# Bitcoin and Blockchain

**Pascal Lafourcade**

ESC January 2021

# Organisation

$6 = 4 + 2$ sessions in 2 days : 12 january 2021 and 3 february 2021

1. Bitcoin + Blockchain
2. Projects
3. Introduction to Cryptography
4. GDPR
5. Computer Security Introduction
6. Security and Mobility of the futur

# Grade

Imagine you are the boss of your own company.

1. Describe your company activities in 2 pages maximum
2. Write the GDPR report for your company

Deadline : 1st March 2021

# Outline

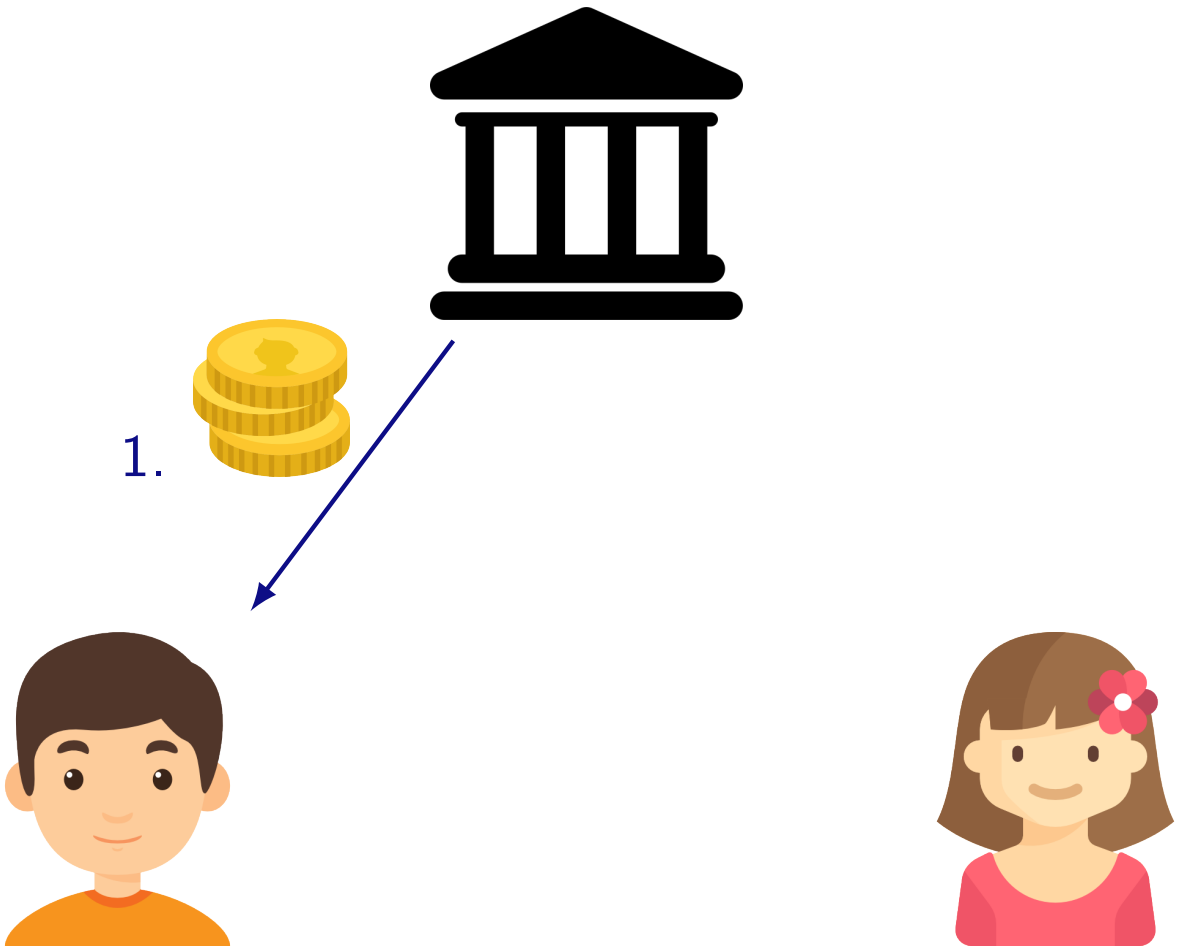
# Sumerians around 3.500 bef. J.C

# Money as a functionality: a currency

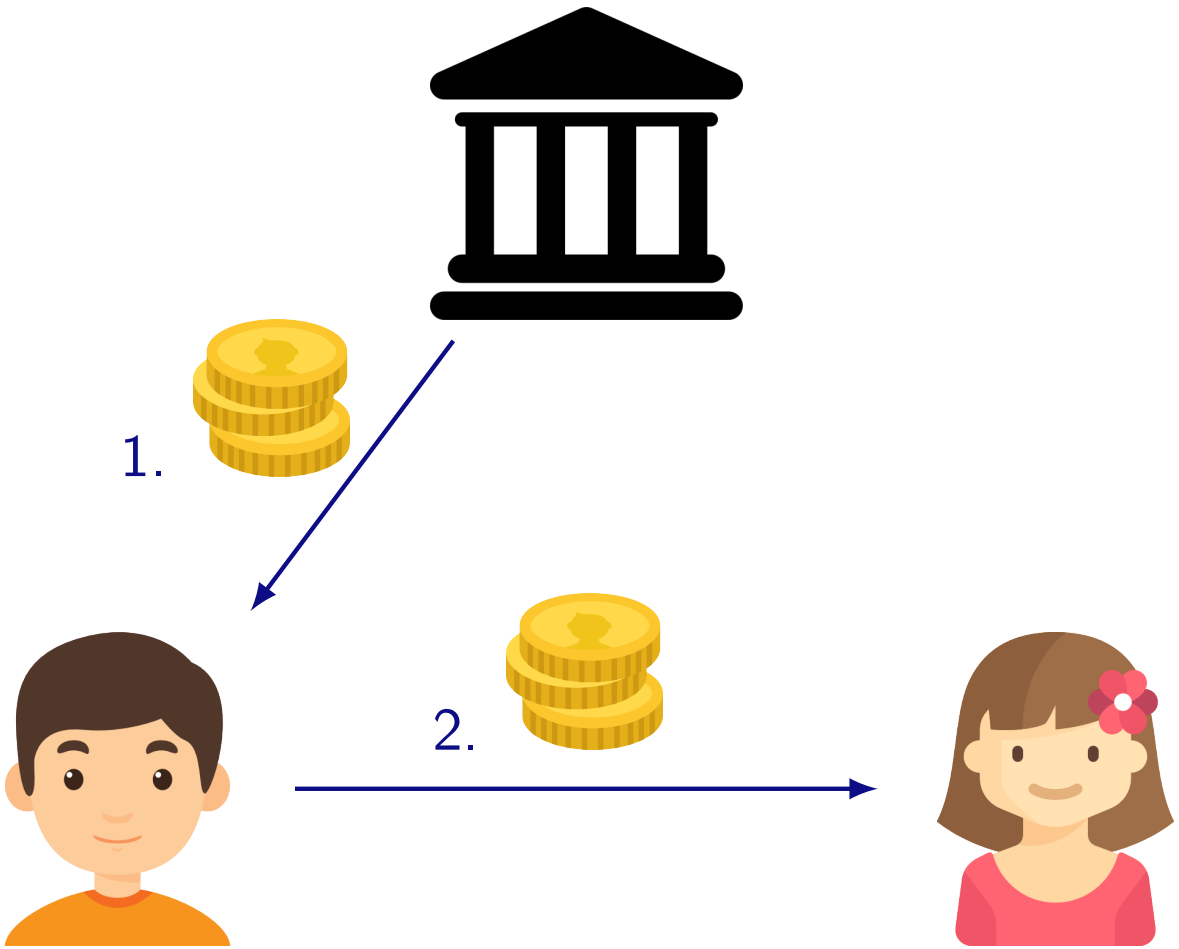

1. Medium of Exchange of goods and services between people
2. Store of Value
3. Unit of Account (measure of value)

# Many currencies

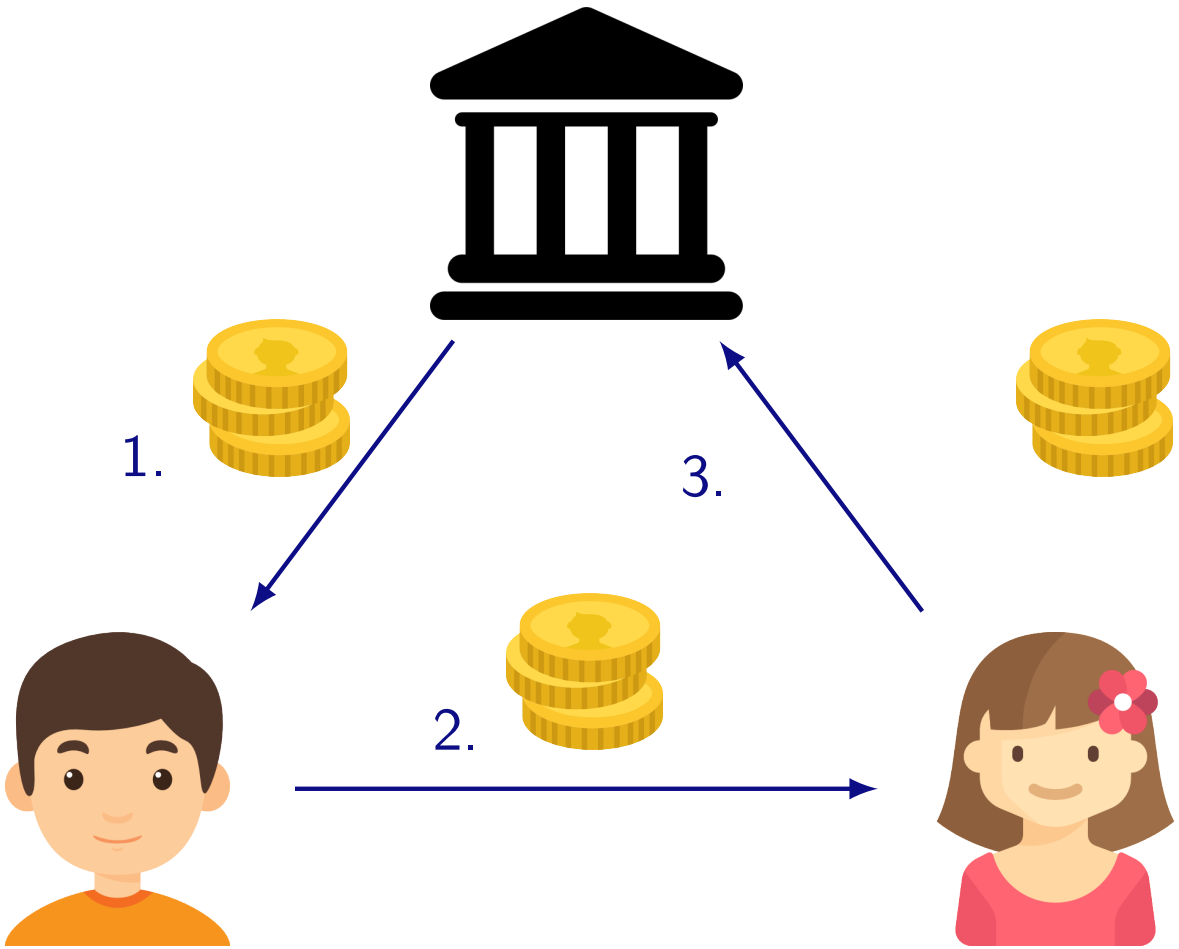
# Principle: central Bank



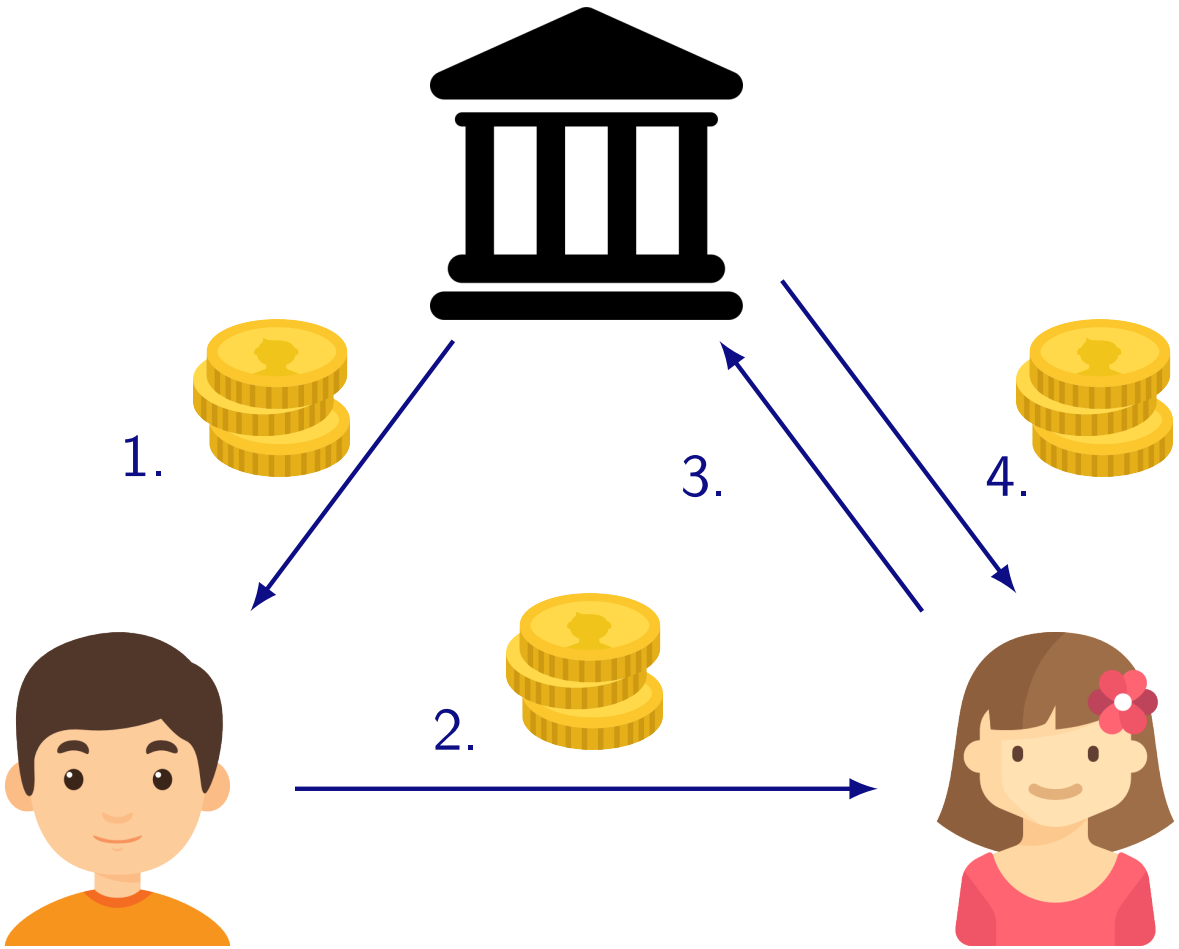
# Principle: central Bank



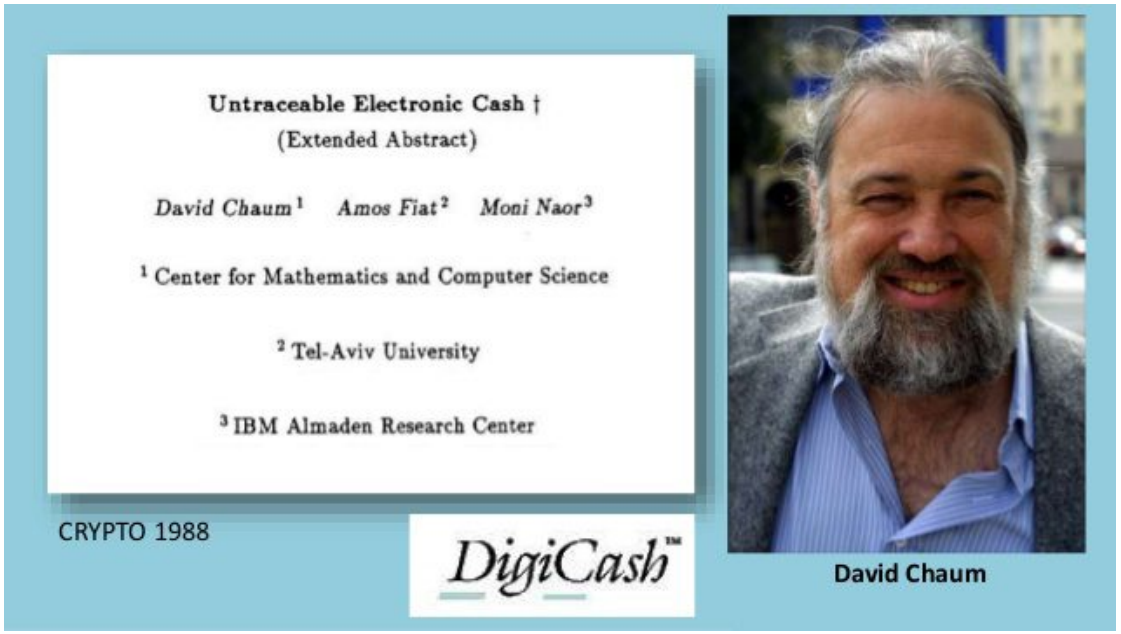
# Principle: central Bank



# Principle: central Bank



# 1988: Digitcash




- Preserves privacy
- Use cryptographic primitives
- Requires a third party (bank)

