Introduzione alle Cryptovalute

Capitolo 1: I Bitcoin

Pietro Speroni di Fenizio

I've been working on a new electronic cash system that's fully peer-to-peer, with no trusted third party.

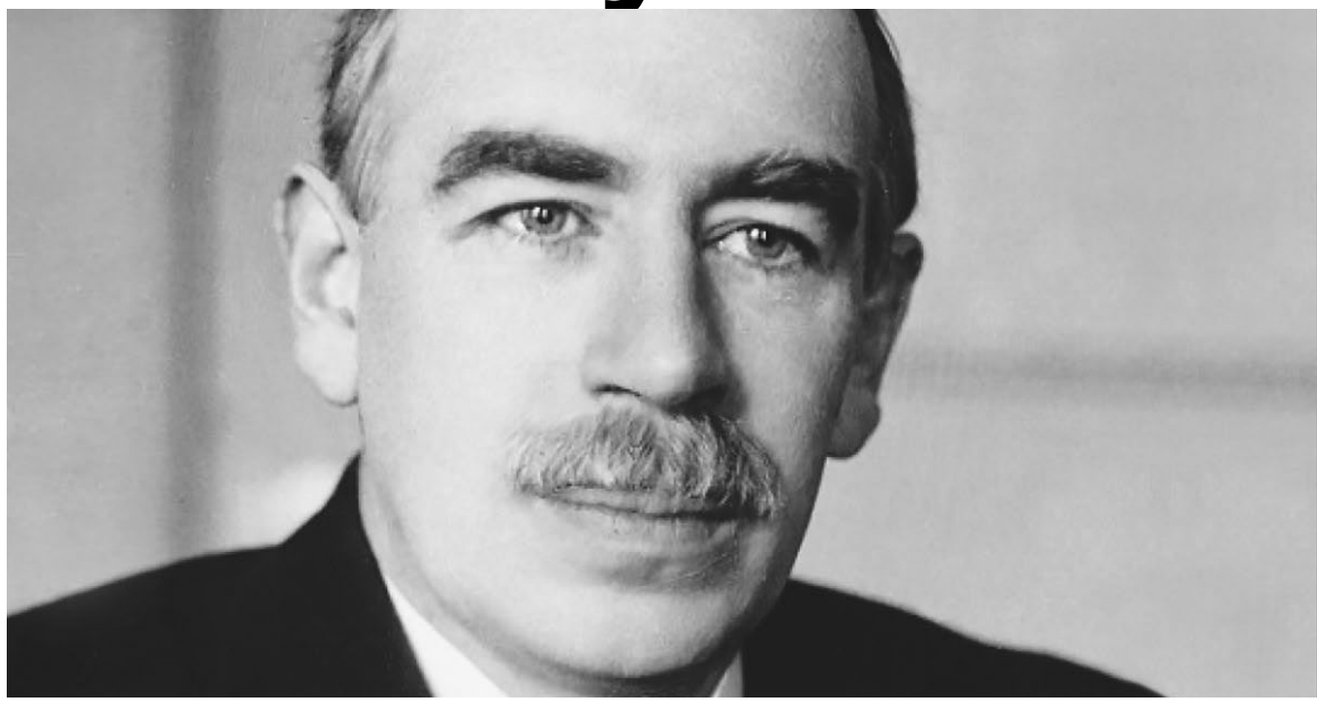
The paper is available at:
http://www.bitcoin.org/bitcoin.pdf

The main properties:

- Double-spending is prevented with a peer-to-peer network.
- No mint or other trusted parties.
- Participants can be anonymous.
- New coins are made from Hashcash style proof-of-work.
- The proof-of-work for new coin generation also powers the network to prevent double-spending.

Il Contesto: La Battaglia tra Keynes e Hayek

KEYNES



HAYEK

Funzioni di una moneta

- Misura del Valore (Unit of Account)
- Mezzo di Scambio (Medium of Exchange)
- Riserva di Valore (Store of Value)

Caratteristiche di una moneta

- Si deve mantenere nel tempo
- Deve poter essere trasportata
- Deve poter essere suddivisa
- Deve essere “vendibile” (salability)

La moneta è una proprietà emergente delle società

- Tutte le società hanno almeno una moneta.

- È più efficiente del baratto

- Si può insegnare a usare la moneta anche alle scimmie
  (la prostituzione compare subito)

- Quando culture diverse si mischiano una sola moneta tende a sopravvivere. Ma a volte ci vogliono molti anni.

Forme di moneta

- Sigarette
- Oro
- Argento
- Rame
- Euro (moneta stampata)
- Bitcoin
- Perline di Vetro
- Dollari
- Conchiglie
- Sale
- Bestiame
- Statue

Come si capisce quale moneta sopravvivrà?

- Stock vs Flusso

- Stock: Quantità disponibile di quella moneta

- Flow: Crescita dello Stock nel tempo

- La moneta con il minor rapporto
  Flusso su Stock (Flusso/Stock) *tende* a vincere

- Ma il Flusso non è costante (e può essere anche negativo)

Come cambia il Flusso

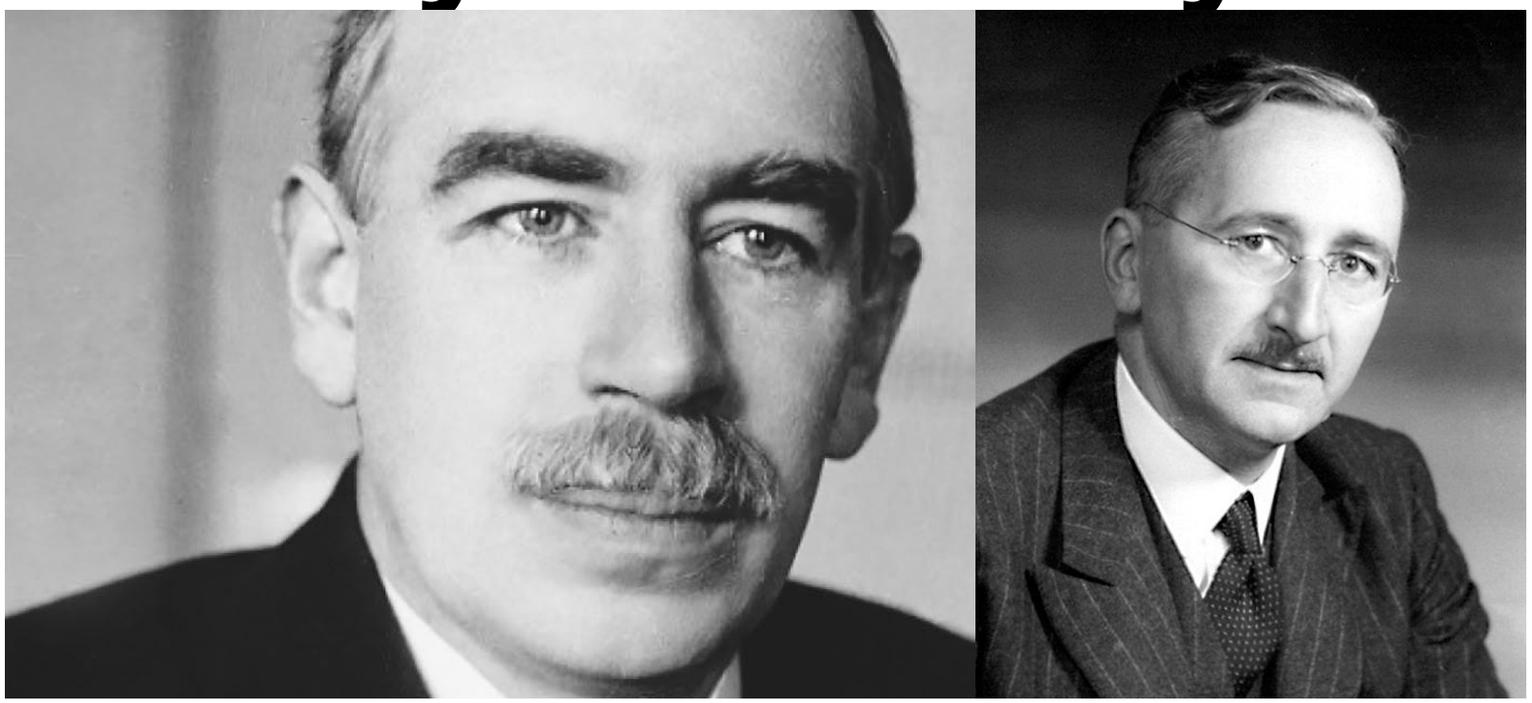
- Più materiale viene minato
- Nuove tecnologie permettono una produzione maggiore
- Tecnologie di un’altra civiltà permettono una produzione maggiore
- Lo Stato stampa moneta

- Il valore di una moneta varia al variare dello Stock.
- Questo genera Inflazione, Deflazione e Iperinflazione

- Si può definire l’inflazione
  sia come aumento dei prezzi (scuola Keynesiana)
  che come aumento della quantità di moneta (scuola Austriaca)

Il Contesto: La Battaglia tra Keynes e Hayek

KEYNES



HAYEK

Lo Stato può intervenire sulla quantità di Moneta

Una bassa inflazione è ottimale

Tra 1% e 2%

Stampare permette l'intervento dello Stato e aiuta la popolazione

Lo Stato non deve intervenire sulla quantità di Moneta

Nessuna Inflazione è ottimale

Stampare moneta provoca Bolle e Crolli

Stampare inibisce l'imprenditorialità

Storia della moneta

- Baratto
- Uso di un mezzo di scambio
- Metalli
- Oro, Argento
- La Nascita dell’Inflazione
- The Golden Standard-Fiat Currencies
- Brettonwood Agreement
- Francia Germania richiedono il loro oro - Nixon fa default sulla loro promessa
- Bitcoin

Storia della moneta

- Baratto
- Uso di un mezzo di scambio
- Metalli
- Oro, Argento
- **La Nascita dell’Inflazione**
- The Golden Standard-Fiat Currencies
- Brettonwood Agreement
- Francia Germania richiedono il loro oro - Nixon fa default sulla loro promessa
- Bitcoin

Inflazione durante l’Impero Romano

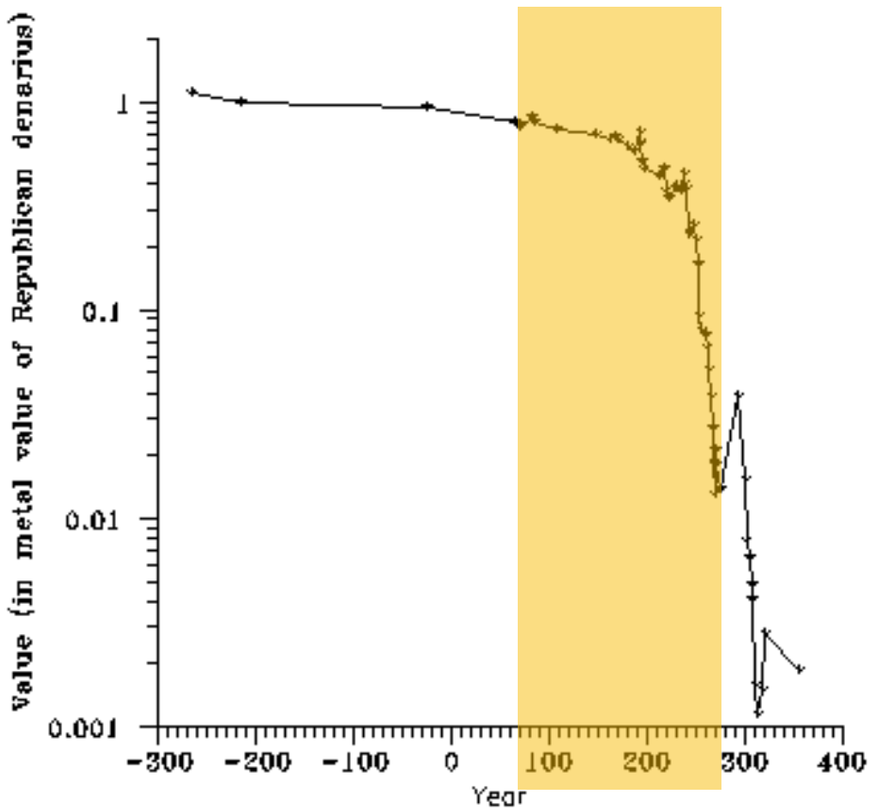
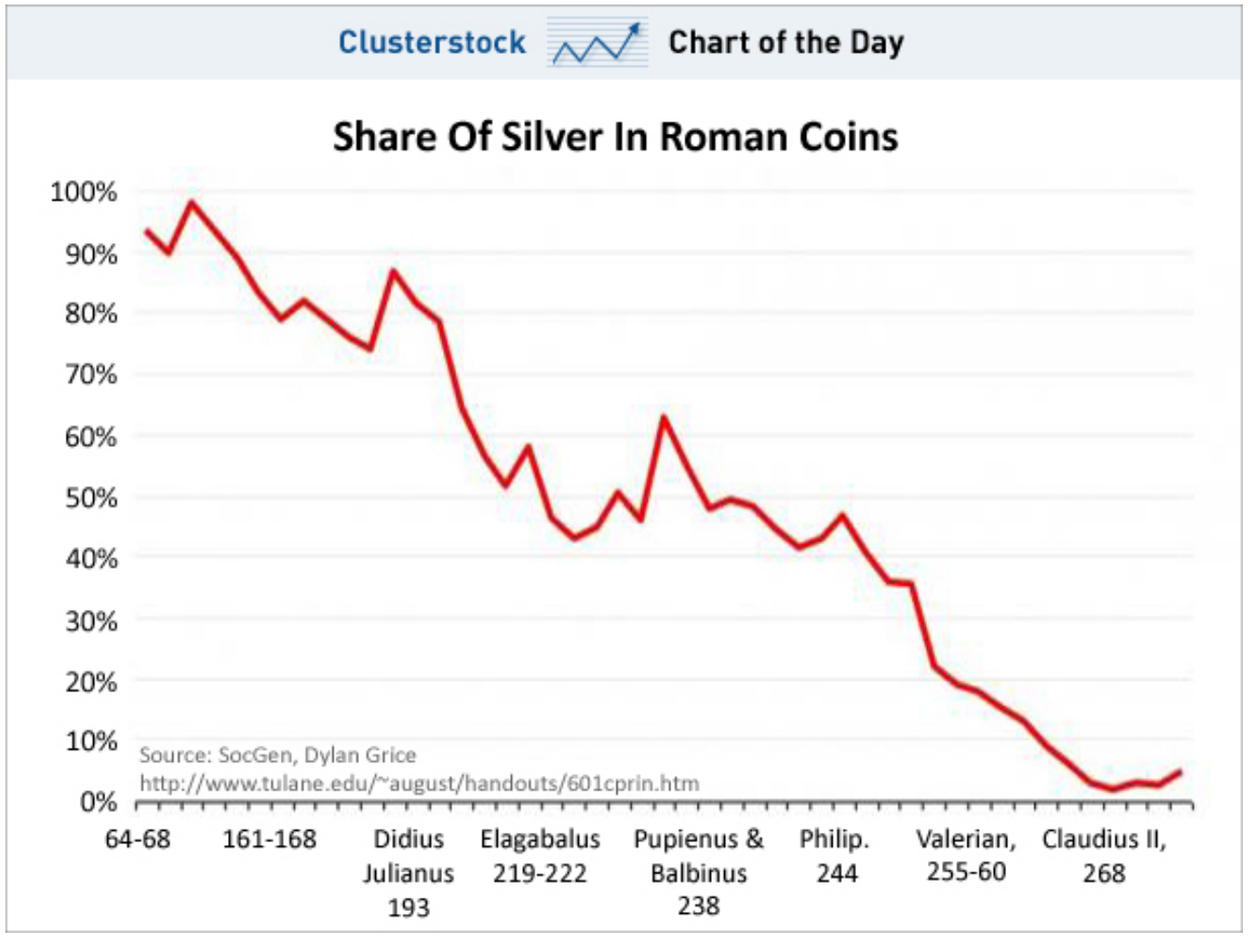
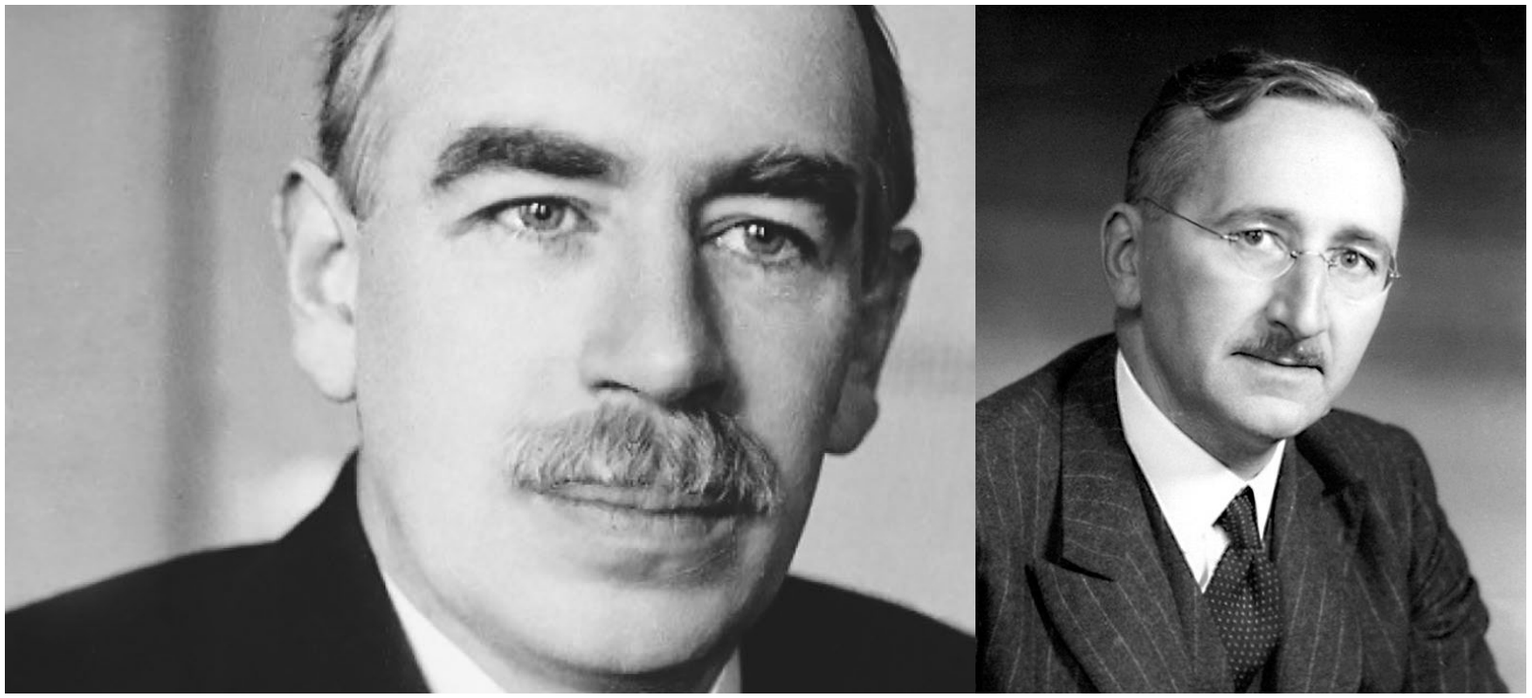


Fig. 4: The natural (silver) value of denarius. Ag/Cu=61. Scale: New Republic denarius is 1.



Il Contesto: La Battaglia tra Keynes e Hayek

KEYNES



HAYEK

- Il Potere Politico non è neutrale rispetto alla decisione se stampare moneta

- Stampare moneta permetta la soddisfazione e risoluzione di problemi di adesso al costo di possibili problemi futuri (Ma sono se credi alla scuola austriaca!)

Storia della moneta

- Baratto
- Uso di un mezzo di scambio
- Metalli
- Oro, Argento
- La Nascita dell’Inflazione
- The Golden Standard-Fiat Currencies
- Brettonwood Agreement
- Francia Germania richiedono il loro oro - Nixon fa default sulla loro protemessa
- Bitcoin

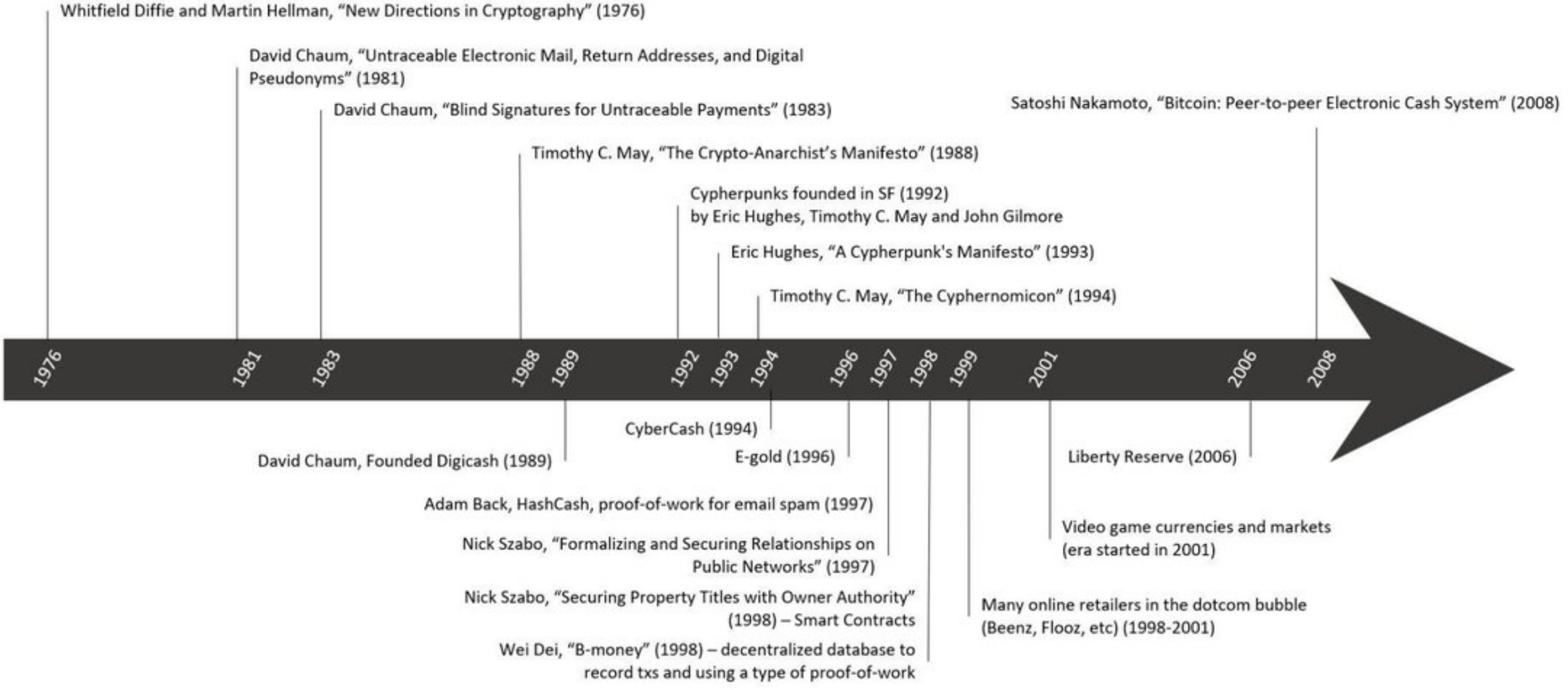
Il Contesto: La Battaglia tra Keynes e Hayek

HAYEK

I don't believe we shall ever have a good money again before we take the thing out of the hands of government, that is,
we can't take it violently out of the hands of government, all we can do is by *some sly roundabout way introduce something that they can't stop*

Hayek 1984

La Ricerca della Moneta Elettronica



I've been working on a new electronic cash system that's fully peer-to-peer, with no trusted third party.

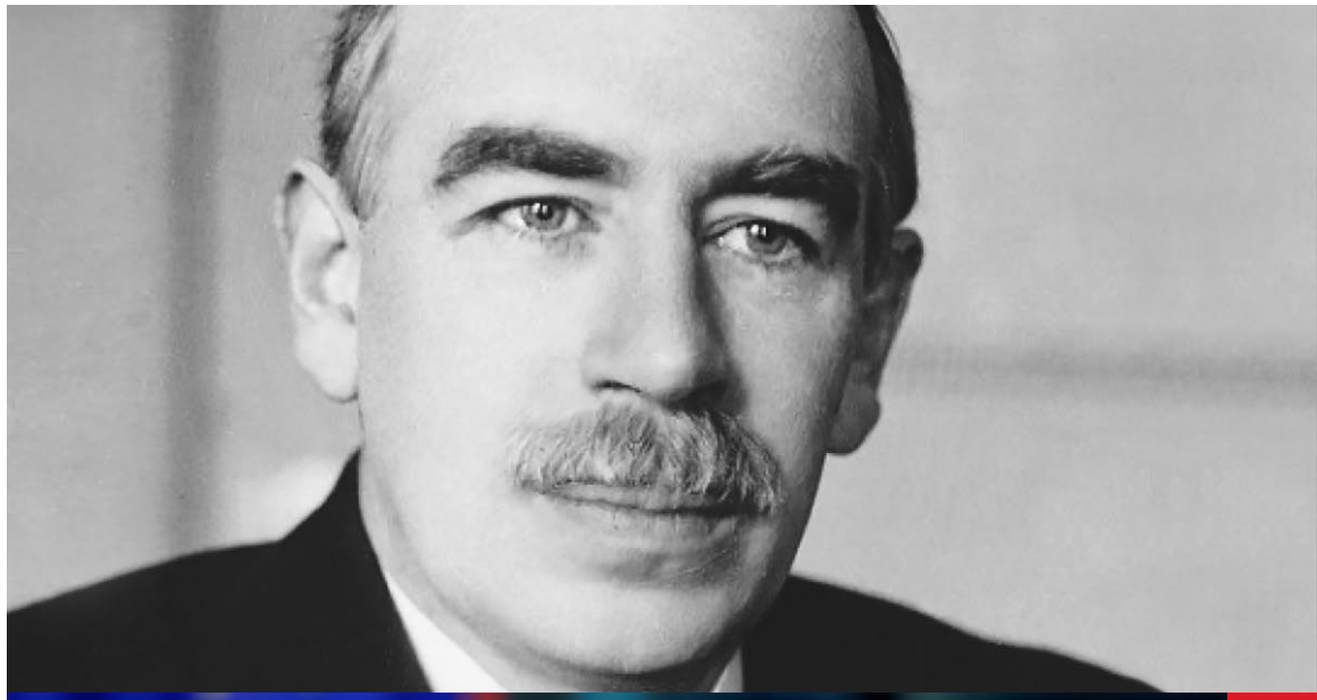
The paper is available at:
http://www.bitcoin.org/bitcoin.pdf

The main properties:

- Double-spending is prevented with a peer-to-peer network.
- No mint or other trusted parties.
- Participants can be anonymous.
- New coins are made from Hashcash style proof-of-work.
- The proof-of-work for new coin generation also powers the network to prevent double-spending.

Politica Monetaria

KEYNES



HAYEK

DRAGHI

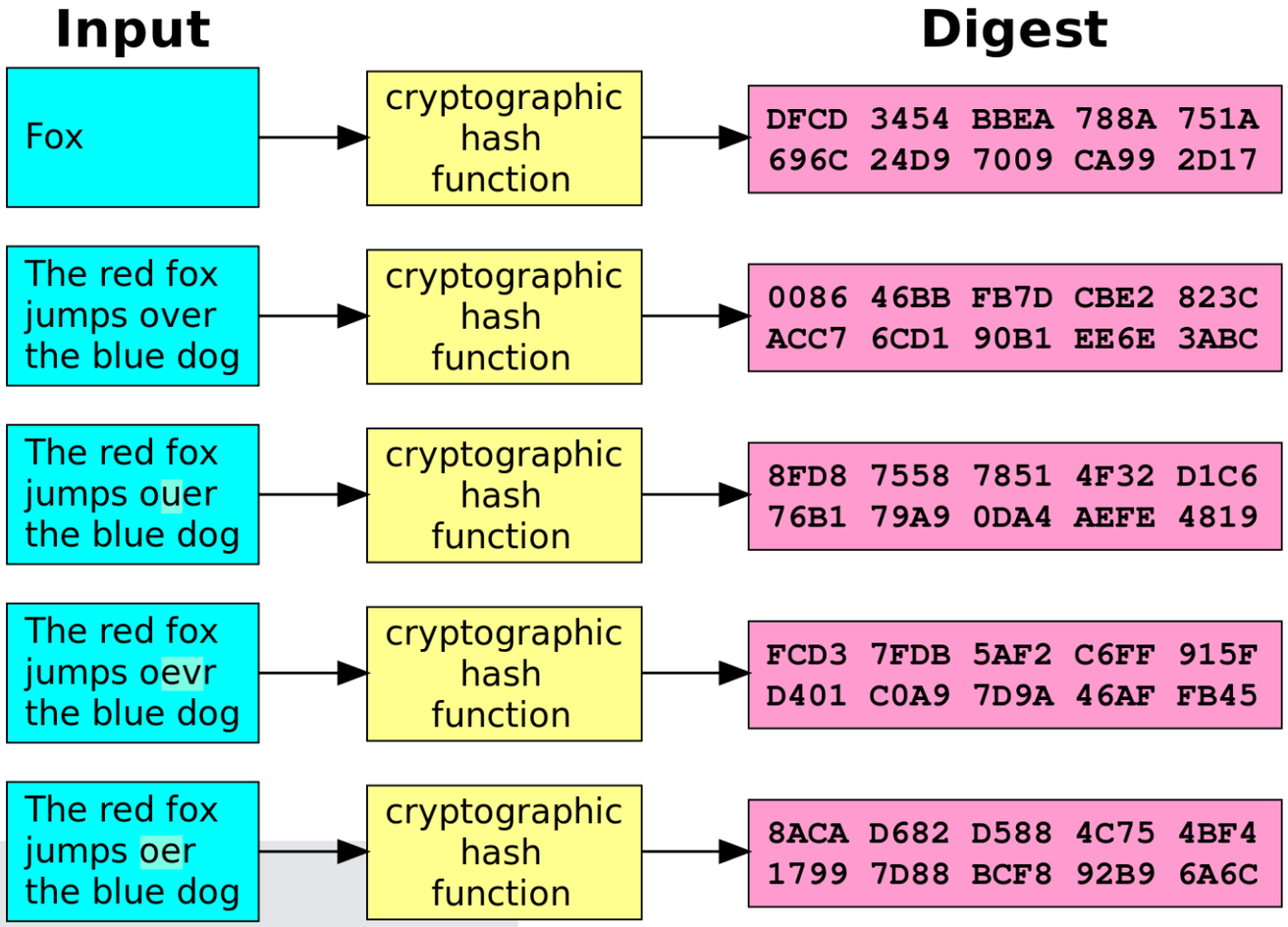
“NAKAMOTO”

La Ricerca della Moneta Elettronica

- Digicash — Bankrupt
- E Gold — Arrested
- Liberty Reserve — Arrested
- Napster — Programma = punto debole
- Gnutella / Kazaa — Azienda = punto debole
- Bittorrent — Protocollo Decentralizzato

Solo un sistema decentralizzato può funzionare

Hash Function



È una funzione deterministica.
Lo stesso input porta allo stesso output

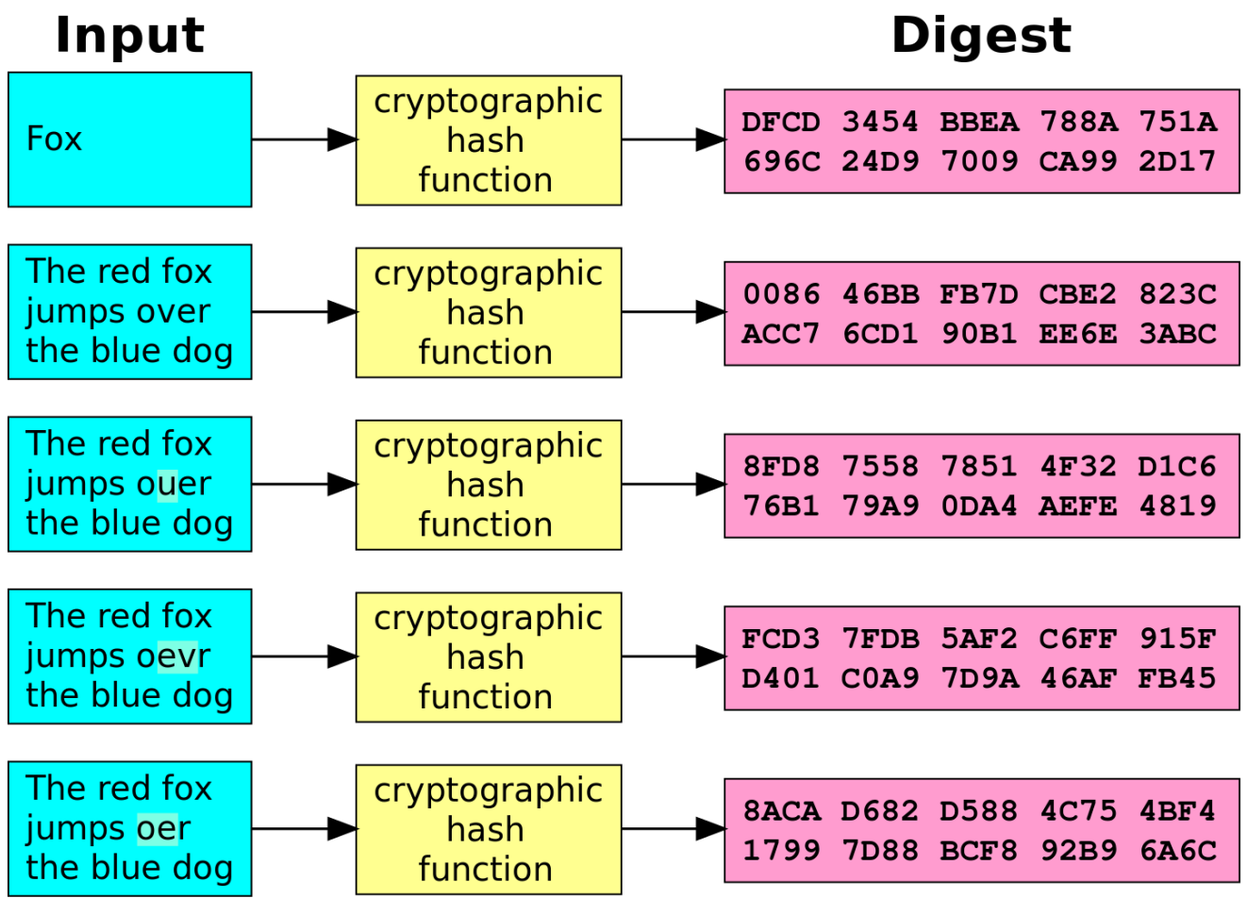
È veloce calcolare dall'input, l'output

Non è possibile calcolare l'input a partire dall'output
a meno di provare tutti i possibili input

