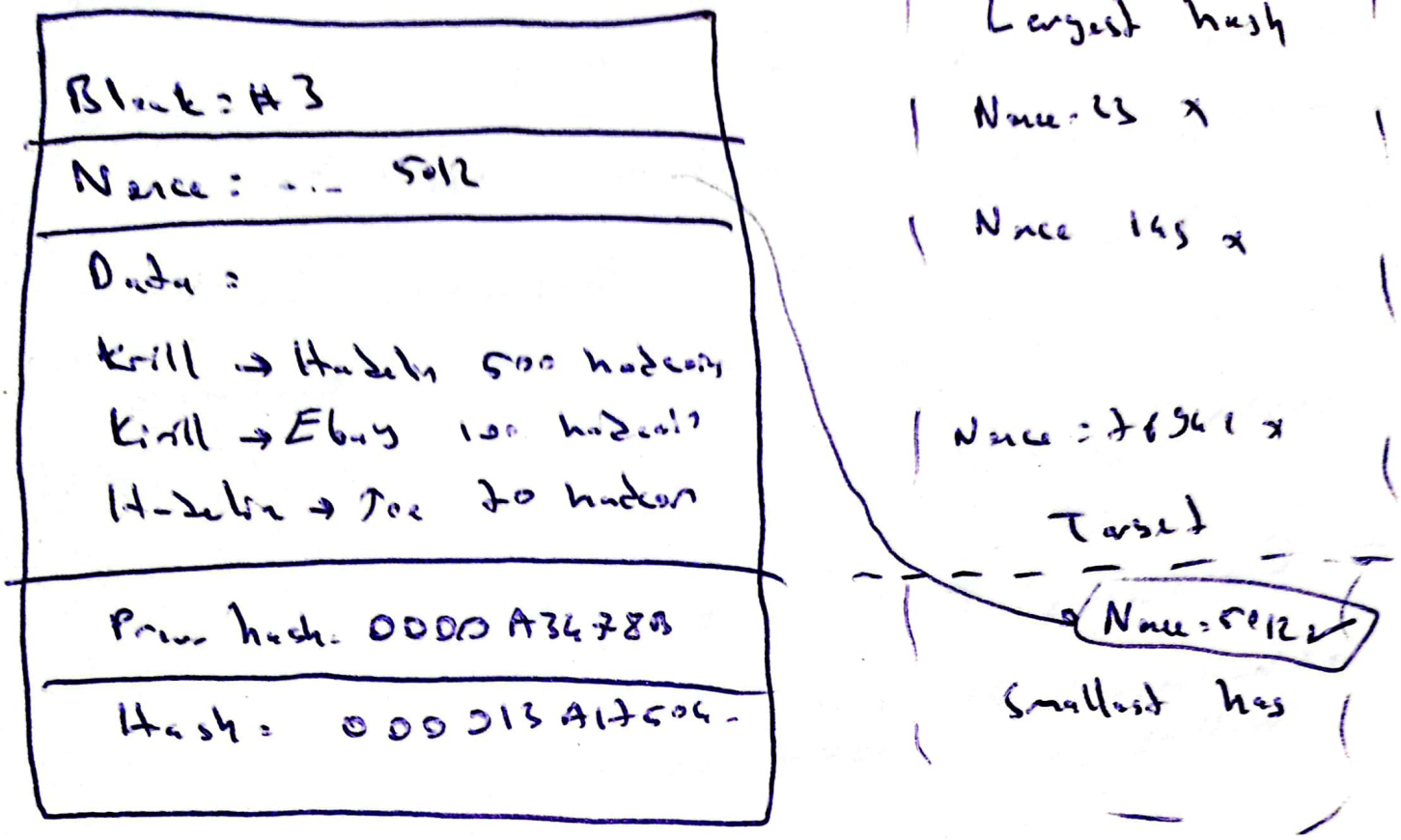
= Distributed P2P Network =



All computers in the network are interconnected and each separately stores all the blocks in the network. In this way, if an undesired information exchange occurs, one peer will be synchronized with the other peers. This decision is made by the majority of the peers in the network i.e. 51%.