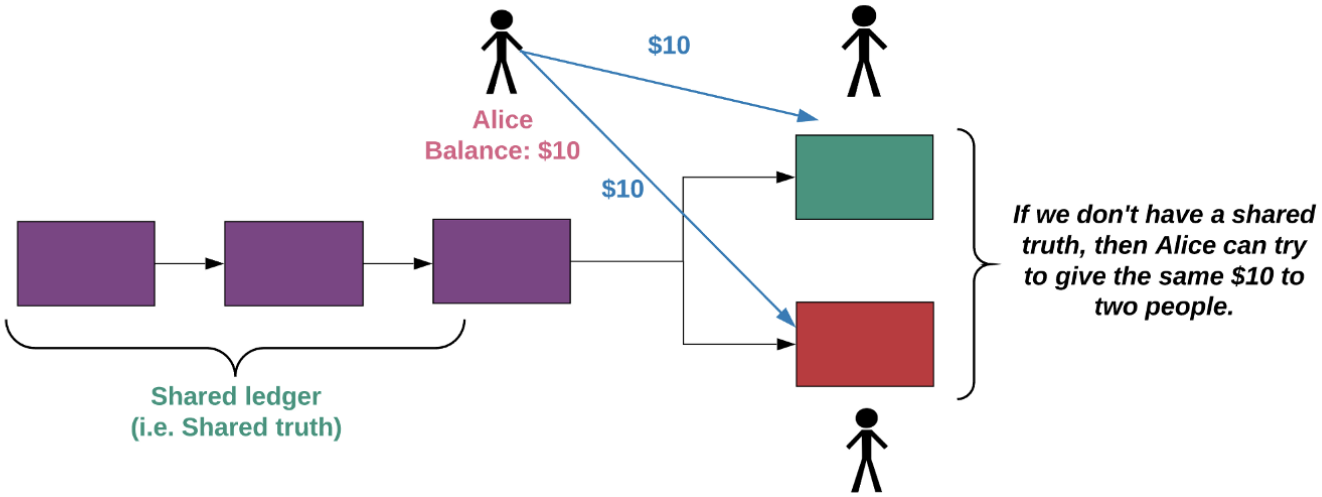
# Cryptocurrency

- Money
  1. Medium of exchange
  2. Store of value
  3. Unit of account

- Cryptocurrency: electronic cash, without a third party
  4. Preserving privacy
  5. Unforgeable
  6. Preventing double-spending

# Properties: Unforgeability

# Properties: Preventing double spending




- Fraud identification

- Presumption of innocence

# Properties: Preserving privacy

- Weak anonymity: non identification of a buyer

- Strong anonymity: non tractability of a buyer

# What is a currency? (money creation)

- Standard currency
  - Guaranteed by gold,
  - Then by US Dollars (Bretton-Woods),
  - Then simply fiduciary:
    - Legal tender & forced tender
    - Creation by authorized institutions
    - Guaranteed by a central bank

Nowadays: only debt

# What is a currency? (money creation)

- Standard currency
  - Guaranteed by gold,
  - Then by US Dollars (Bretton-Woods),
  - Then simply fiduciary:
    - Legal tender & forced tender
    - Creation by authorized institutions
    - Guaranteed by a central bank
- Cryptocurrency
  - Various creation mechanisms:
    - Fixed number
    - Capped/linear/bounded growth / year
    - etc.

⚠ Gathering of mining farms (money supply)

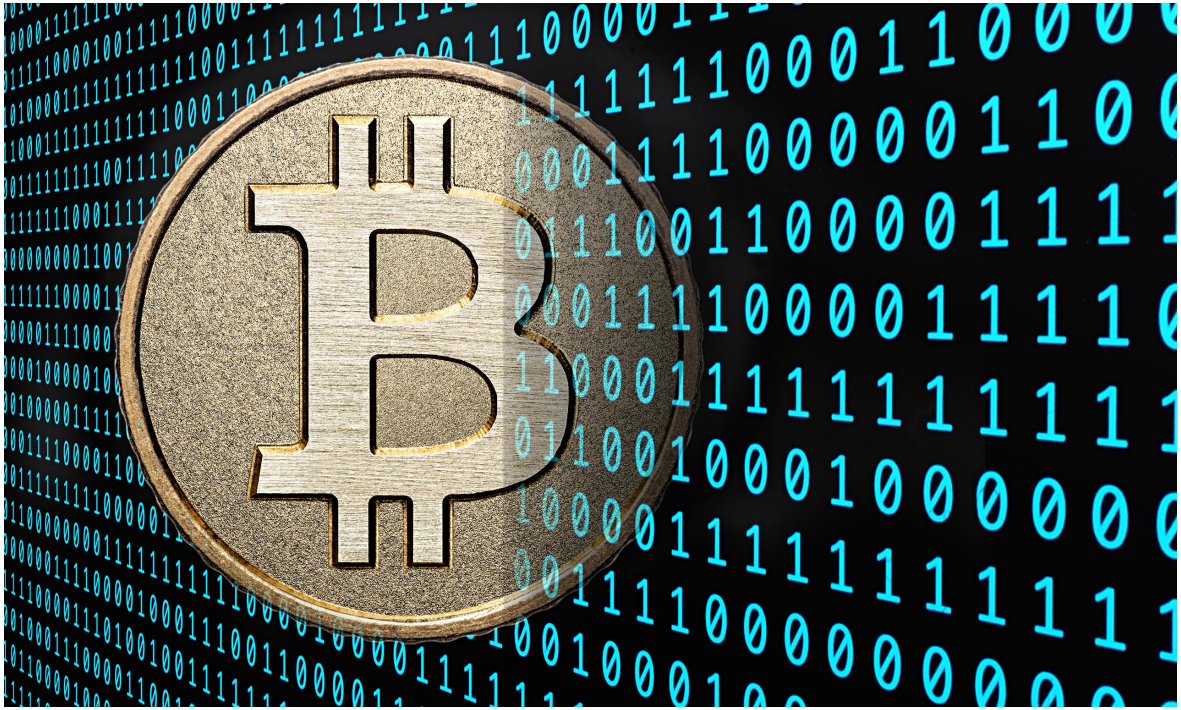
Nowadays: only debt

# Classical and cryptographic currencies

| | Classical currency | | Cryptocurrency |
|---|---|---|---|
| | Cash | Electronic | |
| Medium of exchange | ✓ | ✓ | ✓ |
| Store of value | ✓ | ✓ | ✓ |
| Unit of account | ✓ | ✓ | ✓ |
| Creation | central Bank | Debt | Automatic |
| Privacy | ✓ | ✗ | ✓ |
| Peer 2 peer | ✗ | ✗ | ✓ |
| Legal guaranty, stabilization | ✓ | ✓ | ✗ |

# Outline

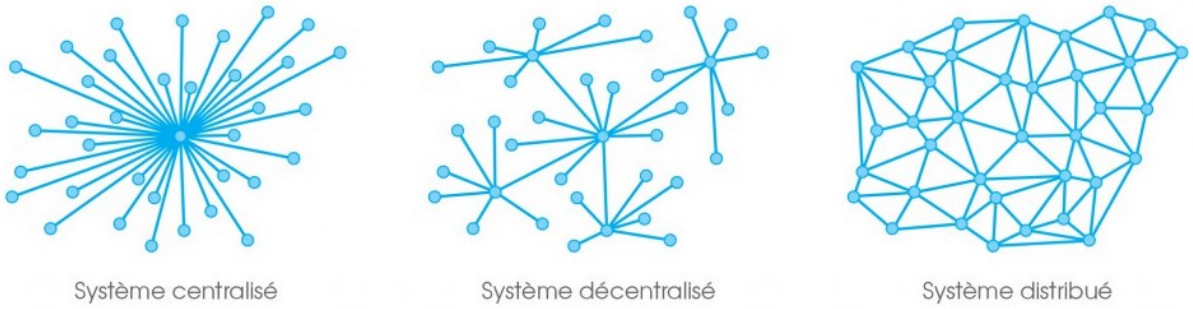
# The Bitcoin revolution 2009



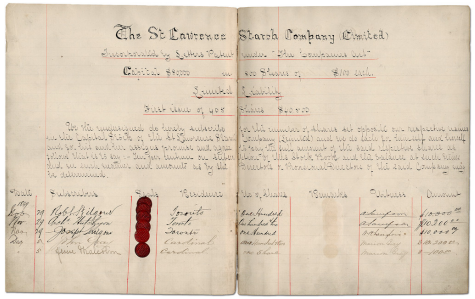

21 millions BTC

# Bitcoin

- Decentralized and distributed cryptocurrency



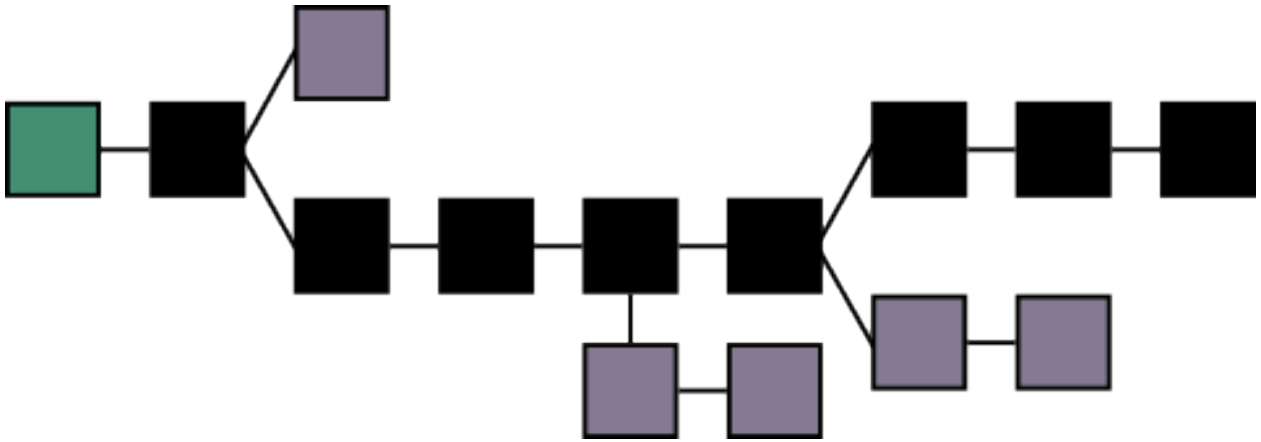

- Uses a *blockchain*: a shared ledger, known to all participants



# Unstoppable, because distributed

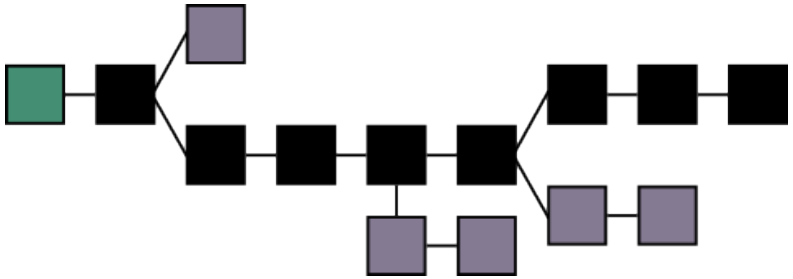

- Broadcast of all the transactions to all the nodes of the network

# Unforgeable



- A fingerprint (hash) of each transaction block is added to each new block of transaction (chain of hashes) ...

# Auditable



- Every participant owns, locally, a copy of the complete history of every transactions

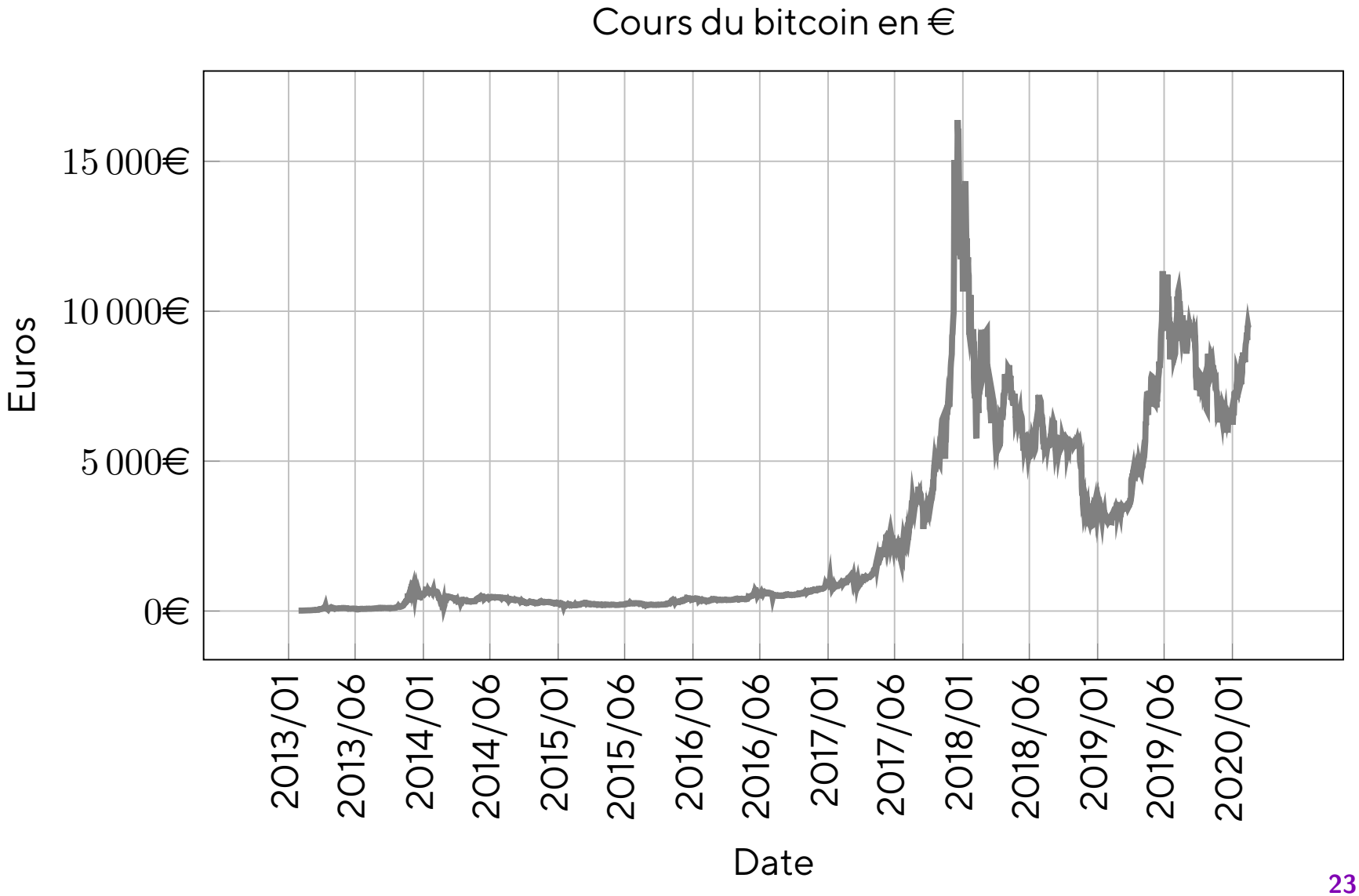
# Bitcoin: electronic cash

Created at the end of 2008 by Satoshi Nakamoto

- 1 BTC $\approx$ 15 401 € (December 30, 2020)

| | | |
|---|---|---|
| 1 | BTC = 1 Bitcoin | |
| 0,01 | BTC = 1 cBTC | = 1 centiBitcoin (or bitcent) |
| 0,001 | BTC = 1 mBTC | = 1 milliBitcoin |
| 0,000 001 | BTC = 1 $\mu$BTC | = 1 microBitcoin |
| 0,000 000 01 | BTC = 1 Satoshi | |