Una piccola differenza nell'Input
porta a una differenza nell'output così grande
da sembrare non correlata

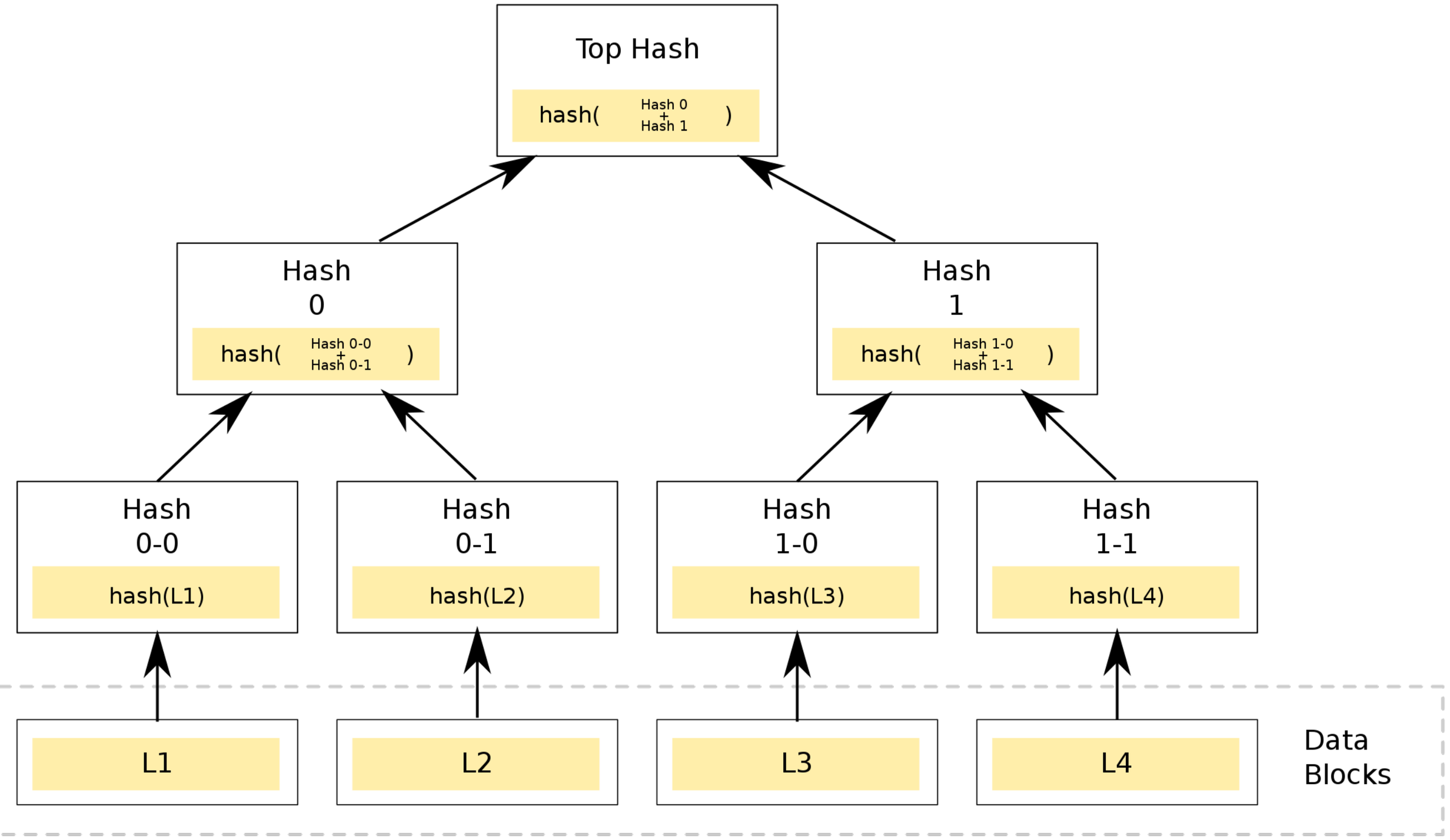
Non è possibile trovare due input che abbiano il medesimo output

Hash Function

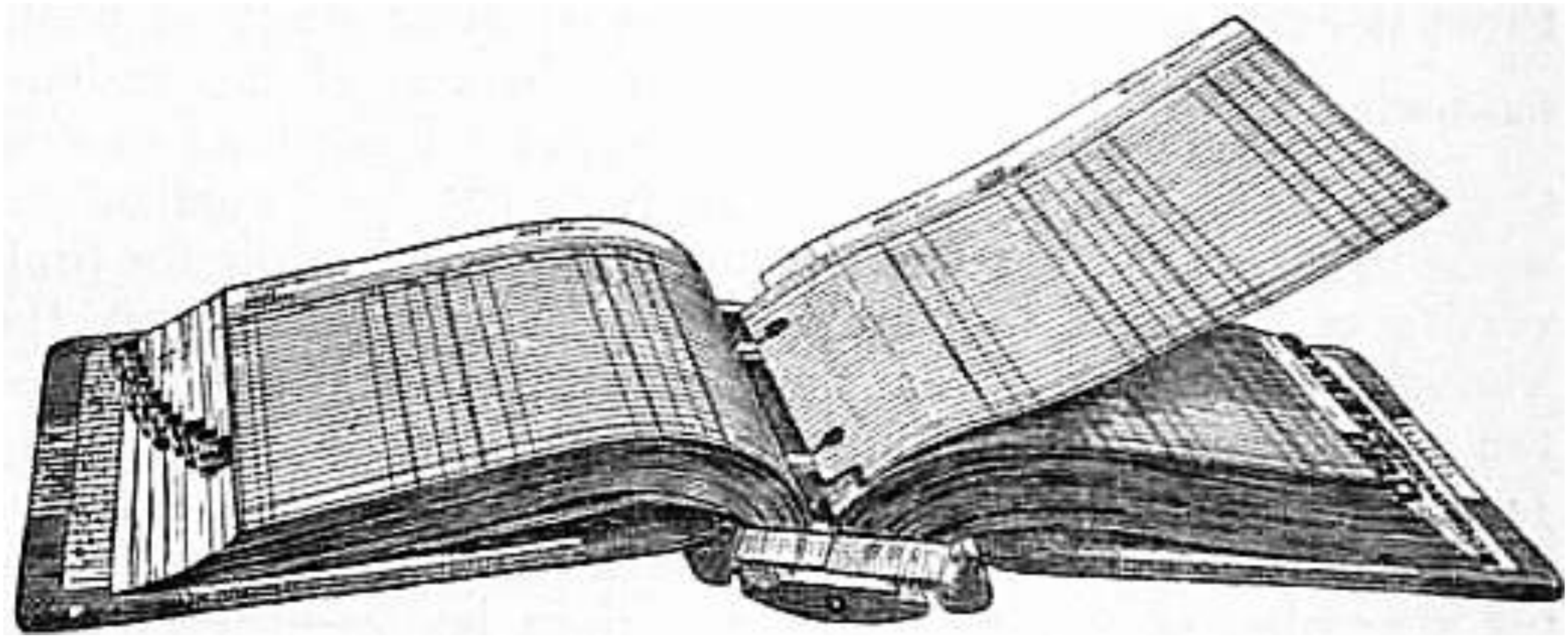


- **È possibile avere un problema a difficoltà variabile, in cui è però facile controllare se la soluzione è corretta**
  - Esempio:
    trova un input il cui hash ha come primi **3** caratteri degli 0
    trova un input il cui hash ha come primi **4** caratteri degli 0
    trova un input il cui hash ha come primi **5** caratteri degli 0

Merkle Tree

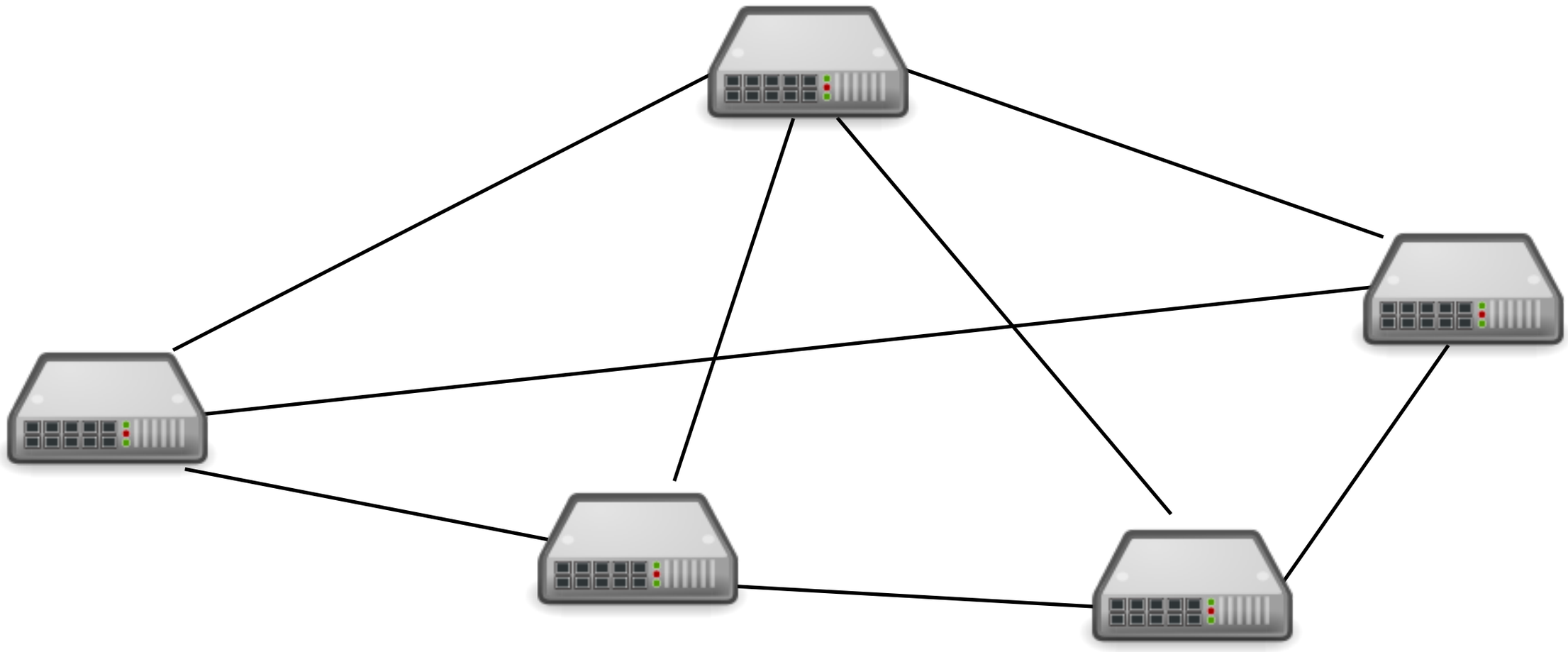

Top Hash
hash(Hash 0 + Hash 1)
Hash 0
hash(Hash 0-0 + Hash 0-1)
Hash 1
hash(Hash 1-0 + Hash 1-1)
Hash 0-0
hash(L1)
Hash 0-1
hash(L2)
Hash 1-0
hash(L3)
Hash 1-1
hash(L4)
L1
L2
L3
L4
Data Blocks

Public Ledger
(Libro Mastro)



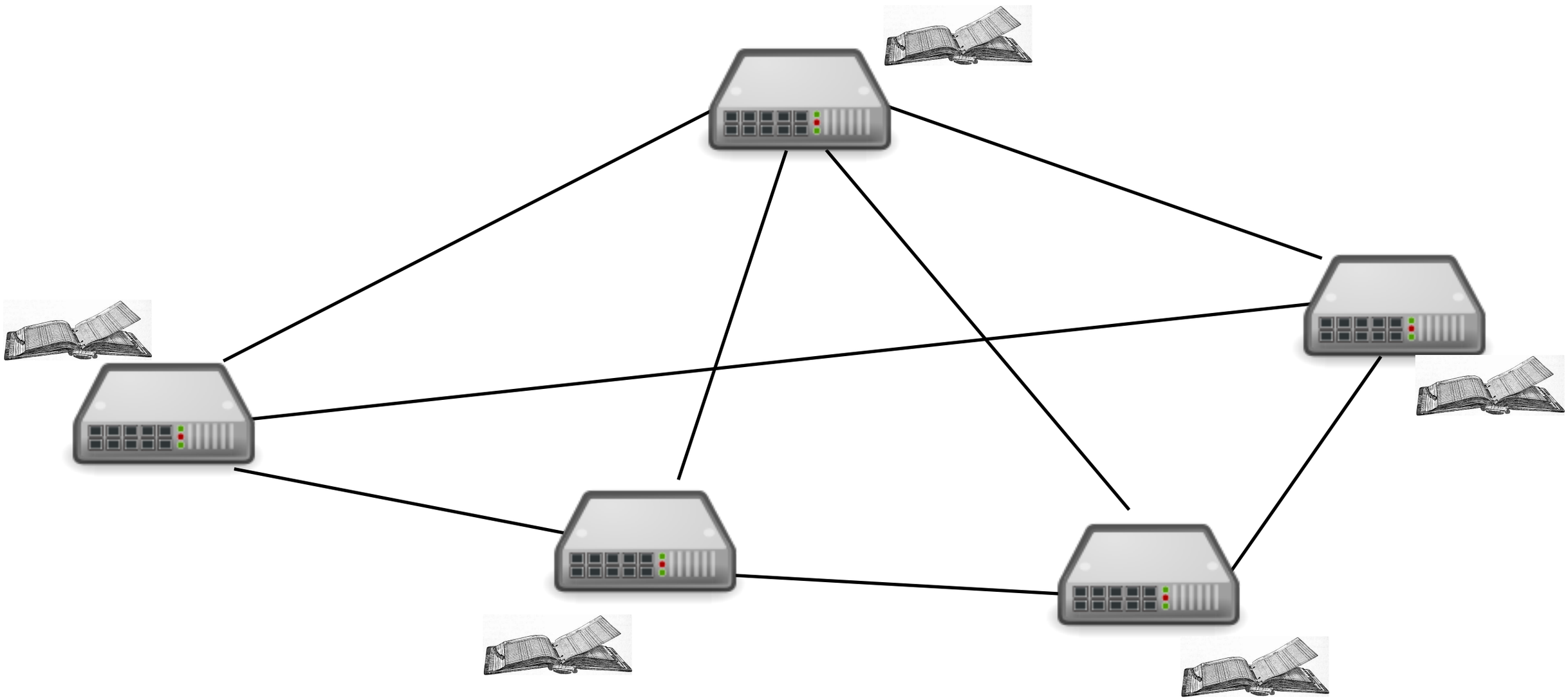
Ipotesi

- **Supponiamo di avere una rete di computer, ciascuno con una copia del public ledger**



Ipotesi

- **Supponiamo di avere una rete di computer, ciascuno con una copia del public ledger**

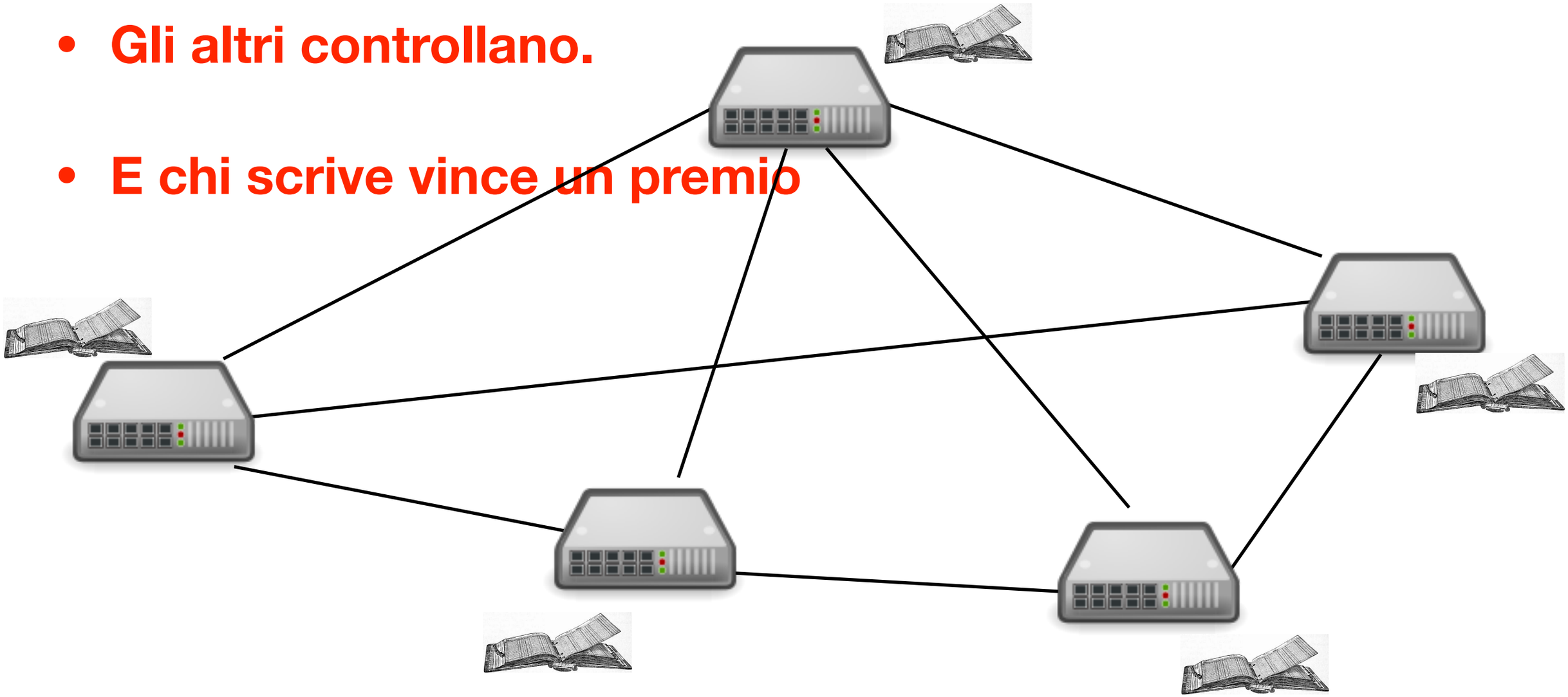


Ipotesi

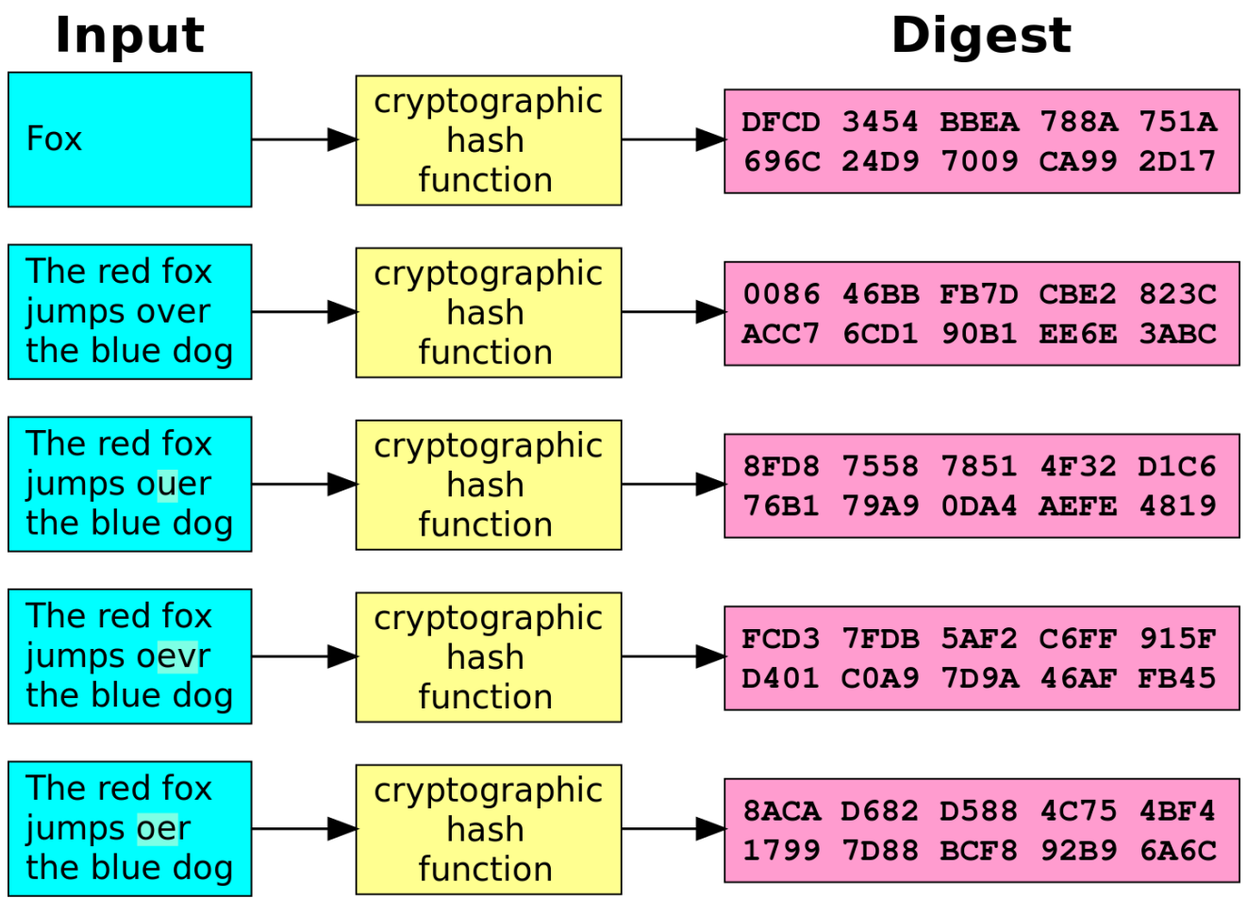
- **Supponiamo di avere una rete di computer, ciascuno con una copia del public ledger**

Come si scrive una nuova pagina?

- **Scrivere una pagina è difficile.**
- **Il primo server che ci riesce la scrive.**
- **Gli altri controllano.**
- **E chi scrive vince un premio**



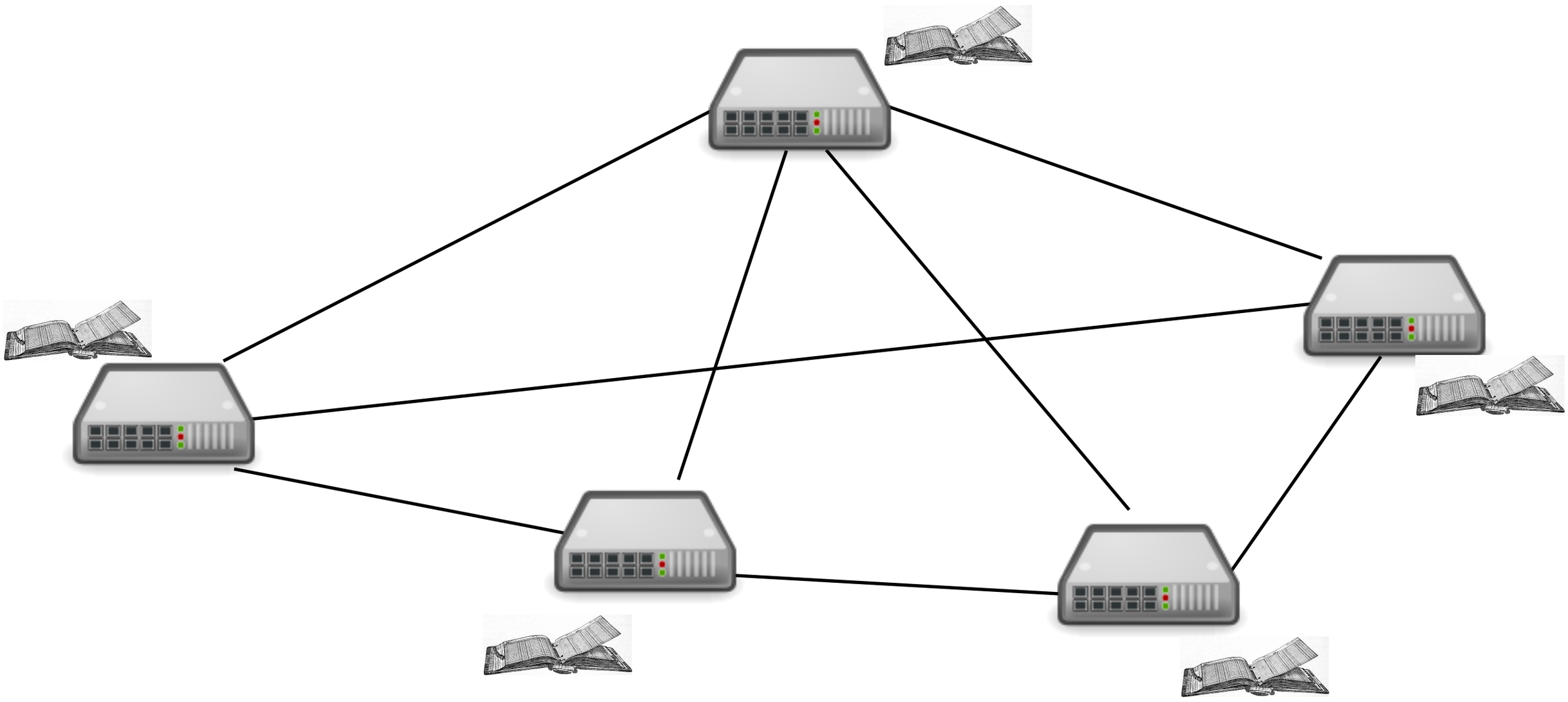
Hash Function



- **È possibile avere un problema a difficoltà variabile, in cui è però facile controllare se la soluzione è corretta**
  - Esempio:
    trova un input il cui hash ha come primi **3** caratteri degli 0
    trova un input il cui hash ha come primi **4** caratteri degli 0
    trova un input il cui hash ha come primi **5** caratteri degli 0

Quanto difficile?

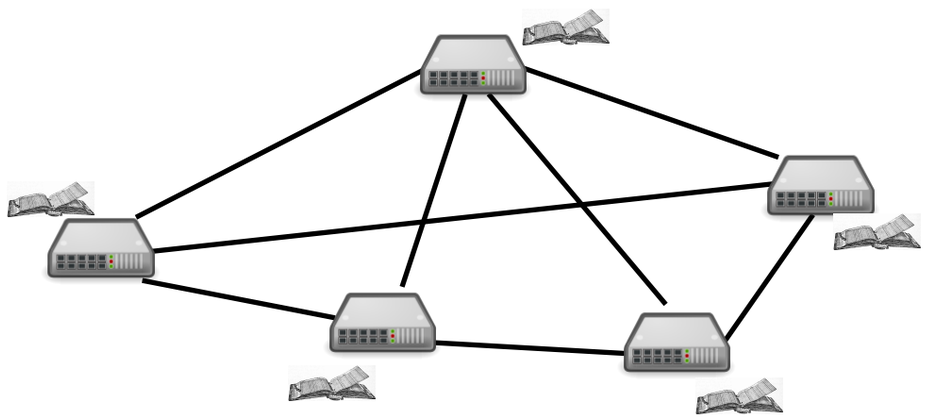
- **Così difficile che tutti i computer nel mondo che cercano di scriverlo, riescono a ottenere il risultato in media una volta ogni 10 minuti**



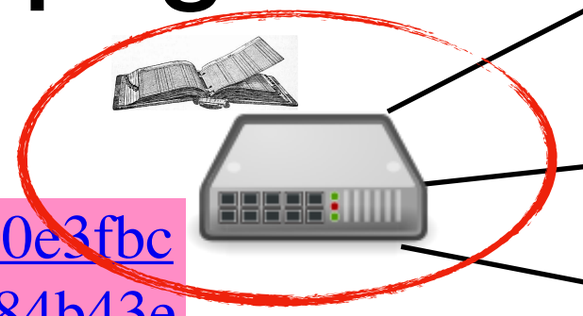
Ipotesi

- **Supponiamo di avere una serie di nuove transazioni da scrivere sul public ledger**

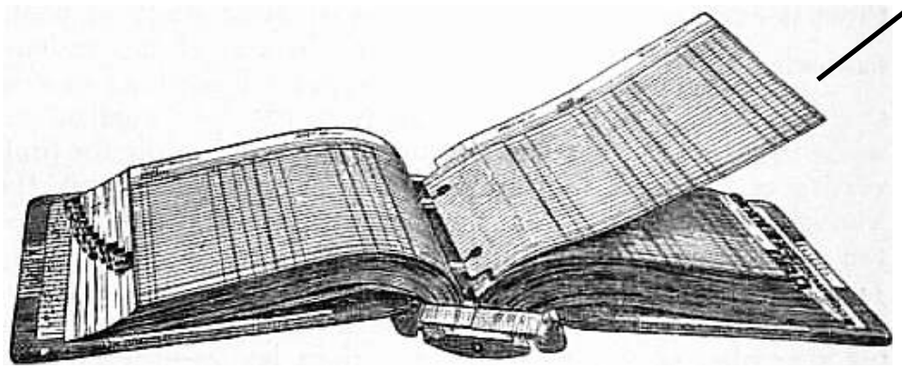
Da	A	Quanti
Giovanni	Antonio	5 BTC
Carlo	Luigi	2 BTC
Marco	Giuseppe	3.5 BTC
Ada	Maria	7 BTC
Giovanni	Claudio	4 BTC
Mirco	Mattia	3 BTC
Antonia	Andrea	0.1 BTC
Mino	Vittoria	3 BTC



Ciascun server crea una possibile pagina



Hash della pagina precedente



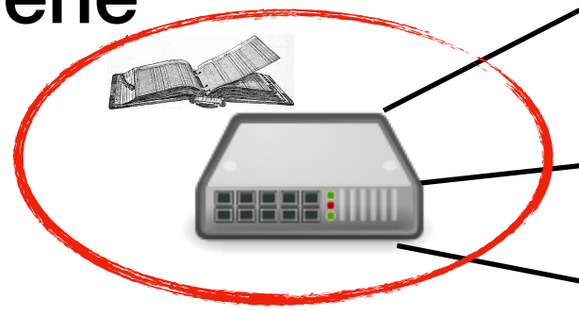
000000000000000000036ae01700e3fbc9e75c69d50d99664341f512d1b84b43e

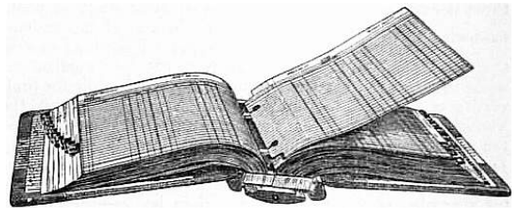
Da	A	Quanti
Giovanni	Antonio	5 BTC
Carlo	Luigi	2 BTC
Marco	Giuseppe	3.5 BTC
Ada	Maria	7 BTC
~~Giovanni~~	~~Claudio~~	~~4 BTC~~
Mirco	Mattia	3 BTC
Antonia	Andrea	0.1 BTC
Mino	Vittoria	3 BTC

Da un controllo risulta che Giovanni non ha 9 BTC

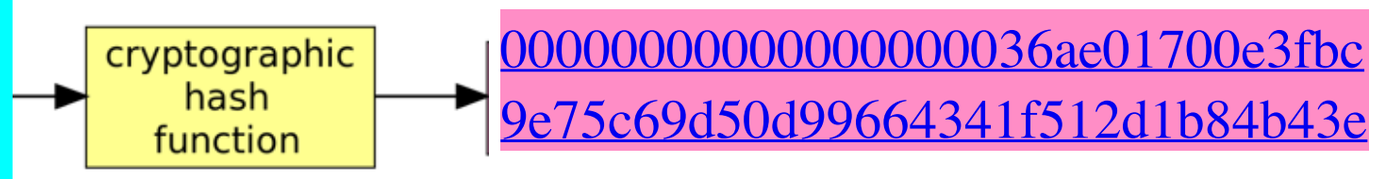
Nonce 2237985216

Si cambia il Nonce
finché non si trova una soluzione che va bene





Esempio

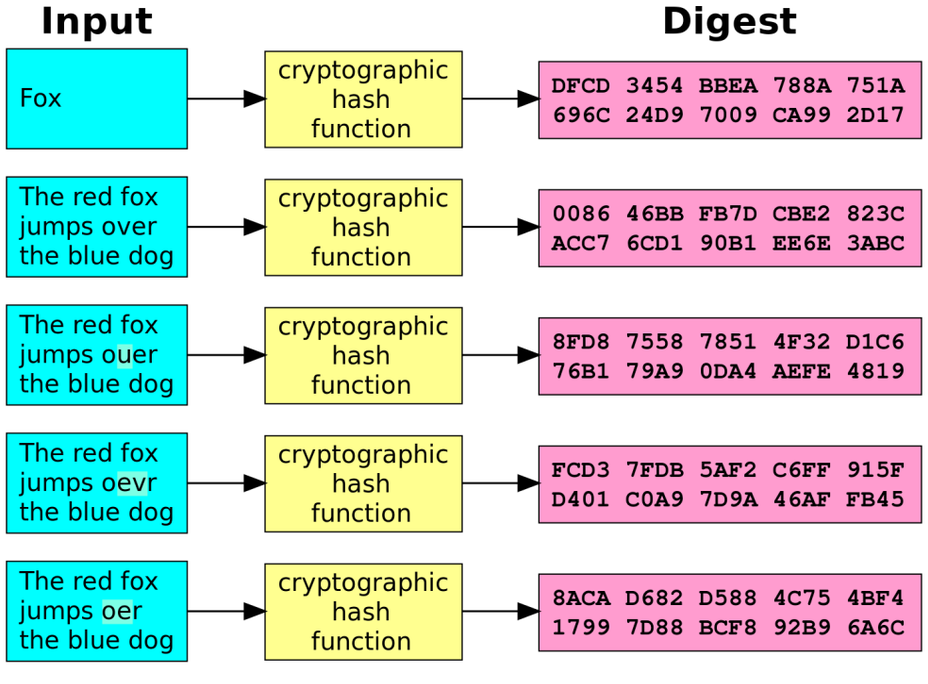


00000000000000000036ae01700e3fbc
9e75c69d50d99664341f512d1b84b43e

Da	A	Quanti
Giovanni	Antonio	5 BTC
Carlo	Luigi	2 BTC
Marco	Giuseppe	3.5 BTC
Ada	Maria	7 BTC
~~Giovanni~~	~~Claudio~~	~~4 BTC~~
Mirco	Mattia	3 BTC
Antonia	Andrea	0.1 BTC
Mino	Vittoria	3 BTC

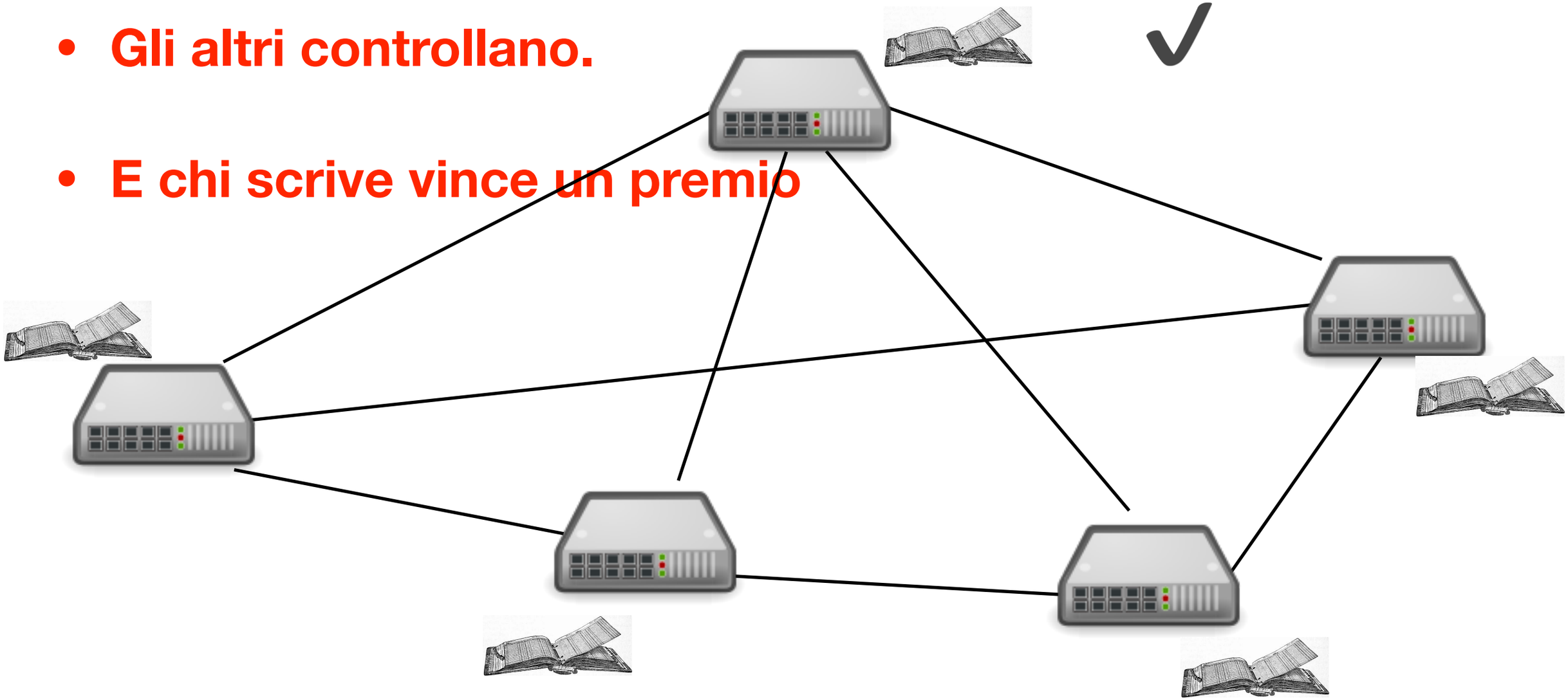
Nonce

2237985216



Come si scrive una nuova pagina?

