Blockchains

Introduzione alla tecnologia blockchain, applicazioni, e prospettive future

Enrico Bacis

enrico.bacis@unibg.it

whoami

Enrico Bacis
---

enricobacis.com
enrico.bacis@unibg.it

Dottorando - Università degli Studi di Bergamo

* Database/Cloud/Mobile Security
* Encryption modes e Blockchains

Unibg Seclab - seclab.unibg.it

* Progetti europei su cloud data security

* Competizioni di (sicurezza) informatica
* Membro di BgLUG e Hacklab Bergamo

Agenda

Parte I

- **Cosa** è bitcoin
- **Perché** ha valore
- Principi di **funzionamento**
- **Come** vengono prodotti

Parte II

- Come si **acquistano** bitcoin
- Tipi di **portafogli**
- Come e dove **usarli**
- **Pericoli** e **Anonimato**

Parte III

- **Possibilità**
- **Smart contracts** e **ICO**

Parte I

Introduzione e punto di vista tecnico

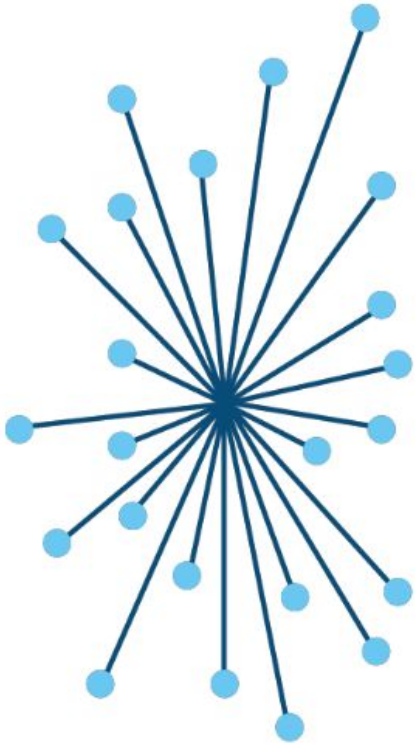
È possibile creare una moneta digitale senza una autorità centrale?

Questa domanda è rimasta senza risposta fino al 2008

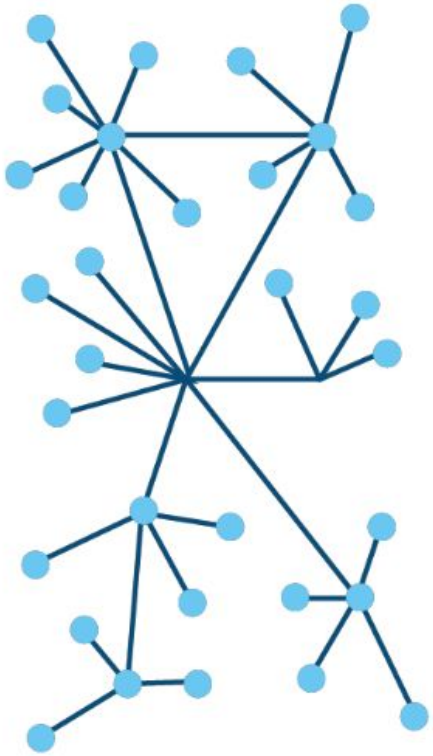
"What is needed is an electronic payment system based on **cryptographic proof instead of trust**, allowing any two willing parties to transact directly with each other **without the need for a trusted third party**."

- Satoshi Nakamoto

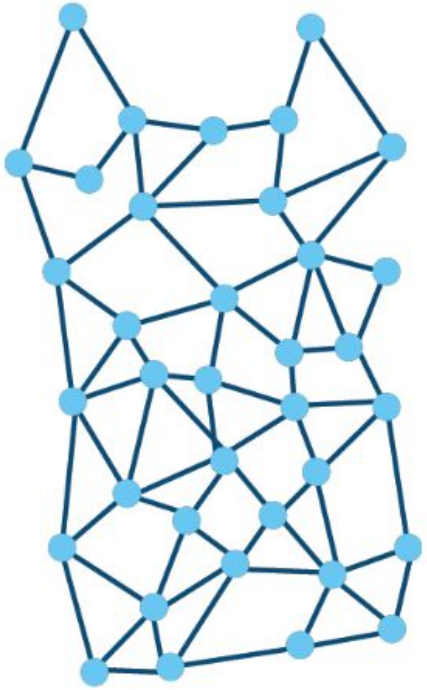
"*A peer-to-peer electronic cash system*" [2008]



Centralized



Decentralized



Distributed

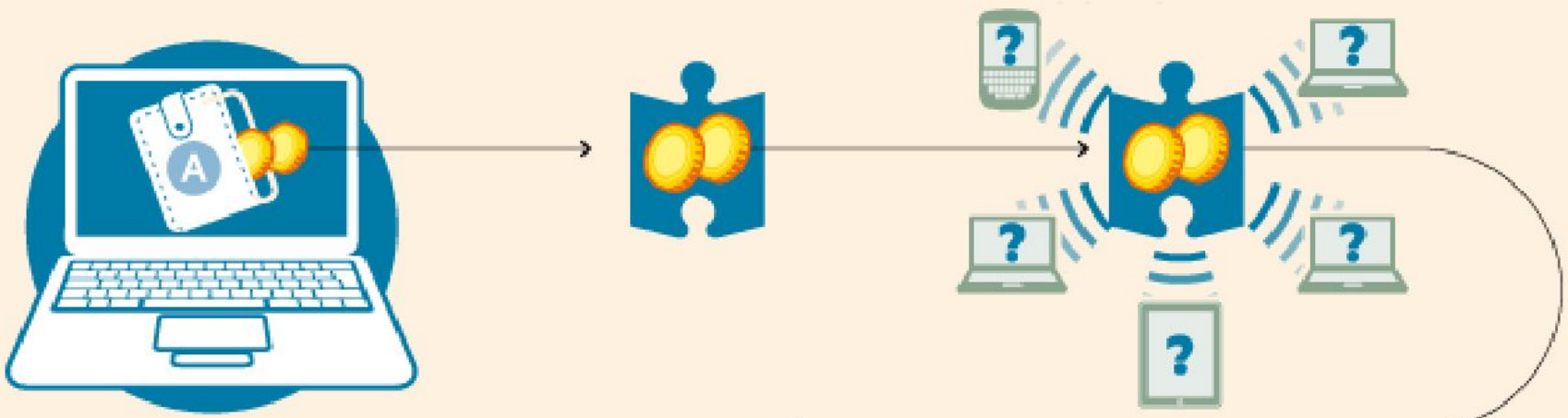
Cosa è Bitcoin?