# Bitcoin € exchange rates



# Outline

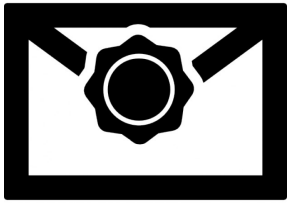

## Examples

- 3DES
- AES

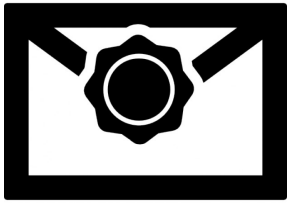
# Public key cryptography

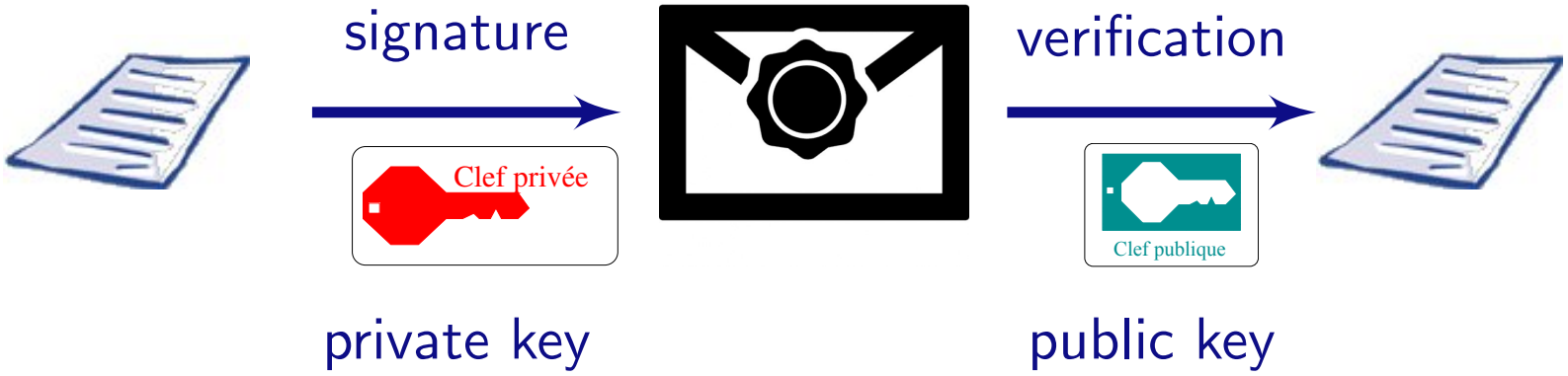

## Examples

- RSA: $c = m^e \mod n$
- ElGamal: $c \equiv (g^r, h^r \cdot m)$



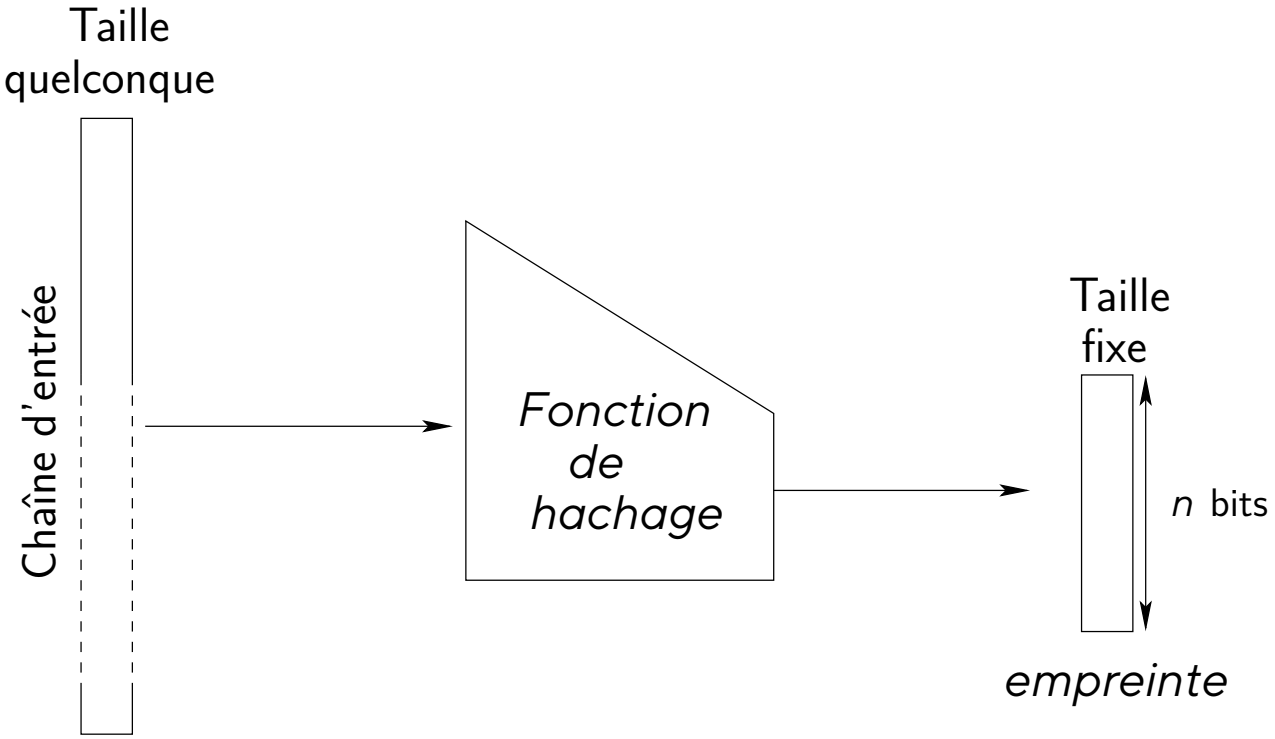

FORTUNES DE MER
MARITIME L.A.W.




- RSA: $m^d \mod n$
- ElGamal: $(g^k; (H(m) - xg^k)k^{-1} \mod p - 1)$

# Cryptographic hash function (RIPEMD-160, SHA-256, SHA-3)

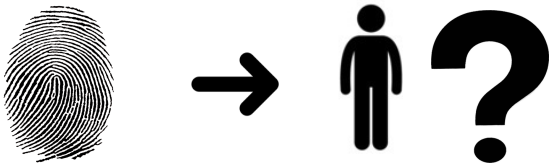



- uniformity property: $\forall a \neq b \xleftarrow{\$}, \mathcal{P}(h(a) = h(b)) \approx \frac{1}{n}$

# Cryptographic hash function (RIPEMD-160, SHA-256, SHA-3)

## Resisting properties

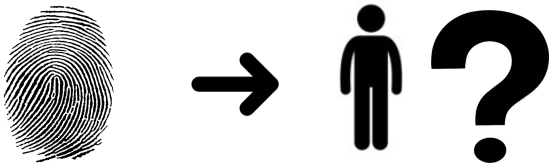
- Pre-image



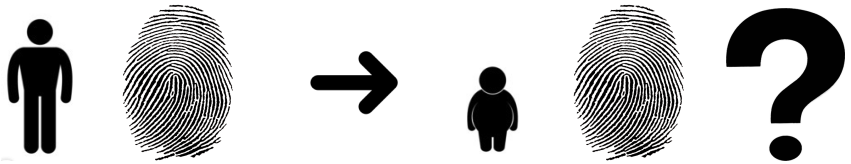
# Cryptographic hash function (RIPEMD-160, SHA-256, SHA-3)

## Resisting properties

- Pre-image



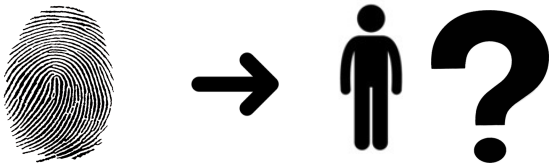
- Second Pre-image



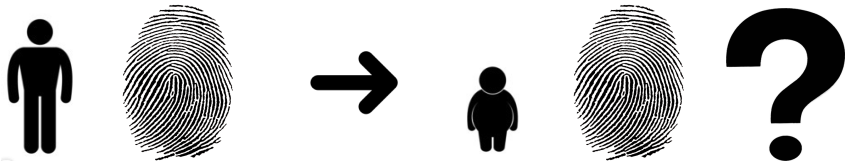
# Cryptographic hash function (RIPEMD-160, SHA-256, SHA-3)

## Resisting properties

- Pre-image



- Second Pre-image



- Collision

# Outline

# Bitcoins: main characteristics

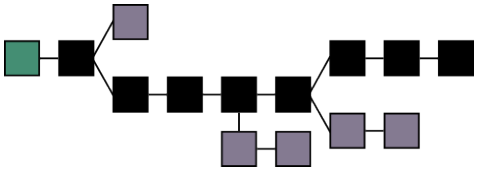
- the total number of bitcoins is finite

  21 millions BTC

- Transactions use electronic signatures
- Account number:

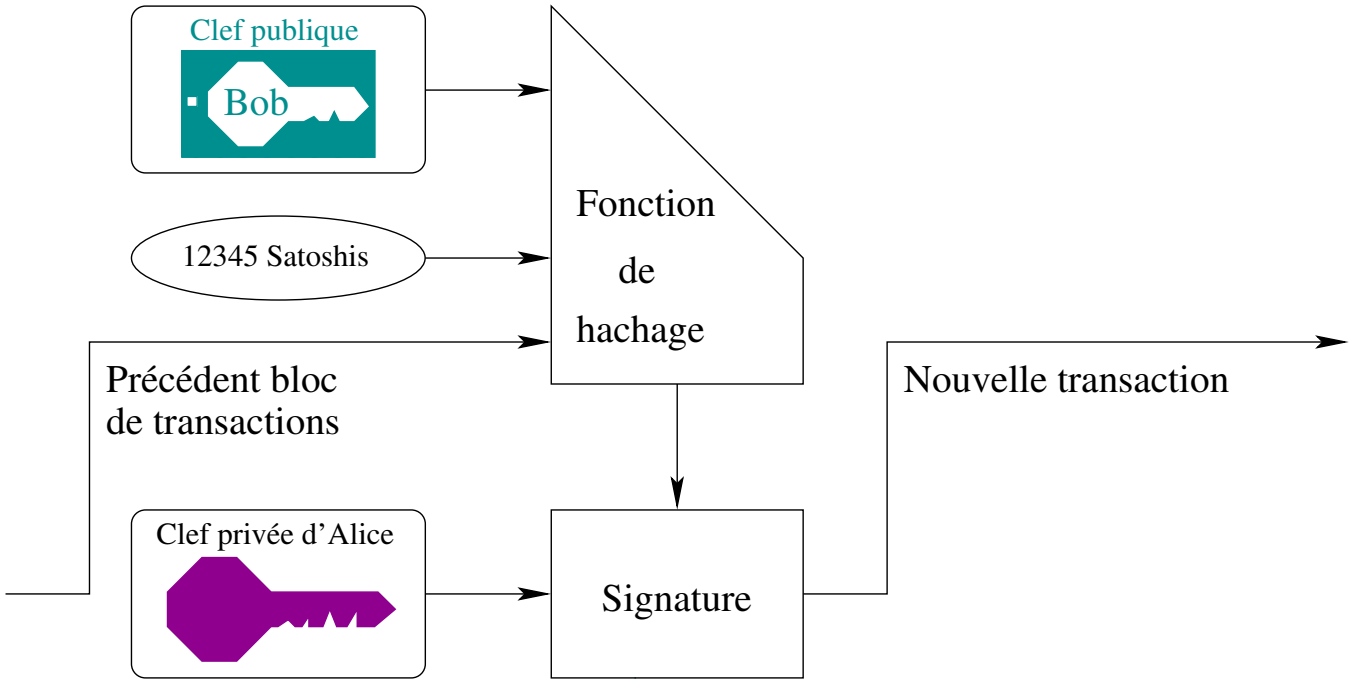
  $$\text{RIPEMD-160}(\text{SHA-256}(\text{ECDSA}_{pub}))$$

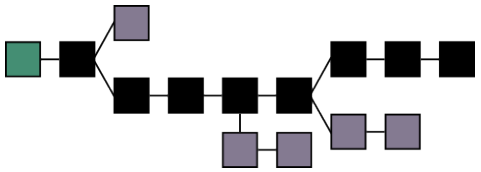
- All the transactions are public
- Blockchain: a peer-to-peer system guaranteeing the validity of transactions



# How to perform a transaction?

Alice gives 12345 Satochis (a few cents) to Bob.



# Electronic wallet

- Consultation of the balance
- Completion of a transaction
- Coins storage management
- Creation of new account keys

⚠ Where are my private keys?

# Digital wallet solutions

1. Security
2. Availability
3. Ease of access

# Digital wallet solutions

1. Security
2. Availability
3. Ease of access


Hardware

Digital

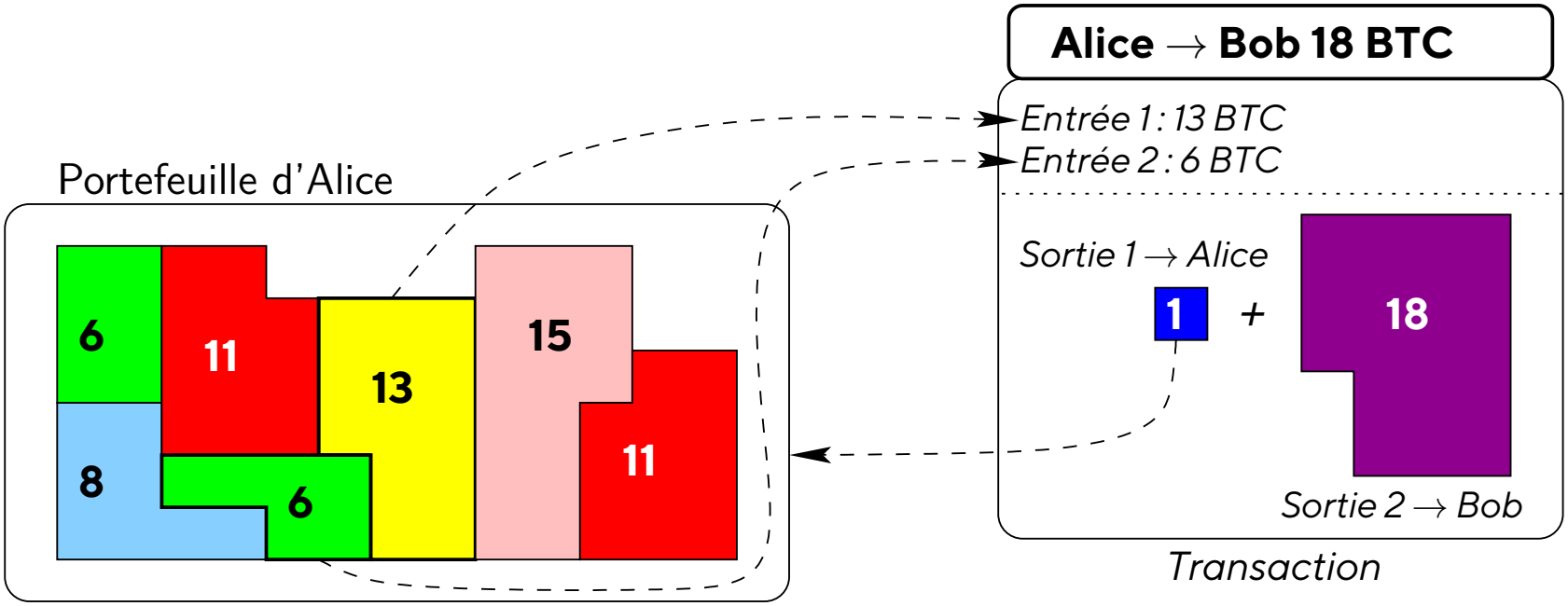

Clouded

# Main digital wallets

| Type | Storage | Security | Example | #currencies | mobile version |
|---|---|---|---|---|---|
| **Hardware** | physical (cold wallet) | +++ | Ledger Nano S | 27 | n/a |
| | | | KeepKey | 7 | n/a |
| | | | Trezor | 8 | n/a |
| **Software** | local | + | Bither | 1 | ✓ |
| | | | Coplay | 150 | ✓ |
| | | | Electrum | 1 | ✓(Android) |
| | | | Exodus | 30 | × |
| | | | Jaxx | 60 | ✓ |
| **Cloud** | distant | – | Blockchain.info | 2 | n/a |
| | | | Coinbase | 3 | n/a |
| | | | Kraken | 1 | n/a |
| | | | Bittrex | 190 | n/a |

(march 2018)