= How Mining Works =

A hash is a Number.



In order to keep the mining block hash number below a certain number (starting with "0000") it is to try Nonce value randomly and reach the hash value below the target.

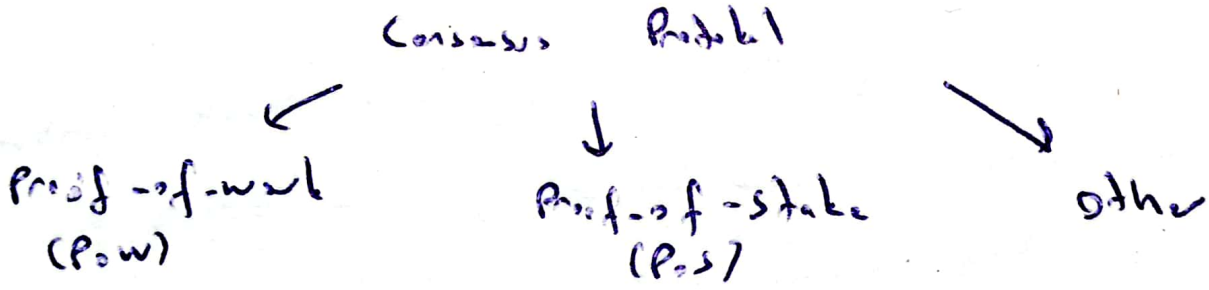
= Byzantine Fault Tolerance =

In short, Byzantine fault Tolerance (BFT) is the property of a system that can withstand the types of failures resulting from the Byzantine generals problem dilemma. This means that the BFT system can continue to work even if some

There is more than one solution to the Byzantine Generals Problem and so there is more than one way to create a BFT system. Similarly, there are different approaches for a blockchain to achieve Byzantine fault tolerance, and that brings us to "consensus algorithms":

= Consensus Protocol =

→ Challenge 1: Attackers
Challenge 2: Competing Chains



→ The longest chain is king!

= Cryptocurrency =

1. What is Bitcoin:

Technology : Blockchain

Protocol / Coin :	Waves	Ethereum	Bitcoin	NEO	Ripple
Token :	WCT, BIT, TRX, AE, WGR, WAVES, REP, SNT, Rhoc, MKR	X		ACAT, TNC, IDSC, RPX, IONT, IAN,	X

Bitcoin is a actually a protocol.

The Bitcoin Ecosystem :

- Nodes
- Large Miner
- Miners
- Mining Pools

= Bitcoin's Monetary Policy

→ The halving → Every 4 years BTC/block rate drops (half) (50 → 25 → 12 → 6.5 → ...)

→ Block Frequency =

Cryptocurrency	Average time
Bitcoin	10 min
Ethereum	15 sec
ripple	3.5 sec
litecoin	2.5 min

Understanding Mining Difficulty

Current Target: 00000000000000000005297c
(18 zeros)
0000000000000000000000000000000000000000

Probability:

Total possible 64-digit hexadecimal = $16^{64} \approx 10^{77}$

Total valid hash (with 18 zeros) $\approx 16^{64-18} = 2 \times 10^{55}$

Probability that a Randomly picked hash is valid

$= 2 \times 10^{55} / 10^{77} = 0.000000000000000000002\%$

→ Difficulty = current target / max target

Curr. target: 00000000000000000005297c0000000000000000000000000000000000000000

Max target: 00000000FFFF0000000000000000000000000000000000000000000000000000

Nonce Range → 32-bit Number = 0 - 4 Billion

→ Since the Nonce value has a maximum point, it can not always give a solution, so Timestamp is used for this.

→ Timestamp → use Unix Time (universal time)

= CPUs vs GPUs vs ASICs

CPU = Central Processing Unit	General	< 10 MH/s
GPU = Graphics Processing unit	Specialized	< 1 GH/s
ASIC = Application-Specific Integrated Circuit	Totally specialized	> 1000 GH/s

= How do Mempools Works

→ Every nodes has a mempools.