un libro mastro (ledger)
pubblico e distribuito
basato sul consenso

1 A vuole inviare denaro a B

2 La transazione viene rappresentata come un 'blocco'

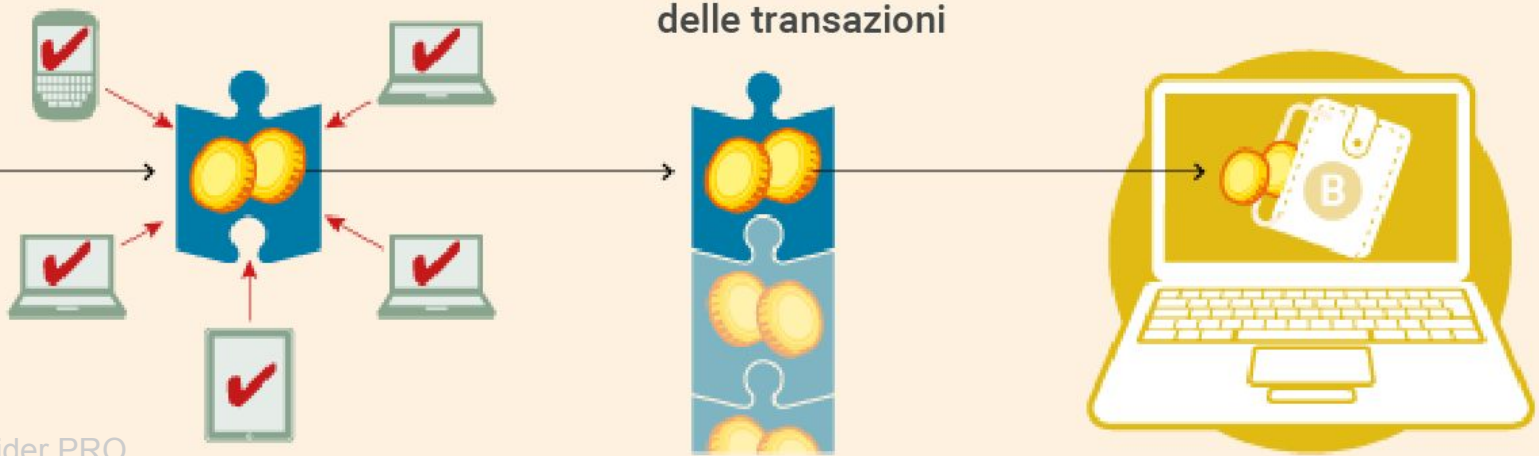
3 Il blocco viene trasmesso a ogni nodo della rete



4 I nodi nella rete approvano la transazione e la convalidano

5 Il blocco dopo può essere aggiunto alla catena, che fornisce un registro indelebile e trasparante delle transazioni

6 Il denaro va da A a B



Fonte: FT, Insider PRO

Chi ha creato Bitcoin?

Satoshi Nakamoto

- **31 Ottobre 2008**

  Satoshi Nakamoto pubblica l'articolo *"A peer-to-peer electronic cash system"*

- **3 Gennaio 2009**

  Satoshi pubblica il codice sorgente di Bitcoin

- **23 Aprile 2011**

  Satoshi dice "*Moved onto other things*" e sparisce ...

  … senza più utilizzare il suo patrimonio di 980,000 bitcoins

Are you Satoshi?

Dorian Nakamoto

- Informatico Giapponese
- Nel 2014 la rivista Newsweek dice di avere le prove del fatto che lui sia Satoshi
- *“I am not Dorian Nakamoto”*
  - satoshi