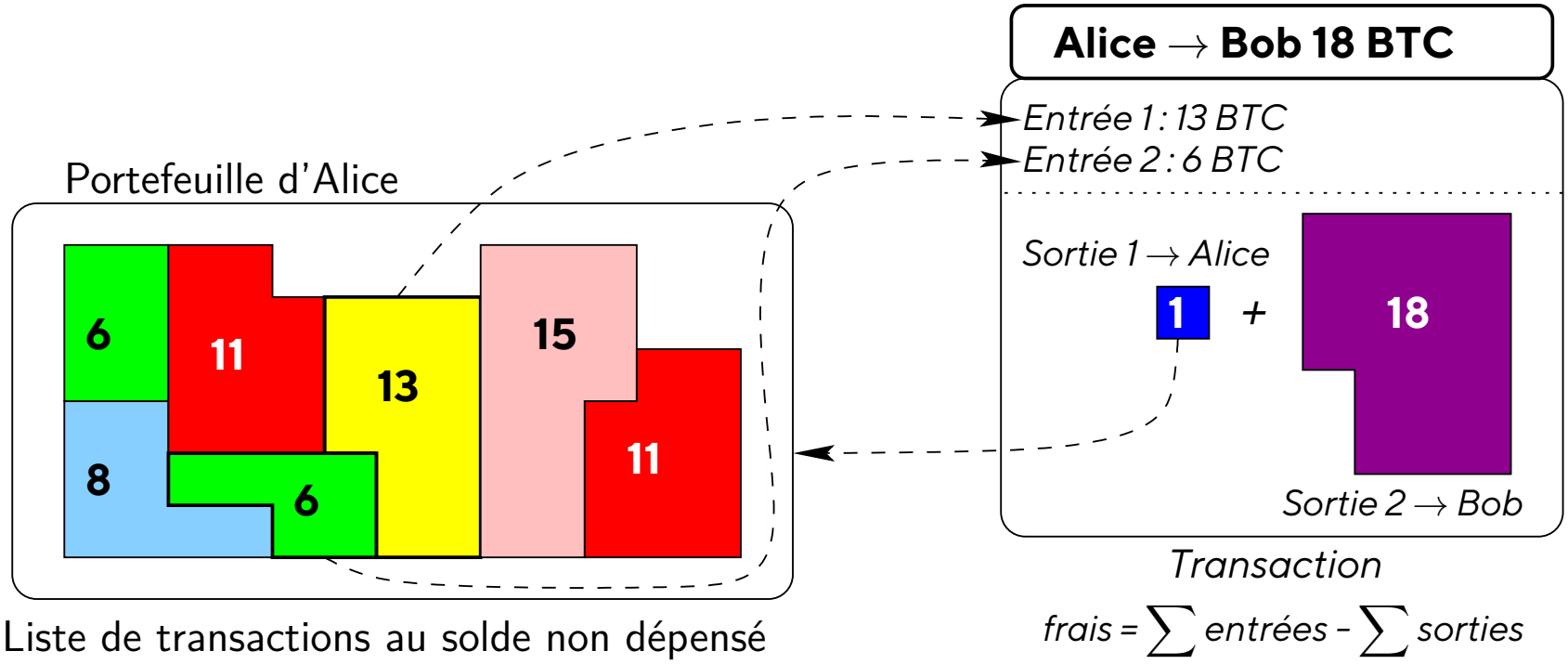
# Pay 18 BTC with coins




Liste de transactions au solde non dépensé

$$frais = \sum entrées - \sum sorties$$

# Pay 18 BTC with coins

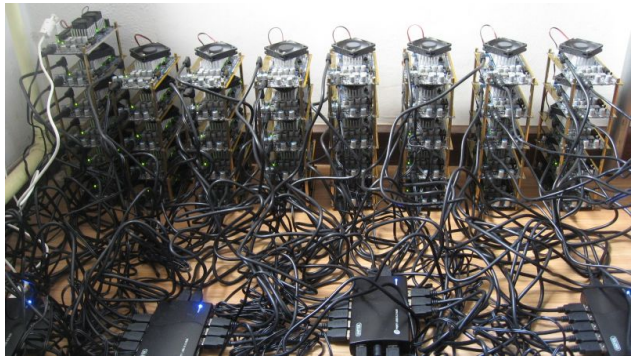



- Only owned bitcoins can be spend

# Mining Bitcoins

# Mining Bitcoins

The "*miners*" validate transactions and are paid in bitcoins



# Mining security

⚠ Who is going to mine my transaction?

- Will validate or not (accounts verifications), independently

# Mining security

⚠ Who is going to mine my transaction?

- Will validate or not (accounts verifications), independently

A miner is randomly chosen

- Prevents collusions

# Mining security

⚠ Who is going to mine my transaction?

- Will validate or not (accounts verifications), independently

A miner is randomly chosen

- Prevents collusions

OK, as soon as a majority of miners is honest

- Correct validations are rewarded

# Mining Bitcoins = race to be selected

- Mining = solving **hashing target**
  - Proof of work: **hard** puzzle to solve & **easy** to check
  - Uniform partition of the validators

# Mining Bitcoins = race to be selected

- Mining = solving **hashing target**
  - Proof of work: **hard** puzzle to solve & **easy** to check
  - Uniform partition of the validators

- Initial reward: 50 BTC for a validation
- Divided by 2 every 210000 validations (4 years)

$$\sum_{i=0}^{32} \frac{50}{2^i} \times 210\,000 = 21 \text{ millions BTC}$$

# Mining: hashing target as a Proof-of-work

Example target:

`0000 0000 0000 0000 002e 8fcc c211 838c 7d12 c913 d13b 9686 e8f6 3127 cb57 e712`

Find a number $n$ such that:

$$\text{SHA-256}(\text{SHA-256}(\text{Transactions}, \textit{nonce})) = x < \text{Target}$$

Must have at least 18 zeroes (even $18 * 4 + 2 = 74$ bits) for the msb of $x$

# Mining: hashing target as a Proof-of-work

Example target:

`0000 0000 0000 0000 002e 8fcc c211 838c 7d12 c913 d13b 9686 e8f6 3127 cb57 e712`

Find a number $n$ such that:

$$\text{SHA-256}(\text{SHA-256}(\text{Transactions}, \textit{nonce})) = x < \text{Target}$$

Must have at least 18 zeroes (even $18 * 4 + 2 = 74$ bits) for the msb of $x$

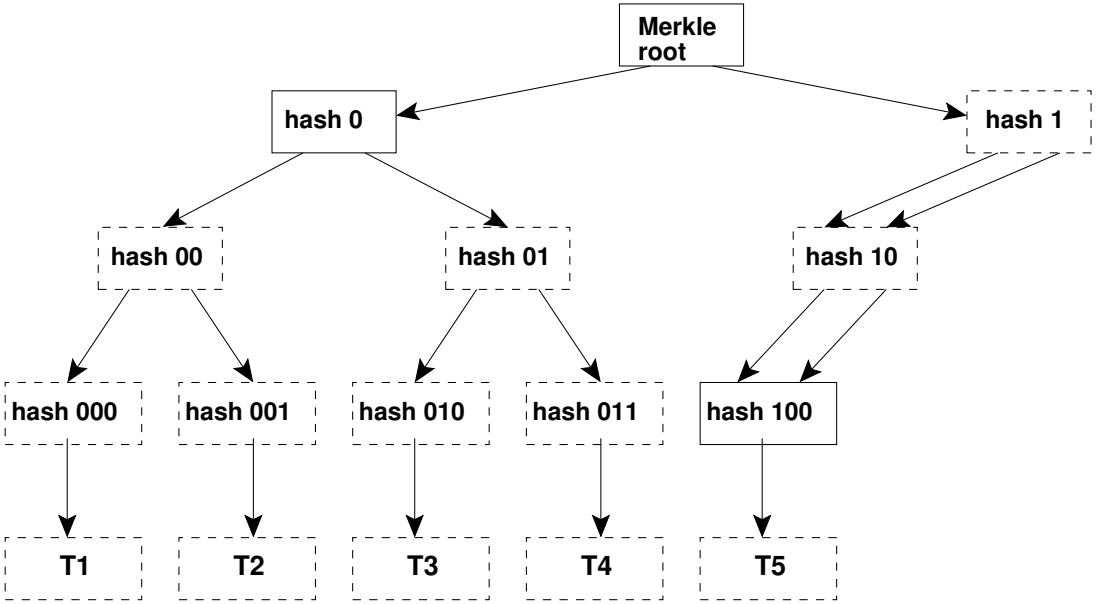
**Strategy: brute force**

Randomly try the possible values for *nonce*

# Mining Algorithm

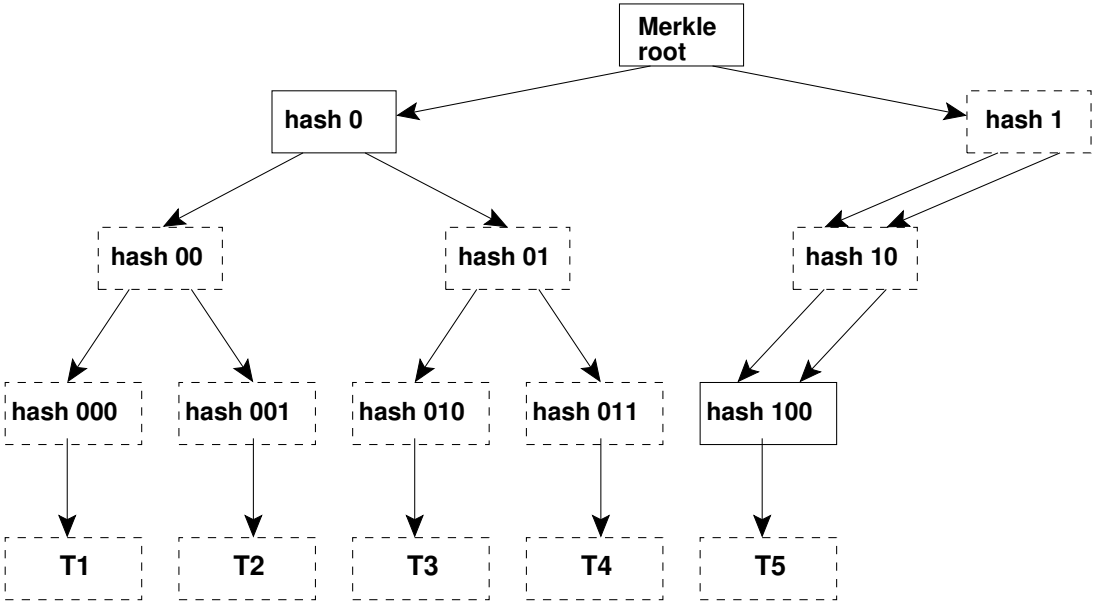
```
Nonce := random value;
repeat
    hashPrevBlock := last validated (by the network) block;
    Fetch all the not yet validated transactions;
    hashMerkleRoot := hash of the transactions to be validated;
    Time := time in seconds;
    Bits := current hashing target;
    Nonce := Nonce + 1;
    header := (Version||hashPrevBlock||hashMerkleRoot||Time||Bits||Nonce)
until SHA-256(SHA-256(block header)) < Target
```

# Verify that transactions are present within the chain?




Recompute the Merkle tree + check coherency of the root

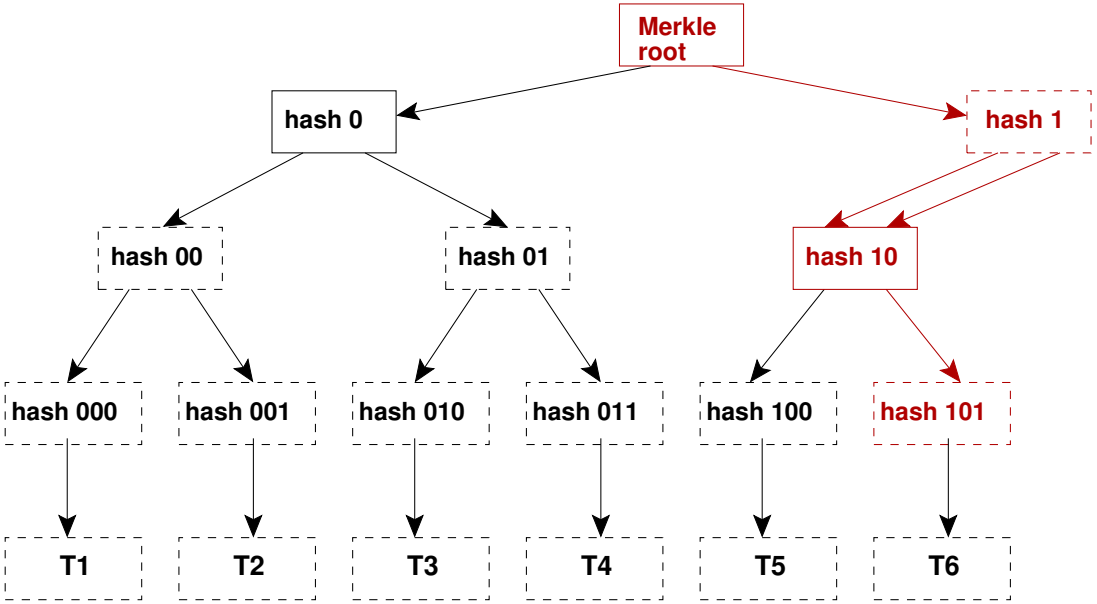
# Efficiently add transactions as they come?




dashed zones are not preserved:

- a double arrow is a duplication

# Efficiently add transactions as they come?




dashed zones are not preserved:

- a double arrow is a duplication
- only $\log_2(n)$ fingerprints are recomputed/added

# ASCII proof of work simulator

| dec | 45 | 46 | 47 | 48 | 49 | 50 | 51 | 52 | 53 | 54 | 55 | 56 | 57 | 58 | 59 | 60 | 61 | 62 | 63 | 64 |
|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|
| char | - | . | / | 0 | 1 | 2 | 3 | 4 | 5 | 6 | 7 | 8 | 9 | : | ; | < | = | > | ? | @ |

| dec | 65 | 66 | 67 | 68 | 69 | 70 | 71 | 72 | 73 | 74 | 75 | 76 | 77 | 78 | 79 | 80 | 81 | 82 | 83 | 84 |
|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|
| char | A | B | C | D | E | F | G | H | I | J | K | L | M | N | O | P | Q | R | S | T |

| dec | 85 | 86 | 87 | 88 | 89 | 90 | 91 | 92 | 93 | 94 | 95 | 96 | 97 | 98 | 99 | 100 | 101 | 102 | 103 | 104 |
|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|
| char | U | V | W | X | Y | Z | [ | \ | ] | ^ | _ | ‘ | a | b | c | d | e | f | g | h |

**Validator**

ASCIISUM( ASCIISUM( A, B, 1234, nonce ) ) divisible by 15

# ASCII proof of work simulator

| dec | 45 | 46 | 47 | 48 | 49 | 50 | 51 | 52 | 53 | 54 | 55 | 56 | 57 | 58 | 59 | 60 | 61 | 62 | 63 | 64 |
|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|
| char | - | . | / | 0 | 1 | 2 | 3 | 4 | 5 | 6 | 7 | 8 | 9 | : | ; | < | = | > | ? | @ |

| dec | 65 | 66 | 67 | 68 | 69 | 70 | 71 | 72 | 73 | 74 | 75 | 76 | 77 | 78 | 79 | 80 | 81 | 82 | 83 | 84 |
|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|
| char | A | B | C | D | E | F | G | H | I | J | K | L | M | N | O | P | Q | R | S | T |

| dec | 85 | 86 | 87 | 88 | 89 | 90 | 91 | 92 | 93 | 94 | 95 | 96 | 97 | 98 | 99 | 100 | 101 | 102 | 103 | 104 |
|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|
| char | U | V | W | X | Y | Z | [ | \ | ] | ^ | _ | ‘ | a | b | c | d | e | f | g | h |

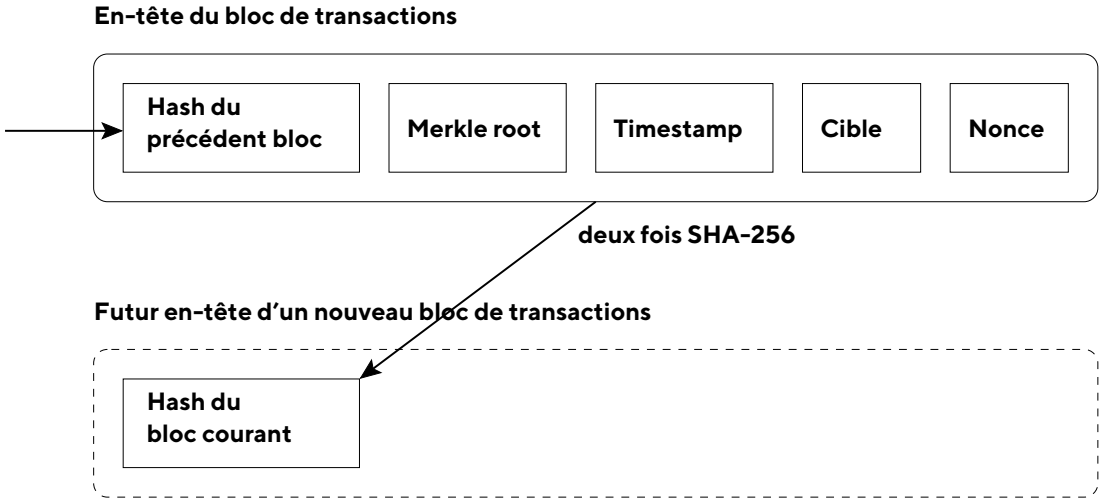
**Validator**

ASCIISUM( ASCIISUM( A, B, 1234, nonce ) ) divisible by 15

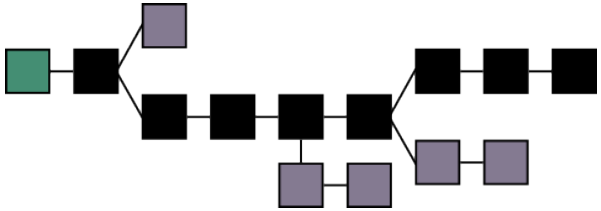
Example:

ASCIISUM( ASCIISUM( A, B, 1234, 0 ) )
= ASCIISUM(65+66+49+50+51+52+48)
= ASCIISUM ( 333 + 48 ) = ASCIISUM ( 381 )
= 51+56+49 = 156

# Mining: chain of blocks

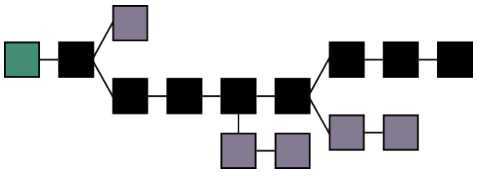



SHA-256(SHA-256(header))

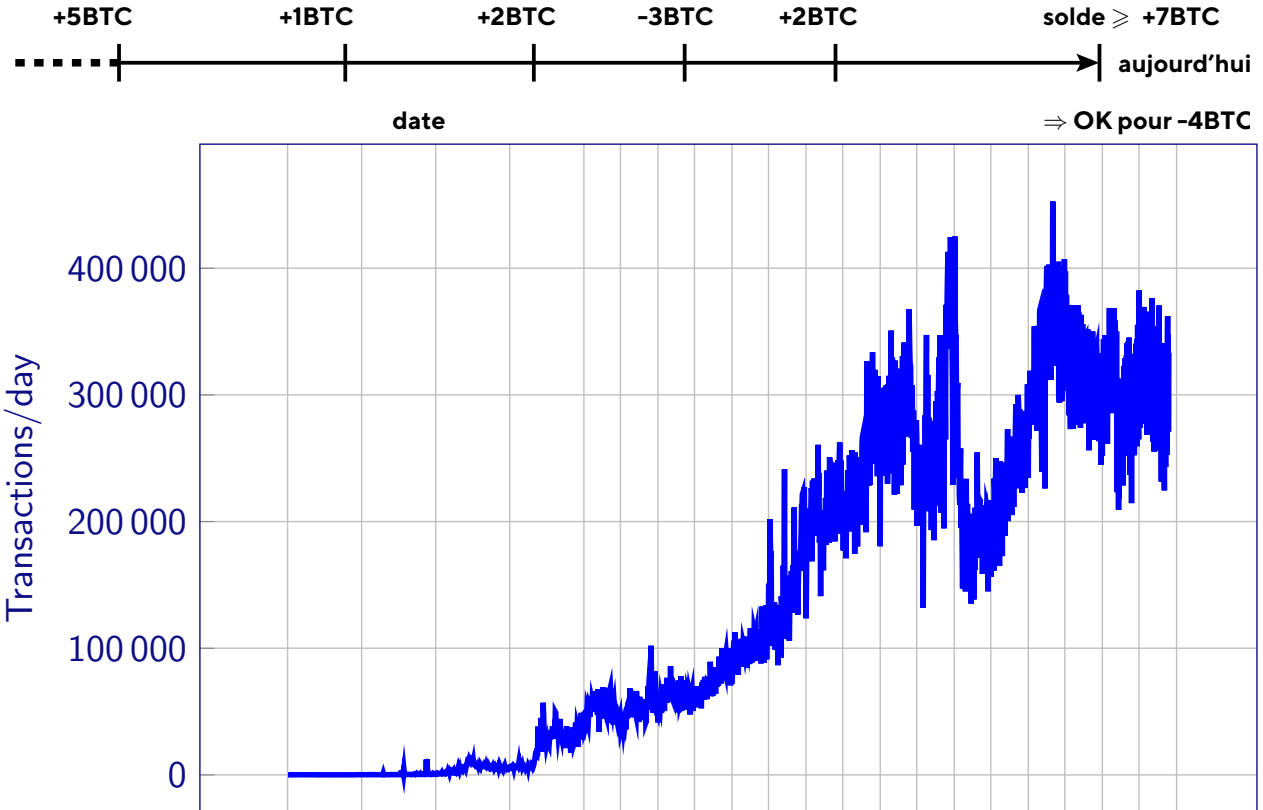


- previous transactions
- to be validated transactions (max. 1MB/block)
- seconds since 01/01/1970
- a nonce

# Mining = Validation of transactions



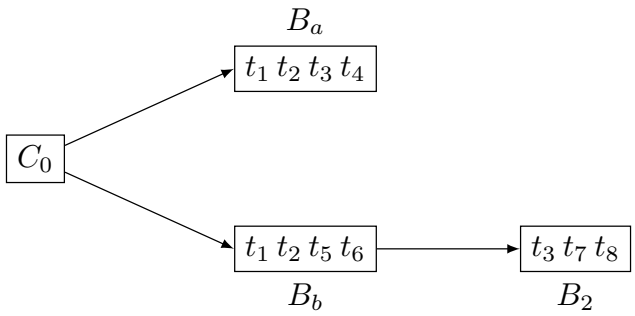
- Validation every 10 minutes (6 confirmations recommended)
- Larger blocks make full nodes more expensive to operate

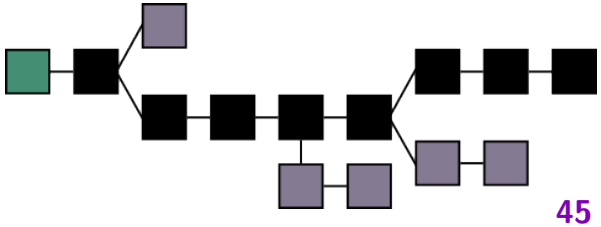


# Forks: Longest Chain Rule

- Longest Chain Rule: chain with most work is the main chain (51 % attack)

1. Simultaneously: Alice mines $B_a$ & Bob mines $B_b$
   Both chains are valid for now: Fork

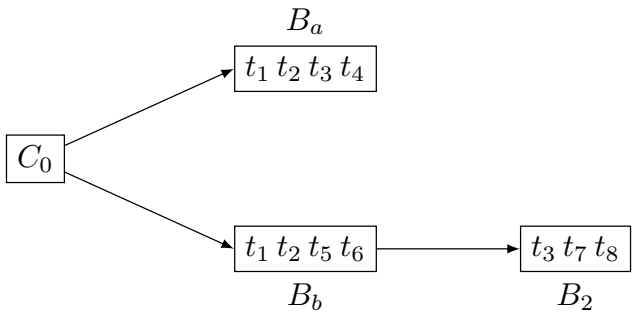


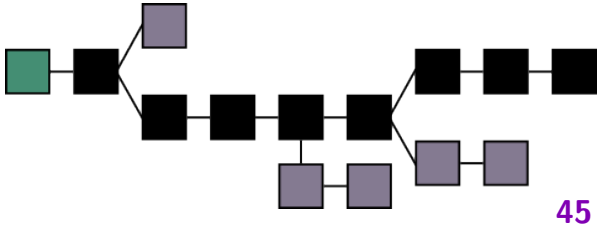



# Forks: Longest Chain Rule

- Longest Chain Rule: chain with most work is the main chain (51 % attack)

1. Simultaneously: Alice mines $B_a$ & Bob mines $B_b$
   Both chains are valid for now: Fork
2. Next miners mine either after $B_a$ or $B_b$

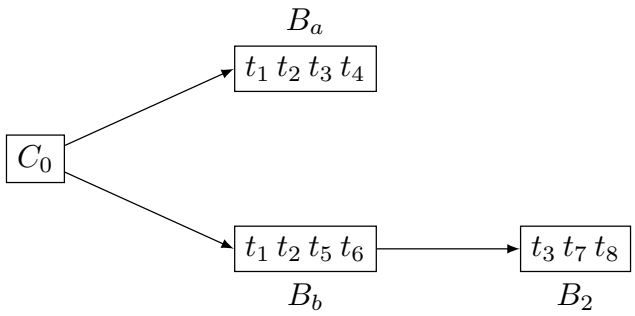


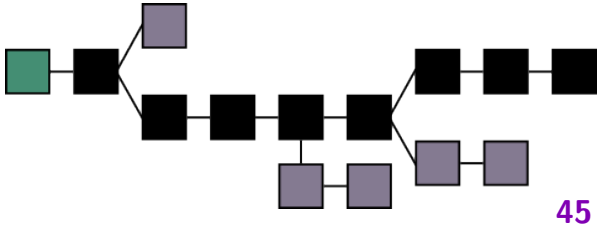



# Forks: Longest Chain Rule

- Longest Chain Rule: chain with most work is the main chain (51 % attack)

1. Simultaneously: Alice mines $B_a$ & Bob mines $B_b$
   Both chains are valid for now: Fork
2. Next miners mine either after $B_a$ or $B_b$
3. Charlie mines $B_2$
   Longest chain wins:
   $(\ldots \rightarrow C_0 \rightarrow B_b \rightarrow B_2)$

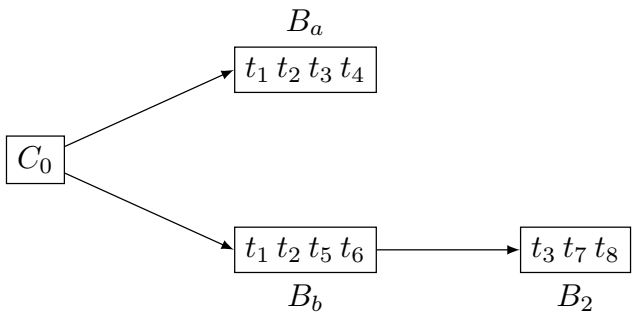


# Forks: Longest Chain Rule

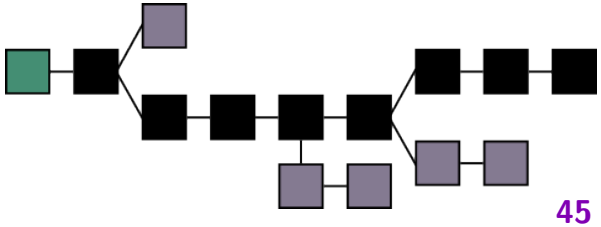
- Longest Chain Rule: chain with most work is the main chain (51 % attack)

1. Simultaneously: Alice mines $B_a$ & Bob mines $B_b$
   Both chains are valid for now: Fork
2. Next miners mine either after $B_a$ or $B_b$
3. Charlie mines $B_2$
   Longest chain wins:
   $(\ldots \rightarrow C_0 \rightarrow B_b \rightarrow B_2)$

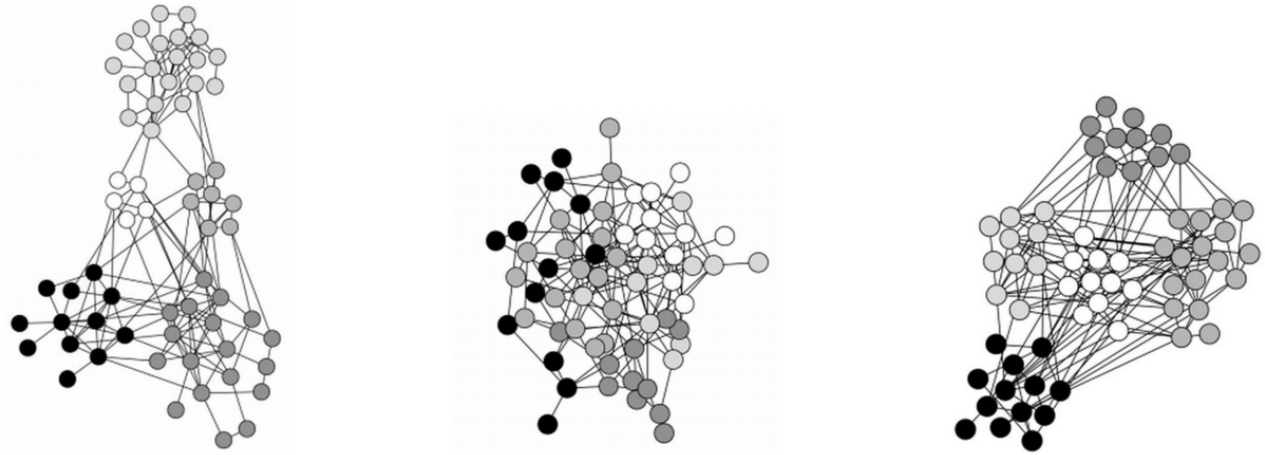



## Double spending?

If transactions $t_4$ & $t_5$ are mutually exclusive then $t_4$ will never be included by honest miners



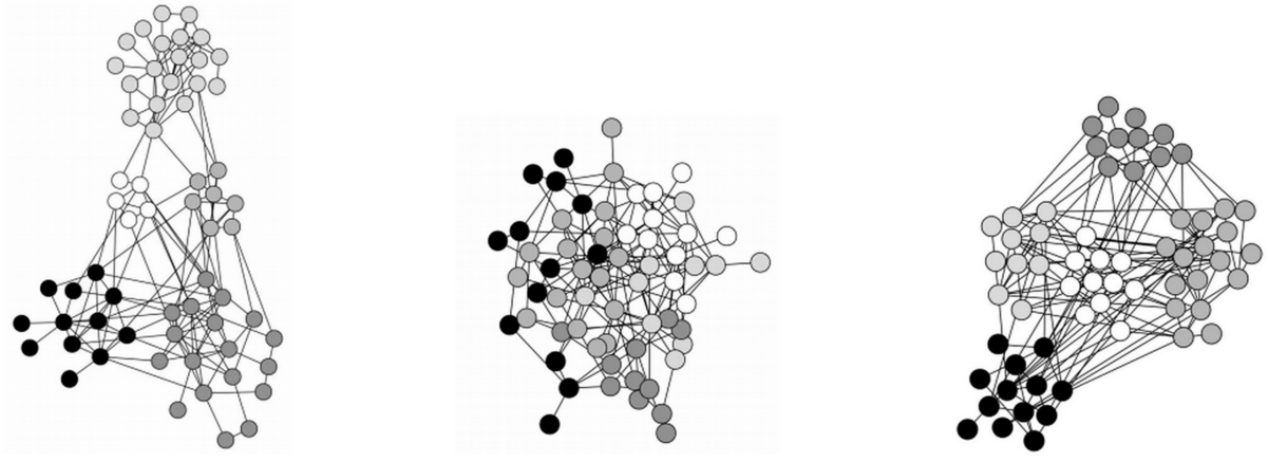
# Low Probability of simultaneous mining, except attacks



(a) (b) (c)

- # Nodes in the network at a given time
- Respective power, stake, activity, communication speed, etc.

# Low Probability of simultaneous mining, except attacks



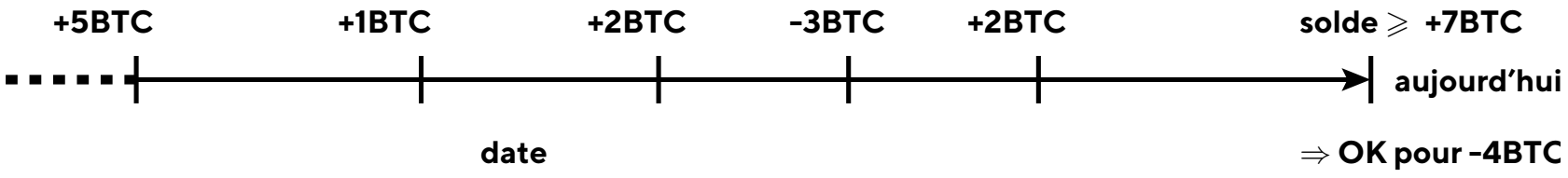
(a) (b) (c)

- # Nodes in the network at a given time
- Respective power, stake, activity, communication speed, etc.

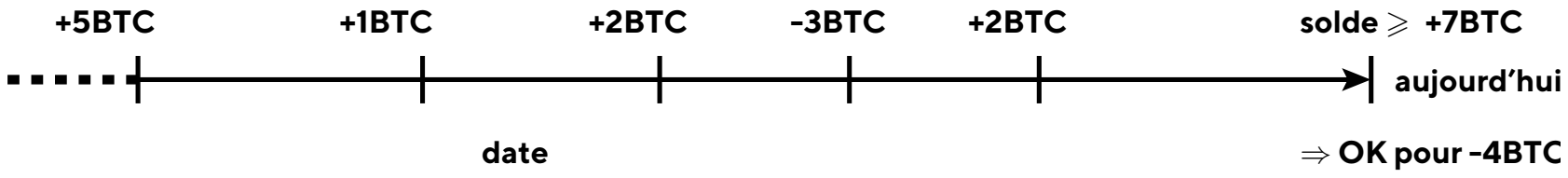
**Example: 10% of the world computing power, 6 confirmations**

$$\mathcal{P}(\text{fake longest chain}) < 1/1000$$

# Overdraft is not allowed



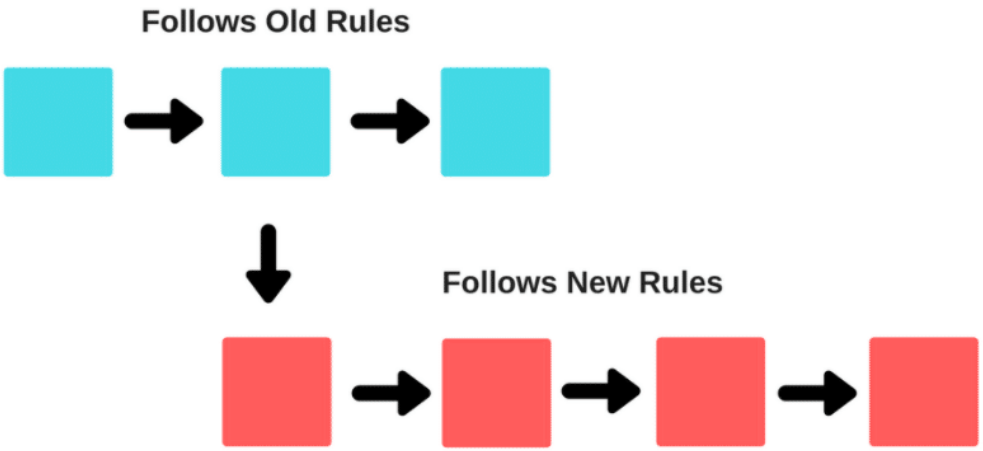
# Overdraft is not allowed




Preventing double spending

- All the balances must be positive
- Chain of two distinct honest minors cannot differ much;
- Chain of blocks: any modification must modify all the following blocks
  (depth and length of forks);
- The network adapts (every 2 weeks) to validate on average every 10 minutes.