→ Mempools are where participants' transaction are kept until they process on blockchain

Transactions and UTXOs

Mark → Me 0,1 BTC
Hadelin → Me 0.3 BTC
~~Helen → Me 0.6 BTC~~
Susan → Me 0.7 BTC

} UTXOs (Unspent Transaction outputs)

I want to buy a bicycle for 0.5 BTC

Transaction

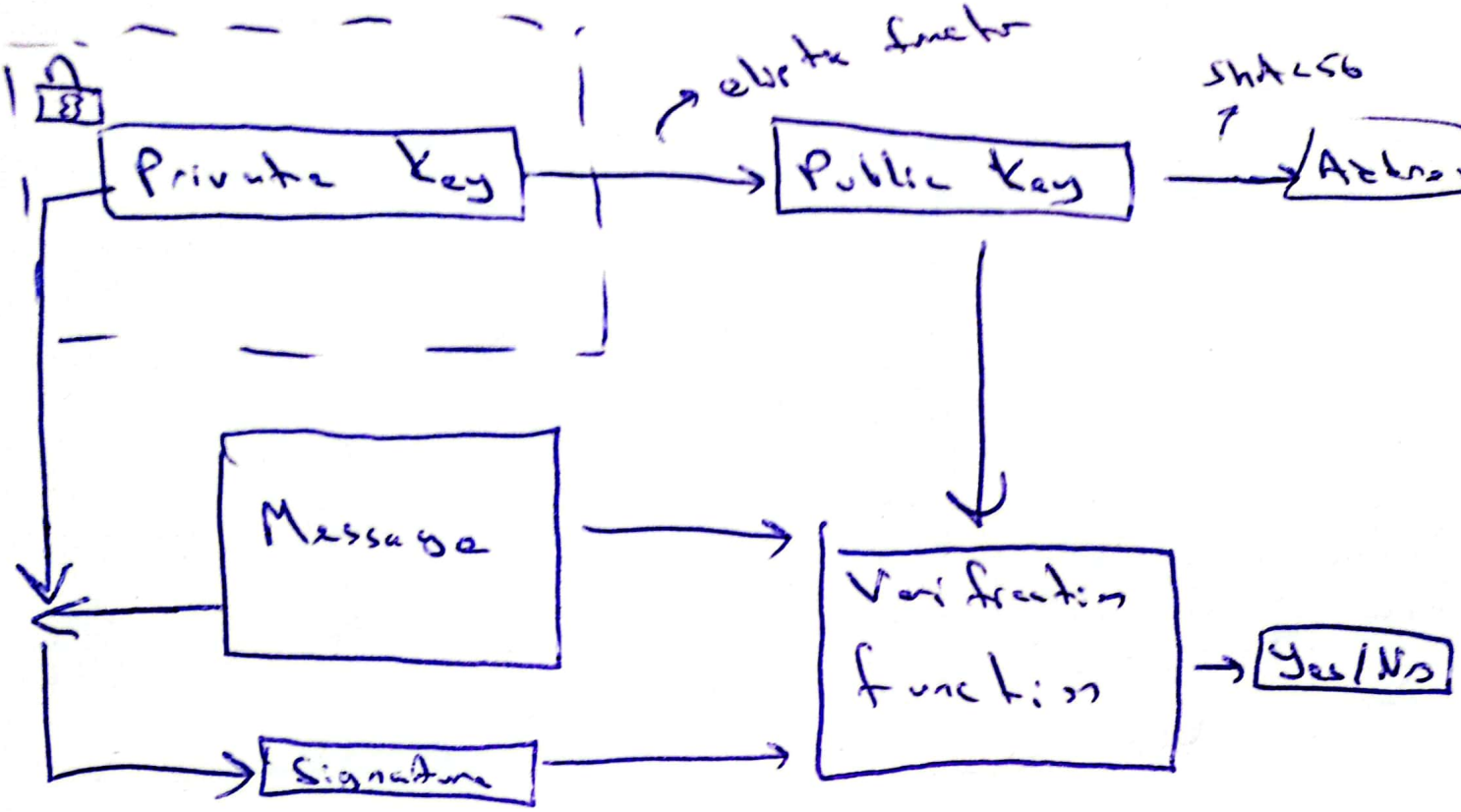
Input:
→ 00,6 BTC from Helen

Output
0.5 BTC to the bike shop → UTXO for the bike shop
0.1 BTC back to myself → UTXO for me