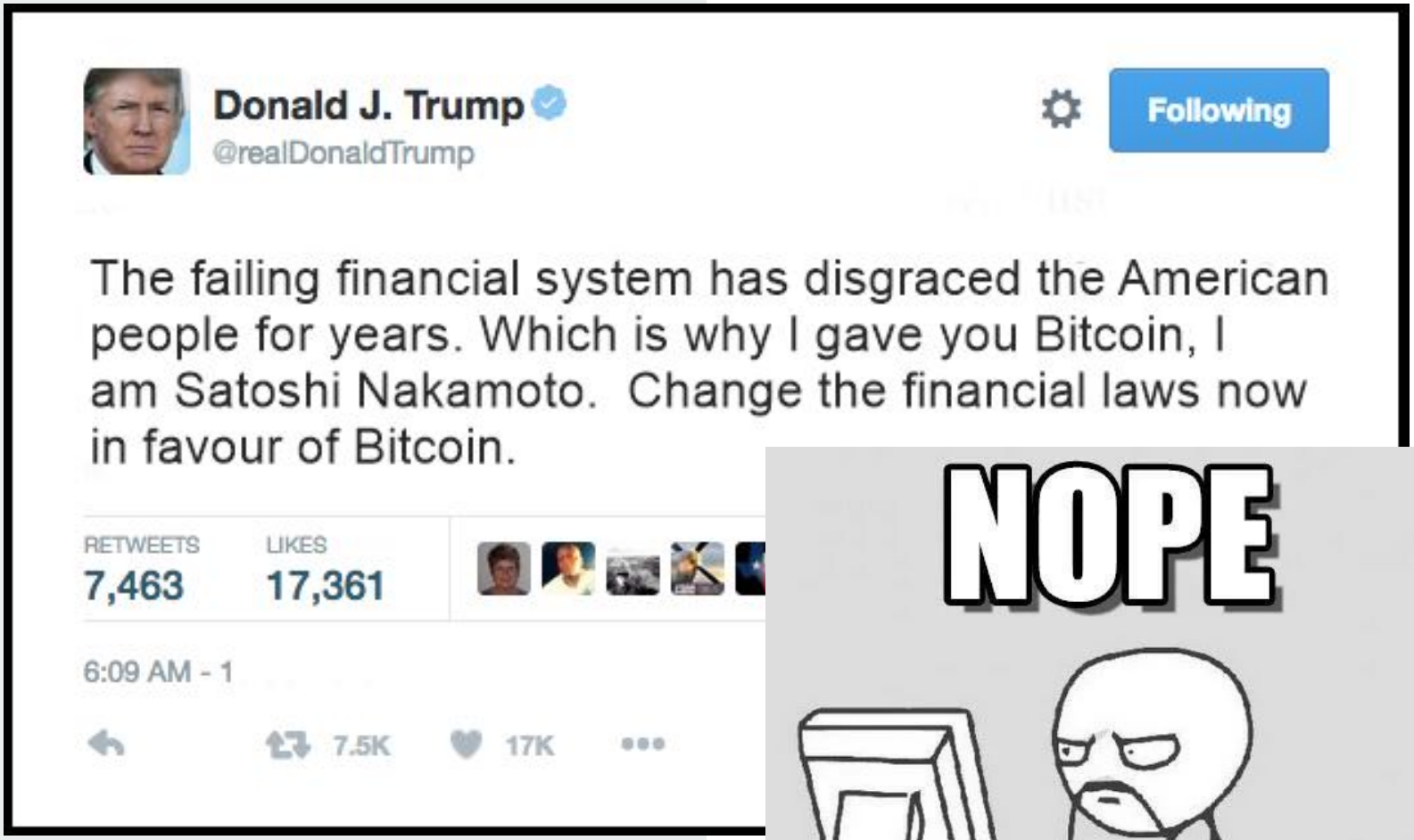
Are you Satoshi?

Craig Wright

- Informatico Australiano
- Nel 2016 si proclama l’inventore di Bitcoin
- Fallisce il Satoshi Test
- Nel 2018 viene denunciato per aver rubato 5 miliardi di dollari in Bitcoin

¯_(ツ)_/¯

Are you Satoshi?



Are you Satoshi?

- I dati del suo account lo ritraggono come un uomo di 38 anni che vive in Giappone.
- Estremamente esperto di programmazione in C++, economia, crittografia e reti peer-to-peer.
- Scrive in inglese perfetto. Il suo primo post usa spelling americano, tutti gli altri britannico.
- Legge il *"The Times"*.
- La sua attività non si concentra in un particolare fuso orario.

Si pensa che Satoshi Nakamoto sia lo pseudonimo del gruppo di individui che hanno creato Bitcoin.

Are you Satoshi?

Hal Finney

Dorian Nakamoto

… and many others ...

Perché Bitcoin ha valore?

1. Ha valore tutto ciò
   a cui diverse persone
   attribuiscono valore.

Il primo acquisto in Bitcoin

17 Maggio 2010
Laszlo Hanyecz posta una richiesta per comprare della pizza con Bitcoin

22 Maggio 2010
Laszlo conferma di aver effettuato una transazione di 10,000 BTC per queste due pizze.

2010: Valore di 10,000 BTC = 41 $
2018: Valore di 10,000 BTC = **60,000,000 $**

Il 22 Maggio si commemora il **Bitcoin Pizza Day**

1. Ha valore tutto ciò
   a cui diverse persone
   attribuiscono valore.

2. È sia ***commodity*** (*bene*) che
currency (*moneta di scambio*)

commodity

VS

Commodity - Bitcoin vs Oro

	Bitcoin	Oro
Risorsa Scarsa	Il numero massimo di Bitcoin in circolazione è fisso	Può ancora essere estratto in quantità difficilmente stimabili
Duraturo	Decentralizzato -> sopravviverebbe ad un attacco nucleare	Ft. Knox no *Punto fusione oro: 1064 gradi* *Esplosione nucleare: 10^7 gradi*
Portabile	Può essere inviato istantaneamente, utilizzando una connessione	Pesante e deve essere dichiarato
Divisibile	Può essere diviso in 100 milioni di pezzi (1 satoshi = 10^-8 bitcoin)	Non può essere diviso in altrettante parti senza distruggerne parte
Verifica di Autenticità	Può essere verificato con algoritmi	Richiede un occhio esperto e test chimici