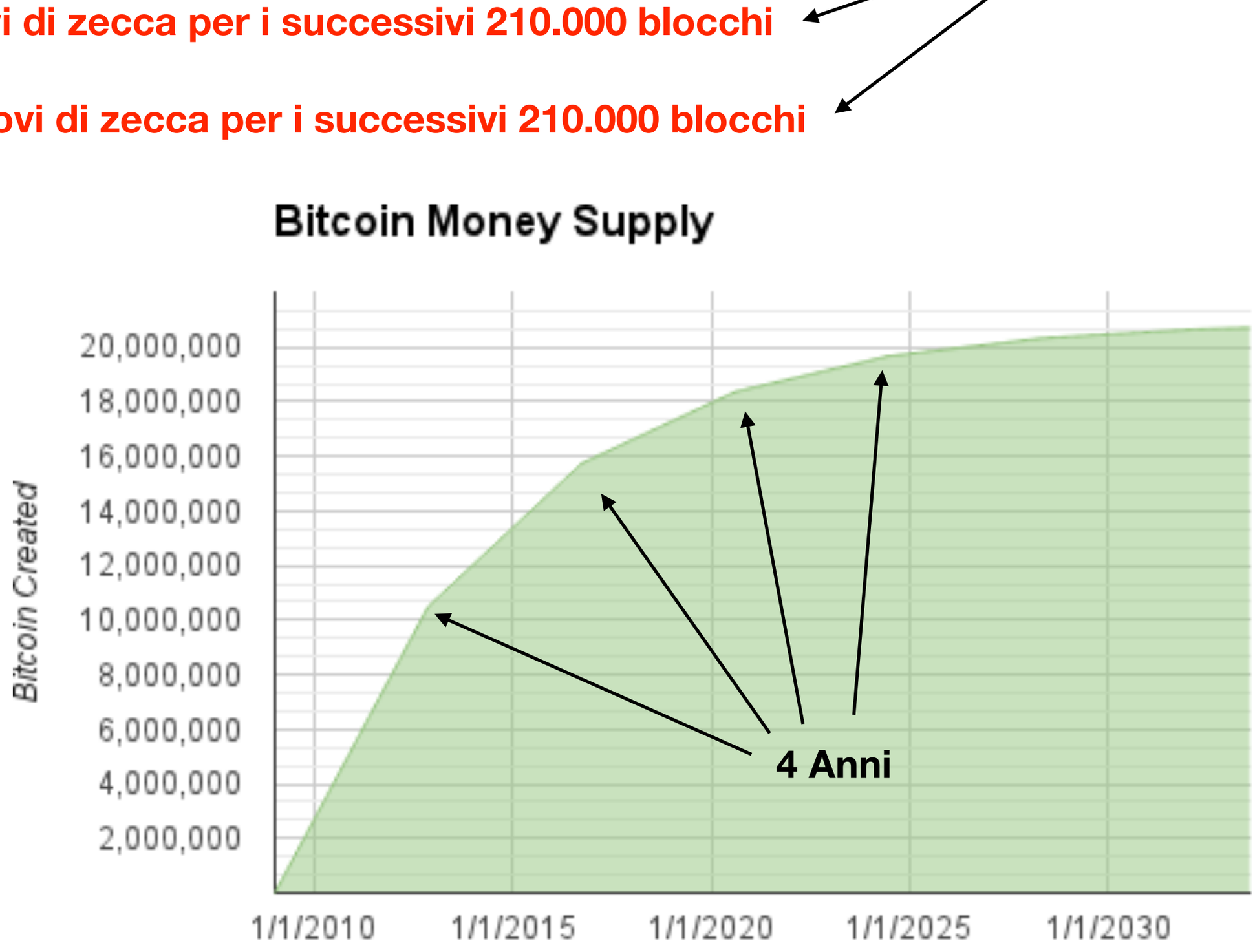
- **Scrivere una pagina è difficile.** ✓
- **Il primo server che ci riesce la scrive.** ✓
- **Gli altri controllano.** ✓
- **E chi scrive vince un premio**



Che premio si vince?

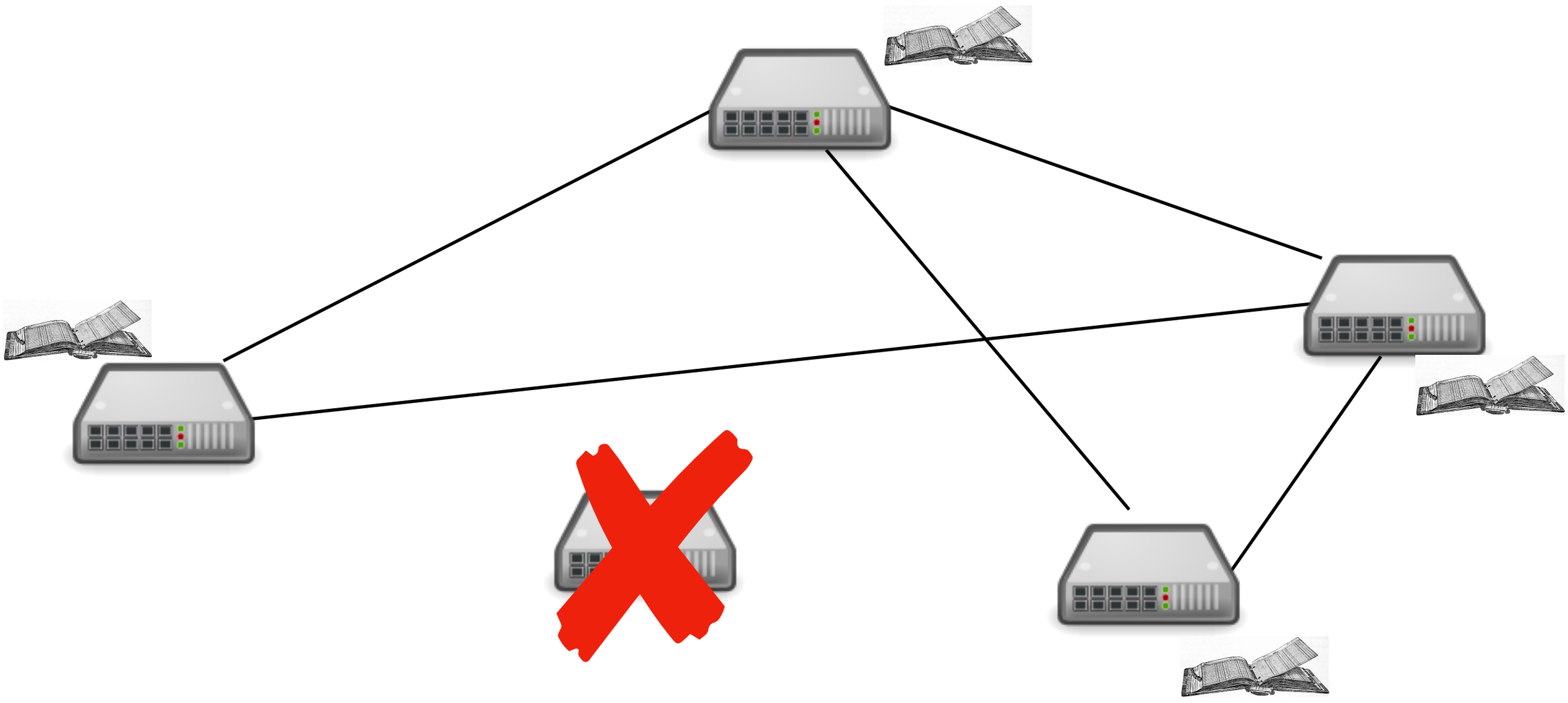
- 50 bitcoin nuovi di zecca per i primi 210.000 blocchi
- 25 bitcoin nuovi di zecca per i successivi 210.000 blocchi
- 12.5 bitcoin nuovi di zecca per i successivi 210.000 blocchi
- …

4 Anni



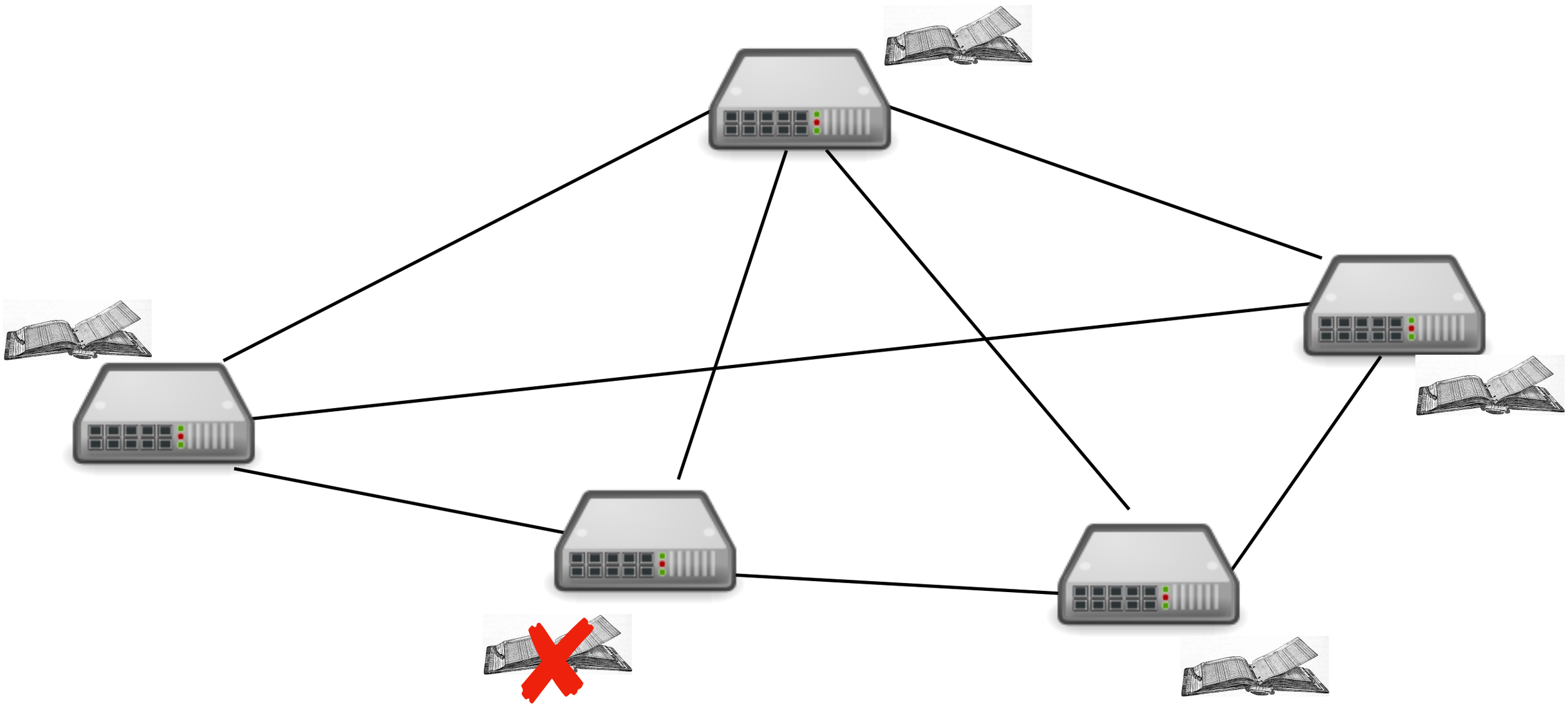
Che succede se si elimina un computer?

- **Nulla, la rete funziona con un computer in meno**



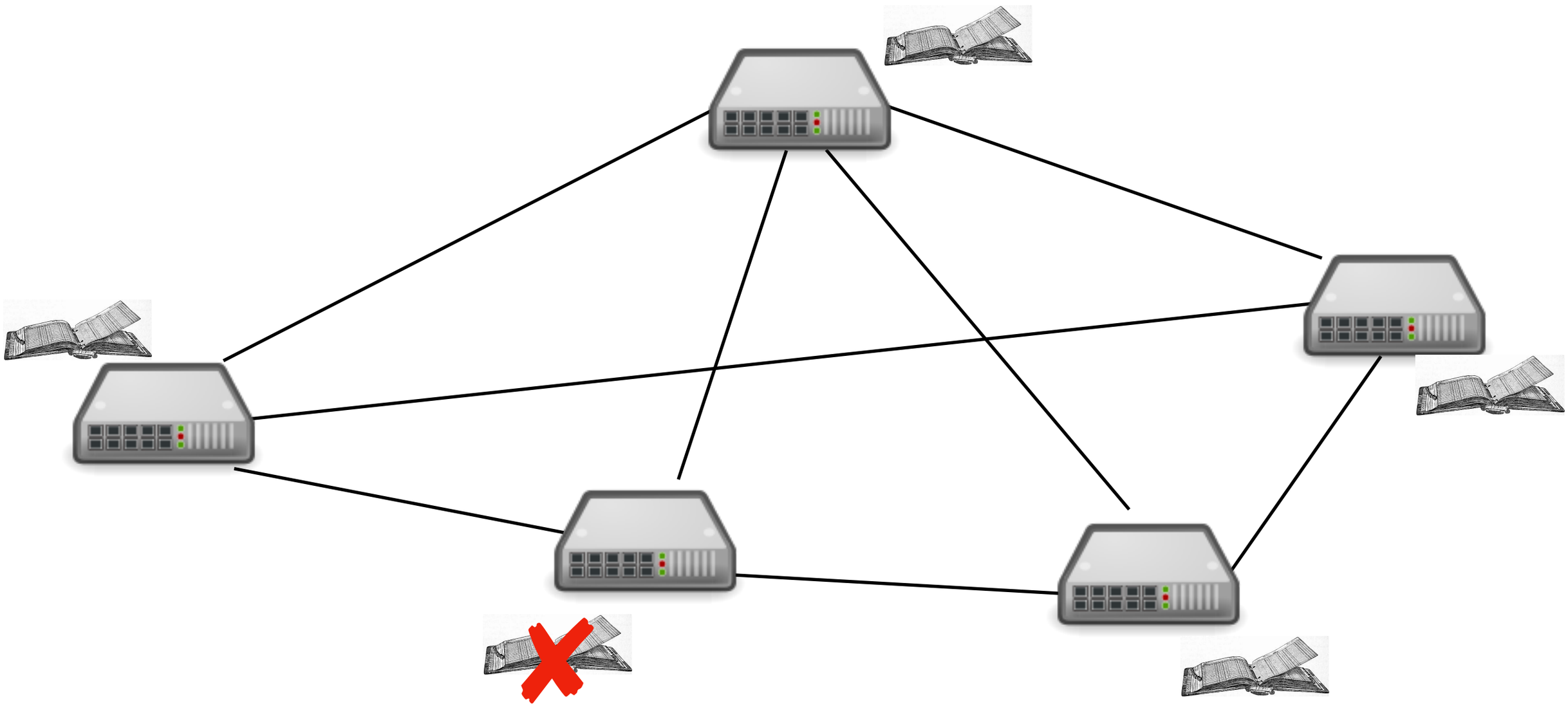
Che succede se qualcuno cambia il Libro Mastro?

- **Non può farlo perché dovrebbe ricalcolare tutte le pagine da quella che ha cambiato (perchè ogni pagina ha l'hash di quella precedente)**



Che succede se qualcuno accetta transazioni sbagliate?

- La sua pagina non viene accettata dal resto della rete



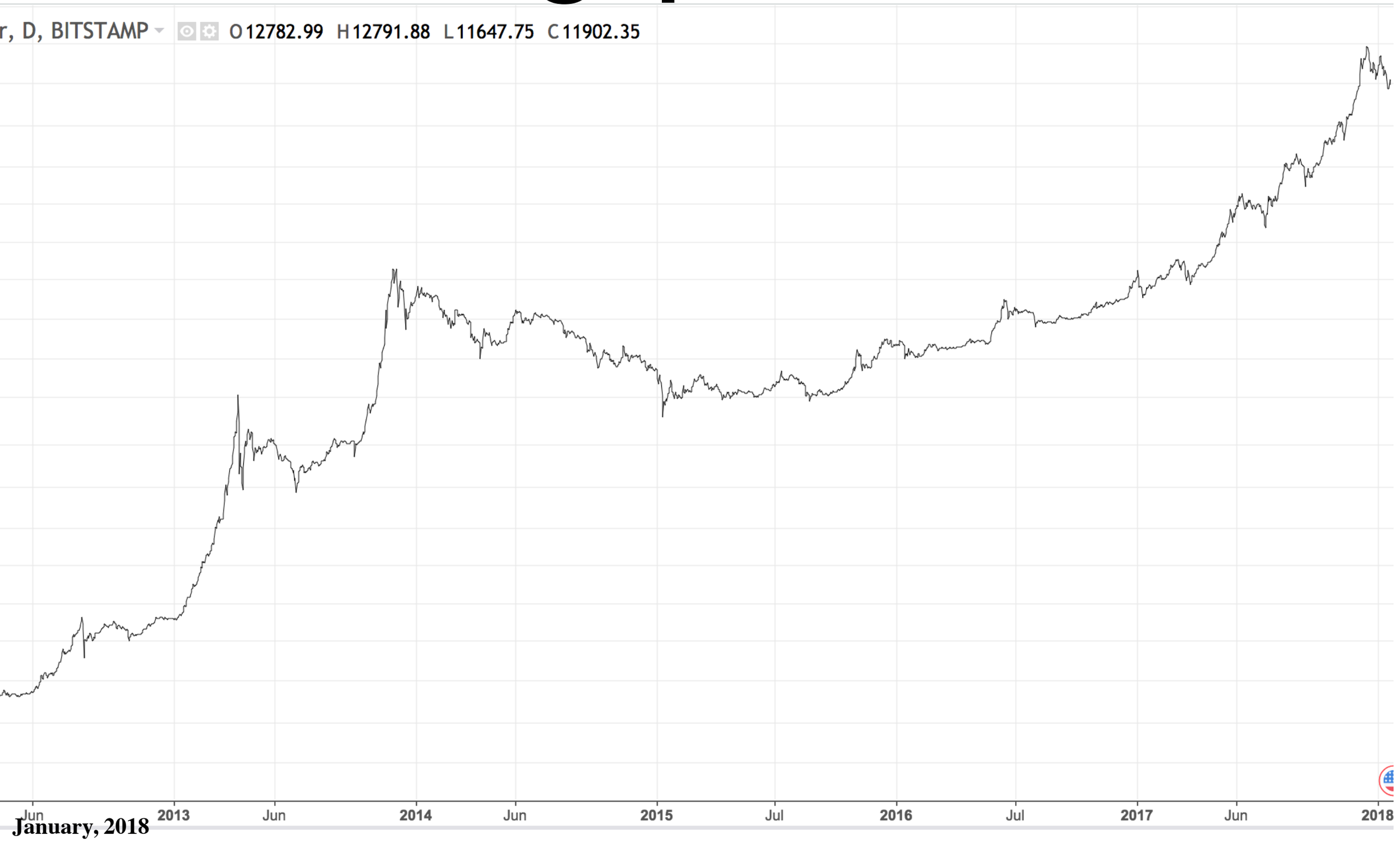
Esercizio

- Che succede se non si trova il blocco successivo?

Cosa abbiamo imparato

- I bitcoin sono una rete distribuita
- Non è possibile controllare questa rete
- Generano bitcoin in maniera controllata e arriveranno a un totale di 21 milioni
- Sono una moneta deflazionistica
- Se hai dei bitcoin nessuno te li può congelare ne levare

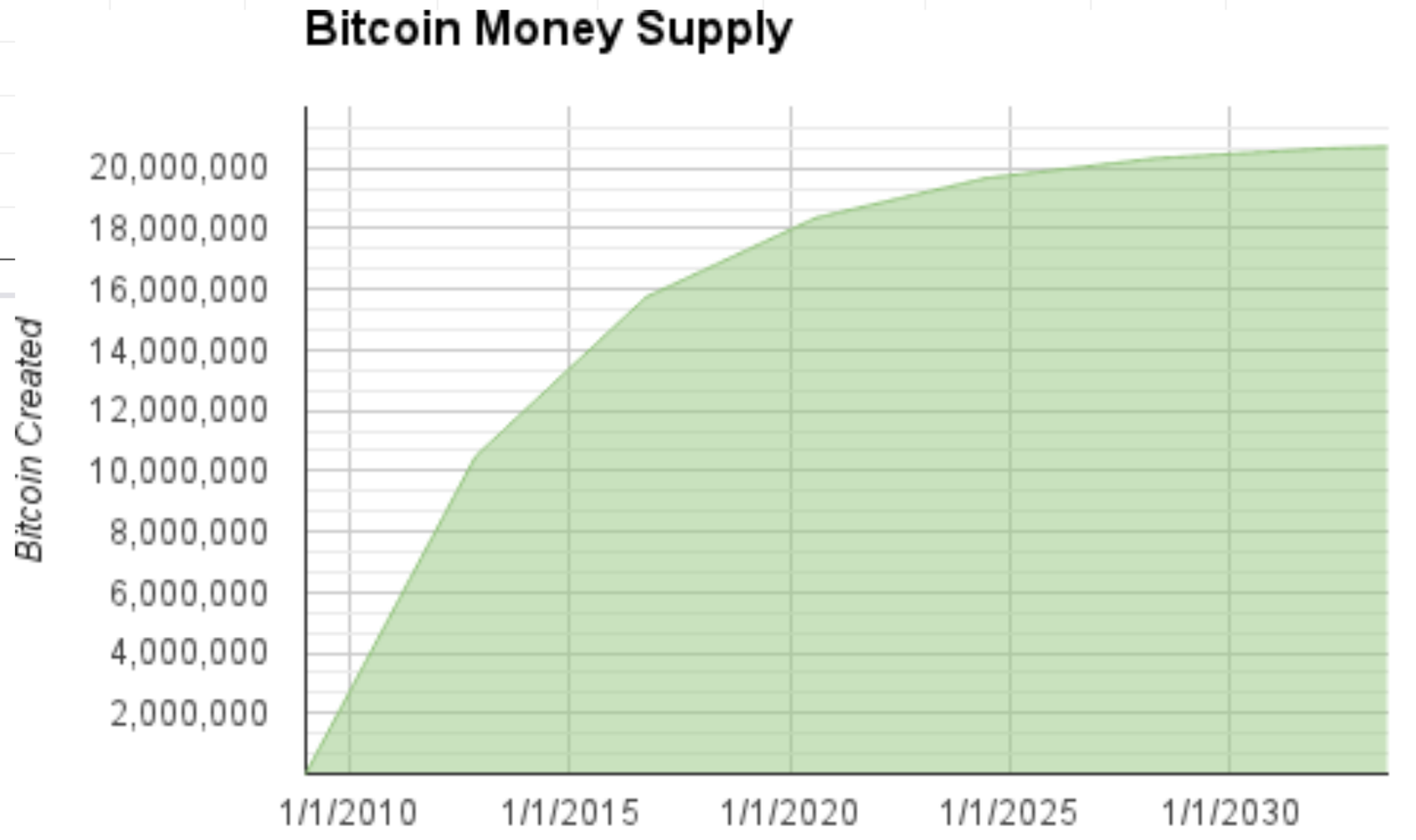
Necrologi per i Bitcoin



January, 2018

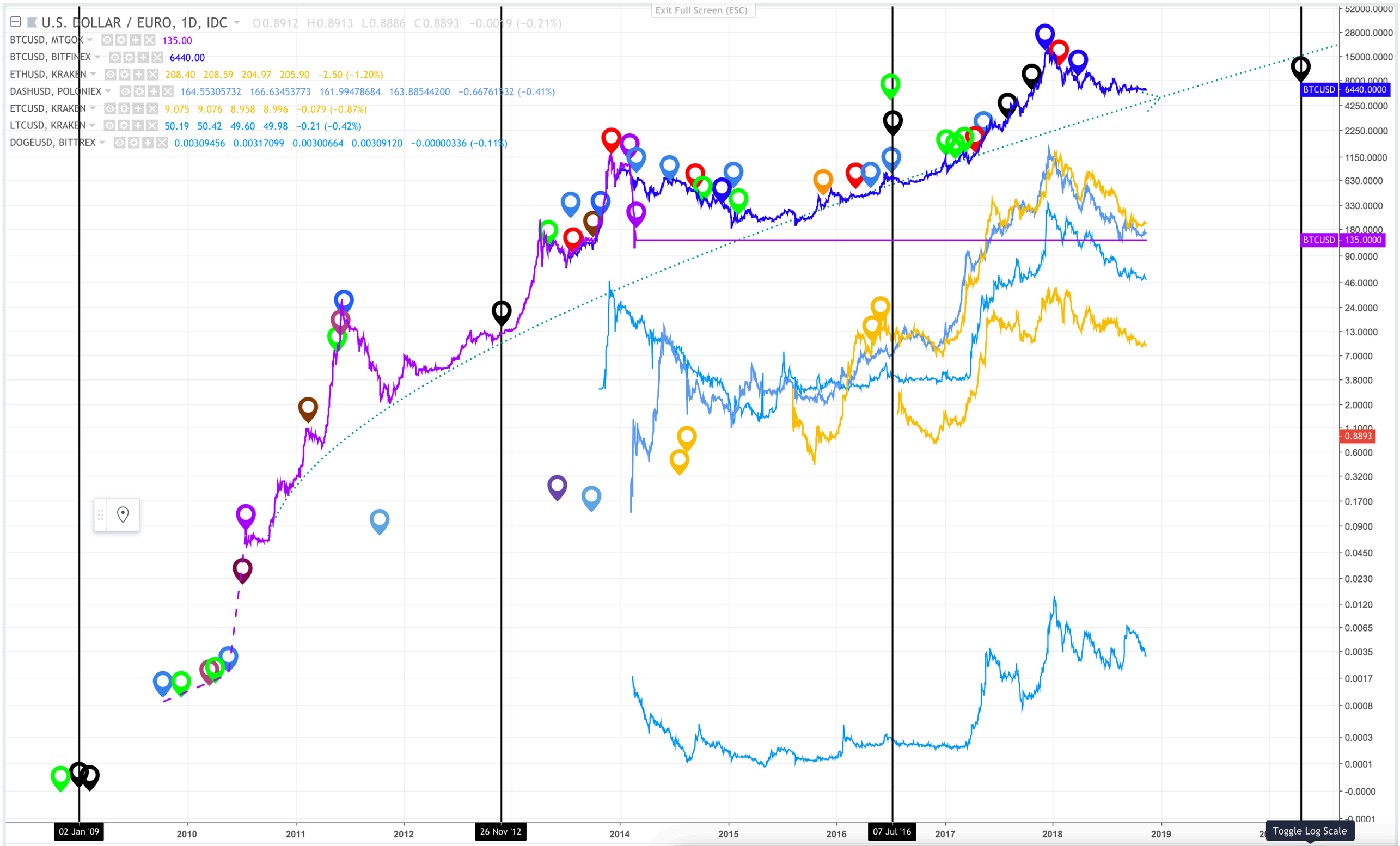
Jan 12 "Bitcoin's Demise Moves Closer" – The Motley Fool | $13,869.76

La crescita dei bitcoin



Storia dei bitcoin

- https://www.tradingview.com/chart/Af3iiYyR/

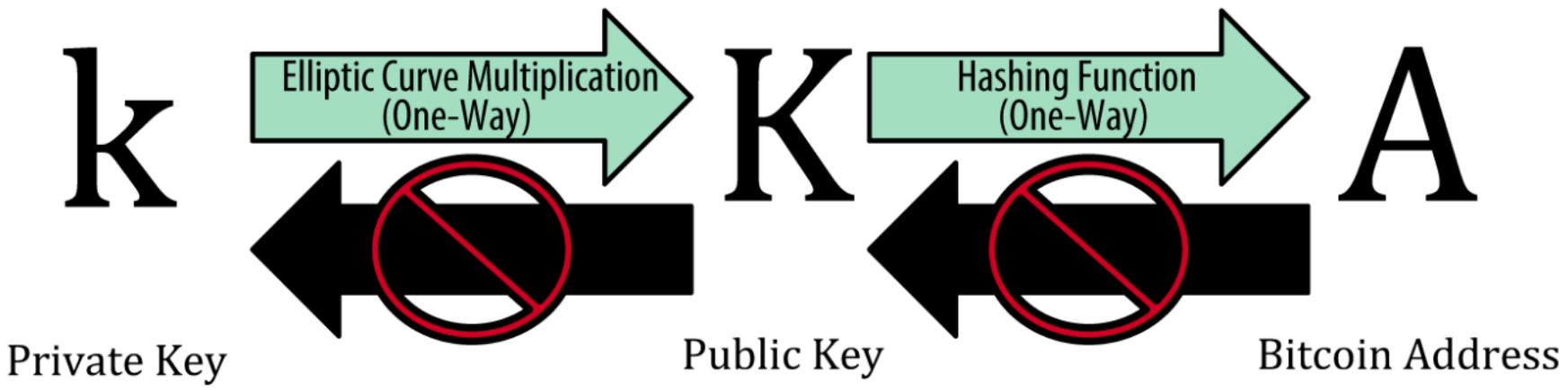


2a lezione

- L’importanza di Geordie di De Andrè
- Chiavi pubbliche, chiavi private, indirizzi
- Curve ellittiche e operazioni sulle curve ellittiche
- Base 58 e prefissi
- Transazioni come contratti
- Ethereum, Dao
- Code is Law

Chiavi Private e Chiavi Pubbliche

- Chiave Privata (un qualunque numero di 256 bit)
- Chiave Pubblica
- Indirizzo

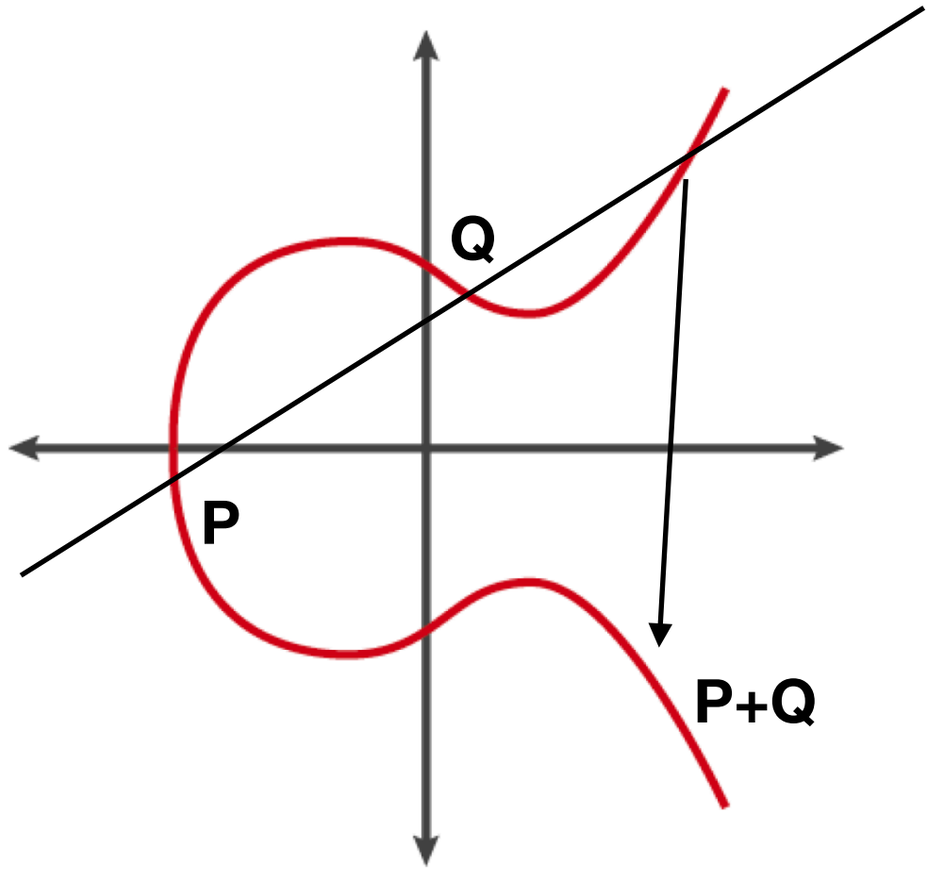


Chiavi Private e Chiavi Pubbliche

- $Y^2=X^3-7$ su Z_p

- Con p = 2^{256} - 2^{32}- 2^9- 2^8- 2^{32}- 2^7- 2^6- 2^4-1

- Dato p+q punti sulla curva, p+q è il terzo punto che incrocia una retta per p e q