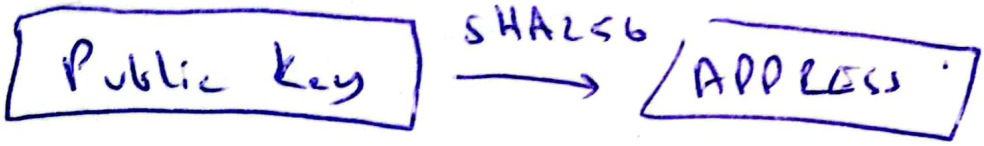
= How Wallets Work =

→ Normally, there is no such thing as a "balance" in blockchain, there are only transactions. Wallets collect/sum their own UTXOs and create a "balance"

Signatures: Private and Public Keys

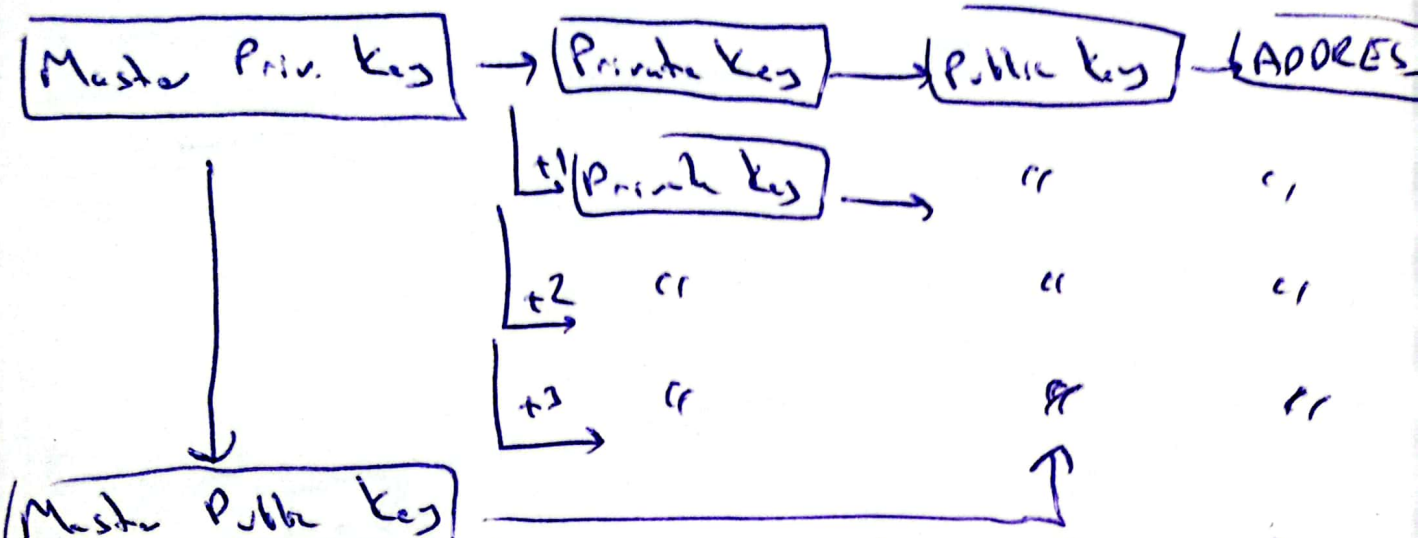


Public Keys vs Bitcoin Address



A money can be sent to both public key and Address. All kinds of public keys are used when making transaction. but there is no need to ~~disclose~~ disclose your public key when receiving money, so address is used for security

Hierarchically Deterministic (HD) Wallets



→ With a master key, different private and public keys can be created deterministically

Master Private Key → Stored 12 word seed phrase (mnemonic)

= Smart Contract =

Ethereum is a blockchain-based decentralized platform on which decentralized applications (DApps) can be built.