Commodity - Bitcoin vs Oro

	Bitcoin	Oro
Conservazione	Bisogna solo salvare le chiavi di cifratura	Conservazione difficile per grandi quantità
Fungibile	Tutti i bitcoin sono uguali, per ognuno si ha la storia completa	Diversi livelli di purezza
Contraffazione	Matematicamente non fattibile	L'oro non può essere contraffatto, ma i lingotti possono essere manomessi
Uso Diffuso	Utilizzato come commodity, inizia ad essere utilizzato come currency	Una volta era una currency, ora solo una commodity (conserva valore)

currency

VS

Currency - Bitcoin vs Dollaro

	Bitcoin	Dollaro
Risorsa Scarsa	Il numero massimo di Bitcoin in circolazione è fisso	Esistono 10 trilioni $ (1.2 circolanti). La Federal Reserve ha triplicato la Monetary Base dal 2008
Duraturo	Bitcoin sono stati persi e rubati, ma mai deteriorati	Le banconote si deteriorano (e vengono sostituite)
Portabile	Può essere inviato istantaneamente, utilizzando una connessione	È facile trasportare denaro contante. Grosse somme richiedono infrastruttura.
Divisibile	Può essere diviso in 100 milioni di pezzi (1 satoshi = 10^-8 bitcoin)	1 dollaro può essere diviso in 100 parti
Verifica di Autenticità	Può essere verificato con algoritmi	La validità della banconota può essere verificata con test ottici / chimici

Currency - Bitcoin vs Dollaro

	Bitcoin	Dollaro
Conservazione	Bisogna solo salvare le chiavi di cifratura	Conservazione difficile per grandi quantità
Fungibile	Tutti i bitcoin sono uguali, e si conosce la storia completa	Le banconote sono intercambiabili, E non si conosce la storia completa
Contraffazione	Matematicamente non fattibile	La contraffazione delle banconote è una pratica che si combatte da sempre
Uso Diffuso	Utilizzato come commodity, inizia ad essere utilizzato come currency	La valuta assume valore per via di un decreto governativo