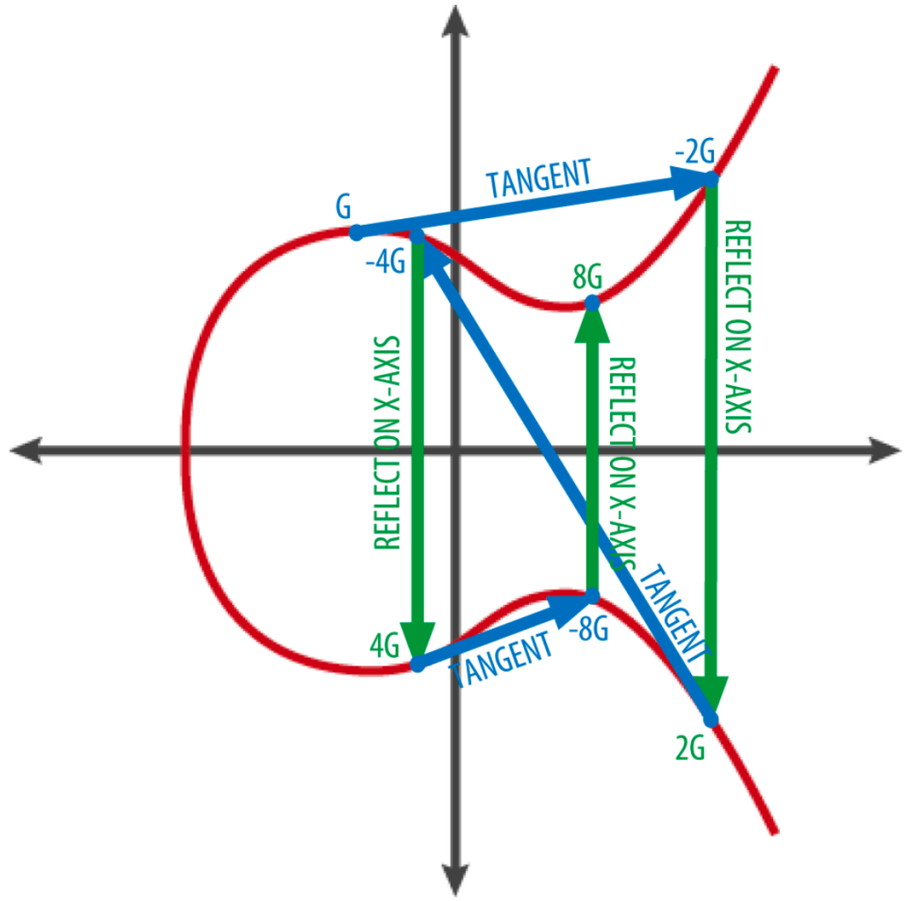


Chiavi Private e Chiavi Pubbliche

- Se p=q si prende la retta tangente e si prende il valore riflesso

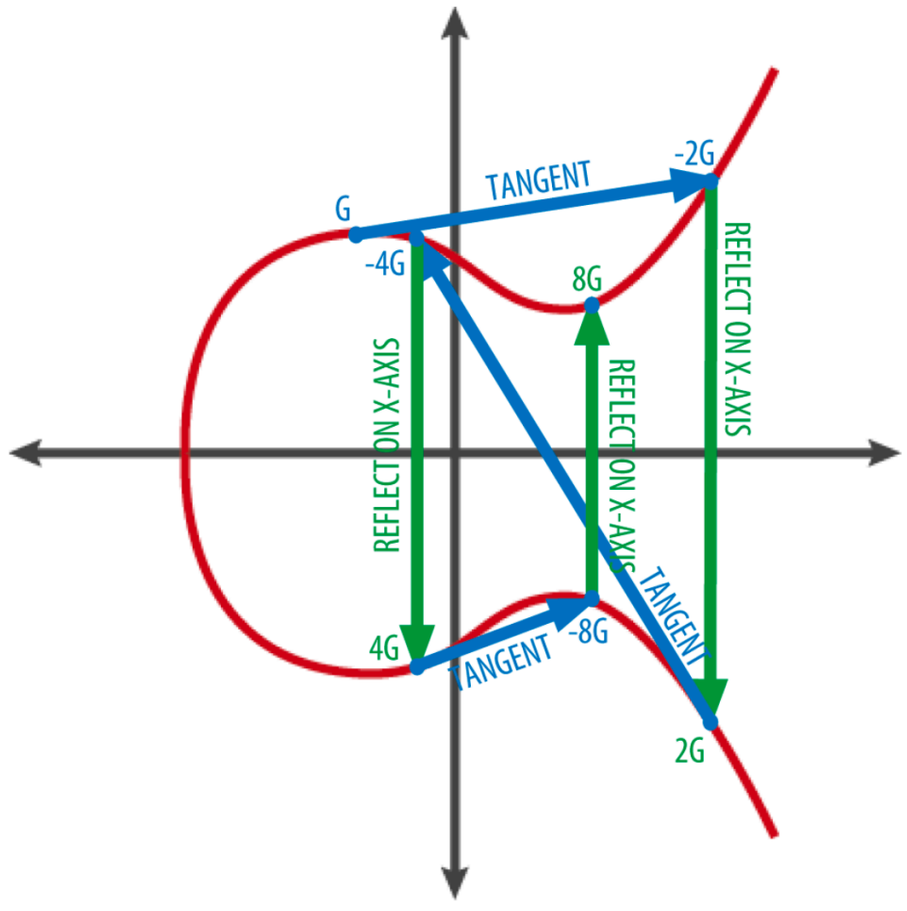
- ‘+’ è associativo, ha un elemento neutro (punto all’infinito), ha un inverso, commutativo

- x*p=p+p+p+… +p (x volte)



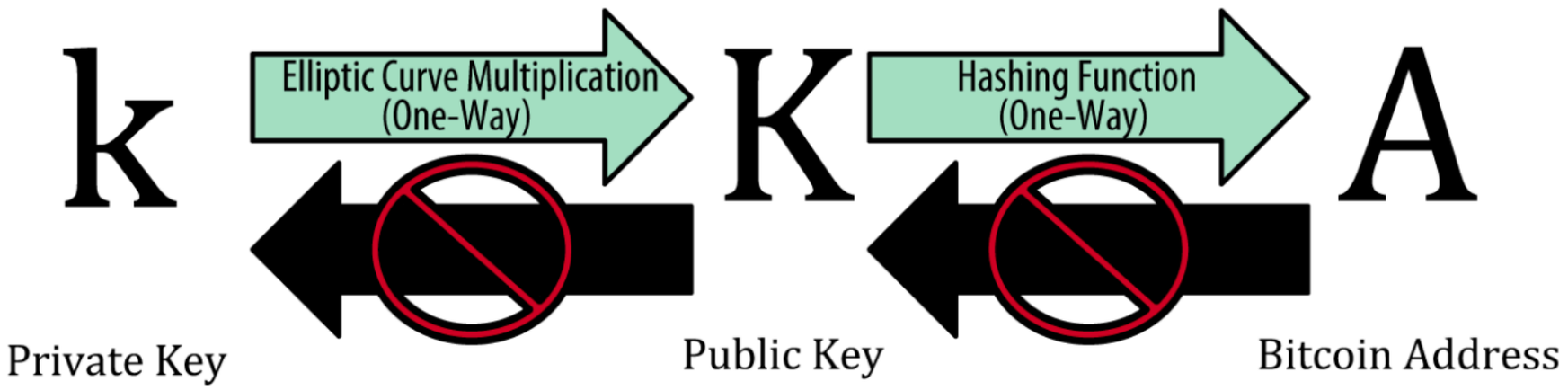
Chiavi Private e Chiavi Pubbliche

- Chiave Privata (un qualunque numero di 256 bit) = k
- G un punto fisso (dato dallo standard secp256k1)
- K, chiave pubblica è data da
- K=k*G

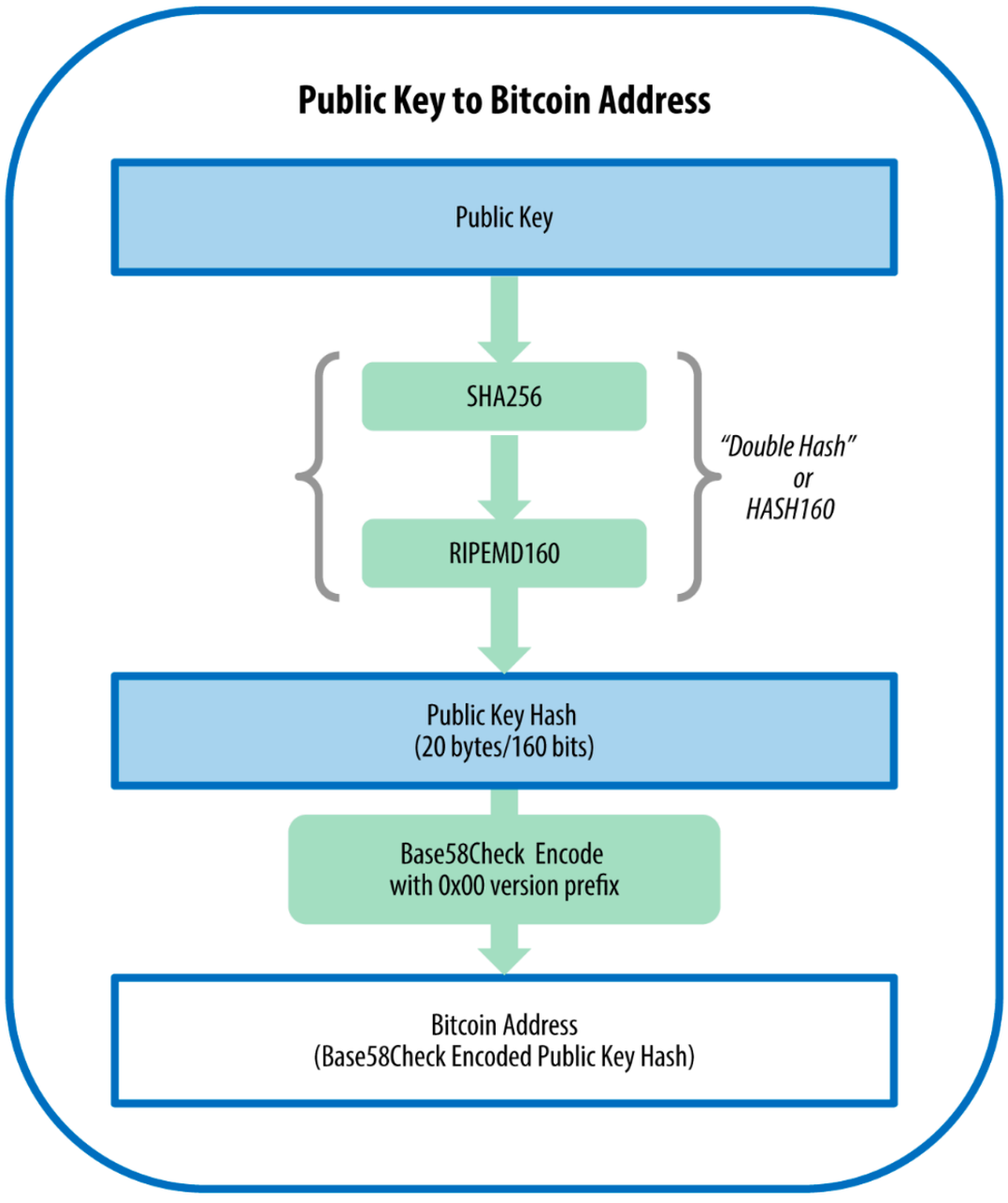


Chiavi Private e Chiavi Pubbliche

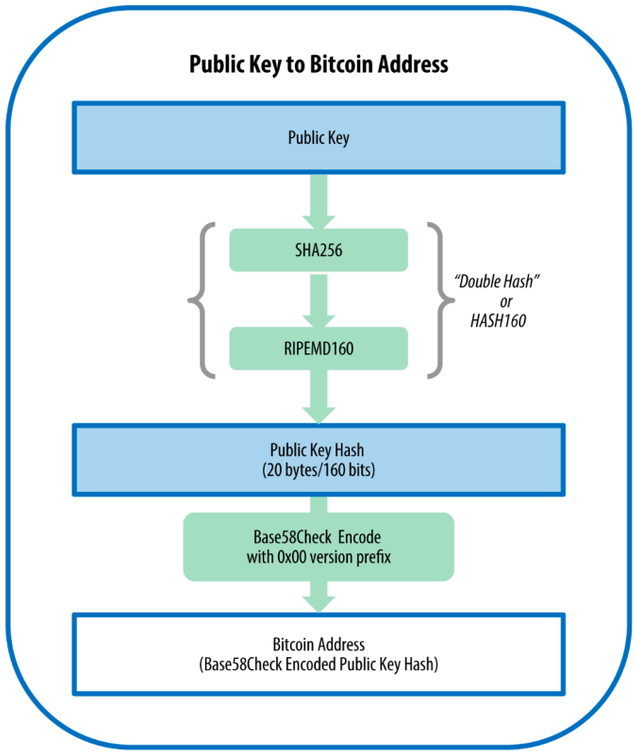
- Chiave Privata (un qualunque numero di 256 bit)
- K = k * G
- Chiave Pubblica

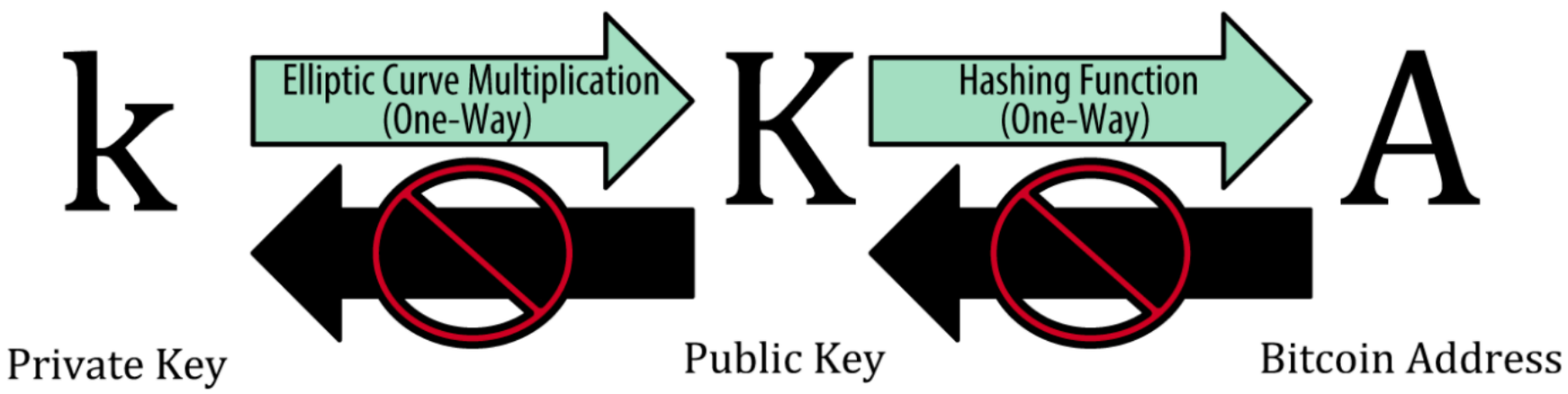


Chiavi Pubbliche e Indirizzi



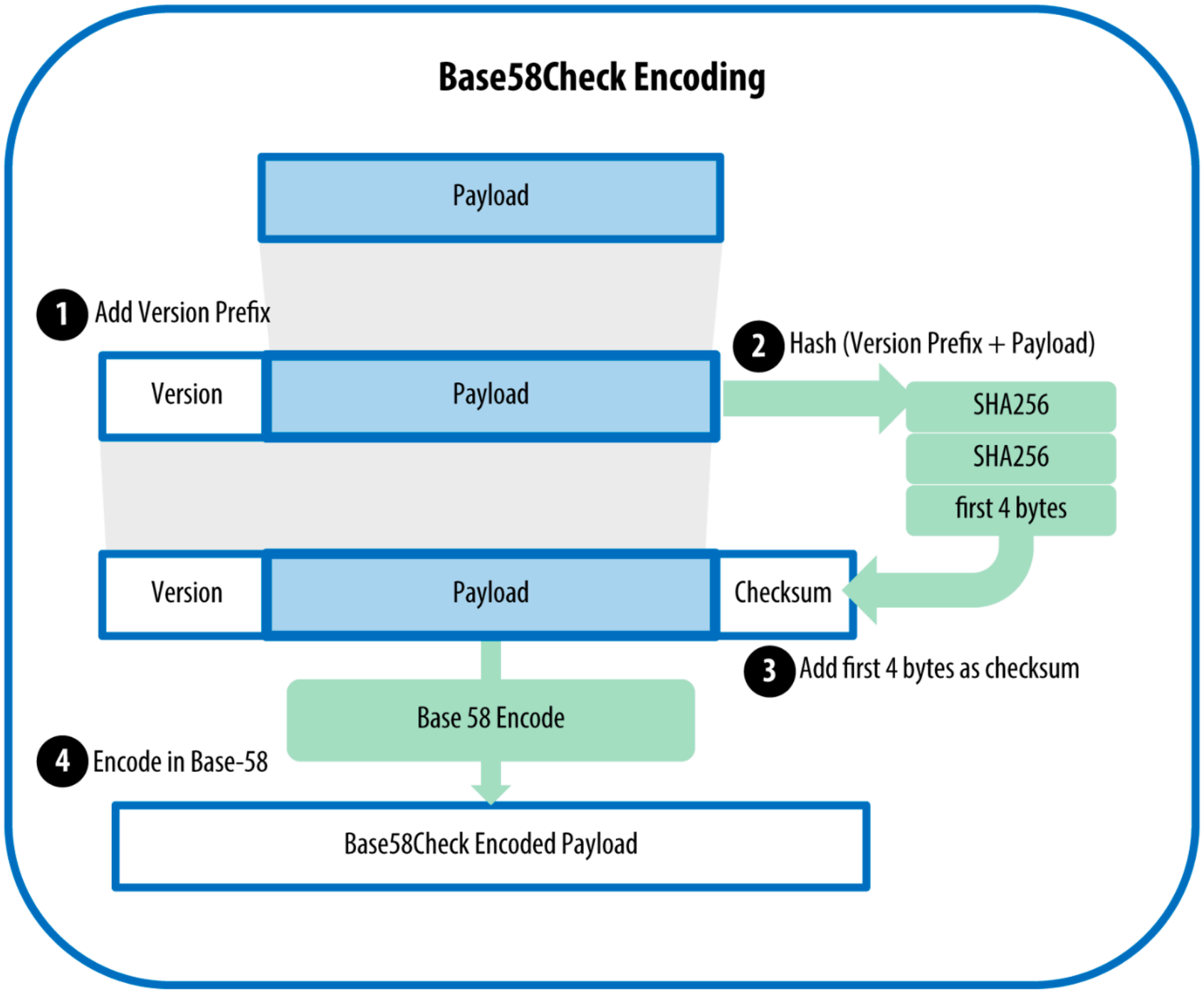
Chiavi Private e Chiavi Pubbliche





La Base 58

123456789ABCDEFGHJKLMNPQRSTUVWXYZabcdefghijkmnopqrstuvwxyz



Il prefisso

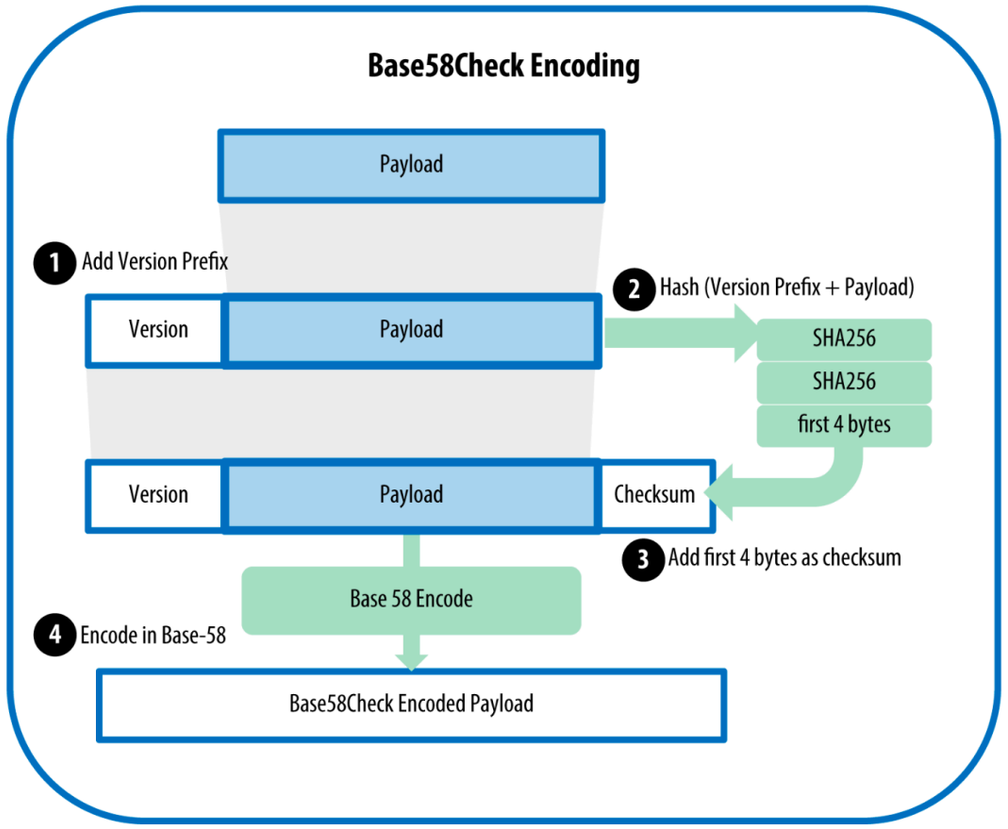
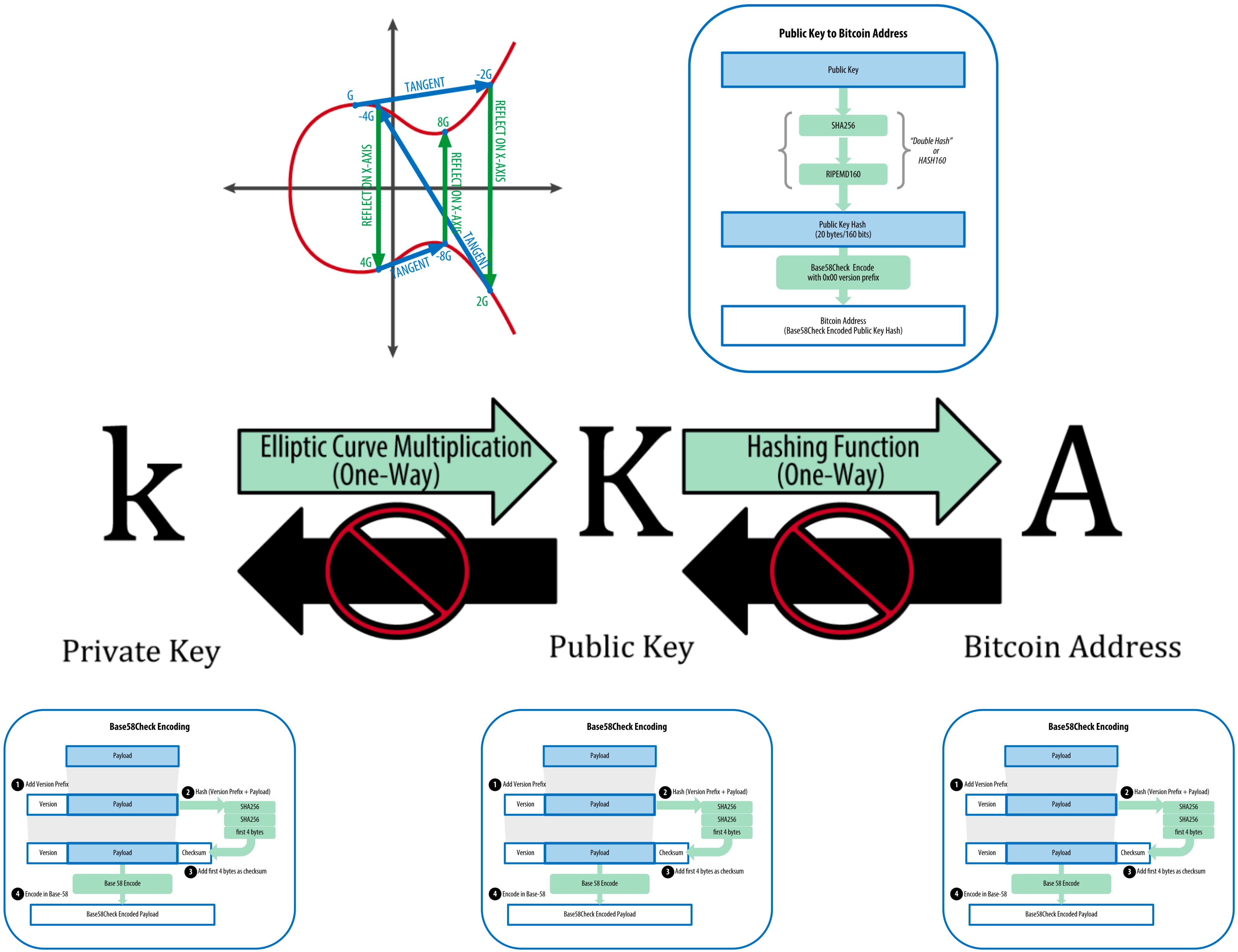


Table 1. Prefisso di versione Base58Check e esempi del risultato

Tipo	**Prefisso di versione (esadecimale)**	**Prefisso del risultato Base58**
Indirizzo Bitcoin	0x00	1
Indirizzo Pay-to-Script-Hash	0x05	3
Indirizzo Bitcoin Testnet	0x6F	m o n
Private Key WIF	0x80	5, K or L
Chiave Privata Criptata BIP38	0x0142	6P
Chiave Pubblica Estesa BIP32	0x0488B21E	xpub

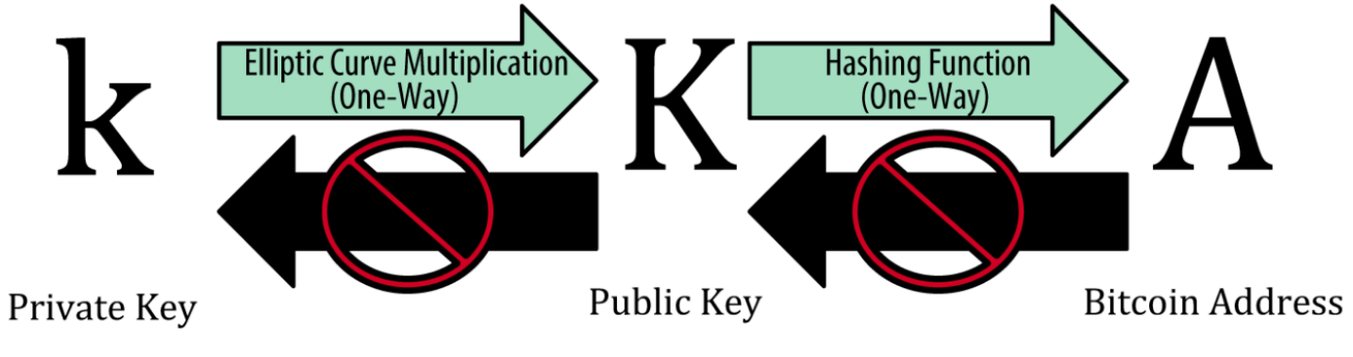

G
TANGENT
-2G
-4G
8G
REFLECT ON X-AXIS
REFLECT ON X-AXIS
REFLECT ON X-AXIS
TANGENT
4G
TANGENT
-8G
2G
Public Key to Bitcoin Address
Public Key
SHA256
RIPEMD160
"Double Hash" or HASH160
Public Key Hash (20 bytes/160 bits)
Base58Check Encode with 0x00 version prefix
Bitcoin Address (Base58Check Encoded Public Key Hash)
k
Elliptic Curve Multiplication (One-Way)
K
Hashing Function (One-Way)
A
Private Key
Public Key
Bitcoin Address
Base58Check Encoding
Payload
1 Add Version Prefix
Version
Payload
2 Hash (Version Prefix + Payload)
SHA256
SHA256
first 4 bytes
Version
Payload
Checksum
3 Add first 4 bytes as checksum
Base 58 Encode
4 Encode in Base-58
Base58Check Encoded Payload

UTXO
Unspent Transaction Output

- I bitcoin non “sono” in indirizzi.

- Sono “disponibili” a chi è in grado di risolvere un puzzle crittografico.