# Other separations: Soft Fork

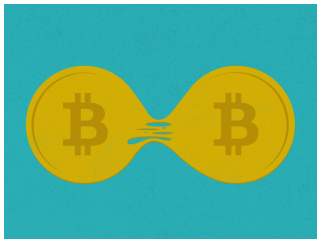


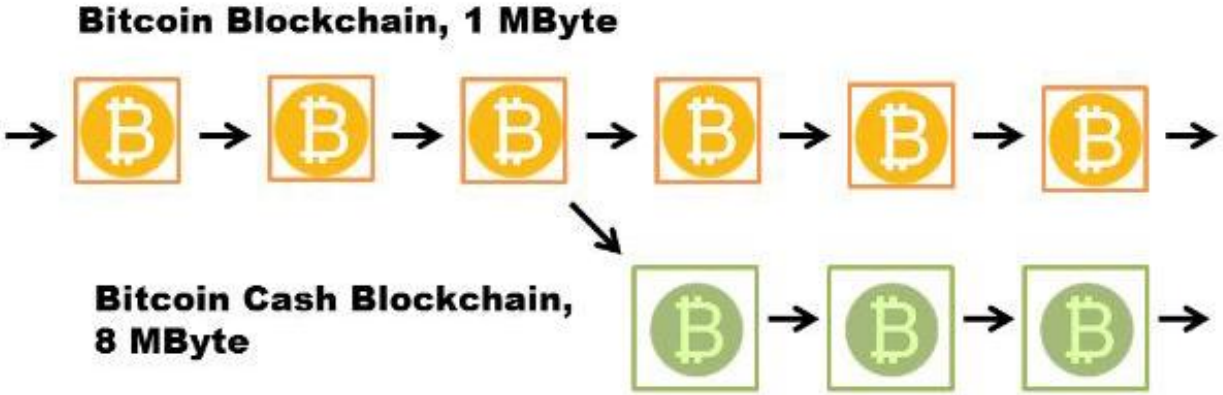

The primary difference between a soft fork and hard fork is that it is not backward compatible

## Modification of the code

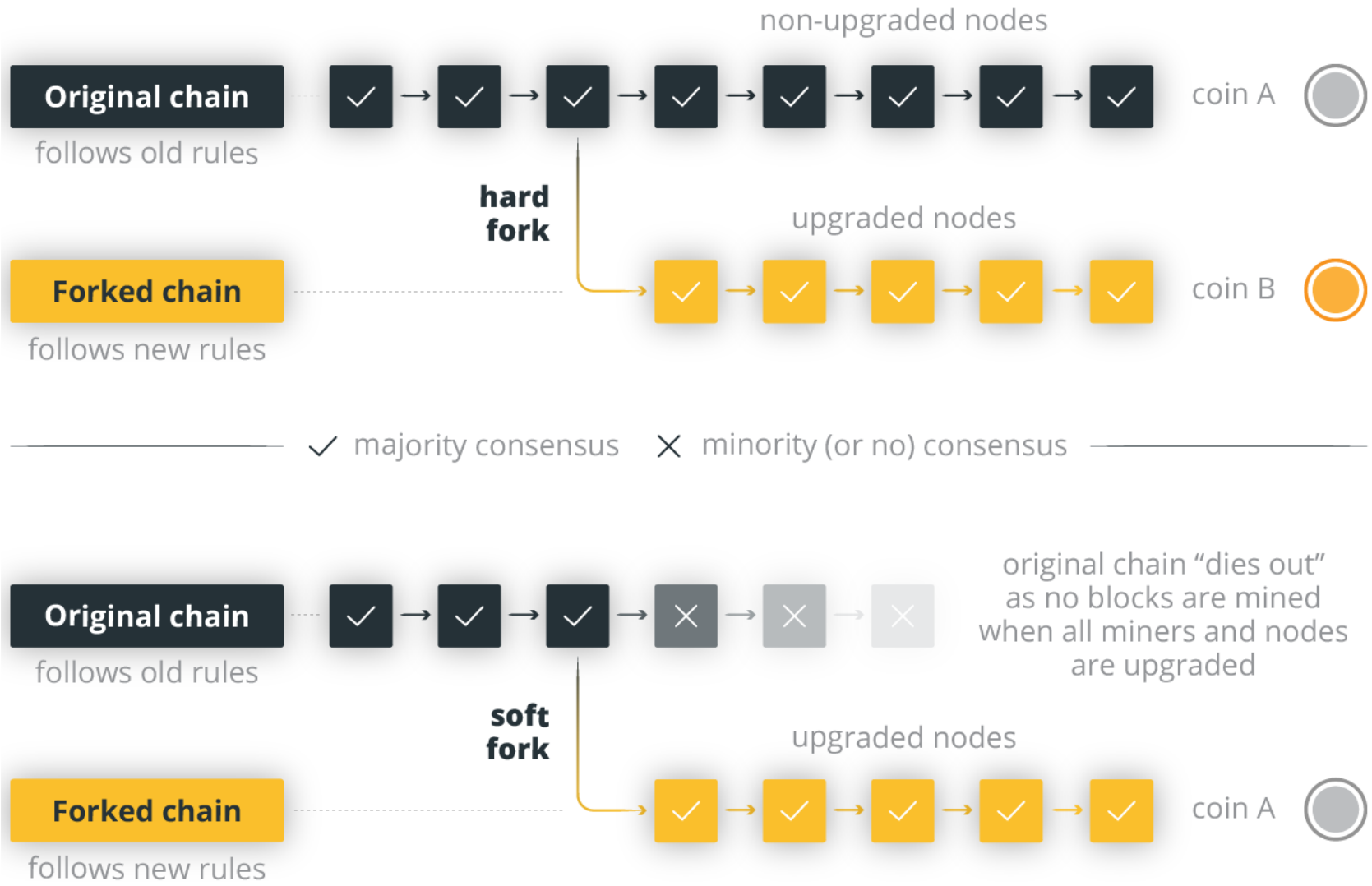
- Bug corrections
- Agreed (consensual) improvements

# Hard Fork



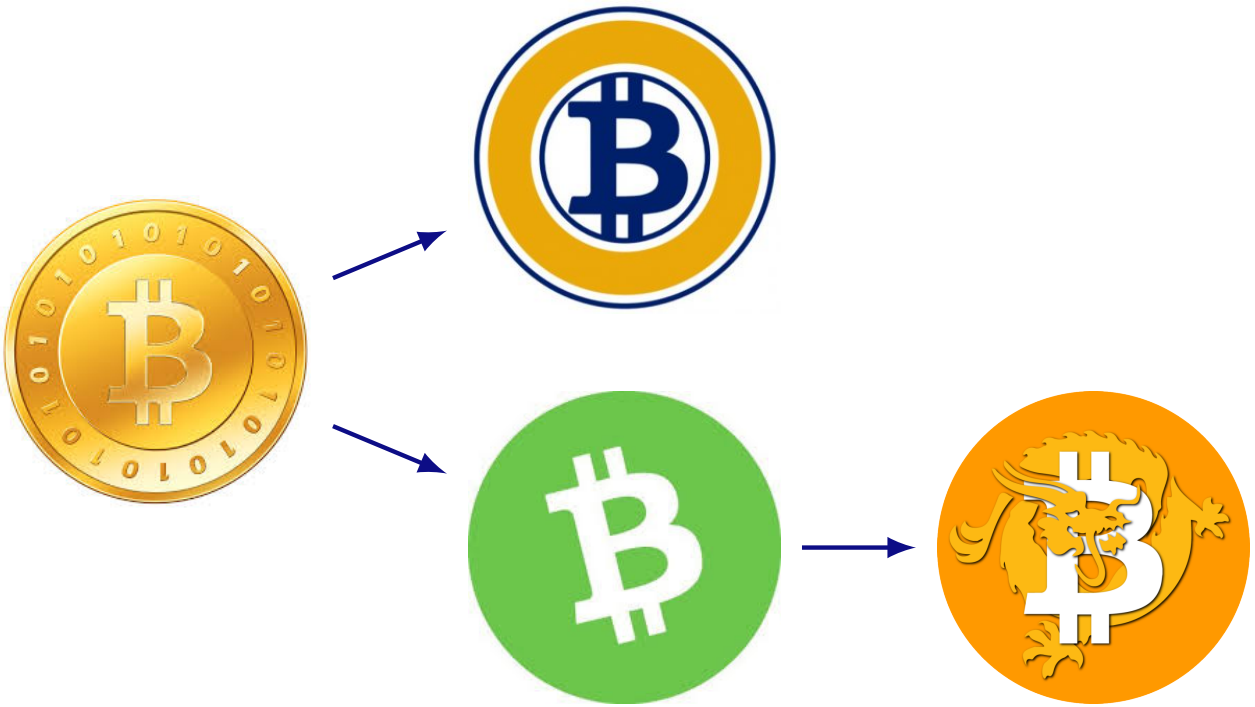

Bitcoin Blockchain, 1 MByte
Bitcoin Cash Blockchain,
8 MByte

# Hard or Soft Fork



# Bitcoin Hard Fork History

- **BCH** (Bitcoin Cash) for Bitcoin
  - August 1, 2017: block 478558
- **BTG** (Bitcoin Gold, ASIC→GPU) for Bitcoin
  - October 24, 2017: bloc 491407
- **BSV** (Bitcoin SV, Satoshi Version, 64MB) for Bitcoin Cash
  - November 15, 2018: bloc 556766



# Hard Fork History

| Logo | Fork Name | Fork Symbol | Blockchain | Fork Date | Fork Block | Coin Distribution |
|---|---|---|---|---|---|---|
| | Bitcoin Zero | BZX | Bitcoin | Sunday, September 30, 2018 | 0 | 1 HXX : 1 BTC = 1 BZX |
| | Micro Bitcoin | MBC | Bitcoin | Wednesday, May 30, 2018 | 525000 | 1 BTC = 10000 MBC |
| | ClassicBitcoin | CBTC | Bitcoin | Sunday, April 01, 2018 | 516095 | 1 BTC = 10000 CBTC |
| | Bitcoin Lite | BTCL | Bitcoin | Tuesday, January 30, 2018 | 0 | 1 BTC = 1 BTCL |
| | Bitcoin Atom | BCA | Bitcoin | Wednesday, January 24, 2018 | 505888 | 1 BTC = 1 BCA |
| | Bitcoin Interest | BCI | Bitcoin | Monday, January 22, 2018 | 505083 | 1 BTC = 1 BCI |
| | BitVote | BTV | Bitcoin | Sunday, January 21, 2018 | 505050 | 1 BTC = 1 BTV |
| | Bitcoin Smart | BCS | Bitcoin | Sunday, January 21, 2018 | 505050 | 1 BTC = 100 BCS |
| | Bitcoin Rhodium | BTR | Bitcoin | Wednesday, January 10, 2018 | 0 | 1 BTC = 1 BTR |
| | Bitcoin Private | BTCP | Bitcoin | Monday, January 01, 2018 | 0 | 1 BTC/ZCL = 1 BTCP |
| | Bitcoin All | BTA | Bitcoin | Monday, January 01, 2018 | 0 | 1 BTC = 1 BTA |
| | Bitcoin Pizza | BPA | Bitcoin | Monday, January 01, 2018 | 501888 | 1 BTC = 1 BPA |
| | BitcoinBoy | BCB | Bitcoin | Sunday, December 31, 2017 | 501888 | 1 BTC = 100 BCB |
| | Bitcoin Ore | BCO | Bitcoin | Sunday, December 31, 2017 | 501949 | 1 BTC = 1 BCO |
| | Bitcoin Uranium | BUM | Bitcoin | Sunday, December 31, 2017 | 0 | 1 BTC = 1 BUM |
| | Quantum Bitcoin | QBTC | Bitcoin | Thursday, December 28, 2017 | 0 | 1 BTC = 1QBTC |
| | Bitcoin SegWit2X x11 | B2X | Bitcoin | Thursday, December 28, 2017 | 501451 | 1 BTC = 1 B2X |
| | Bitcoin File | BIFI | Bitcoin | Wednesday, December 27, 2017 | 501225 | 1 BTC = 1000 BIFI |
| | Bitcoin God | GOD | Bitcoin | Wednesday, December 27, 2017 | 501225 | 1 BTC = 1 GOD |
| | Bitcoin Top | BTT | Bitcoin | Tuesday, December 26, 2017 | 501118 | 1 BTC = 1 BTT |

| Logo | Fork Name | Fork Symbol | Blockchain | Fork Date | Fork Block | Coin Distribution |
|---|---|---|---|---|---|---|
| | Bitcoin New | BTN | Bitcoin | Monday, December 25, 2017 | 501000 | 1 BTC = BTN |
| | Lightning Bitcoin | LBTC | Bitcoin | Tuesday, December 19, 2017 | 499999 | 1 BTC = 1 LBTC |
| | Bitcoin Stake | BTCS | Bitcoin | Tuesday, December 19, 2017 | 499999 | 1 BTC = 100 BTCS |
| | Bitcoin Faith | BTF | Bitcoin | Tuesday, December 19, 2017 | 500000 | 1 BTC = 1 BTF |
| | Bitcoin World | BTW | Bitcoin | Sunday, December 17, 2017 | 499777 | 1 BTC = 10000 BTW |
| | UnitedBitcoin | UB | Bitcoin | Tuesday, December 12, 2017 | 498777 | 1 BTC = 1 UB |
| | Bitcoin Hot | BTH | Bitcoin | Tuesday, December 12, 2017 | 498848 | 1 BTC = 100 BTH |
| | BitcoinX | BCX | Bitcoin | Tuesday, December 12, 2017 | 498888 | 1 BTC = 10000 BCX |
| | Super Bitcoin | SBTC | Bitcoin | Tuesday, December 12, 2017 | 498888 | 1 BTC = 1 SBTC |
| | Bitcoin Silver | BTSI | Bitcoin | Friday, December 01, 2017 | 0 | 1 BTC = 1 BTSI |
| | Bitcoin Nano | BTN | Bitcoin | Friday, December 01, 2017 | 501888 | 1 BTC = 1000 BTN |
| | Bitcoin Diamond | BCD | Bitcoin | Friday, November 24, 2017 | 495866 | 1 BTC = 10 BCD |
| | Bitcore | BTX | Bitcoin | Thursday, November 02, 2017 | 0 | 1 BTC = 0.5 BTX |
| | Bitcoin Gold | BTG | Bitcoin | Tuesday, October 10, 2017 | 491407 | 1 BTC = 1 BTG |
| | Bytether | BTH | Bitcoin | Tuesday, August 01, 2017 | 478558 | 1 BTC = 1 BTH |
| | Oil BTC | OBTC | Bitcoin | Tuesday, August 01, 2017 | 498888 | 1 BTC = 1 OBTC |
| | Bitcoin Clashic | BCHC / B | Bitcoin | Tuesday, August 01, 2017 | 478558 | 1 BTC = 1 BCHC / B |
| | Bitcoin Cash | BCH | Bitcoin | Tuesday, August 01, 2017 | 478559 | 1 BTC = 1 BCH |

# Can a hard fork make you richer?

- Instantaneous: doubles the number of coins (same balance in each branch)
- Purchasing power is in fact unchanged at the time of the fork (split in both currencies)

## Example of Bitcoin Gold

| | | |
|---|---|---|
| 23/10/2017: | BTC ≈ | 5 910$ |
| 24/10/2017: | BTG ≈ | 480$ |
| 25/10/2017: | BTC ≈ | 5 380$ |

# Can a hard fork make you richer?

- Instantaneous: doubles the number of coins (same balance in each branch)
- Purchasing power is in fact unchanged at the time of the fork (split in both currencies)
- Then: each cryptocurrency fluctuates in its own right