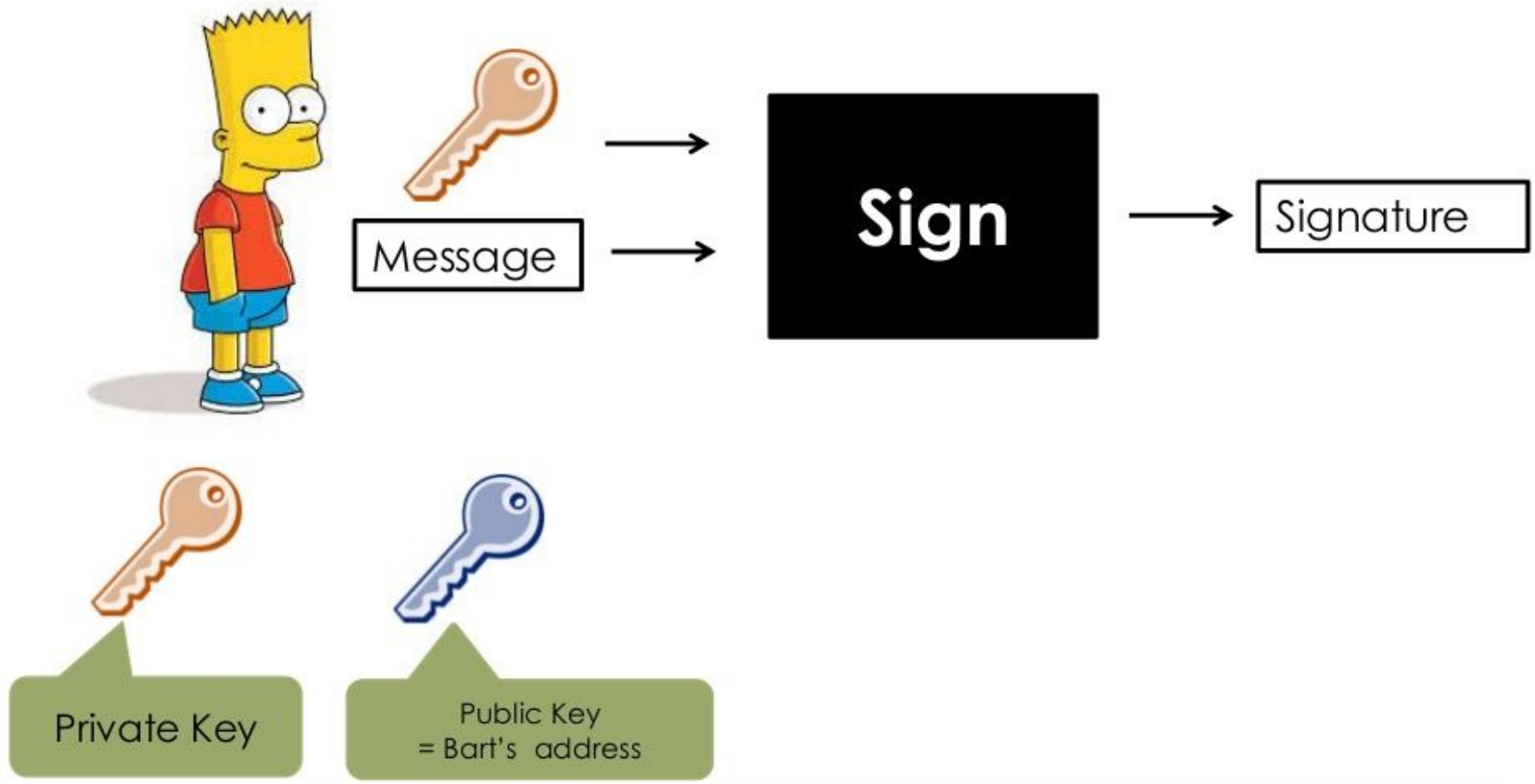
Blockchain e Bitcoin

Principi di Funzionamento

Concetti Base e Terminologia

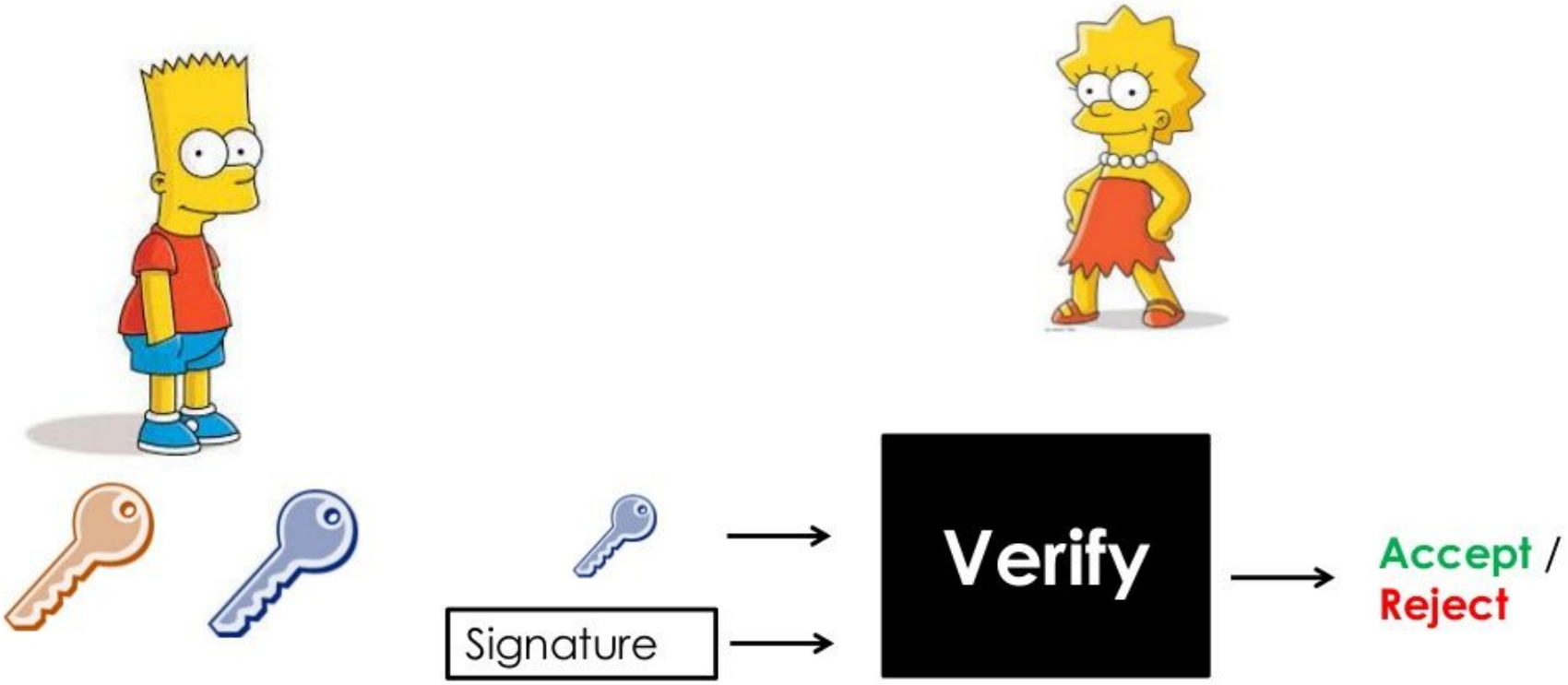
1. Crittografia asimmetrica e firme digitali
2. Indirizzi Bitcoin
3. Blocchi e Transazioni
4. Hash e Controllo di integrità
5. Proof-of-Work e Blockchain
6. Mining

Crittografia asimmetrica e firme digitali



[https://www.slideshare.net/philippecamacho/how-to-explain-bitcoin-to-your-mother]

Crittografia asimmetrica e firme digitali



[https://www.slideshare.net/philippecamacho/how-to-explain-bitcoin-to-your-mother]

Crittografia asimmetrica e firme digitali

Non negabile
(non-repudiable)

Non falsificabile
(unforgeable)

[https://www.slideshare.net/philippecamacho/how-to-explain-bitcoin-to-your-mother]

Indirizzi Bitcoin

Un indirizzo Bitcoin è una chiave pubblica (base-58)