- Per risolverlo, in genere serve avere una chiave privata, che genera una chiave pubblica, che genera un indirizzo a cui i bitcoin sono in genere assegnati



UTXO
Unspent Transaction Output

```
3 OP_ADD 5 OP_EQUAL
```

```
2 3 OP_ADD 5 OP_EQUAL
```

Unlocking Script (scriptSig) + Locking Script (scriptPubKey)

```
<sig> <PubK>  DUP HASH160 <PubKHash> EQUALVERIFY CHECKSIG
```

Unlock Script (scriptSig) is provided by the user to resolve the encumbrance

Lock Script (scriptPubKey) is found in a transaction output and is the encumbrance that must be fulfilled to spend the output

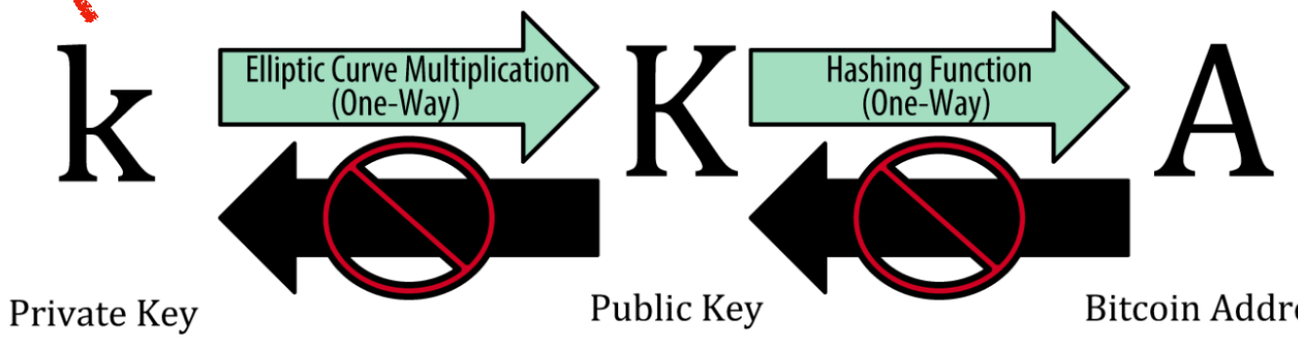
UTXO
Unspent Transaction Output

Unlocking Script (scriptSig) + Locking Script (scriptPubKey)

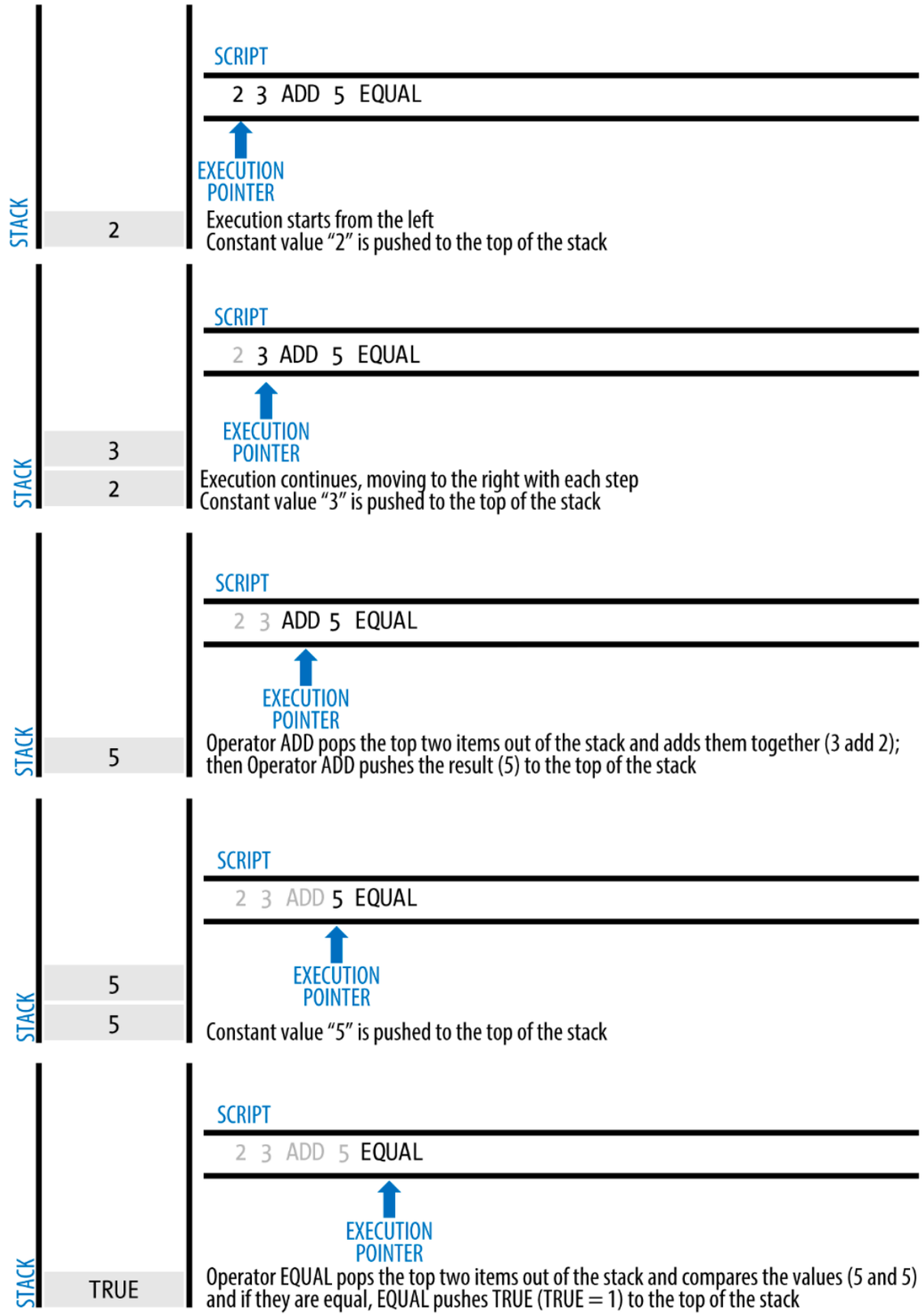
`<sig> <PubK>` `DUP HASH160 <PubKHash> EQUALVERIFY CHECKSIG`

Unlock Script (scriptSig) is provided by the user to resolve the encumbrance

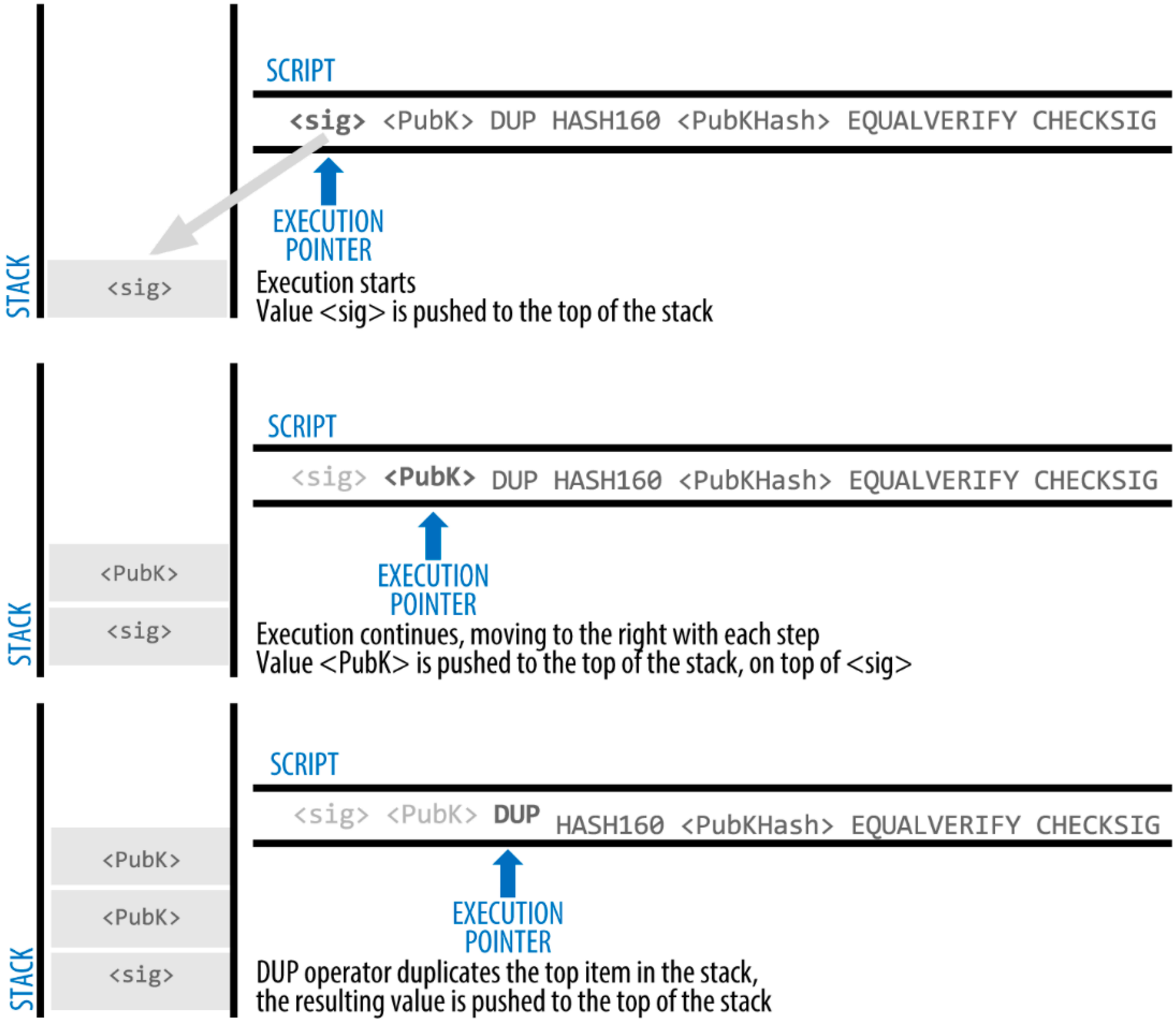
Lock Script (scriptPubKey) is found in a transaction output and is the encumbrance that must be fulfilled to spend the output



Transazioni come contratti

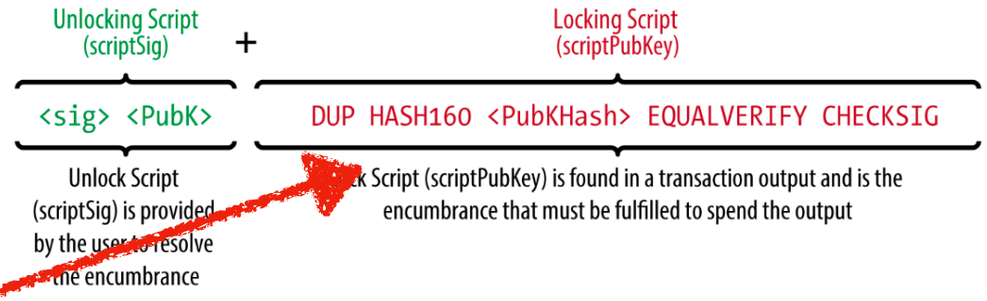


Transazioni come contratti



Transazioni come contratti

Tipi di Transazioni



- Paga a PubKey Hash
- Paga se M di N sono d’accordo
- Congela i fondi fino a una data nel futuro
- …

E se avesse capacità di calcolo universale?

Ethereum

- Ethereum Ico
- Code is Law
- DAO
- Ethereum Classic
- Scaling problems

Firefox | Welcome! | Silk Road | Welcome! | Silk Road

silkroadvb5piz3r.onion

Silk Road

anonymous marketplace

Welcome **Cult Leader**!

messages(0) | **orders(0)** | **account($0.00)** | **settings** | **log out**

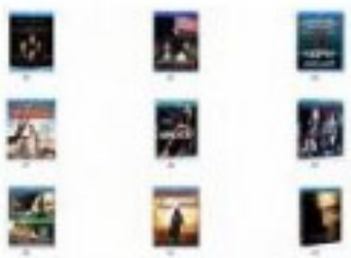
search | (0)

8 days 2 hrs 51 mins 31 secs until Four Twenty!!!

Shop by category:

- Drugs(2679)
  - Cannabis(741)
  - Dissociatives(59)
  - Ecstasy(274)
  - Opioids(214)
  - Other(76)
  - Prescription(515)
  - Psychedelics(348)
  - Stimulants(256)
- Apparel(22)
- Books(283)
- Computer equipment(13)
- Digital goods(220)
- Drug paraphernalia(52)
- Electronics(19)
- Fireworks(1)
- Forgeries(41)
- Hardware(3)
- Home & Garden(5)
- Jewelry(1)

CRANBERRY KUSH & STRAWBERRY...
$36.82



10pc of Genuine Fake Blu Ray Discs
$49.50

30mg Oxycodone (Roxie, Roxy) IR...
$250.00

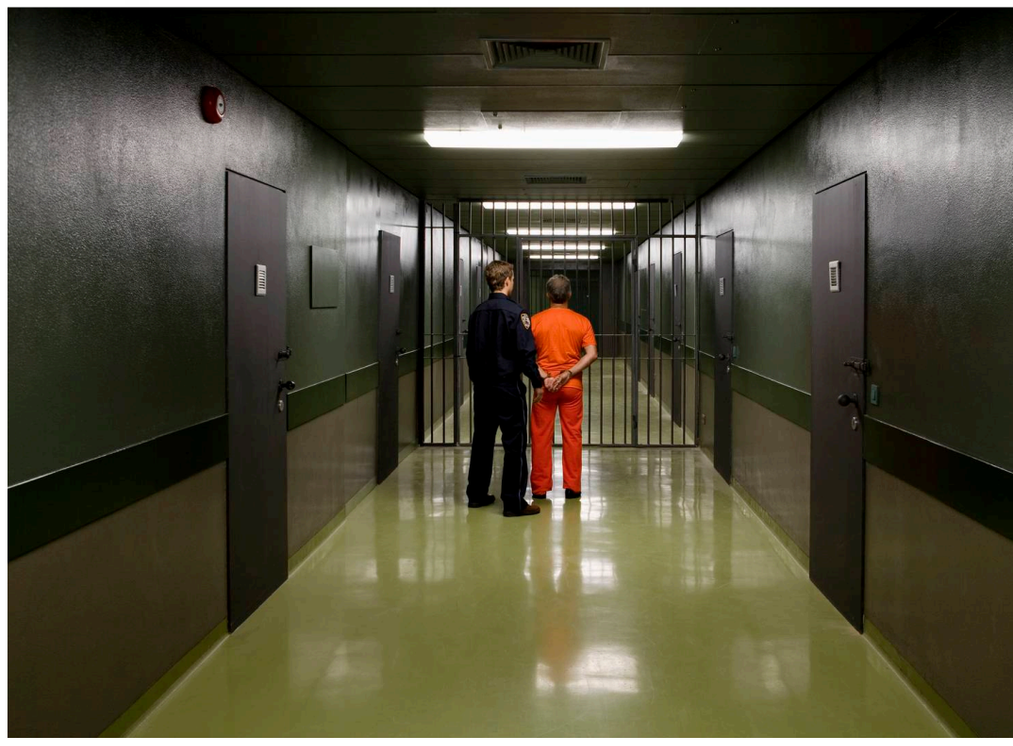
BITCOINS - NOW THE LOWEST PRICE...
$0.00

Diazepam (valium) 10mg - 1000...
$425.50

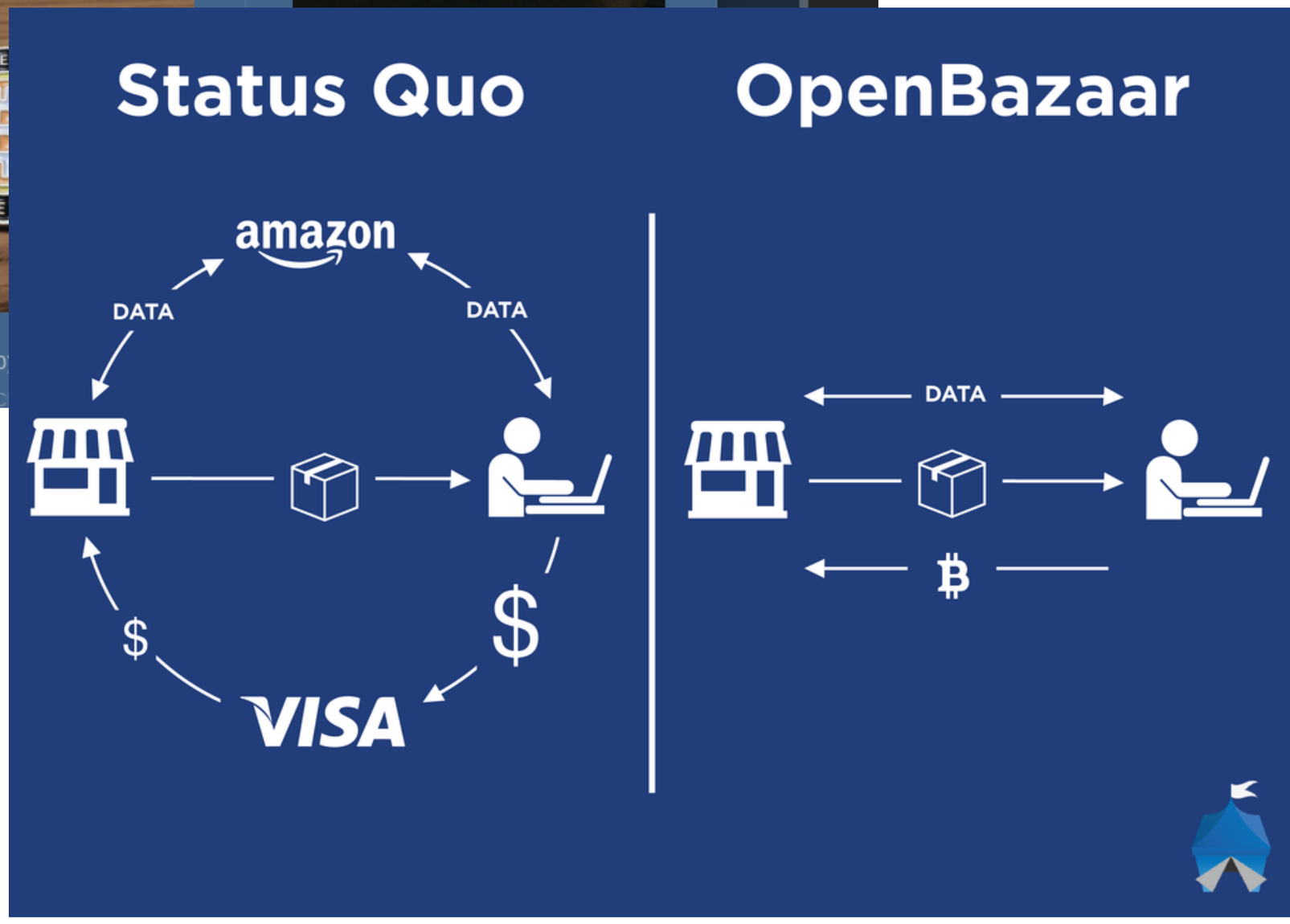
Anarcho47's Magikally Epic...
$2.48

News:

- Who's your **favorite**?
- Acknowledging **Heroes**
- A new annonymous market **The Armory**!
- **State of the Road Address**



@openbazaar/store



Bulgaria discovers it has enough bitcoins to pay off fifth of its debt

Published time: 11 Dec, 2017 11:01
Edited time: 11 Dec, 2017 11:02

Bitcoins Bulgarian police seized from an 'organised crime gang' would now pay off a FIFTH of the country's national debt after value rises by 600% in six months

La Ricerca della Moneta Elettronica

- Digicash — Bankrupt
- E Gold — Arrested
- Liberty Reserve — Arrested
- Napster — Programma = punto debole
- Gnutella / Kazaa — Azienda = punto debole
- Bittorrent — Protocollo Decentralizzato

Solo un sistema decentralizzato può funzionare

3ª Lezione

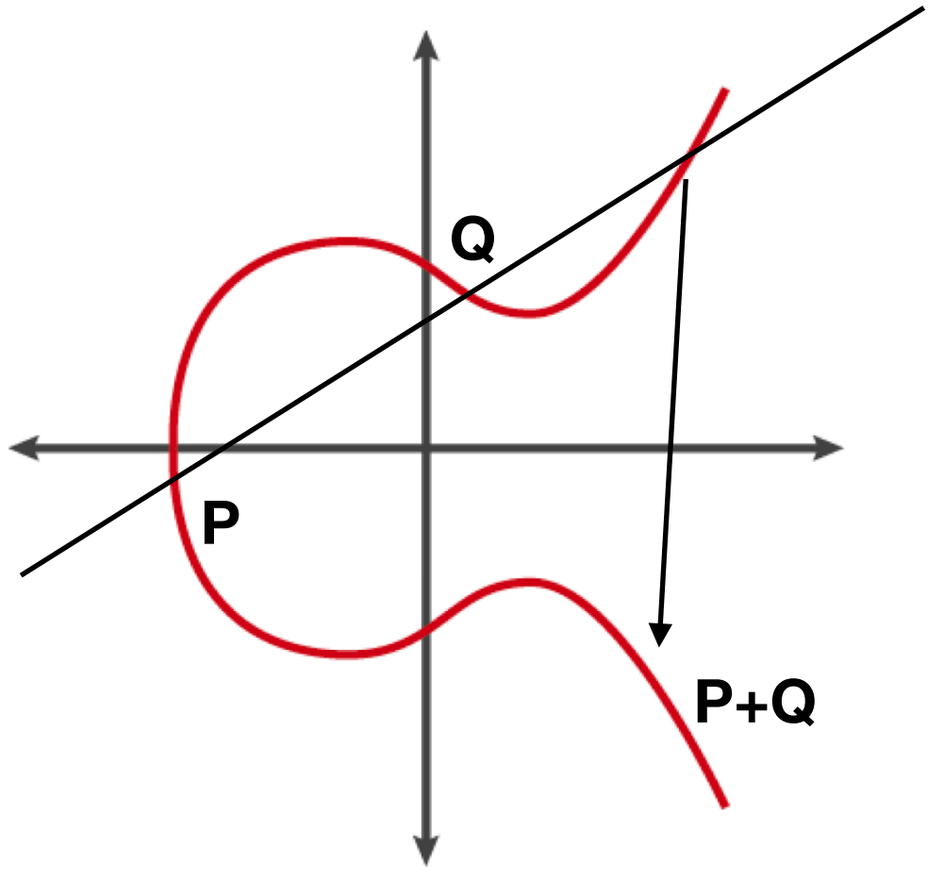
- Transazioni e resto
- Anonimato e Pseudo Anonimato
- Fungibilità
- Masternodes
- Monete Sicure

Chiavi Private e Chiavi Pubbliche

- $Y^2=X^3-7$ su Z_p

- Con p = 2^{256} - 2^{32}- 2^9- 2^8- 2^{32}- 2^7- 2^6- 2^4-1

- Dato p+q punti sulla curva, p+q è il terzo punto che incrocia una retta per p e q

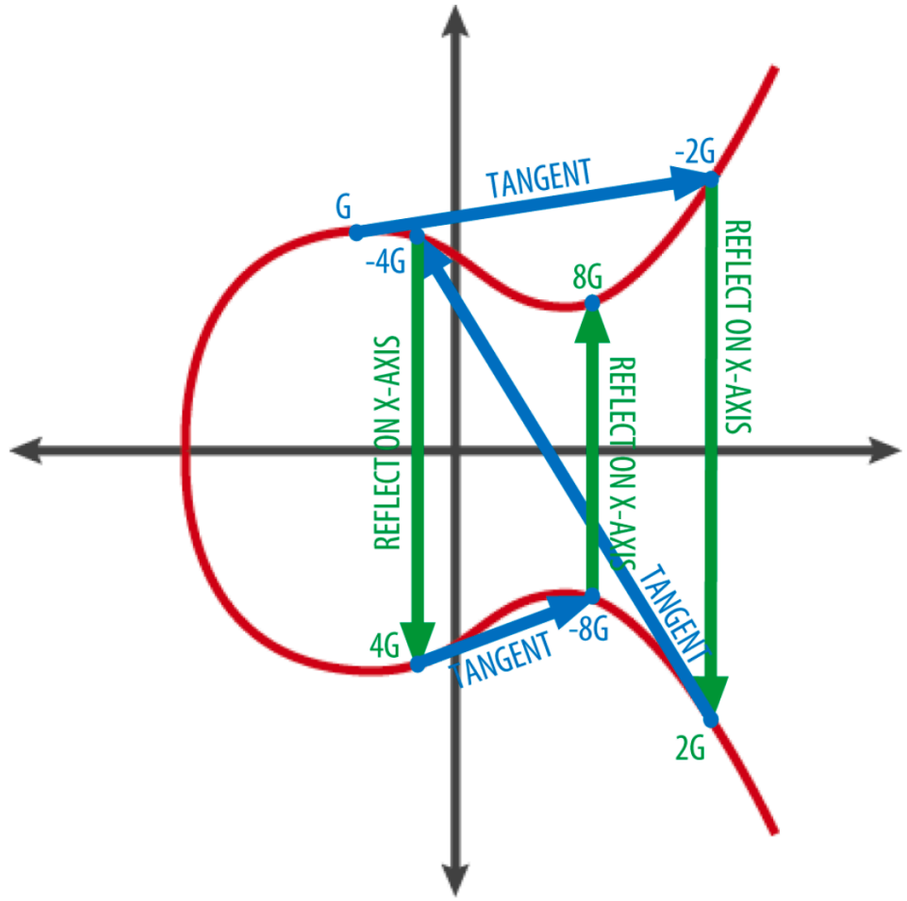


Chiavi Private e Chiavi Pubbliche

- Se p=q si prende la retta tangente e si prende il valore riflesso

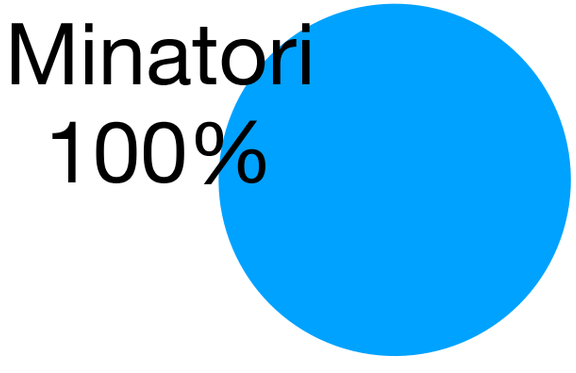
- ‘+’ è associativo, ha un elemento neutro (punto all’infinito), ha un inverso, commutativo

- x*p=p+p+p+… +p (x volte)



Quanto costa minare

- Consideriamo 12.5 bitcoin ogni 10 minuti
- Consideriamo che un bitcoin vale 5000 euro (circa)
- Quanta energia consuma la comunità a minare i bitcoin?



Chi Mina

- Energia a poco prezzo
- Posti Freddi
- Leggi che lo consentono

- Venezuela
- Cina
- Canada
- Islanda

Conviene agli Stati permetterlo?

Transazioni in Bitcoin (che succede del resto?)

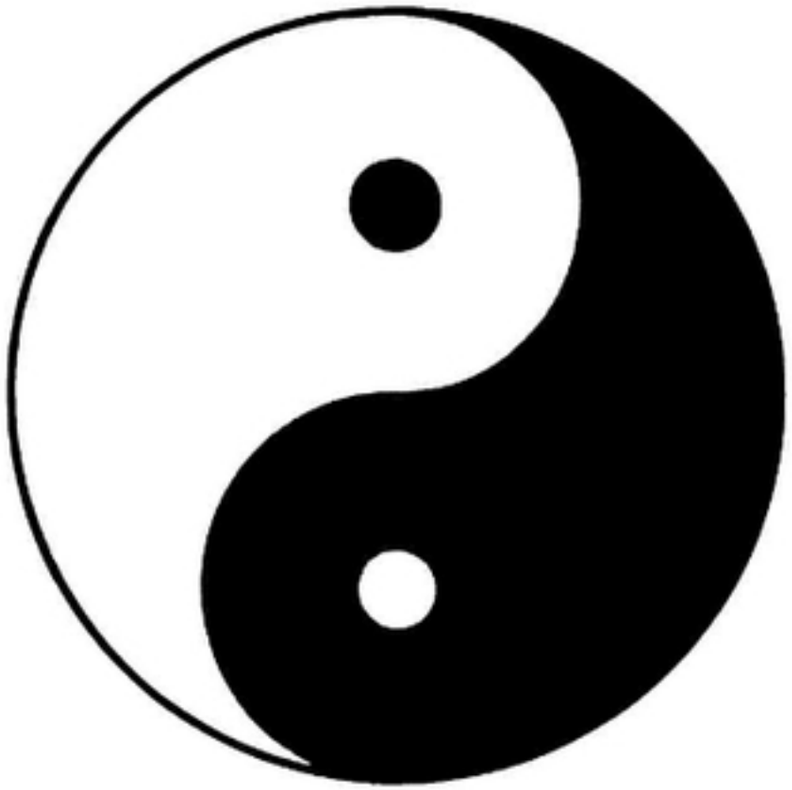
- Nella transazione non si spostano i bitcoin
- Si cambiano le serrature
- Ma che succede se il cambio non è perfetto
- Bisogna indicare dove deve andare se no si perde il cambio (molti wallet lo fanno in automatico)

Blacklisted

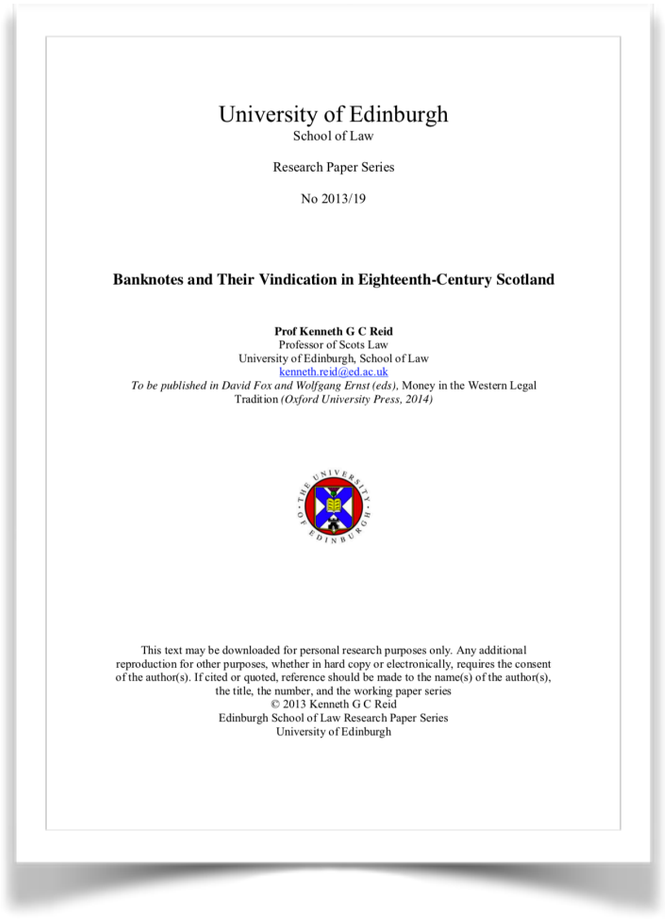
Whitelisted

Know your Costumer

Antiriciclaggio (AML)



Fungibilità



University of Edinburgh
School of Law

Research Paper Series

No 2013/19

Banknotes and Their Vindication in Eighteenth-Century Scotland

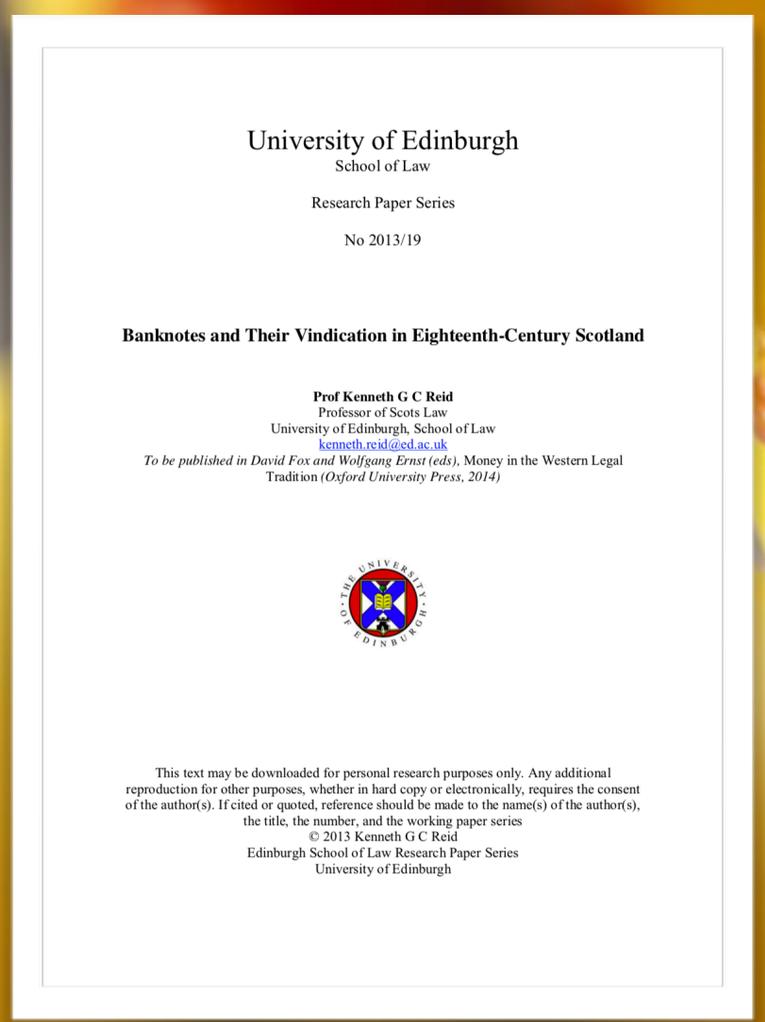
Prof Kenneth G C Reid
Professor of Scots Law
University of Edinburgh, School of Law
kenneth.reid@ed.ac.uk

To be published in David Fox and Wolfgang Ernst (eds), Money in the Western Legal Tradition *(Oxford University Press, 2014)*

Pseudo-anonimato

Anonimato

Fungibilità



University of Edinburgh
School of Law

Research Paper Series

No 2013/19

Banknotes and Their Vindication in Eighteenth-Century Scotland

Prof Kenneth G C Reid
Professor of Scots Law
University of Edinburgh, School of Law
kenneth.reid@ed.ac.uk
To be published in David Fox and Wolfgang Ernst (eds), Money in the Western Legal Tradition *(Oxford University Press, 2014)*

If holders of banknotes were vulnerable to infirmities of title of which they knew nothing, then this would indeed be ‘a barr to the circulation’ of notes and hence a threat to the whole idea of paper money.

La ricerca di una moneta Anonima

- Darkcoin - Dash

- Monero

- ZCash

- Bitcoin coinjoin

- Bitcoin mixers

- Bitcoin gambling

Zcash

Edward Snowden
@Snowden

Segui

Agree. Zcash's privacy tech makes it the most interesting Bitcoin alternative. Bitcoin is great, but "if it's not private, it's not safe."
twitter.com/masonic_tweets …

Hany Rashwan @hany · 28 set 2017
What do you think of Monero?

4 2 52

Edward Snowden
@Snowden

Segui

In risposta a @hany

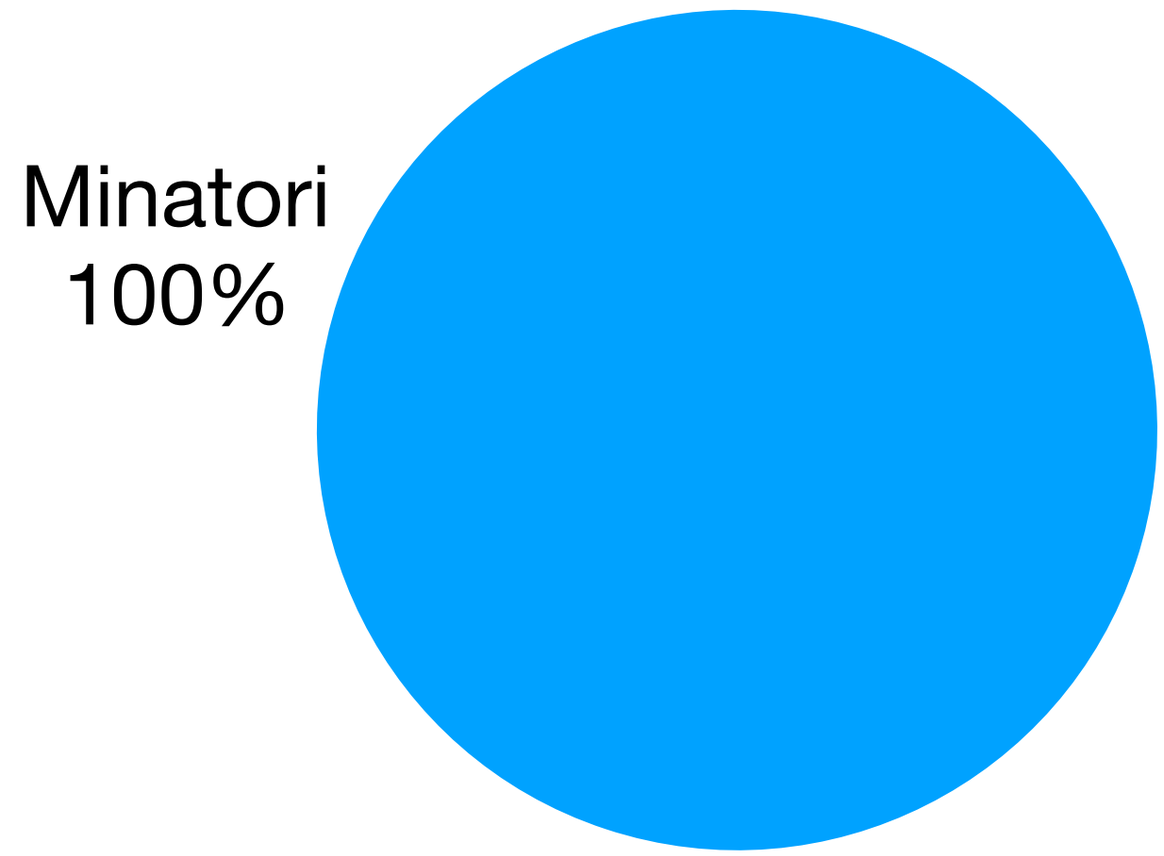
Great project, but the problem with amateur crypto is mistakes happen and have huge consequences for people like me:

Anonimato

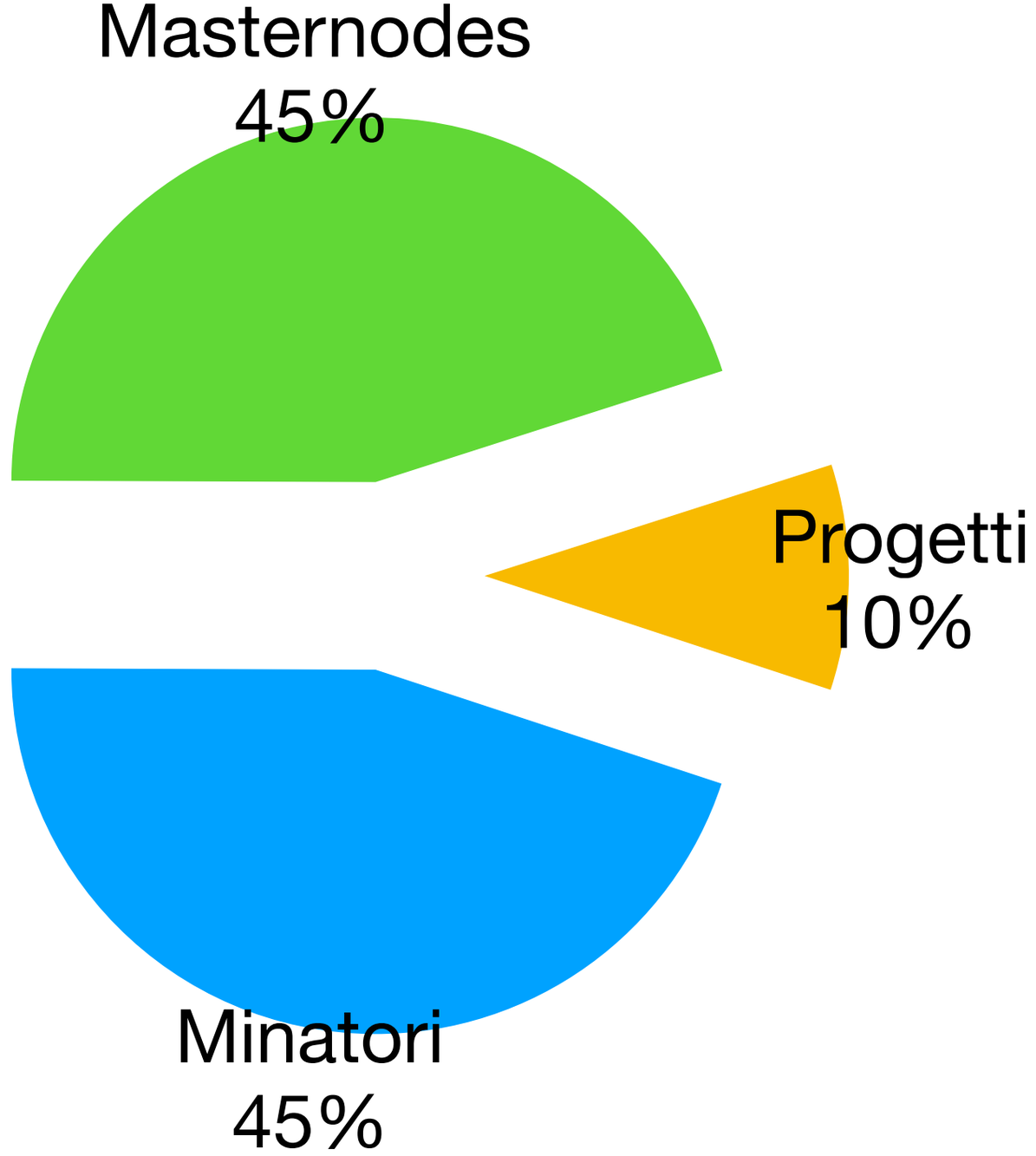
- I bitcoin sono pseudo anonimi
- Altre monete sono invece anonime (Monero, ZCoin, …)
- I bitcoin si possono “mischiare”
- I bitcoin non sono fungibili
- Una proposta di legge (Quintarelli) richiedeva di rendere illegali gli exchange che permettevano di comprare monete anonime
- Il CEO di un Exchange è stato rapito in Bulgaria e l’hanno rilasciato solo quando ha pagato un grosso riscatto

A chi va la moneta creata?