## Example of Bitcoin Gold

| | | | | | |
|---|---|---|---|---|---|
| 23/10/2017: | BTC ≈ | 5 910$ | | | |
| 24/10/2017: | BTG ≈ | 480$ | | | |
| 25/10/2017: | BTC ≈ | 5 380$ | | | |
| 10/03/2019: | BTC ≈ | 3 895$ | 09/11/2020: | BTC ≈ | 15 523$ |
| | BTG ≈ | 12$ | | BTG ≈ | 7$ |

# Traceability

Tracking criminals:

- The list of all the transactions is public!
- Waiving the anonymity (legally) at entry/exit (classical currencies)

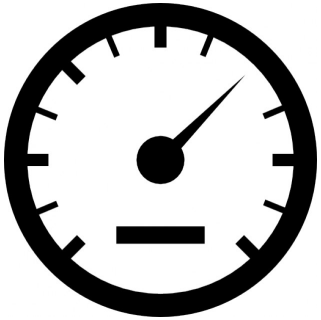
# Traceability

Tracking criminals:

- The list of all the transactions is public!
- Waiving the anonymity (legally) at entry/exit (classical currencies)

MONERO ZCASH

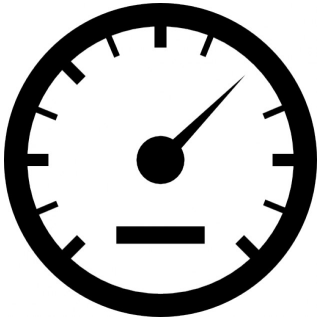
# Limitations



10 minutes = 1 block

Size of transactions 1 MB (4MB, after SegWit, 1st August 2017)

# Limitations



10 minutes = 1 block

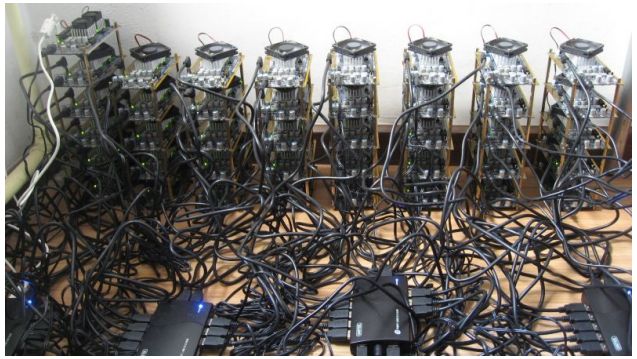
Size of transactions 1 MB (4MB, after SegWit, 1st August 2017)


Lightning Network

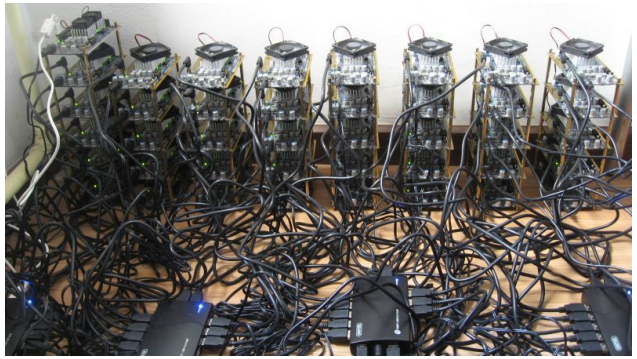
ETHEREUM

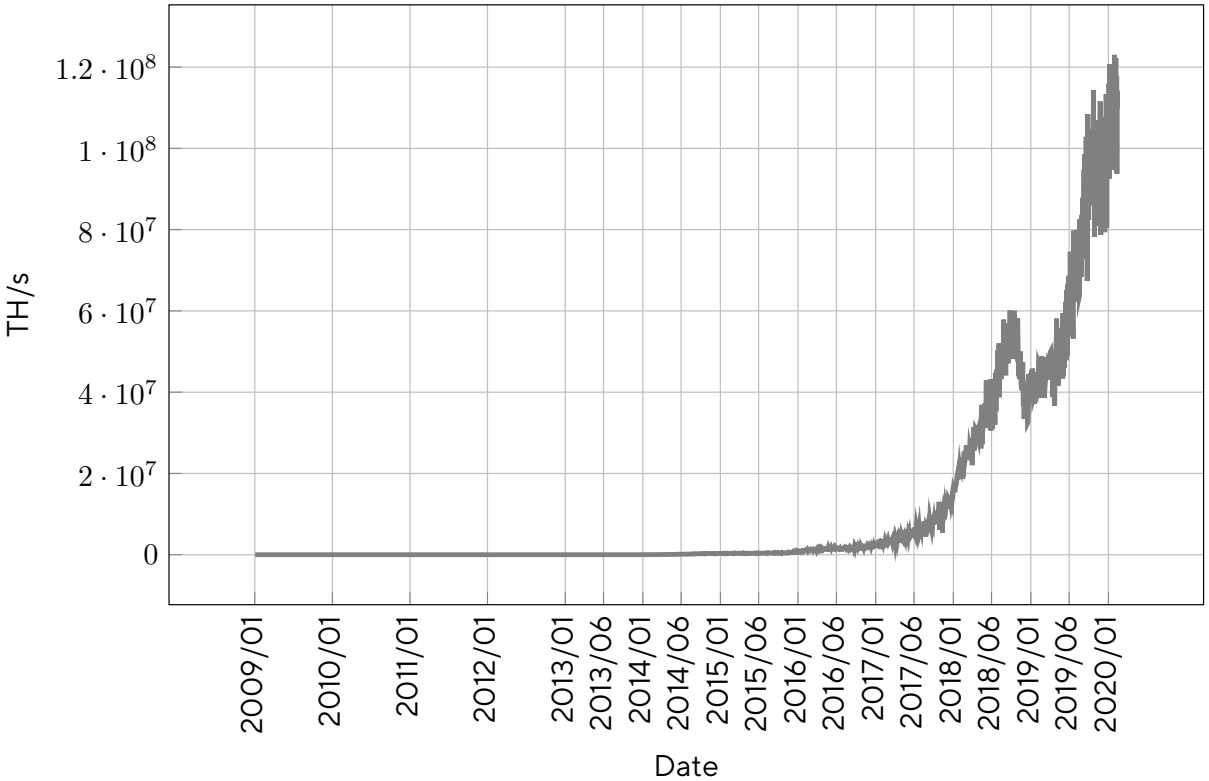
12 seconds

# Energy intensive: Bitcoin power requirements (hashrate)



# Energy intensive: Bitcoin power requirements (hashrate)





# Energy intensive: Bitcoin power requirements (hashrate)

Estimation: several yearly TWh (comparable to a small state comsumption)

⚠ Estimated from 15 to 70 TWh in 2018 (whole of France: 1800 TWh in 2017)

# Energy intensive: Bitcoin power requirements (hashrate)

Estimation: several yearly TWh (comparable to a small state comsumption)

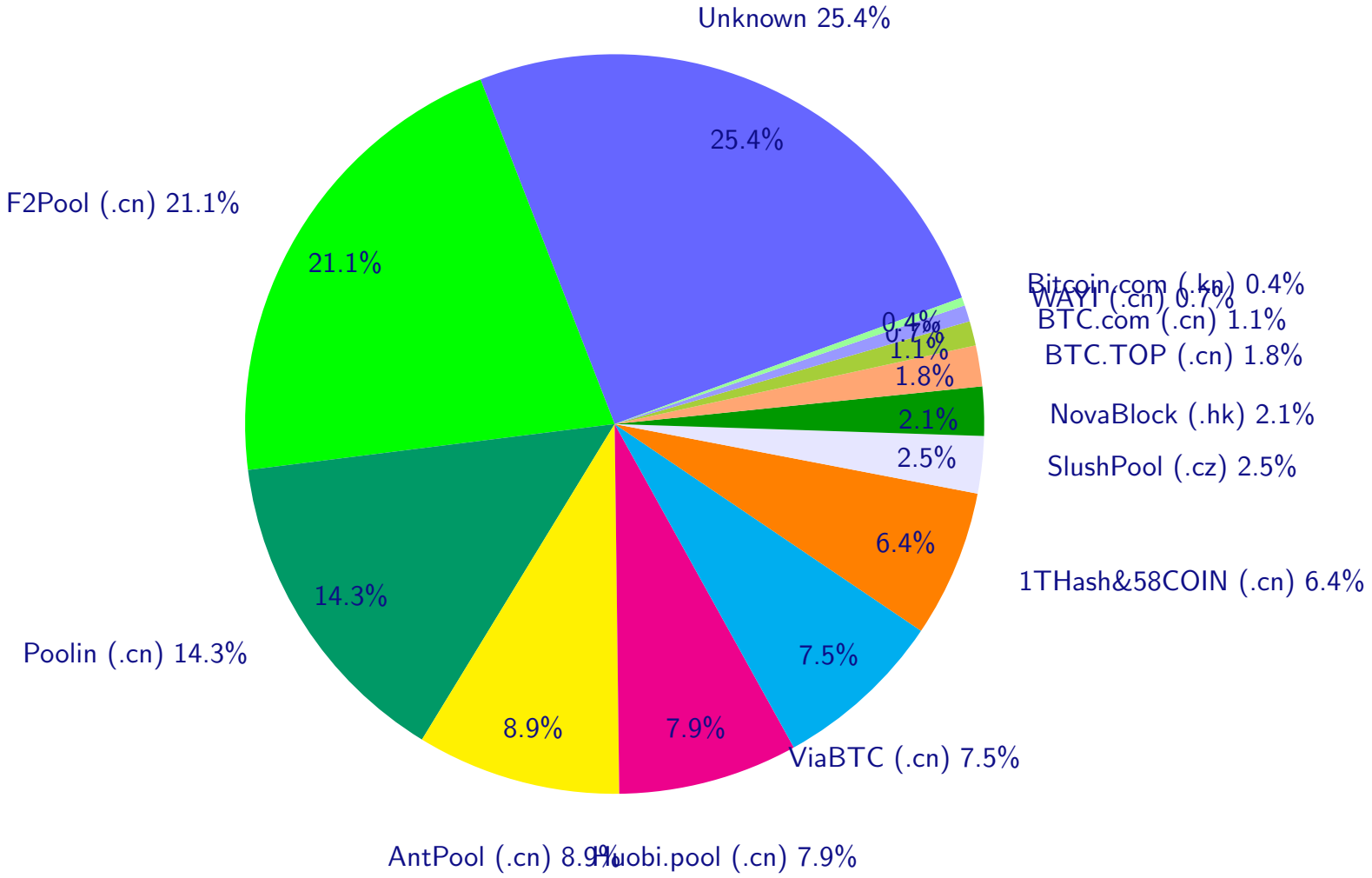
- Lightning Network
- Other consensus algorithm (e.g., Proof of Stake)

# New block every 10 minutes

| Machine | Type | Speed MH/s | Efficiency MH/J | Cost MH/s/€ | Average Mining Years/block |
|---|---|---|---|---|---|
| Core i5-2400 | CPU | 14 | 0.15 | 0.09 | 25.3 Millions |
| PS3 | Cell | 21 | 0.35 | 0.09 | 16.9 Millions |
| ATI 830 | GPU | 325 | 1.98 | 3.30 | 1.1 Millions |
| Ebit E11++ | ASIC | 44 000 000 | 22 200.00 | 8 885.00 | 13.6 |

- Target: 74 initial zeroes, $\frac{1}{2^{74}}$ chances to mine
- $44\,000\,000$ MH/s $= 4.4\,10^{13}$ H/s $\approx 2^{45.3}$ H/s
- $2^{28.7} \approx 4.3\,10^{8}$ s $\approx 5\,000$ days $\approx$ 13.6 years of computations of an Ebit E11++
- World network $\approx$ 700 000 E11

# Mining Farms: share the rewards among the farmers as of November 10, 2020



# Bitcoin: Decentralized Cryptocurrency

- Proof of work = hashing target
- Money creation = reward to miners
- Miner = hard work + energy-intensive

# Bitcoin: Decentralized Cryptocurrency

- Proof of work = hashing target
- Money creation = reward to miners
- Miner = hard work + energy-intensive