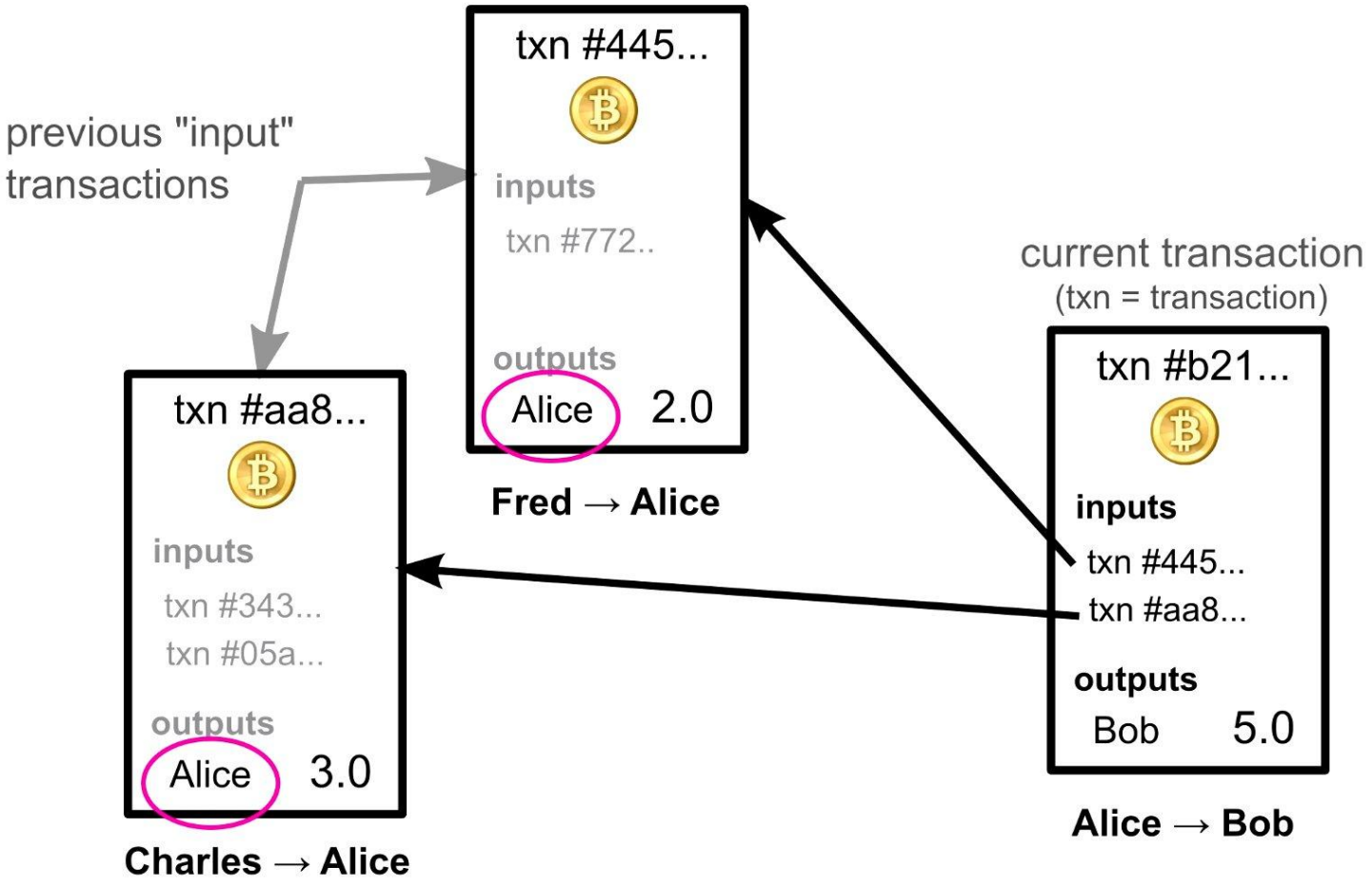
`13NpLwXgEP8d9NpDUHptY6BypFRNXHL3tr`

La chiave privata corrispondente permette di firmare delle transazioni dove si spendono i Bitcoin associati alla chiave pubblica

Indirizzi Bitcoin possono essere creati da chiunque

www.bitaddress.org

Transazioni

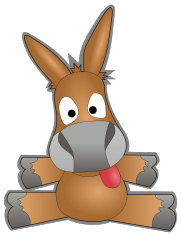


https://blockchain.info

Invio delle transazioni

Peer-to-Peer Network (P2P)

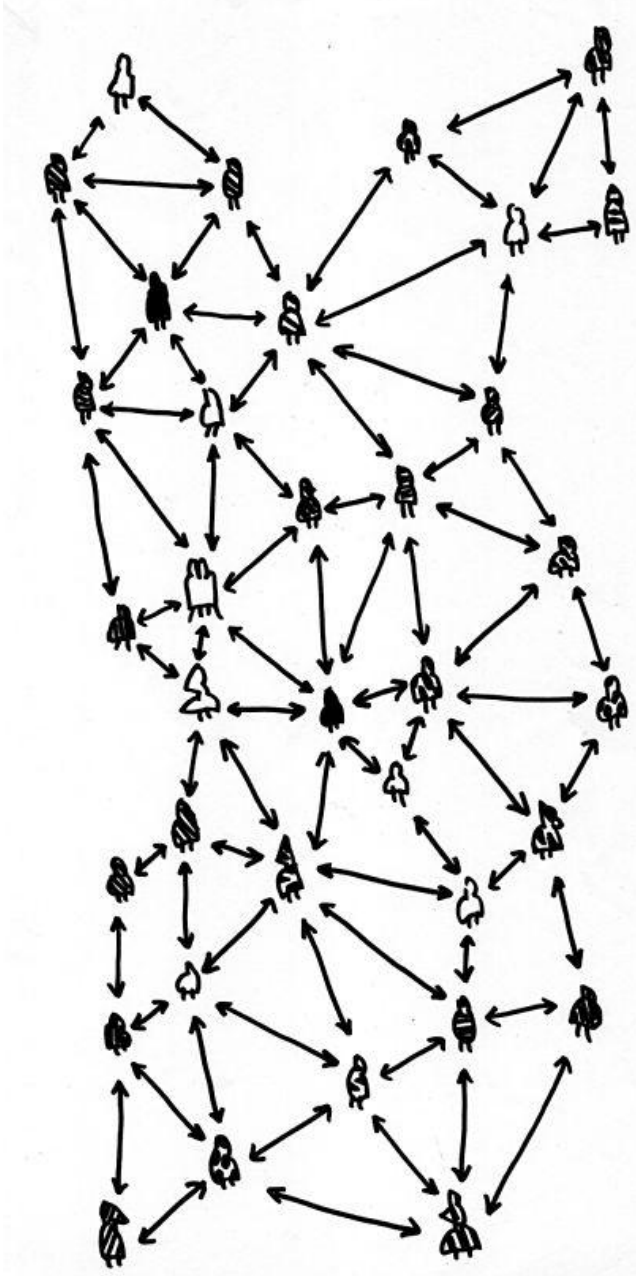
- Le transazioni valide vengono inviate agli altri peers
- In pochi secondi tutti i nodi vengono a conoscenza della transazione