Bitcoin



Dash



Proof of Stake vs Proof of Work

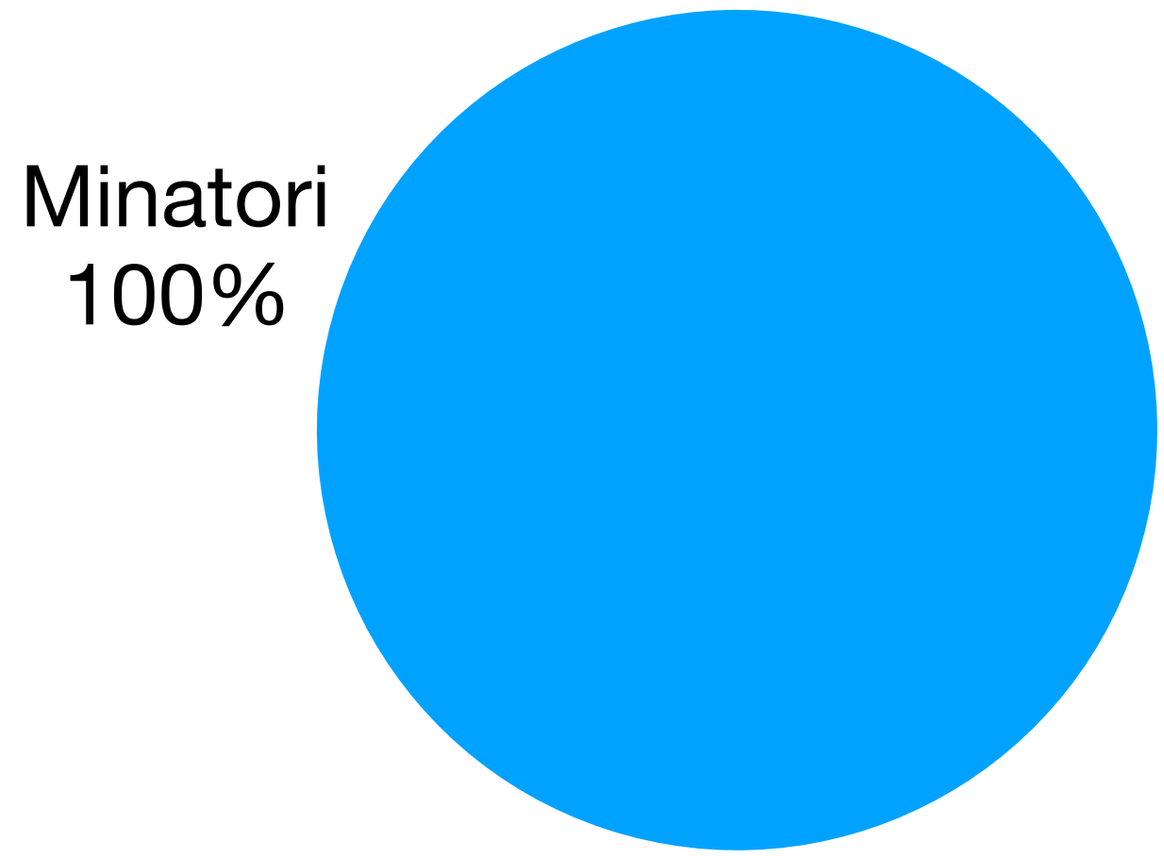
- Si congela una grossa quantità di una moneta (masternode)
- Si scarica l’intera blockchain
- Ogni masternode ha la stessa probabilità di vincere la prossimo produzione

Masternodes

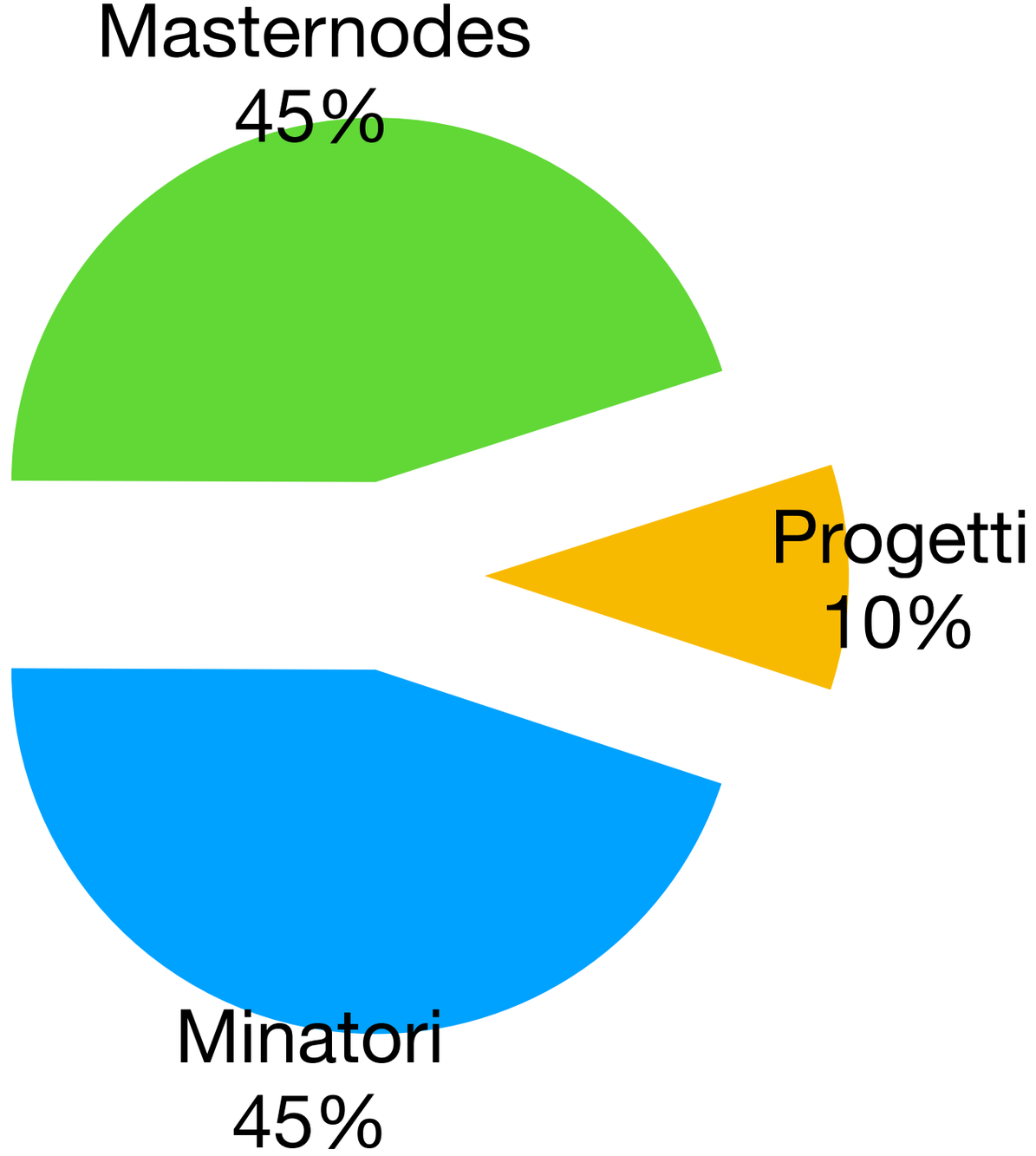
- Rendita Passiva
- La rendita però varia con il variare del prezzo
- Stabilizza la rete
- Il numero di masternode varia, ma sono abbastanza da rendere il sistema decentralizzato e non troppi da metterci troppo negli update
- https://masternodes.online/
- I masternode possono anche avere ulteriori “poteri”

A chi va la moneta creata?

Bitcoin



Dash



A chi va la moneta creata?

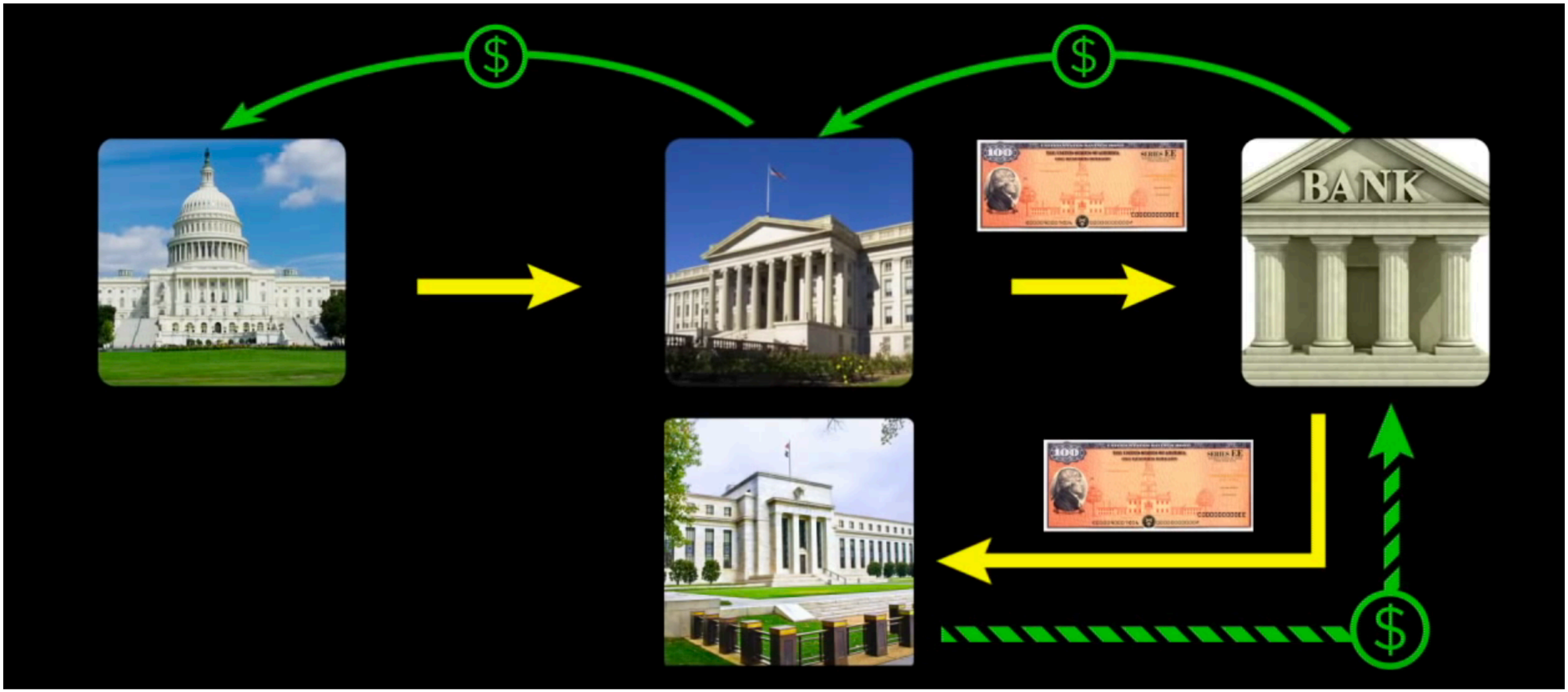
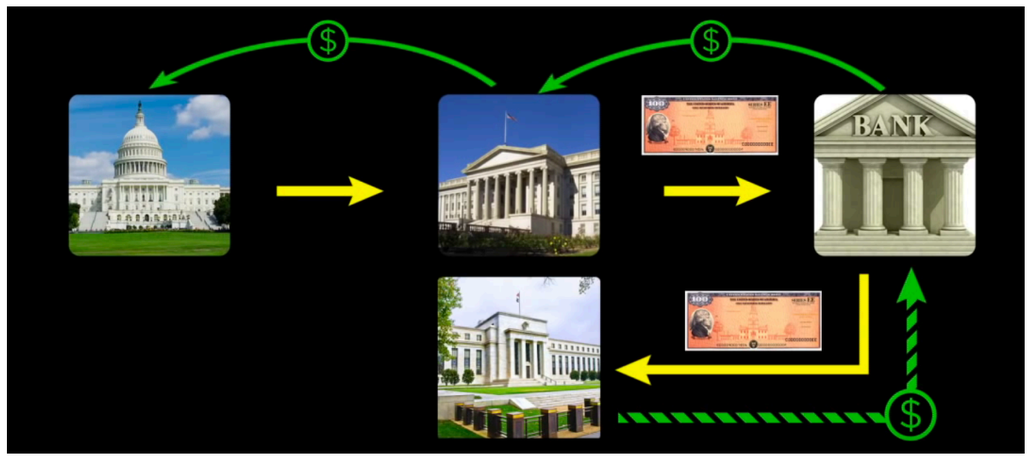
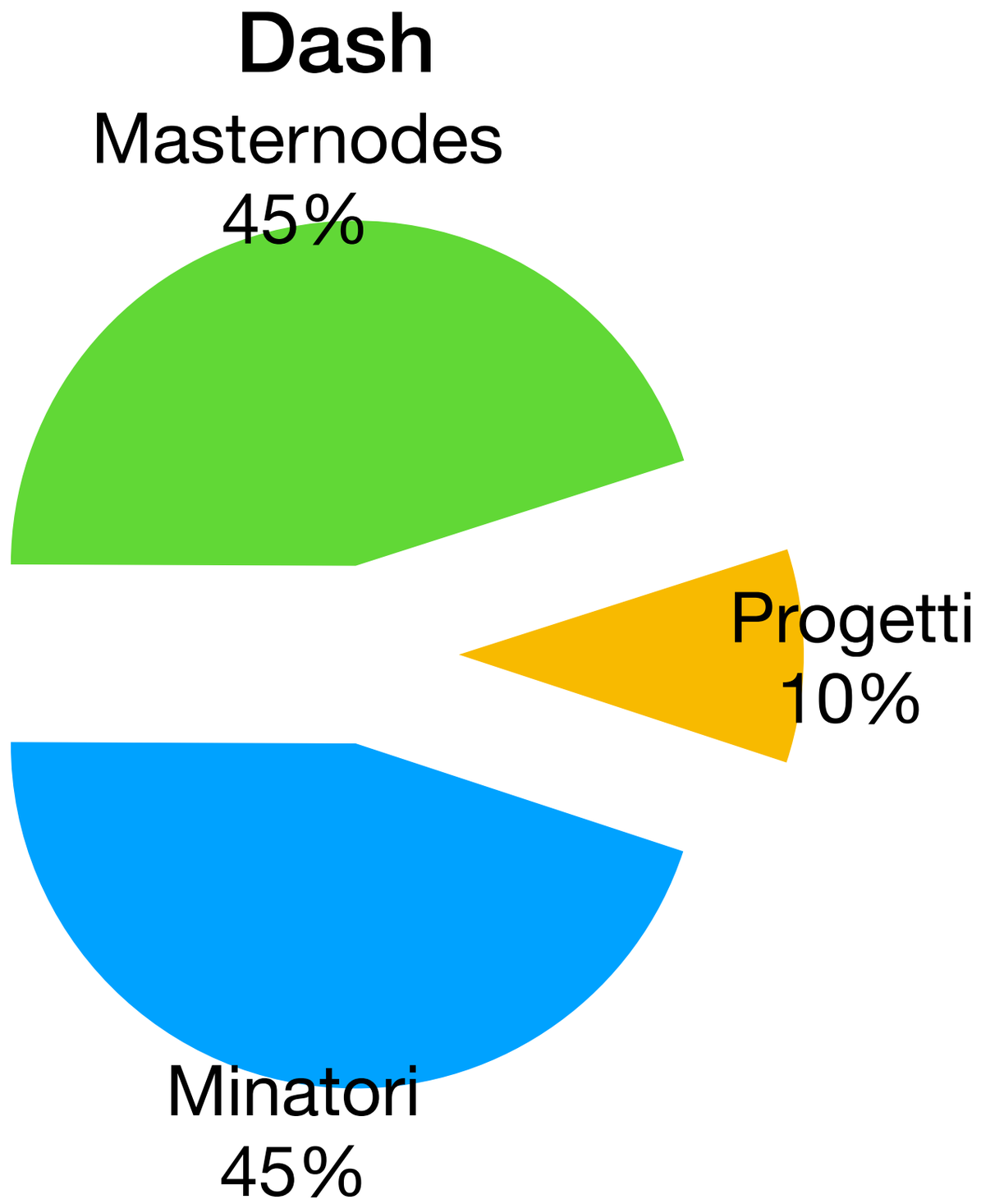


Immagine da Chris Martenson:
The Crash Course, chapter 8, Money Creation

A chi va la moneta creata?

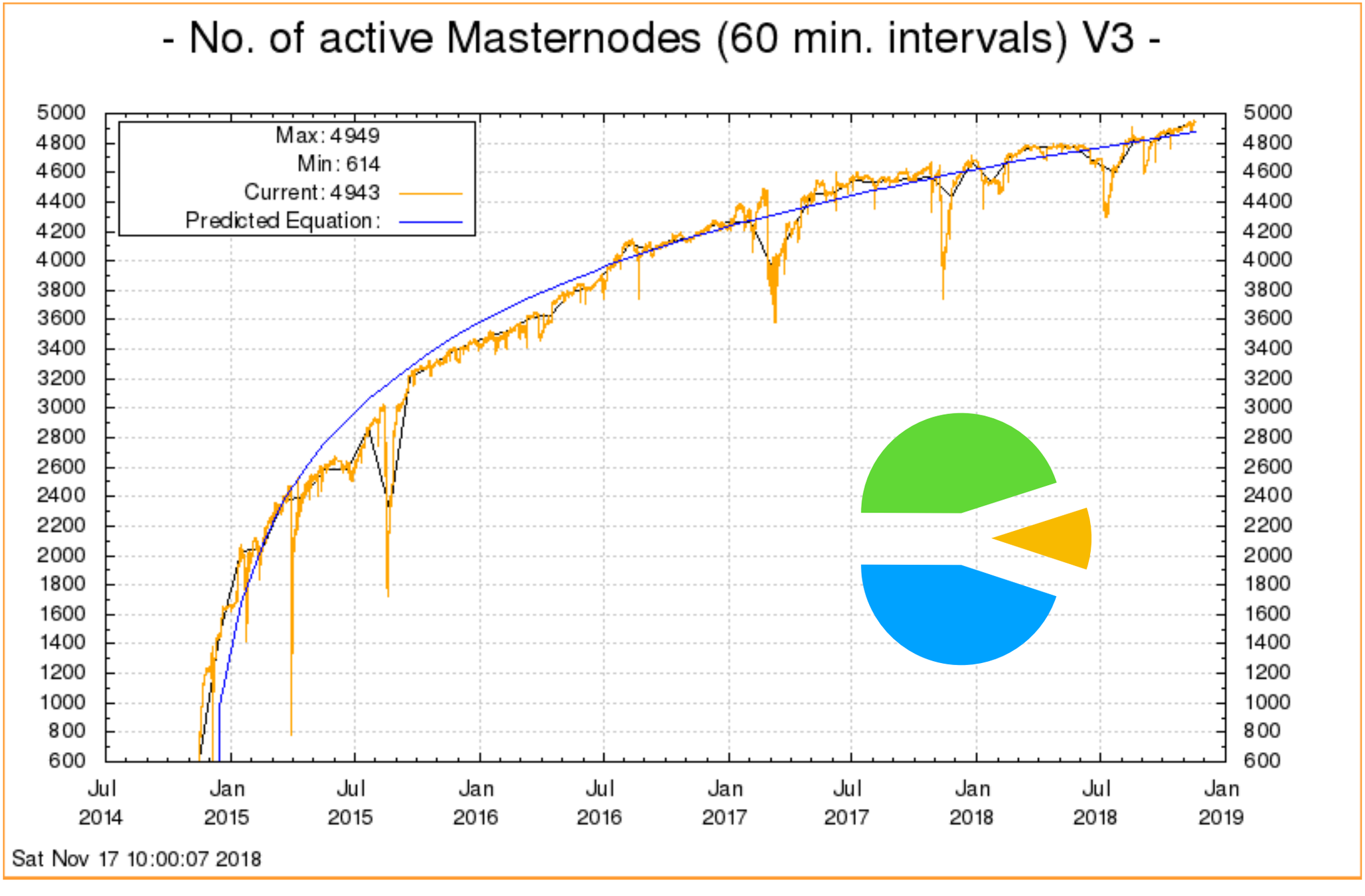




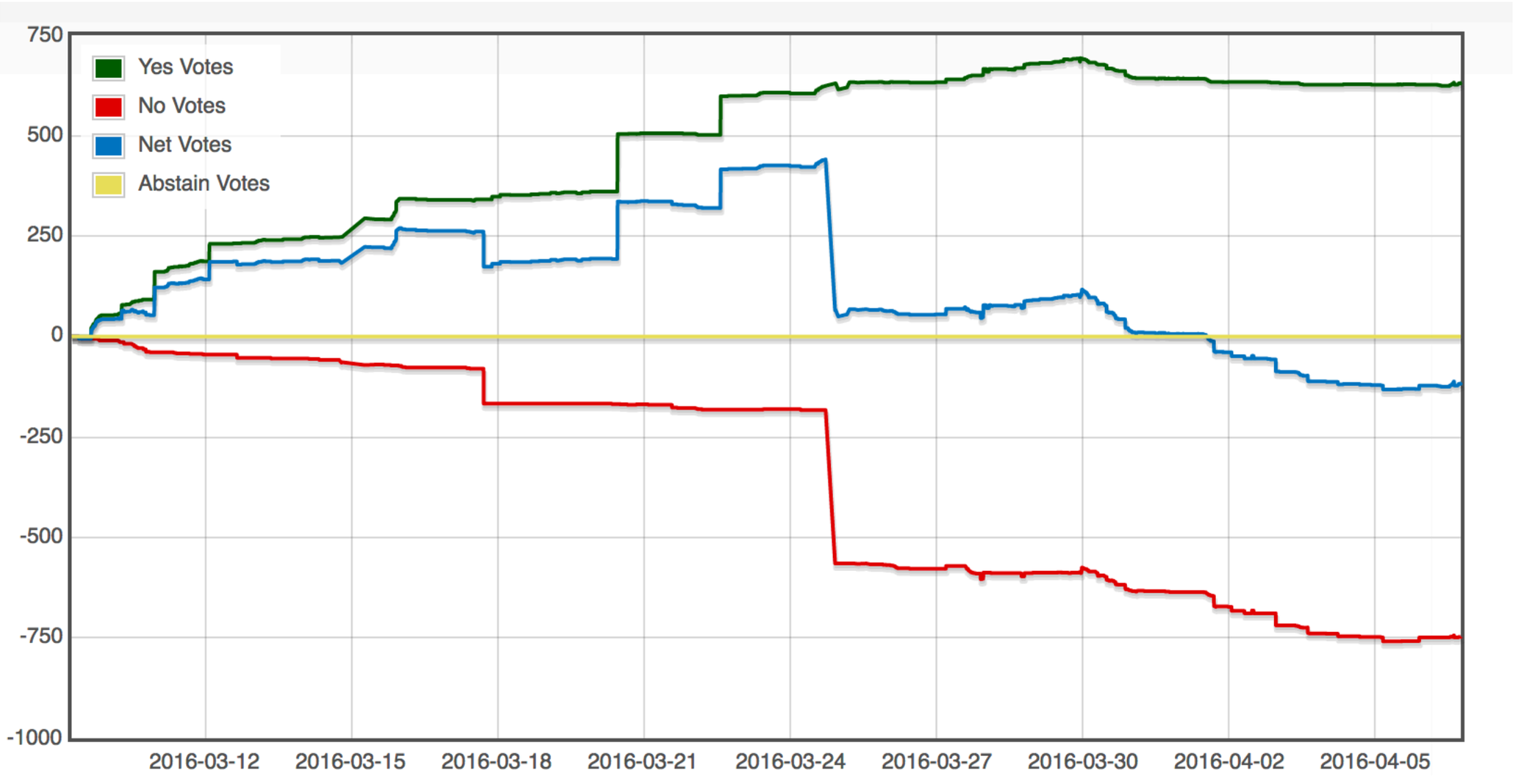
La nascita di darkcoin

- Darkcoin viene annunciata
- Ci vuole ancora un po’ di tempo
- Poi viene rilasciata senza preavviso
- I primi a minarla hanno un enorme vantaggio per un “bug” nel codice
- Si decide di non tornare indietro
- Si cambia il nome in Dash (Digital Cash)

Chi controlla Dash?



Chi controlla Dash?



E chi controlla le altre altcoin?

- ZCore (ZCR)
- Escrow (ESCO)
- Energi (NRG)
- HexxCoin (HXX)
- Bulwark (BWK)
- ColossusXT (COLX)
- Kore (KORE)
- ProjectCoin (PRJ-T2)
- ProjectCoin (PRJ-T1)
- ProjectCoin (PRJ-T3)
- EVOS (EVOS)
- BitSend (BSD)
- TransferCoin (TX)
- Polis (POLIS)
- Delizia (DELIZ)
- ION (ION)
- LUXCoin (LUX)
- Kalkulus (KLKS)
- Thrill (THRL)
- KODCOIN (KOD)
- Deviant (DEV)
- HempCoin (THC)
- Wagerr (WGR)

- 1X2 Coin (1X2)
- AirWire (WIRE)
- Vitae (VITAE)
- Market Arbitrage Coin (MARC)
- Dash Green (DASHG)
- Memetic (MEME)
- PrimeStone (PSC)
- GashCoin (GASH)
- Zio Coin (ZIO)
- QYNO (QNO)
- GINCoin (GIN)
- DarkPayCoin (DKPC)
- SIBCoin (SIB)
- LightPayCoin (LPC)
- PICPOTO (PPO)
- Midas (MIDAS)
- MFIT COIN (MFIT)
- Solaris (XLR)
- ALQO (XLQ)
- Dynamic (DYN)
- PACcoin (PAC)
- Bitcoin Incognito (XBI)
- MonetaryUnit (MUE)

- Dash (DASH)
- EtherZero (ETZ)
- Horizen Securenode (ZEN-42)
- Horizen Supernode (ZEN-500)
- Zcoin (XZC)
- SmartCash (SMART)
- Birake (BIR)
- Gold Poker (GPKR)
- SysCoin (SYS)
- PIVX (PIVX)
- Ad Node (ADD)
- StakeNet (XSN)
- SafeInsure (SINS)
- Bithost Coin (BIH)
- Blocknet (BLOCK)
- SkyHub (SHB)
- PHORE (PHR)
- Crux Coin (CUX)
- Lindacoin (LINDA)
- ExclusiveCoin (EXCL)
- LogisCoin (LGS)
- Loki (LOKI)
- GoByte (GBX)
- Crown SN (CRW-SN)
- Crown (CRW)

Progetti Sostenuti da Dash

- Sviluppo del codice
- Conferenze in Venezuela
- Dash TV
- Collaborazione con le università
- …
- Ma anche tanti soldi sprecati
- https://dashvotetracker.com/past.ph

Grafi da guardare

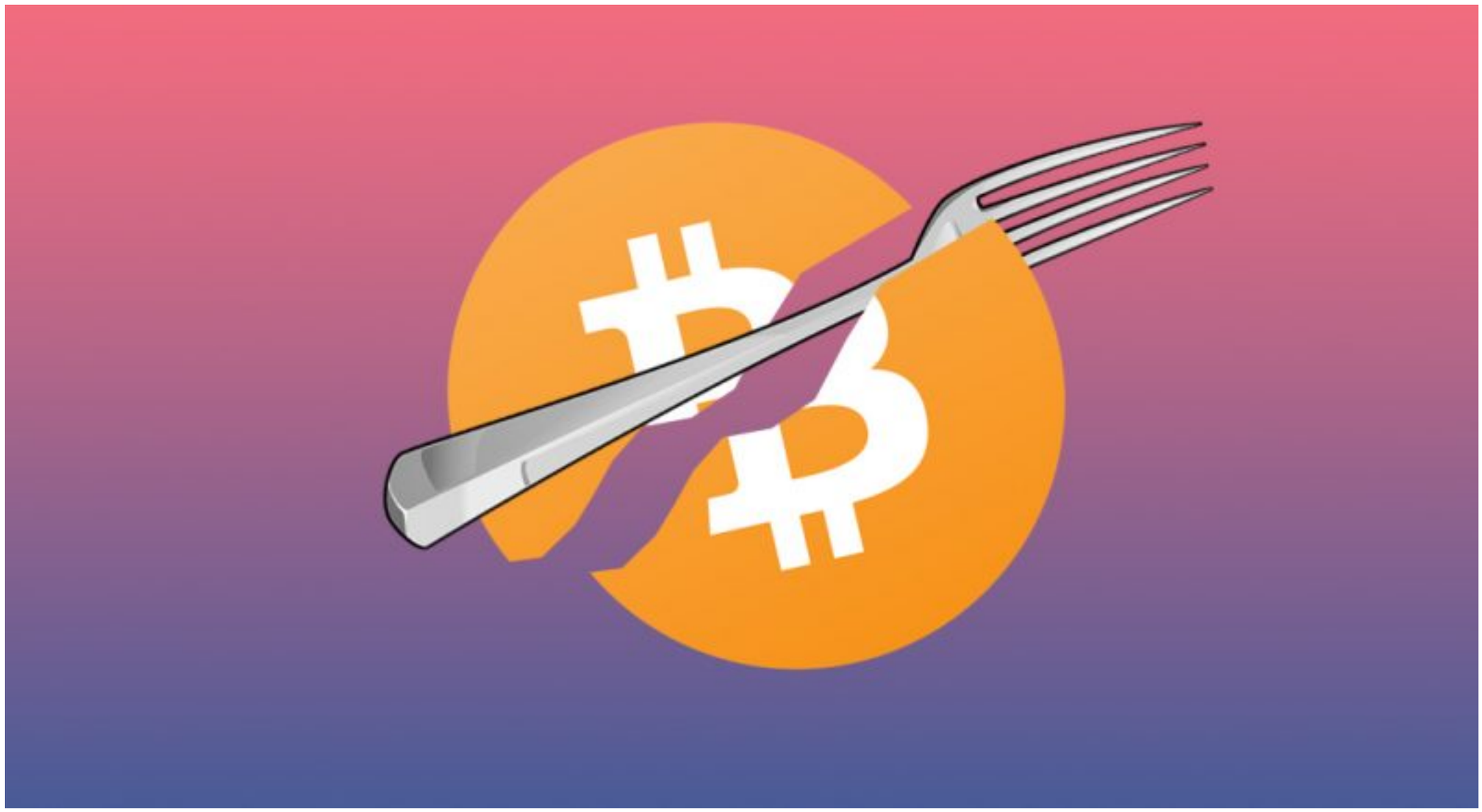
- https://bitinfocharts.com/comparison/bitcoin-price.html#log

- …

4ª Lezione

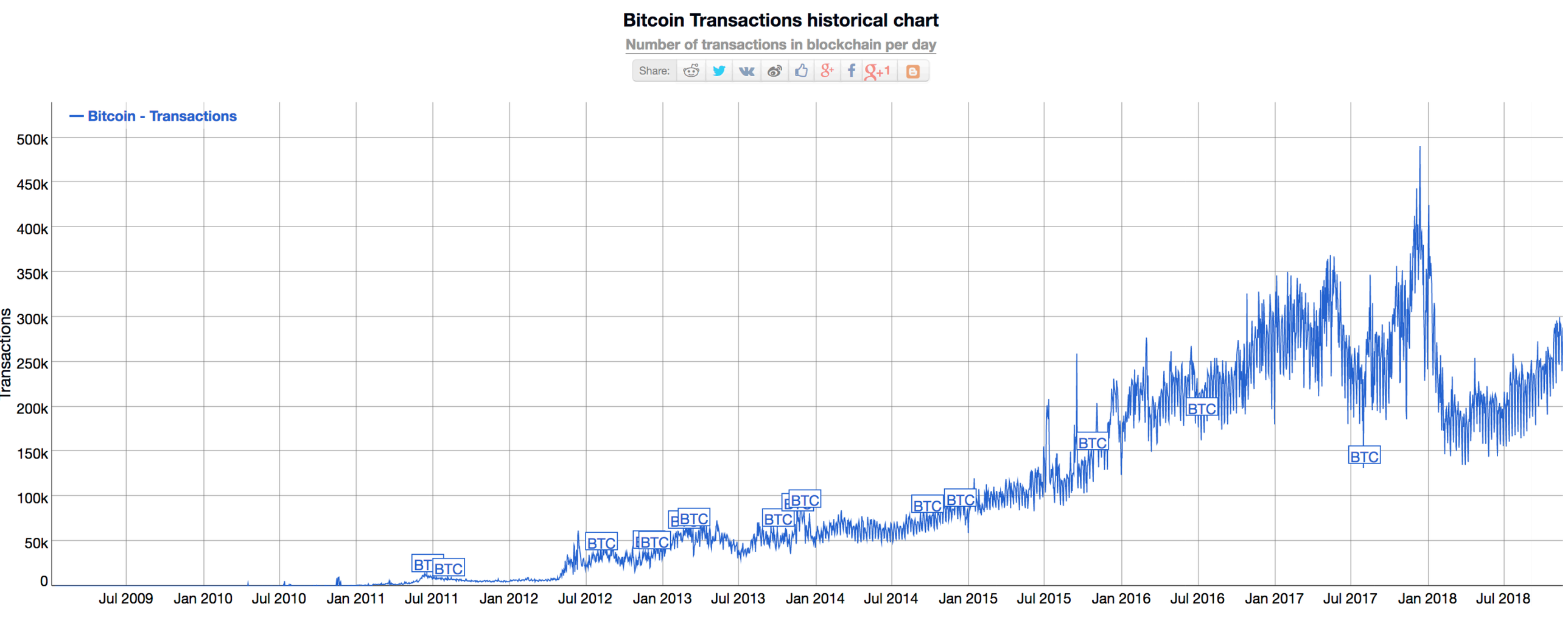
- “La cosa importante non sono i bitcoin, è la blockchain”
  - Cosa è una blockchain?
  - Che tipi di blockchain esistono?
  - Quando conviene usare una blockchain?
- Che tipo di Governo si può usare nella blockchain?
- Applicazione, Bitcoin Scala?