= Smart Contract =

→ Smart Contracts are programs that execute on the blockchain.

Bitcoin Script	Solidity
→ no Turing-Complete (Coding any logic)	yes → Turing Complete (Coding any logic)
→ has no loops	→ include loops

→ Each node has (in Ethereum)

1) History of all smart contract
2) History of all transaction
3) Current state of all smart contract

→ Decentralize Applications (Dapps)

Dapp ↗ An interface which we design to intract to blockchain

↓ ↳

fronten Backend (Smart contact)

= Ethereum Virtual Machine (EVM) and Gas =

EVM is a virtual machine running on the nodes computer. So they do not have a access main memory directly. It protects the pc against ~~viruses~~ viruses. Nothing can out this virtual machine.

Smart contract are required to pay a fee for each process on the blockchain. This is called "gas". This avoids endless loop.

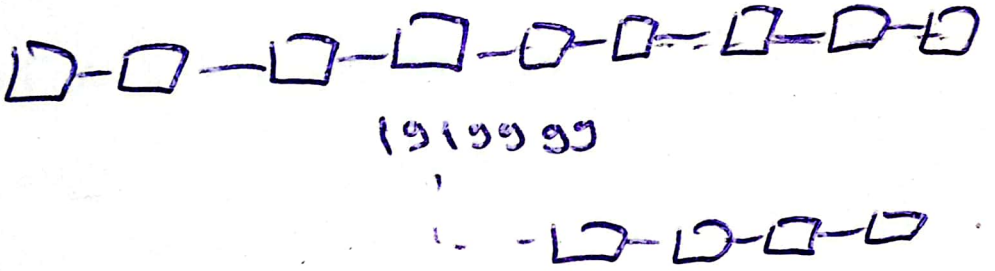
= Decentralized Autonomous Organizations (DAOs)

→ Decentralized and self-executing structures (consisting of smart contract)

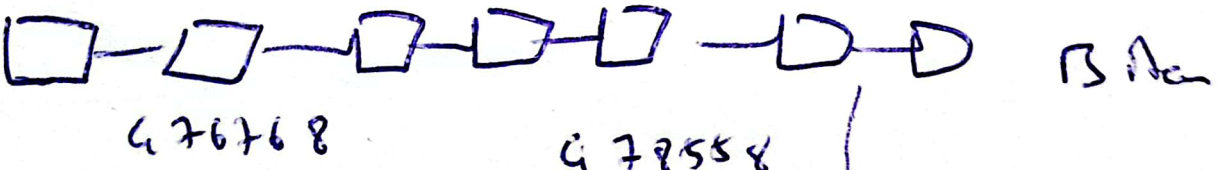
= Soft and Hard forks =

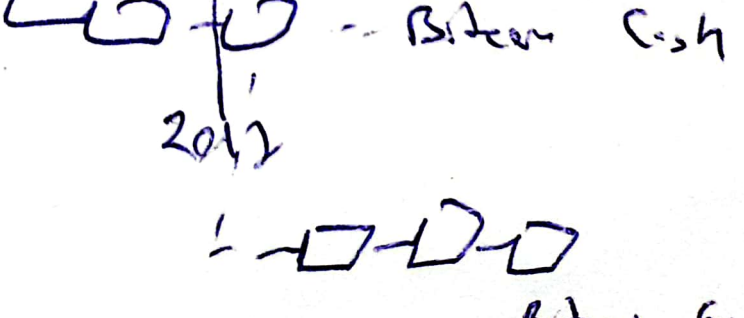
After the DAO attack ethereum split into (Ethereum) New and ETC. → (Ethereum Classic) old

Ethereum (July 2016) (Hard fork)



Bitcoin (July 2017) (Soft fork)





Hard forks
↳ Loosen Rules

Soft Forks
↳ Tighten Rules

= Initial Coin Offerings (ICOs)

↳ Just Tokens

No Mining