BitTorrent™

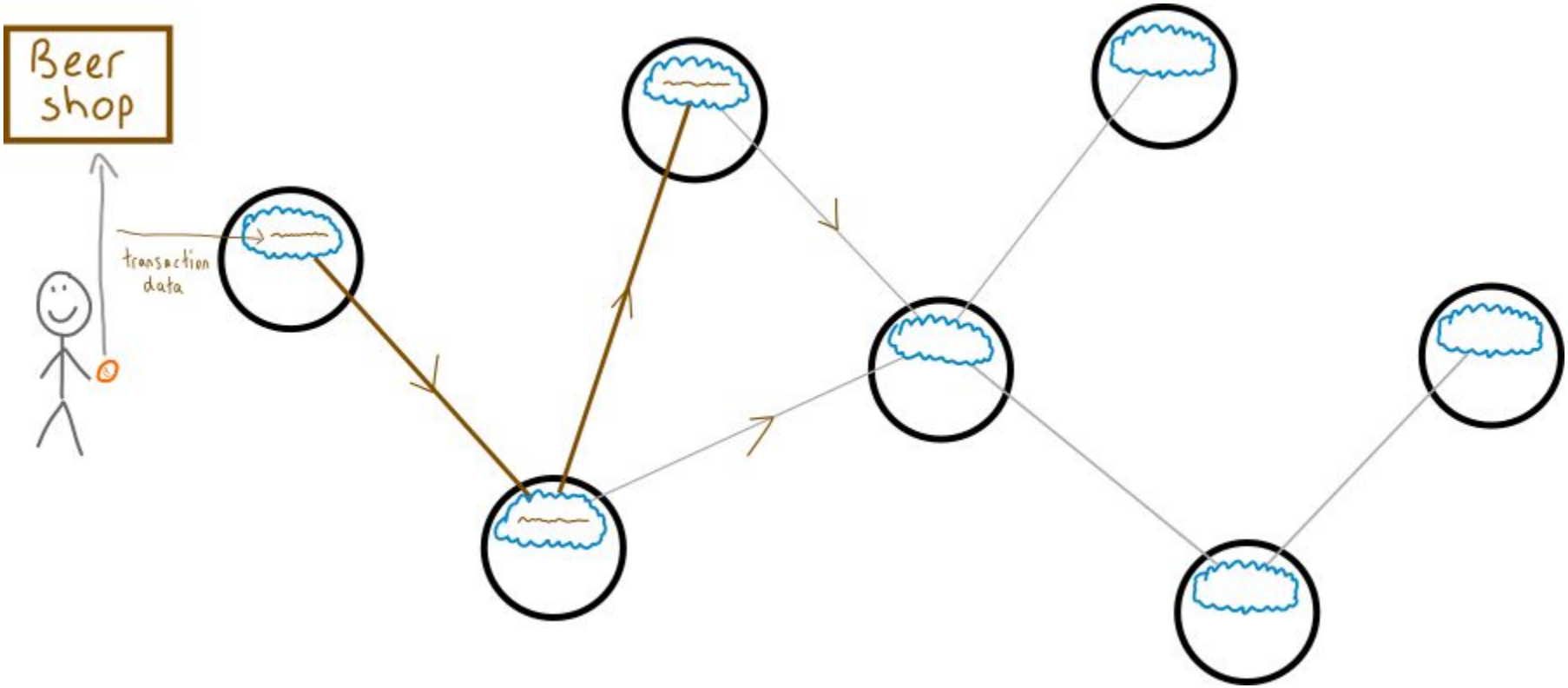
Come evitare spam e attacchi Denial of Service (DoS)