Bitcoin Fork

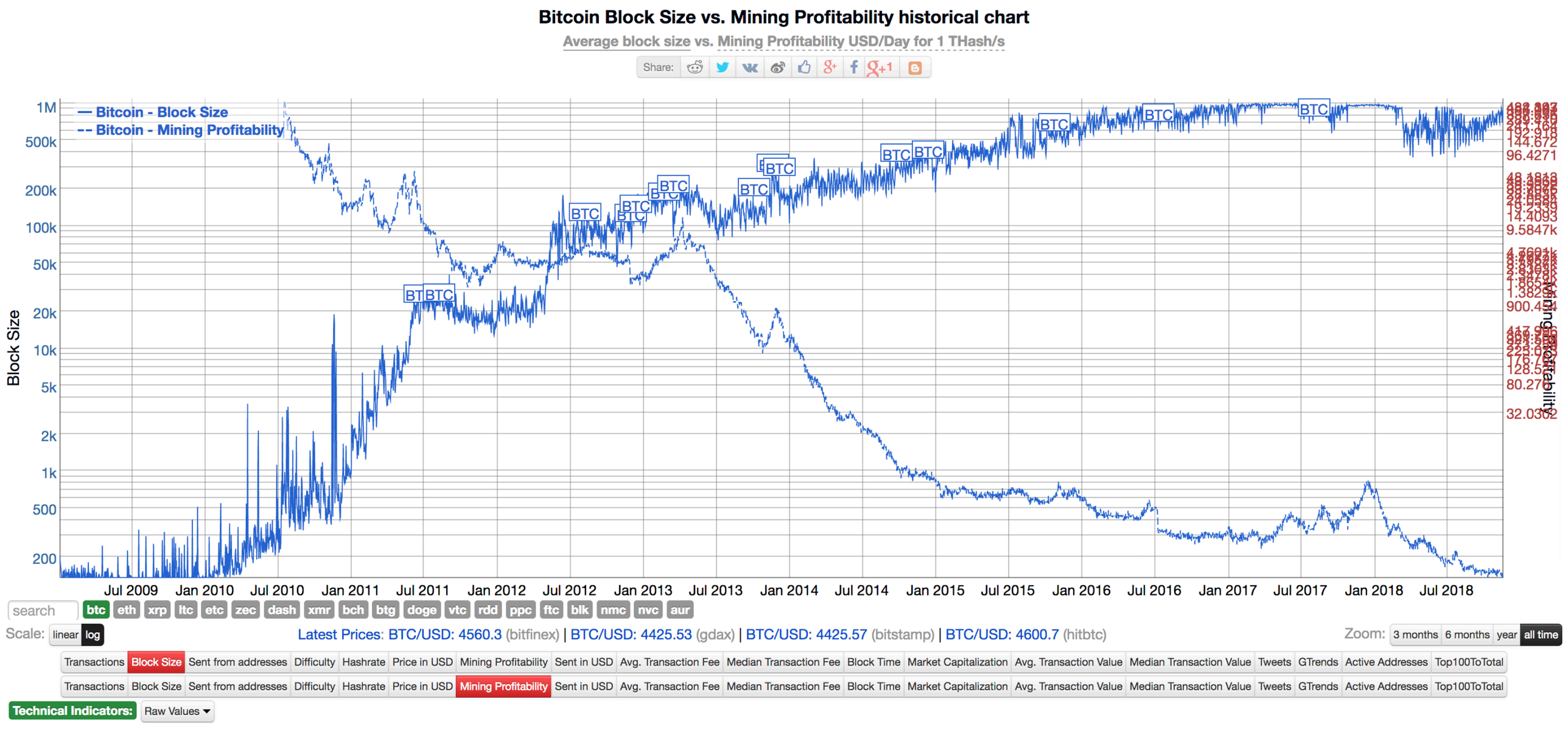


https://blog.bitmex.com/44-bitcoin-fork-coins/

Difficoltà per il bitcoin a “scalare”



Block Size vs Mining Profitability



Strutture di dati più centralizzate sono più efficienti

- Numero di transazioni al momento: 250 K https://bitinfocharts.com/comparison/bitcoin-transactions.html
- Visa: 100 miliardi all’anno = 300M al giorno

Possibili risposte

- Usiamo bitcoin solo come store of value
- Ingrandiamo i blocchi (quanti)
- Sviluppiamo i livelli successivi (lightning network)

Pianificare il governo per la blockchain: Teoremi, Rischi, Opportunità

Forme di Governo

- Bitcoin Governo del Fork (agree or fork off)
- Dash il voto dei masternode
- Tezos: Il codice che si autocambia

Diversi tipi di decisioni

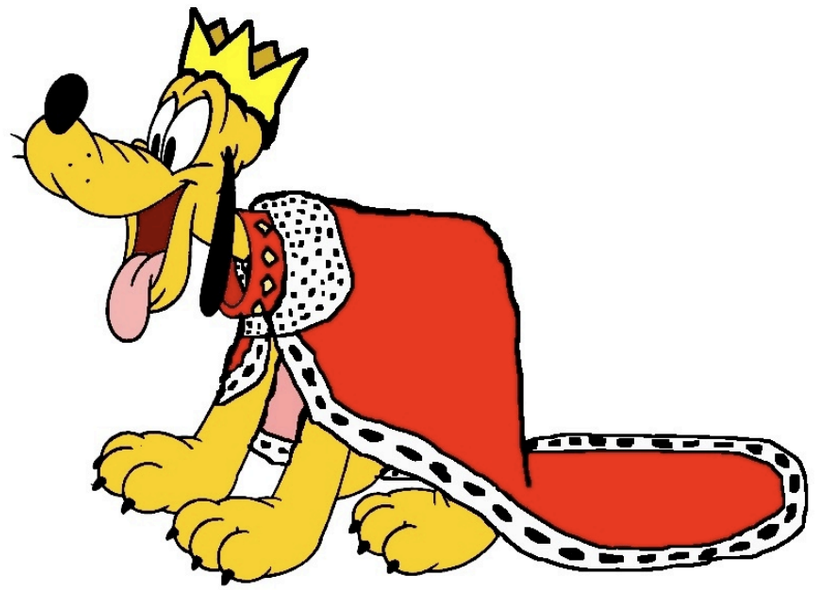
- Quale di queste due proposte?
- Male di queste n proposte?
- Quale valore per questo parametro?
- Trova la risposta giusta tra le infinite possibili?
- Eleggi un team per fare qualche cosa

Problema Aperto:
Come imponi la Consistenza?

Chi può votare

L’equilibrio tra Democrazia e Plutocrazia

- I Minatori
- I possessori di Masternodes
    - Quanto devono essere grandi i masternode?
- “stakeholders” (portatori di interessi)



PROBLEMA APERTO:
COME EVITARE CHE LE PERSONE VOTINO PIÙ VOLTE?

Decisioni
Decisioni
Decisioni

- Produzione di Moneta
- Cambiamenti del codice
- Quali progetti finanziare
- Altre micro decisioni?
- Quali comportamenti sono illegali?

PROBLEMA APERTO:
COME RENDI OPERATIVE LE DECISIONI?

Vincitori di Condorcet

- Elemento che vince tutte le “pairwise comparisons”

Condorcet Winner

- Elemento che vince tutte le “pairwise comparisons”

Possibile ordine di preferenza per
100 votanti su 5 candidati

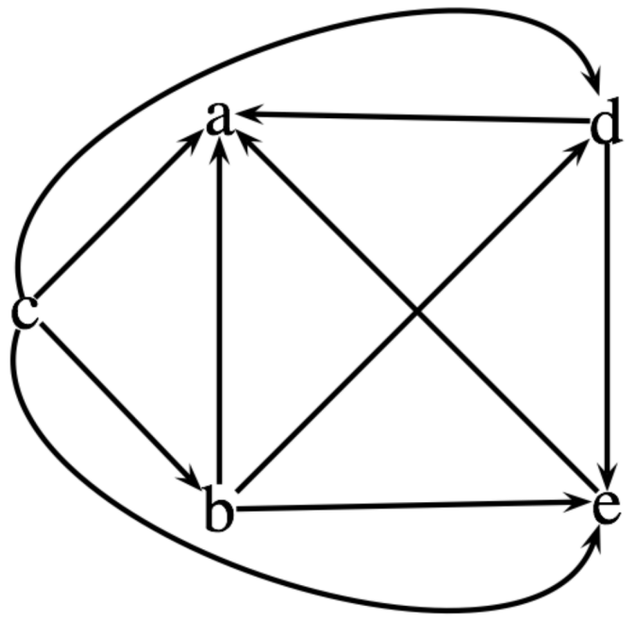
```
33 voti:  Alfio > Biagio >   Caio >   Dino >   Enzo;
16 voti: Biagio >   Dino >   Caio >   Enzo >  Alfio;
 3 voti:   Caio >   Dino > Biagio >  Alfio >   Enzo;
 8 voti:   Caio >   Enzo > Biagio >   Dino >  Alfio;
18 voti:   Dino >   Enzo >   Caio > Biagio >  Alfio;
22 voti:   Enzo >   Caio > Biagio >   Dino >  Alfio;
```

Condorcet Winner

Possible order of preferences for
100 people on 5 candidates

```
33 voti:  Alfio > Biagio >   Caio >   Dino >   Enzo;
16 voti: Biagio >   Dino >   Caio >   Enzo >  Alfio;
 3 voti:   Caio >   Dino > Biagio >  Alfio >   Enzo;
 8 voti:   Caio >   Enzo > Biagio >   Dino >  Alfio;
18 voti:   Dino >   Enzo >   Caio > Biagio >  Alfio;
22 voti:   Enzo >   Caio > Biagio >   Dino >  Alfio;
```

Caio è il vincitore di Condorcet

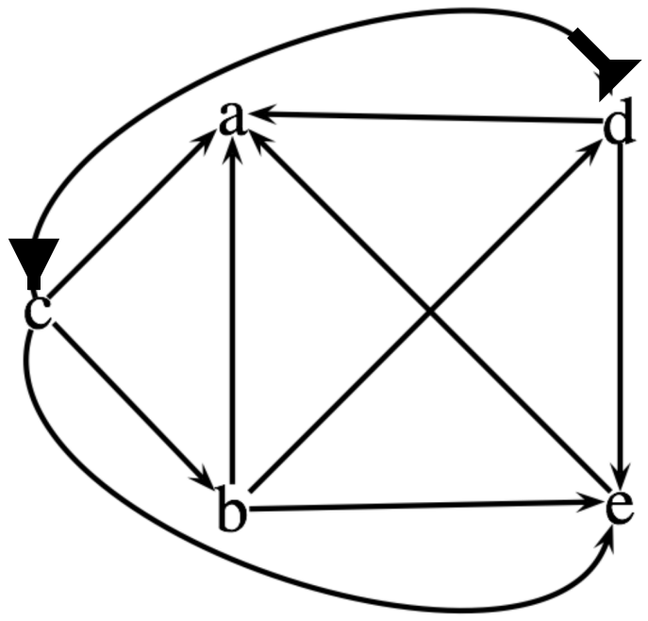


Non c’è sempre un vincitore di Condorcet

Basta che cambiamo l’ordine per 1 gruppo

```
33 votano:  Alfio > Biagio >   Dino >   Caio >   Enzo;
16 votano: Biagio >   Dino >   Caio >   Enzo >  Alfio;
 3 votano:   Caio >   Dino > Biagio >  Alfio >   Enzo;
 8 votano:   Caio >   Enzo > Biagio >   Dino >  Alfio;
18 votano:   Dino >   Enzo >   Caio > Biagio >  Alfio;
22 votano:   Enzo >   Caio > Biagio >   Dino >  Alfio;
```

Nessun vincitore di Condorcet



Vincitori di Condorcet

- Non sempre c’è un vincitore di Condorcet

- Quando c’è è considerato un risultato molto buono

- C’è un caso quando c’è sempre un Vincitore di Condorcet

PROBLEMA APERTO:
CHE SI FA SE NON C’É UN VINCITORE DI CONDORCET?

Teorema del Votante Mediano (Teorema di Black)

- In un'elezione dove la maggioranza dovrebbe vincere,
- Quando dobbiamo estrarre un valore da un insieme ordinato
- In cui tutti I voti hanno un loro valore preferito
- A apprezzano il risultato in maniera decrescente man mano che ci si allontana
- ALLORA
- Esiste sempre un vincitore di Condorcet
- È facile e possibile trovarlo (è la mediana dei valori preferiti).

PROBLEMA APERTO:
CHE SI FA SE CI SONO PIÙ DIMENSIONI O NESSUN ORDINE?

Referendum Unidimensionale

- Una domanda dove la risposta dovrebbe essere un valore su uno spazio unidimensionale (cioè un numero)
- È plausibile che ogni persona ha:
  - Il suo valore preferito
  - Una preferenza che decresce man mano che che ci allontaniamo da quel valore
- Un contesto in cui tutti conoscono il problema

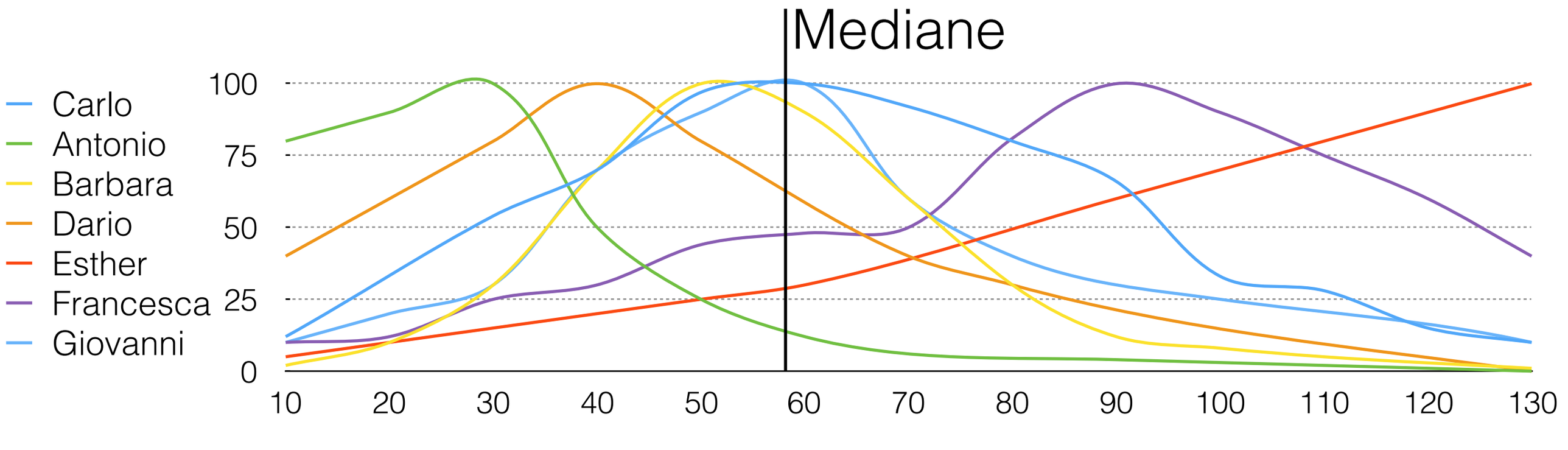
Esempio: Quale dovrebbe essere la velocità massima nelle strade statali?

p. \ v.	10	20	30	40	50	60	70	80	90	100	110	120	130
Antonio	80	90	**100**	50	25	12	6	5	4	3	2	1	0
Barbara	2	10	30	70	**100**	90	60	30	12	8	5	3	1
Carlo	12	32	54	70	97	**100**	92	80	66	33	28	15	10
Dario	40	60	80	100	80	60	40	30	20	15	10	5	0
Esther	5	10	15	20	25	30	40	50	60	70	80	90	**100**
Francesca	10	12	25	30	44	48	50	81	**100**	90	75	60	40
Giovanni	10	20	30	70	90	**100**	60	40	30	25	20	18	10

PROBLEMA APERTO:
CHE SI FA SE LE PERSONE NON CONOSCONO IL PROBLEMA?

Example: What should be the maximum speed on intercity streets

person\speed	10	20	30	40	50	60	70	80	90	100	110	120	130
Antonio	80	90	**100**	50	25	12	6	5	4	3	2	1	0
Barbara	2	10	30	70	**100**	90	60	30	12	8	5	3	1
Carlo	12	32	54	70	97	**100**	92	80	66	33	28	15	10
Dario	40	60	80	**100**	80	60	40	30	20	15	10	5	0
Esther	5	10	15	20	25	30	40	50	60	70	80	90	**100**
Francesca	10	12	25	30	44	48	50	81	**100**	90	75	60	40
Giovanni	10	20	30	70	90	**100**	60	40	30	25	20	18	10



Example: What should be the maximum speed on intercity streets

persona\velocita	10	20	30	40	50	60	70	80	90	100	110	120	130
Antonio	80	90	**100**	50	25	12	6	5	4	3	2	1	0
Barbara	2	10	30	70	**100**	90	60	30	12	8	5	3	1
Carlo	12	32	54	70	97	**100**	92	80	66	33	28	15	10
Dario	40	60	80	**100**	80	60	40	30	20	15	10	5	0
Esther	5	10	15	20	25	30	40	50	60	70	80	90	**100**
Francesca	10	12	25	30	44	48	50	81	**100**	90	75	60	40
Giovanni	10	20	30	70	90	**100**	60	40	30	25	20	18	10

persona\velocita	10	20	30	40	50	60	70	80	90	100	110	120	130
Massimi			1	1	1	2			1				1

We just need the favourite speed
for each person to know that the median is 60

Esperimento: Quale dovrebbe essere il limite oltre il quale le persone non hanno il permesso di pagare in cash?

03/11/2013 10:45:17	0
03/11/2013 11:05:19	50000
03/11/2013 12:36:39	5000
03/11/2013 12:46:07	10000000000
03/11/2013 12:48:05	10000
03/11/2013 12:59:46	20000
03/11/2013 15:43:23	5000
03/11/2013 15:51:00	5000
03/11/2013 20:58:06	5000
04/11/2013 07:34:40	666666666
04/11/2013 09:06:16	1000
04/11/2013 09:42:00	500
04/11/2013 11:20:12	250000
04/11/2013 11:20:15	0
04/11/2013 15:07:09	500
04/11/2013 16:38:58	50000
06/11/2013 13:45:27	999999999

0	500	1k	5k	10k	20k	50k	250K	666666666	999999999	10000000000
2	2	1	4	1	1	2	1	1	1	1

Esperimento: Quale dovrebbe essere il limite oltre il quale le persone non hanno il permesso di pagare in cash?

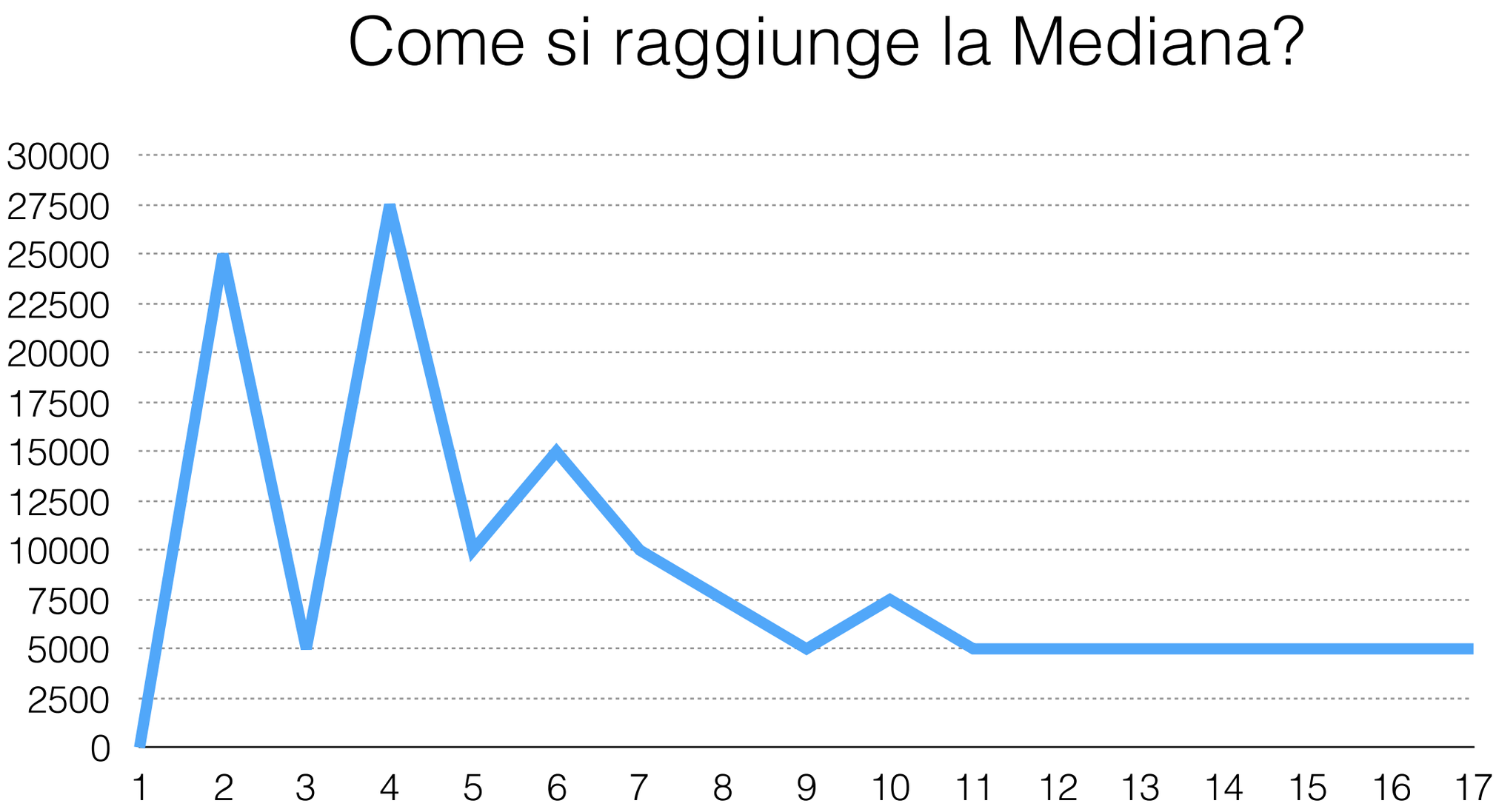
03/11/2013 10:45:17	0
04/11/2013 11:20:15	0
04/11/2013 09:42:00	500
04/11/2013 15:07:09	500
04/11/2013 09:06:16	1000
03/11/2013 12:36:39	5000
03/11/2013 15:43:23	5000
03/11/2013 15:51:00	5000
03/11/2013 20:58:06	**5000**
03/11/2013 12:48:05	10000
03/11/2013 12:59:46	20000
03/11/2013 11:05:19	50000
04/11/2013 16:38:58	50000
04/11/2013 11:20:12	250000
04/11/2013 07:34:40	666666666
06/11/2013 13:45:27	999999999
03/11/2013 12:46:07	10000000000

0	500	1k	5k	10k	20k	50k	250K	666666666	999999999	10000000000
2	2	1	4	1	1	2	1	1	1	1

In questo caso la mediana è 5000

Esperimento: Quale dovrebbe essere il limite oltre il quale le persone non hanno il permesso di pagare in cash?

0
25000
5000
27500
10000
15000
10000
7500
5000
7500
5000
5000
5000
5000
5000
5000
5000



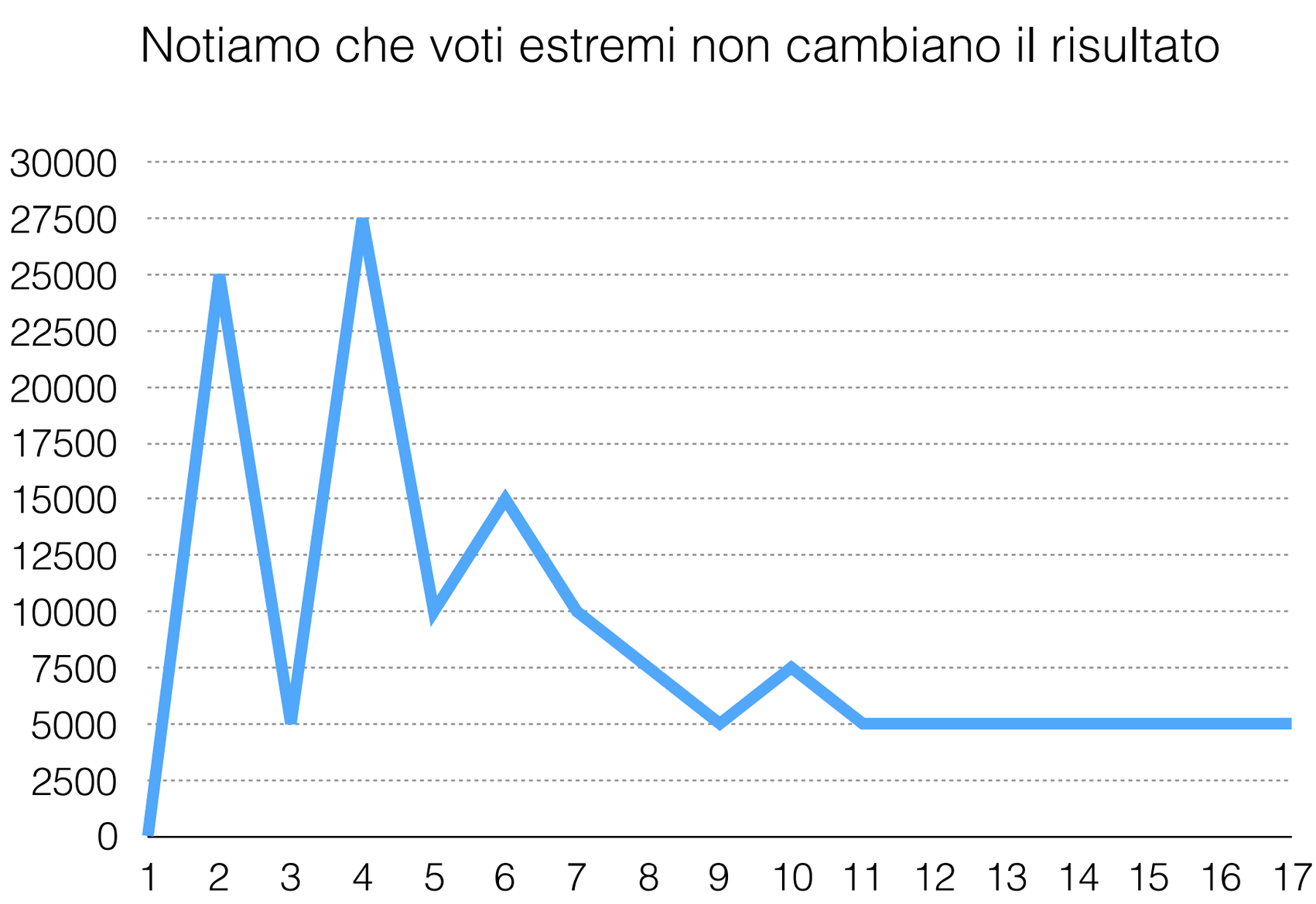
Poche persone sono sufficienti per avere un risultato stabile

Un sistema resistente al voto strategico

- Supponiamo che dobbiamo votare e ci aspettiamo il risultato essere x. Ma preferiremmo il risultato essere y>x=. Come possiamo massimizzare il risultato del nostro voto per approssimare y?
- Risposta: votando per y. Votando per qualsiasi altra cosa non aiuta.

Un sistema resistente al voto strategico

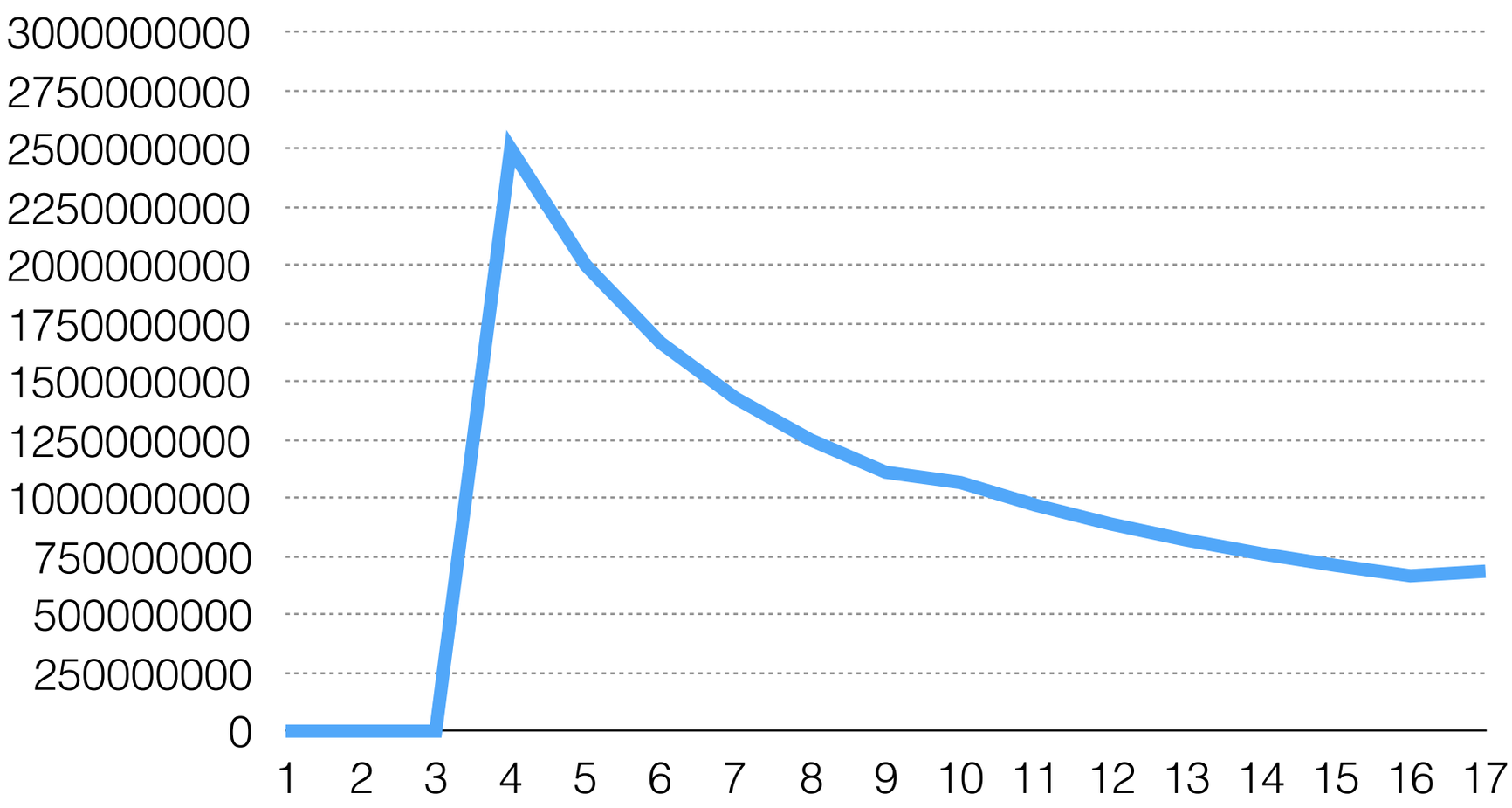
0	0
50000	25000
5000	5000
10000000000	27500
10000	10000
20000	15000
5000	10000
5000	7500
5000	5000
666666666	7500
1000	5000
500	5000
250000	5000
0	5000
500	5000
50000	5000
999999999	5000



Un sistema resistente al voto strategico

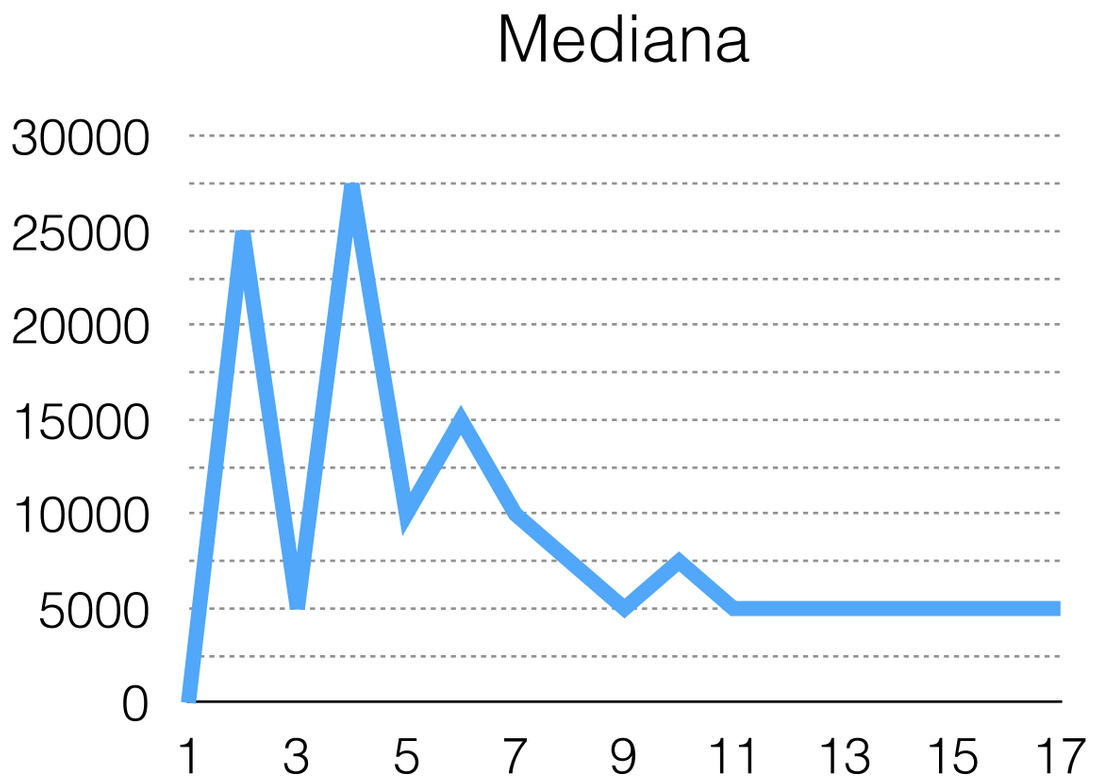
Che succede se si usa la Media?