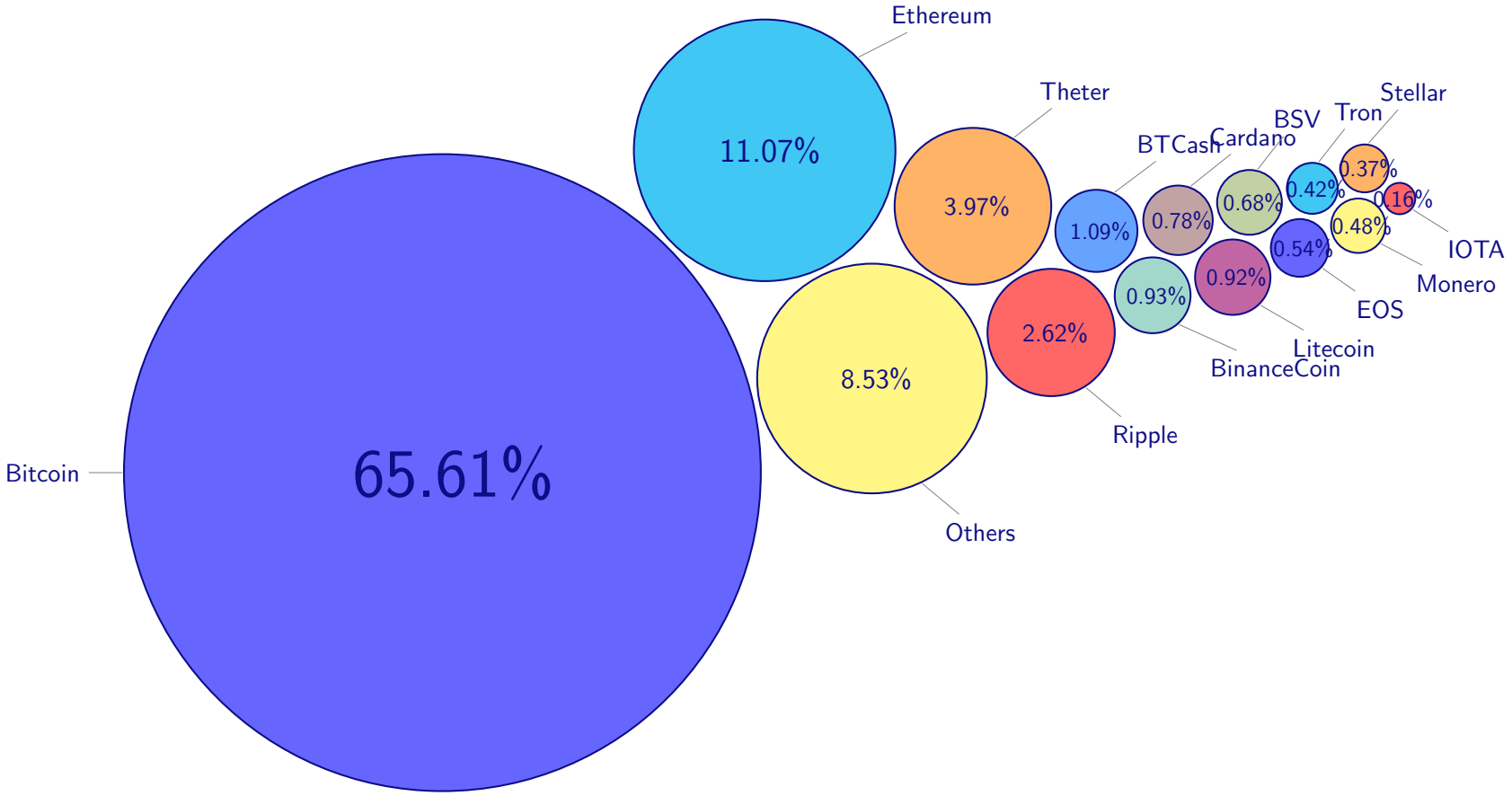



- Loss or theft of the private key: permanent
- Anonymous and traceable currency



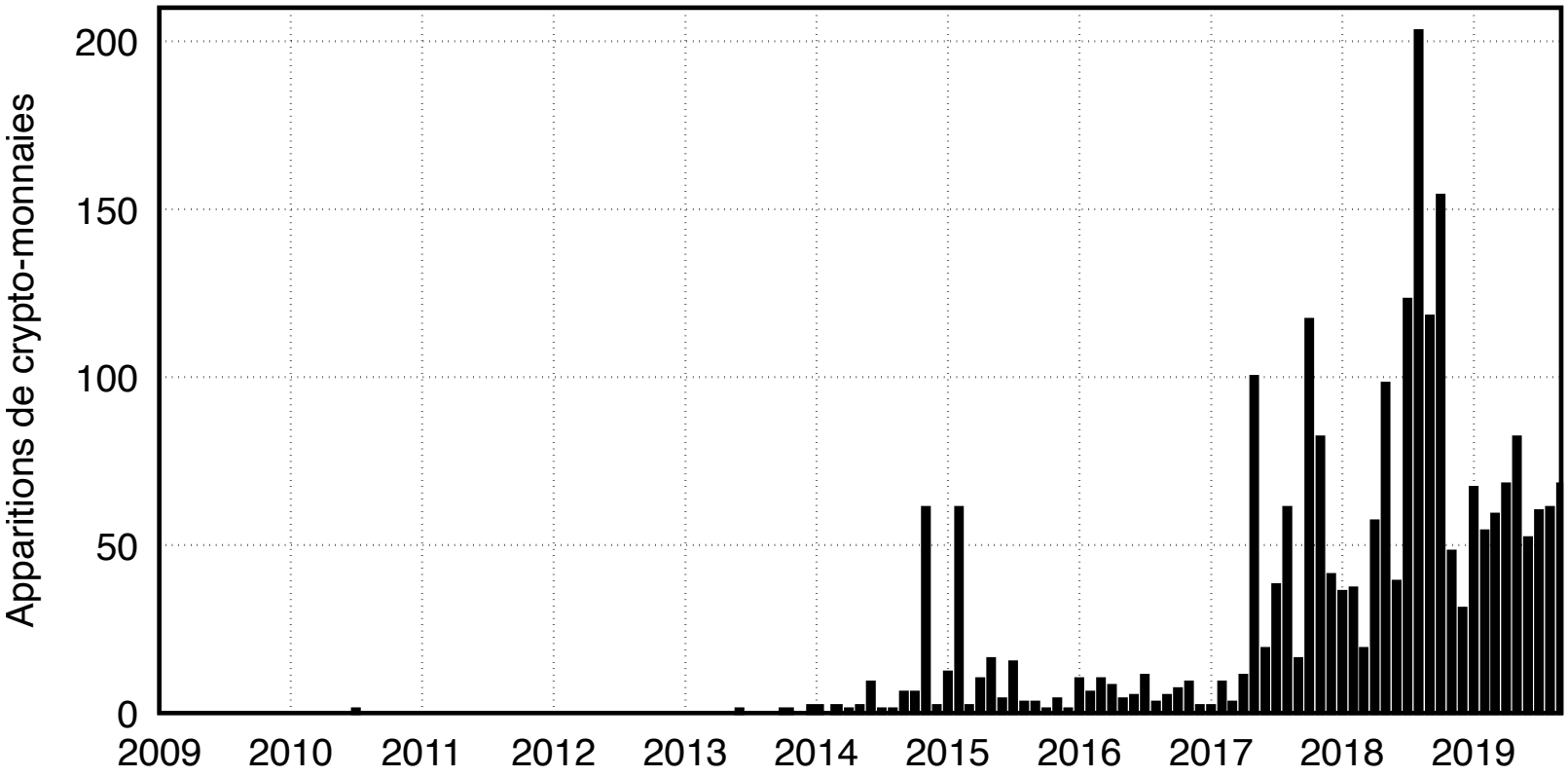
# Outline

# Monetary diversity: marketcap



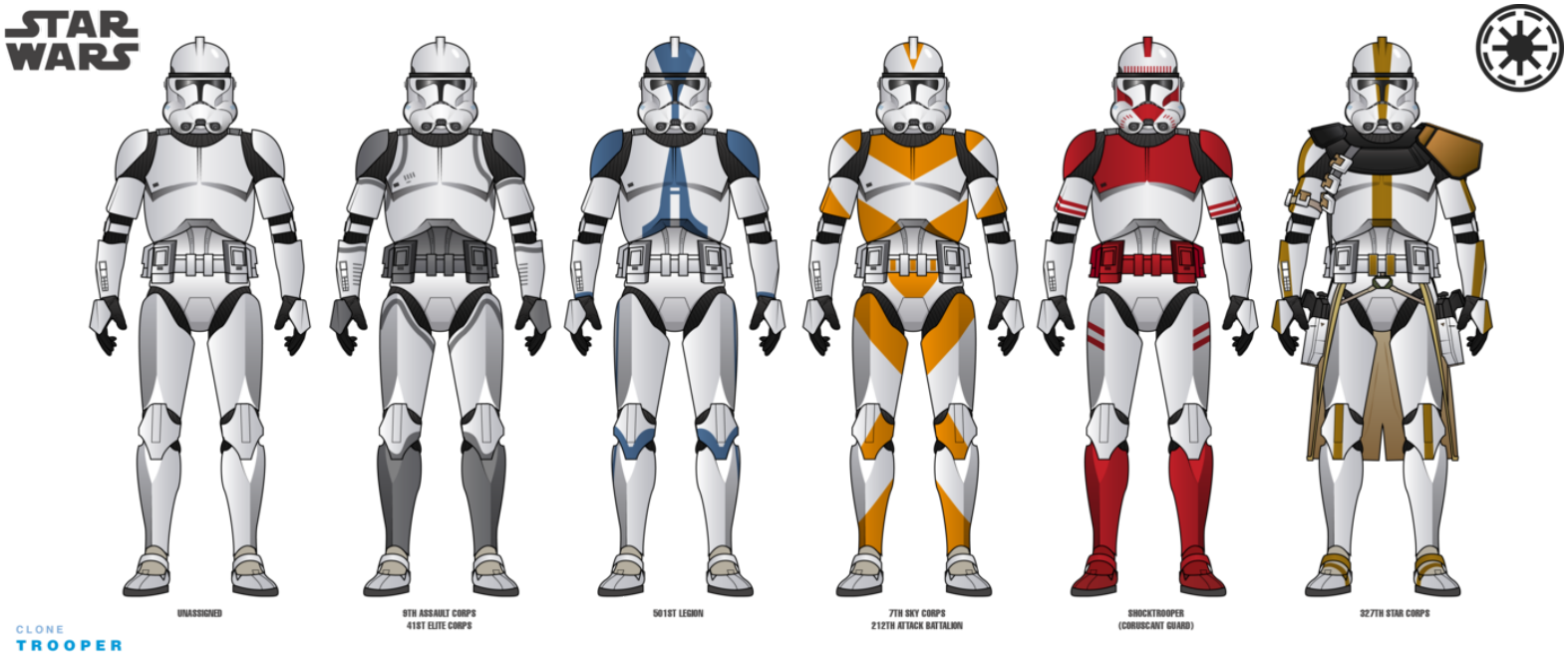
# Other crypto-currencies

# Other crypto-currencies



# Classification I: lousy

# Classification II: Bitcoin Clones



# Classification III: more useful

primes rewarding medical computations HPC

# Classification IV: other consensus algorithms

| PeerCoin | BurstCoin | Ethereum | Ic |
|---|---|---|---|
| PoS | Storage | Hybrid PoW/PoS | goss |

# Classification IV: other consensus algorithms

| PeerCoin | BurstCoin | Ethereum | Ic |
|---|---|---|---|
| PoS | Storage | Hybrid PoW/PoS | gos |


gathering of transactions

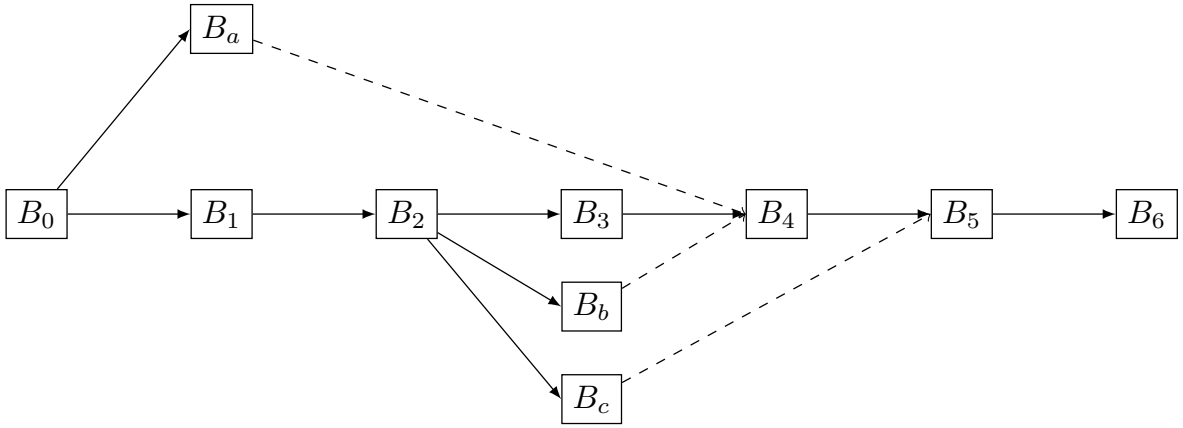
# Etherum

| Unit | wei |
|---|---|
| wei | 1 wei |
| Kwei (babbage) | $10^3$ wei |
| Mwei (lovelace) | $10^6$ wei |
| Gwei (shannon) | $10^9$ wei |
| microether (szabo) | $10^{12}$ wei |
| milliether (finney) | $10^{15}$ wei |
| ether | $10^{18}$ wei |

ethereum

Speed: 12 seconds

## Rewarding uncles




$$\begin{cases} B_4 & \text{receives } 3 \times \left(1 + \frac{2}{32}\right) = 3.185 \text{ ethers} \\ B_b & \text{receives } \frac{7}{8} \times 3 = 2.625 \text{ ethers, } B_a \text{ receives } \frac{5}{8} \times 3 = 1.875 \text{ ethers} \end{cases}$$

# Peercoin: coin age

For 10 coins

| Days | 0 | 1 | 2 | ... |
|---|---|---|---|---|
| Age | 10 | 10 | 20 | ... |

After V 0.3:

- Wait 30 days
- Maximum 90 days

# Peercoin: coin age

For 10 coins

| Days | 0 | 1 | 2 | ... |
|---|---|---|---|---|
| Age | 10 | 10 | 20 | ... |

After V 0.3:

- Wait 30 days
- Maximum 90 days

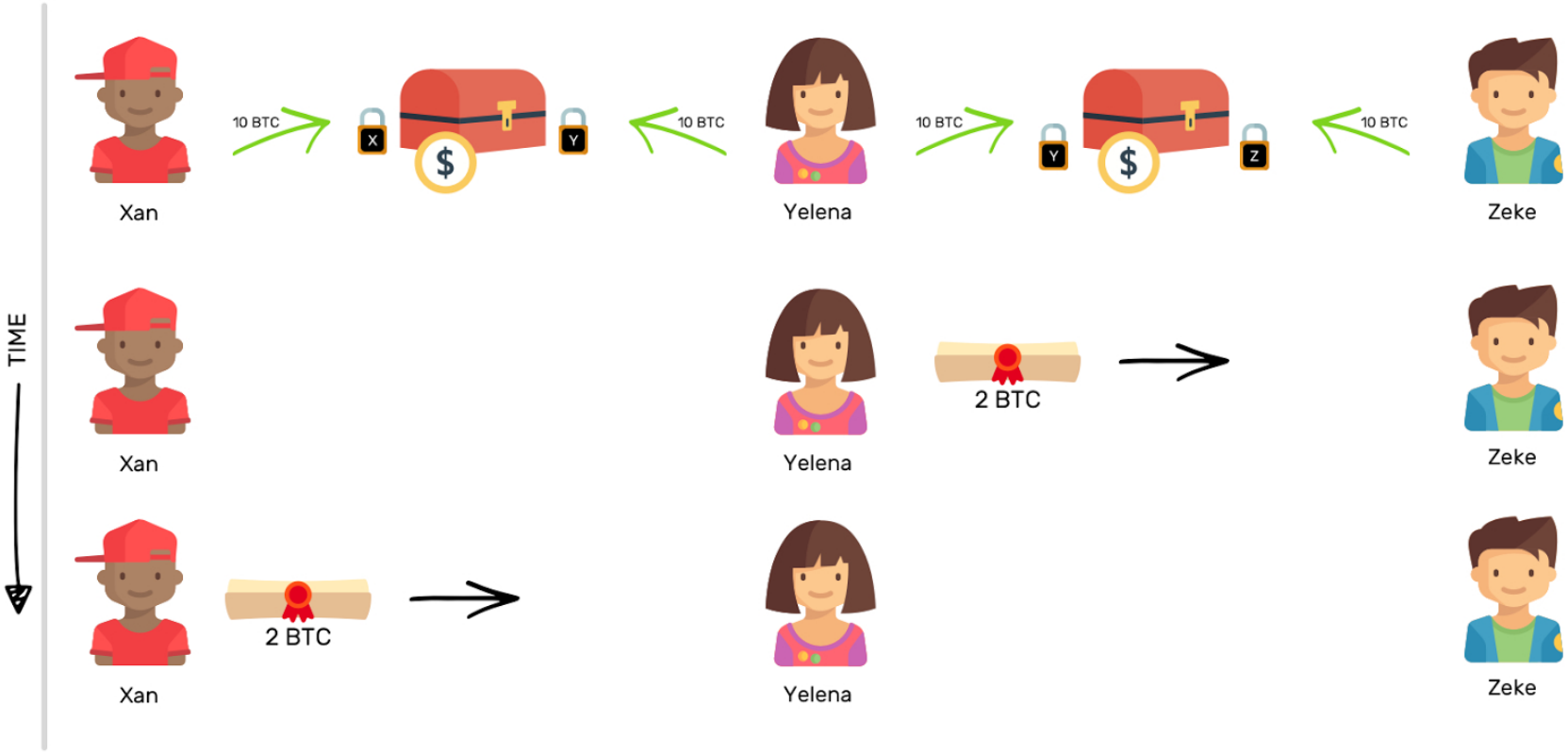
## Hashing target

$$\text{Hash}(\ldots) < C \times A \times \frac{1}{2^{32} \times D}$$

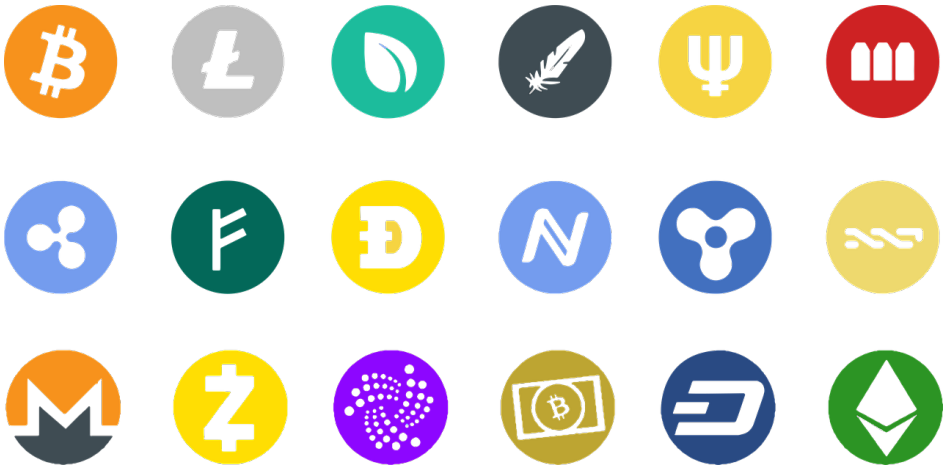
- $C$: number of coins
- $A$: Average Age (days) of the coins
- $D$: Hardness

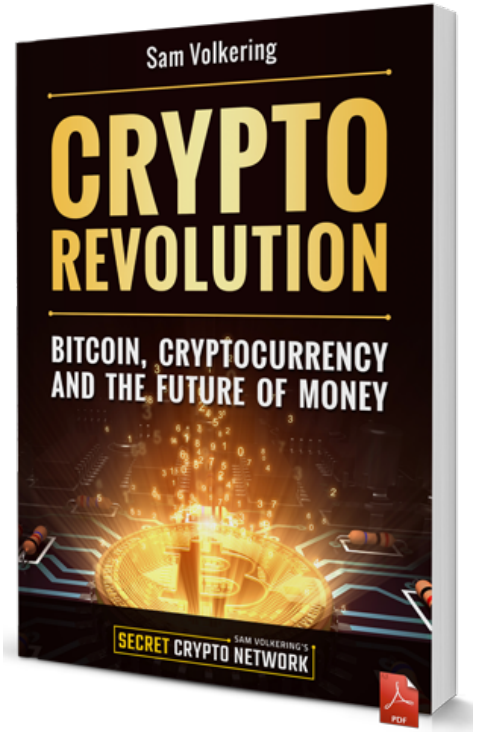
# Xan $\xrightarrow{2\ \text{BTC}}$ Zeke: signed commitments on open channels

# Lightning Network



# Multiculturalism of money creation





# Who embraces these crypto-currencies?

# Another example: Ğ1


- Freedom of access to resources
- Freedom of production
- Freedom of exchange in the currency

Universal Dividend: proof of existence

# More obstacles

Computer hygiene

Awareness

# Outline

# Conclusion

- Bitcoin
- Blockchain

# Projects

3 groups of 3 persons to constitue as soon as possible.

1. EcomobiCoin
2. DriveCoin
3. AssureCoin

# EcoMobiCoin

Design a cryptocurrency that promotes the eco-responsible mobility: walking, running, biking car-pooling, using public transportation ...

# DriveCoin

Design a cryptocurrency that promotes drivers that are using less gaz and have a eco-responible driving.

# AssureCoin

Design a cryptocurrency that promotes drivers that are respecting the rules and they will have adapted prices for their insurrance.