0	0	0
50000	25000	25000
5000	5000	18333,33333
10000000000	27500	2500013750
10000	10000	2000013000
20000	15000	1666680833
5000	10000	1428584286
5000	7500	1250011875
5000	5000	1111122222
666666666	7500	1066676667
1000	5000	969706151,5
500	5000	888897347,2
250000	5000	820539858,9
0	5000	761929869
500	5000	711134577,7
50000	5000	666691791,6
999999999	5000	686298156,8



La Media con il tempo rimane soggetta ai voti degli estremisti

Un sistema resistente al voto strategico

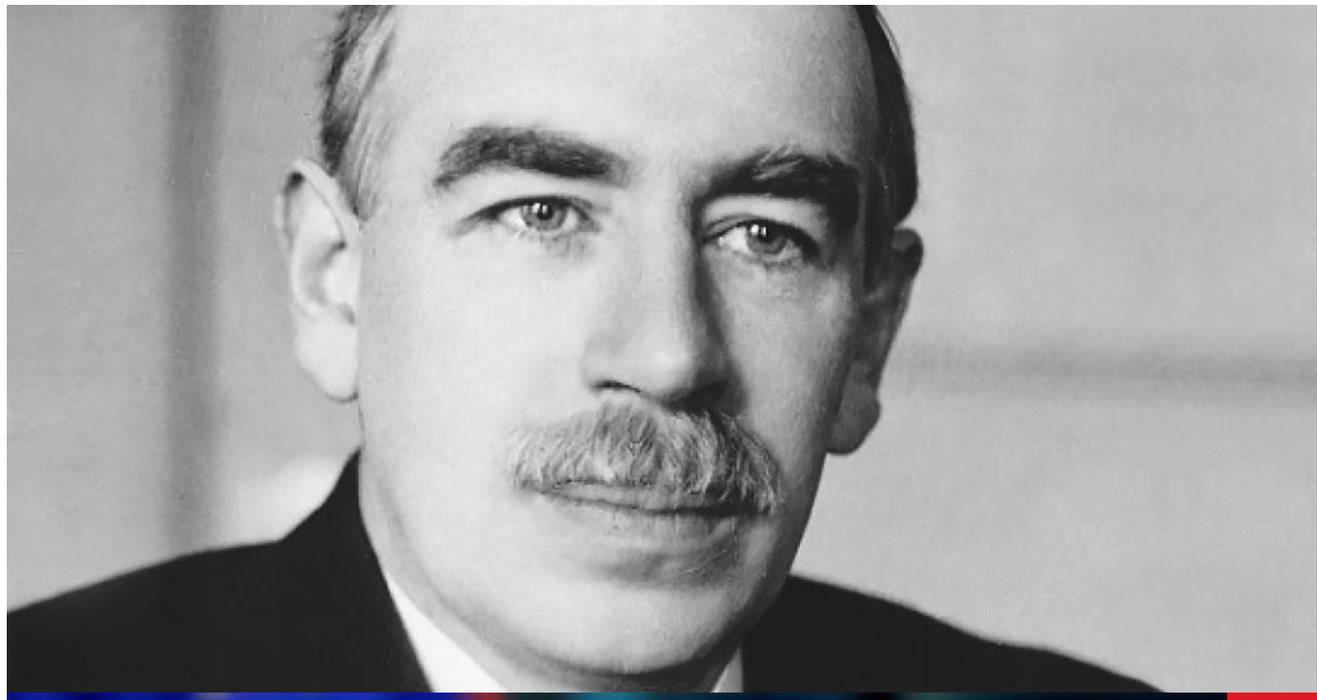


Votare per valori estremi non aiuta a raggiungere il proprio obiettivo

PROBLEMA APERTO:
E I PUNTI DI VISTA DELLE MINORANZE?

Quanti soldi stampare?

KEYNES

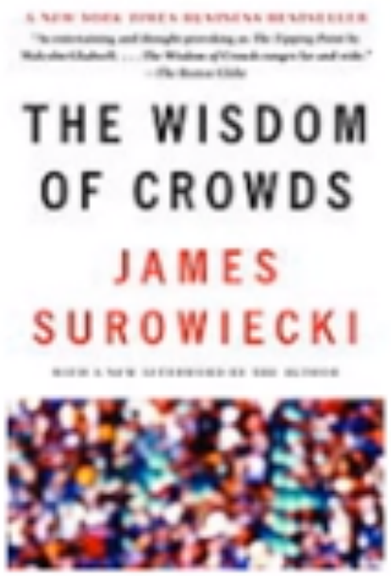


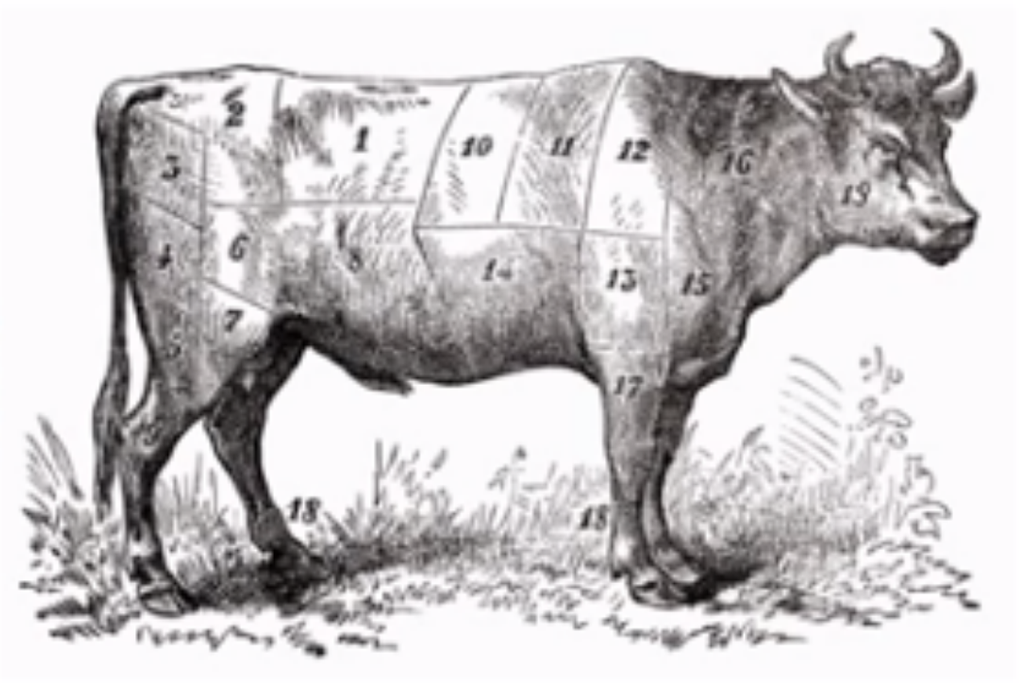
HAYEK

DRAGHI

“NAKAMOTO”

The Wisdom of Crowds





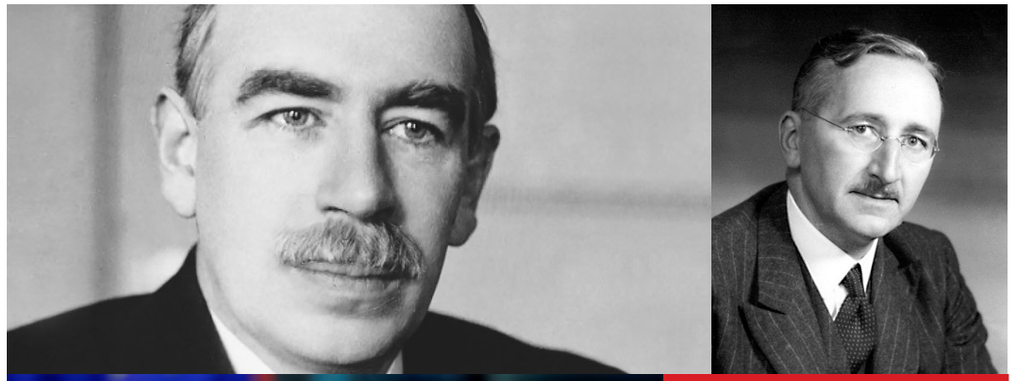
average of 800 guesses = 1,197

actual weight of the ox = 1,198

PROBLEMA APERTO:
IN QUALI CONTESTI É VERO?

Quanti soldi stampare?

- Permetti a tutti i Masternode di votare e prendi la mediana



Diversi tipi di decisioni

- Quale di queste due proposte? **Voto**
- Male di queste n proposte? **Voto di Condorcet**
- Quale valore per questo parametro? **Voto estraendo la Mediana**
- Trova la risposta giusta tra le infinite possibili? **Vilfredo per un Team**
- Eleggi un team per fare qualche cosa **Modified Approval Voting**

PROBLEMA APERTO:
CHI SINCRONIZZA TUTTO QUESTO?

Different Kind of Decisions

- Which of those 2 proposals? **Voting**
- Which of those n proposals? **Condorcet Voting**
- What value for a parameter? **Mediane Voting**
- Find the right answer (among infinite possible) **Vilfredo for a Team**
- Elect a team to do something **Modified Approval Voting**

Confrontati con un problema:

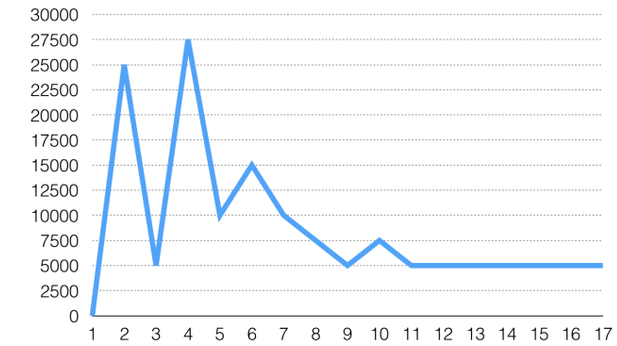
- Che sistema usare? (Q tipo 2)
- Quanto deve essere grande il team? (Q tipo 3)
- Chi dovrebbe essere nel Team? (Q tipo 5)

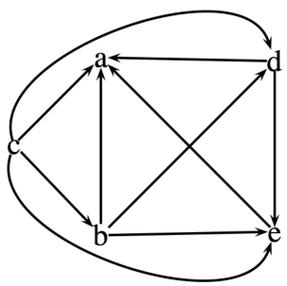
CONCLUSIONI

- Blockchain Governate stanno arrivando

- Ci sono molti problemi aperti

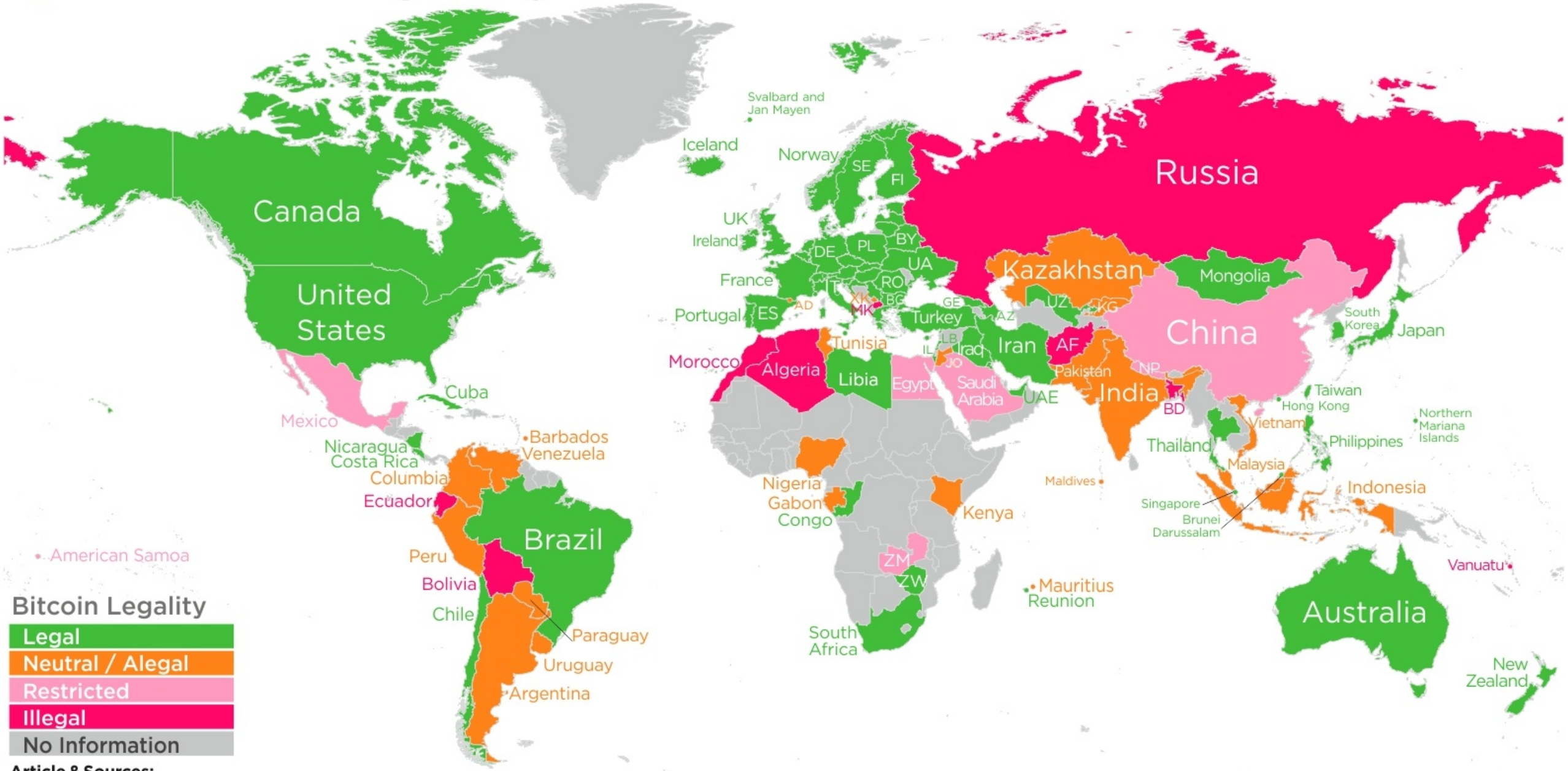
- Ma una volta installati sono difficili da cambiare
  (Ma si può iniziare una nuova blockchain)





- Which of those 2 proposals? **Voting**
- Which of those n proposals? **Condorcet Voting**
- What value for a parameter? **Mediane Voting**
- Find the right answer (among infinite possible) **Vilfredo for a Team**
- Elect a team to do something **Modified Approval Voting**

Bitcoin Legality Around the World



Bitcoin Legality

- Legal
- Neutral / Alegal
- Restricted
- Illegal
- No Information

Article & Sources:

https://howmuch.net/article/bitcoin-legality-around-the-world
https://coin.dance/poli

howmuch.net

5ª Lezione

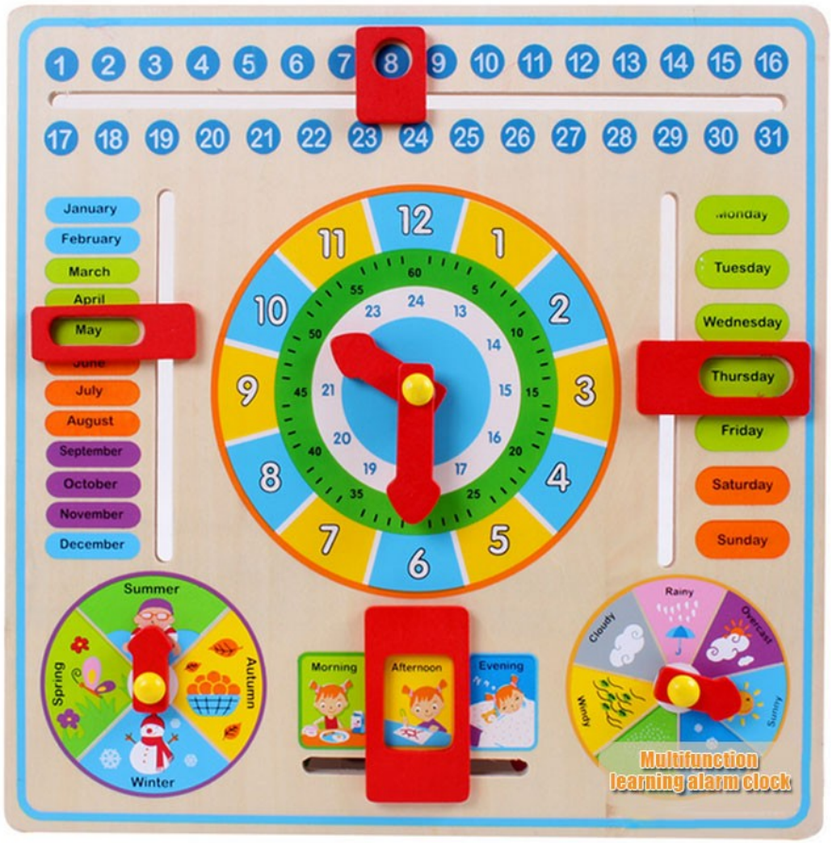
- Trading vs Investing
- Forme di Trading
- Indice di Kelly
- Trading Automatico
- Trading nelle crypto
- Valutazione di un investimento in bitcoin

Tempi

- Intraday
- Interday
- Cassettisti
- Lungo Periodo

Trading

Investimento



Investimento **Trading**

- Tempi
- Quantità
- Rischio
- Tempo investito

trading vs investimento

	Investimento	Trading
Cosa fanno	Selezionano le aziende di successo	Intercettano delle inefficienze del mercato
Risultato	Aiutano a distinguere le aziende di successo	Aiutano a rendere il mercato più efficiente

Grandezza investimenti

- 10’000’000
- 1’000’000
- 100’000
- 10’000
- 1’000
- 100

Non tutte le strategie funzionano ovunque

	Analisi Fondamentale		Analisi Tecnica
Investimento: Anni			
Cassettista: Mesi			
Trading: Giorni			
Trading: Ore			

Suggerimento Semplice

- Investi tutto in un ETF indicizzato sul mercato americano

- Analisi Fondamentale
- Analisi Tecnica
- Event Driven
- Un mix

“Two eyes see better than one”
Gregory Bateson, Mind and Nature

Forme di Trading

- Mean reverting
- Swing Trading
- Trend Following
- Momentum Trading
- Arbitrage
- …

Effetto del trading

- Mean reverting
- Swing Trading
- Trend Following
- Momentum Trading
- Arbitrage
- …

- Stabilizza i prezzi
- Chiude il canale
- Rende le onde più ripide (ma più corte?)
- ^^
- Sincronizza i prezzi
- …

Money Management

- Martingala
    - Aumenti l’investimento ogni volta che perdi

- Anti-martingala
    - Investi sempre la stessa percentuale

Può funzionare se la percentuale è giusta

Indice di Kelly

W = probabilità di vincere

(1-W) = probabilità di perdere

$$R = \frac{Guadagno \quad Medio}{Perdita \quad Media}$$

$$K = W - \frac{(1 - W)}{R}$$

Creazione di una strategia

- Idea
- Testarla sulla serie storica
- Ottimizzare i parametri
- Aggiungere commissioni
- Aggiungere Slippage
- Testarla su una serie successiva
- Metterla a mercato

Uomo-Macchina

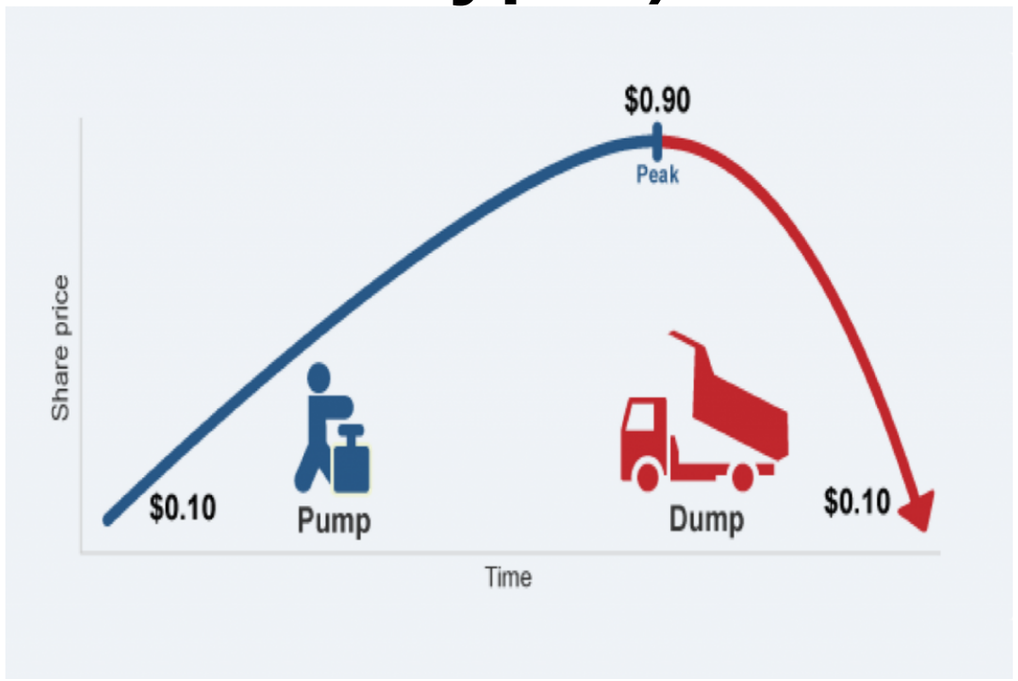
- Discrezionale
- Seguendo una strategia a mano
- Semi automatico
- Automatico
- Automatico su più strategie

Trading in Crypto

Le cripto non sono un mercato liquido

Cose illegali

(ma purtroppo comuni nel mondo Crypto)



- Pump and Dump

- Insider Trading

- Manipolazione del mercato

HODL

WHY AM I HOLDING? I'LL TELL YOU WHY. It's because I'm a bad trader and I KNOW I'M A BAD TRADER.

Yeah you good traders can spot the highs and the lows pit pat piffy wing wong wang just like that and make a million bucks sure no problem bro.

Likewise the weak hands are like
OH NO IT'S GOING DOWN I'M GONNA SELL he he he and then they're like OH GOD MY ASSHOLE when

the SMART traders who KNOW WHAT THE FUCK THEY'RE DOING buy back in but you know what? I'm not part of that group.

When the traders buy back in I'm already part of the market capital so GUESS WHO YOU'RE CHEATING day traders NOT ME~!

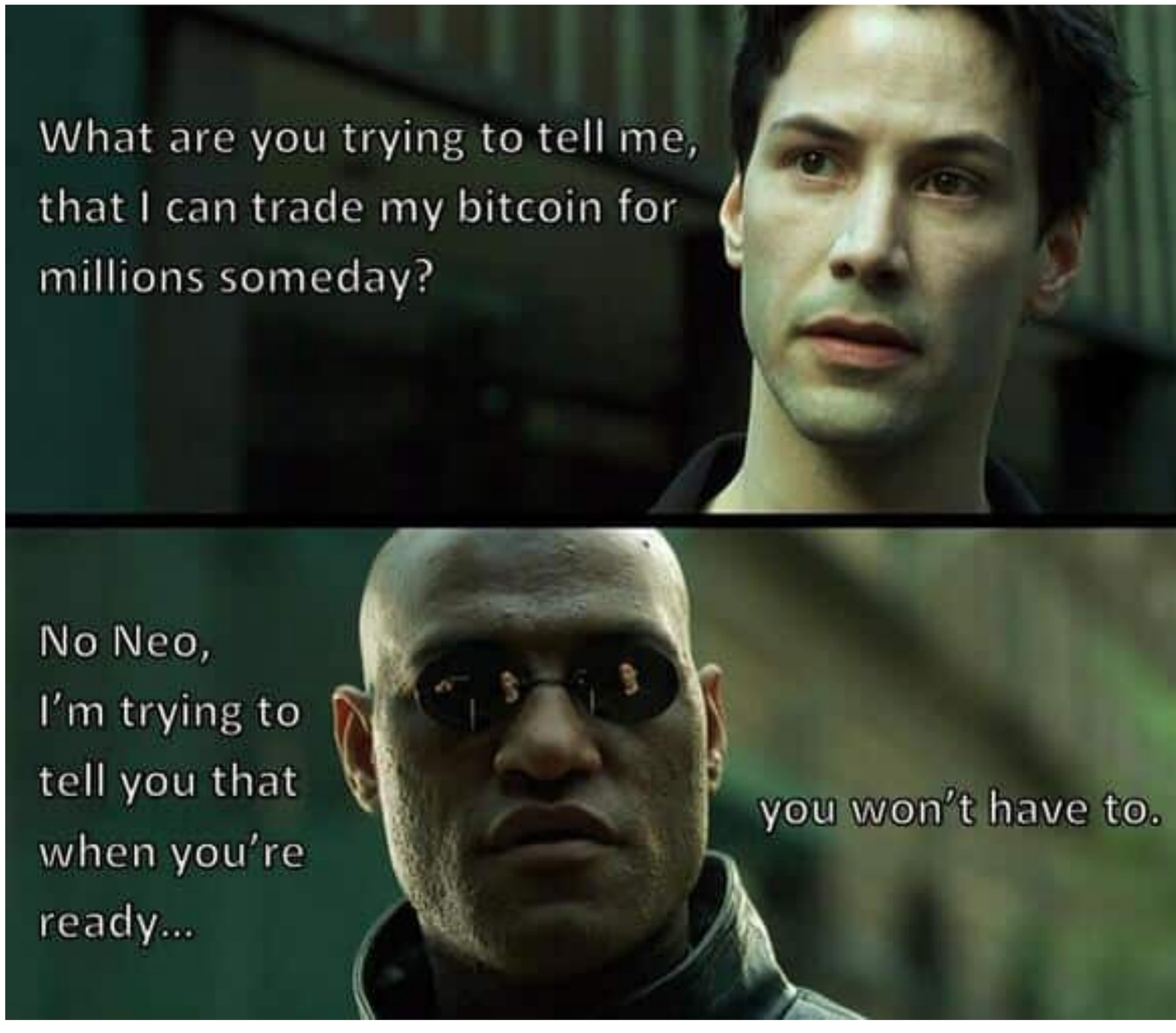
Those taunt threads saying "OHH YOU SHOULD HAVE SOLD" YEAH NO SHIT. NO SHIT I SHOULD HAVE SOLD. I SHOULD HAVE SOLD MOMENTS BEFORE EVERY SELL AND BOUGHT MOMENTS BEFORE EVERY BUY BUT YOU KNOW WHAT NOT EVERYBODY IS AS COOL AS YOU.
You only sell in a bear market if you are a good day trader or an illusioned noob.
The people in between hold.
In a zero-sum game such as this, traders can only take your money if you sell.

Altre tecniche

- Trading Automatico? (se sapete programmare…)
- ICO
- Seguire le mode
- Seguire i blogs
- Seguire le balene

Potrebbero i bitcoin diventare “grandi”

- Diventare la moneta di una nazione
- Diventare la riserva mondiale
- Diventare la moneta di più nazioni



Pagabile a vista al portatore

4 Modelli di Politica Monetaria

1. Si usa una moneta esterna che nessuno può controllare (oro)

2. La politica controlla la produzione della moneta

3. La produzione della moneta è indipendente e nelle mani di una persona che lavora per mantenere un’inflazione dell’1% / 2%.

4. La produzione della moneta è indipendente e nelle mani di un algoritmo che stampa una quantità finita di moneta

Valutiamo il caso: Potrebbero i bitcoin diventare lo standard mondiale?

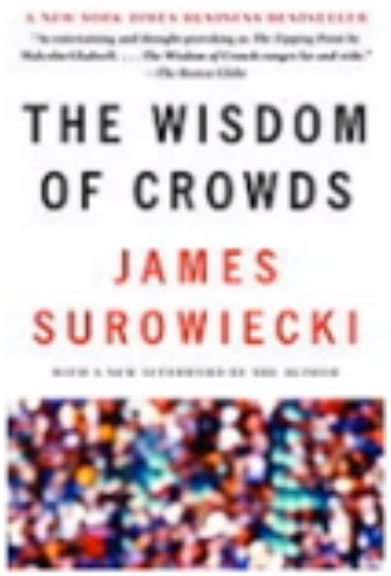
- Quanto varrebbe un bitcoin se fosse lo standard mondiale?
  - Oro ora: 7.7 migliaia di miliardi di dollari = 7.7×10^{12}
  - $\frac{7.7 \times 10^{12}}{21 \times 10^{6}} = 366'666.(6)$

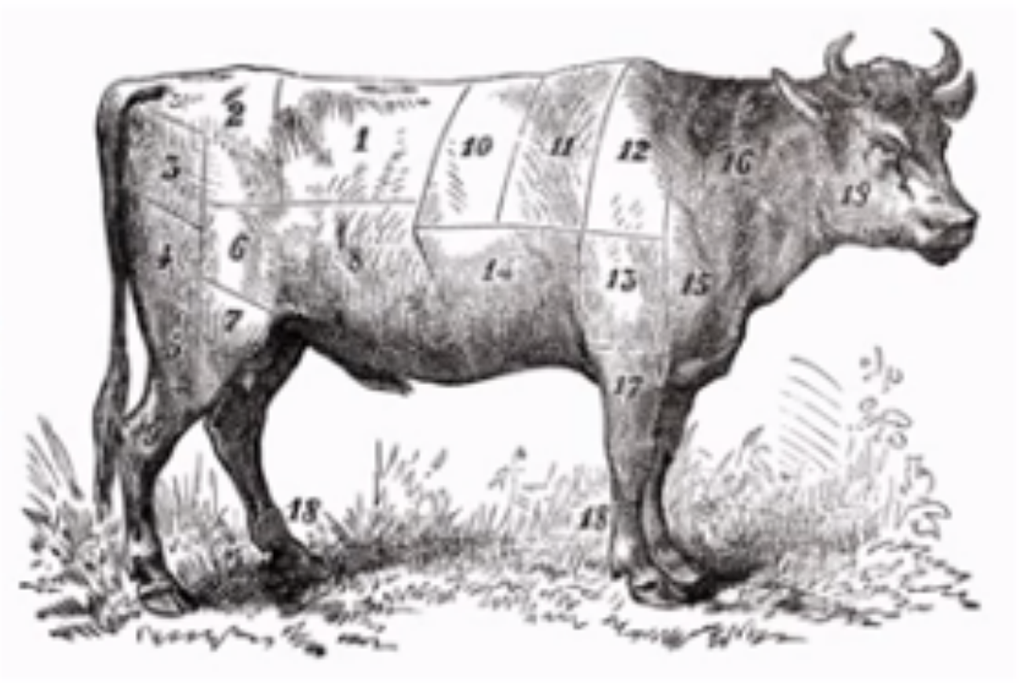
$$(\frac{366'666}{3929} - 1) \times 100 = 9'200\,\%$$

$$R = \frac{9200}{100} = 92$$

$$K = W - \frac{(1 - W)}{92}$$

The Wisdom of Crowds





average of 800 guesses = 1,197

actual weight of the ox = 1,198

PROBLEMA APERTO:
IN QUALI CONTESTI É VERO?

Vale la pena investire in bitcoin?

$$W - \frac{1 - W}{92} = 0$$

$$W = \frac{1 - W}{92}$$

$$92W = 1 - W$$

$$W = \frac{1}{93}$$

Se considerate che la probabilità che bitcoin diventi lo standard di riferimento internazionale sia maggiore dell'1.07% allora conviene investirci

$$K = W - \frac{(1 - W)}{92}$$

Conviene mettere i soldi in Bitcoin? Dipende da dove si vive:

Country	Inflation rate (consumer prices) (%)
Venezuela	4115.0
South Sudan	79.0
Suriname	55.0
Argentina	24.8
Ethiopia	23.4
Malawi	21.4
Burundi	18.0
Eritrea	17.0
Tanzania	15.3
Guinea	15.0
Uganda	14.7
Democratic Republic of the Congo	13.8
Marshall Islands	12.9
Mongolia	12.9
Maldives	12.8
Sierra Leone	12.6
Azerbaijan	12.4

Bibliografia

- **2008 - Whitepaper: Satoshi Nakamoto; bitcoin: A Peer-to-Peer Electronic Cash System**
- 2011 - Video: “We Use Coins”; What is Bitcoin? (V2)
- **2013 - Articolo: Michael Nielsen; How the Bitcoin protocol actually works**
- 2013 - Video: Scott Driscoll; How Bitcoin Works Under the Hood
- 2014 - Articolo: Ken Shirriff; Bitcoins the hard way: Using the raw Bitcoin protocol
- 2014 - Articolo: Ken Shirriff; Bitcoin mining the hard way: the algorithms, protocols, and bytes
- **2016 - FILM: Christopher Cannucciari; Banking on Bitcoin (Netflix)**
- **2017 - Book: Andreas Antonopolous; Mastering Bitcoin**
- **2018 - Book: Saifedean Ammous: The Bitcoin Standard**