- Le transazioni vengono validate prima di essere inoltrate



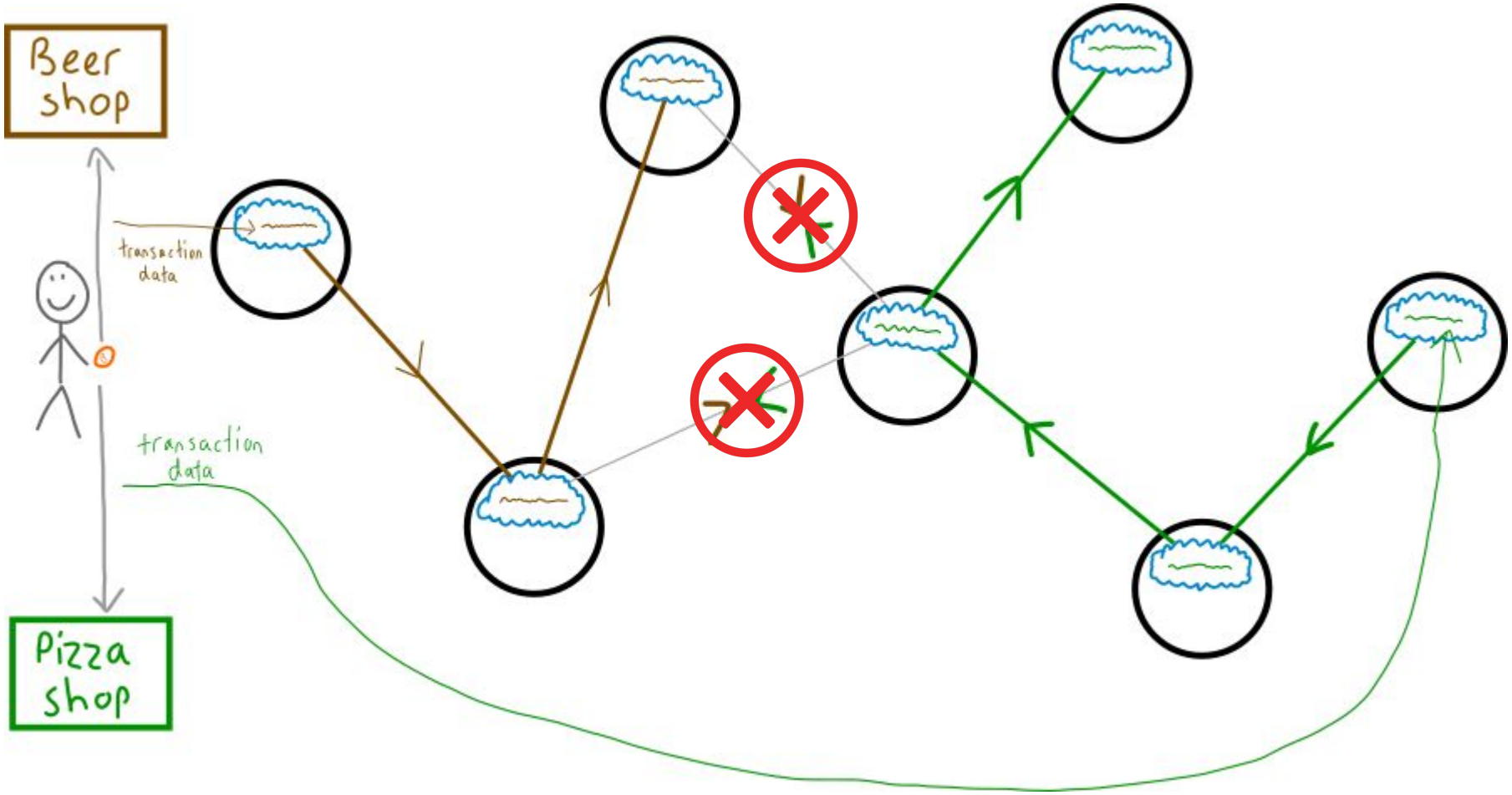
Il problema del Double Spending

Double Spending



[http://learnmeabitcoin.com/guide/mining]

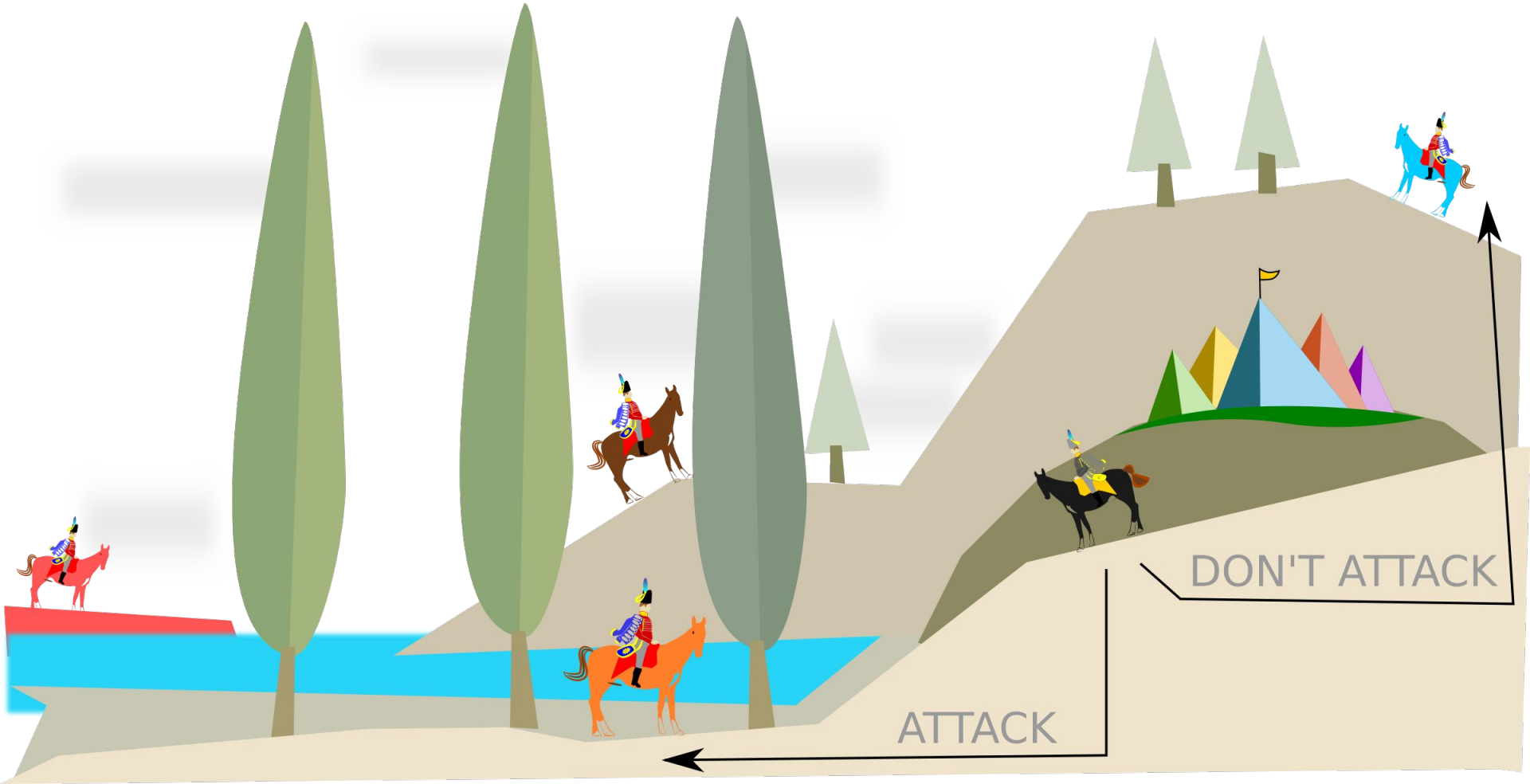
Double Spending



[http://learnmeabitcoin.com/guide/mining]

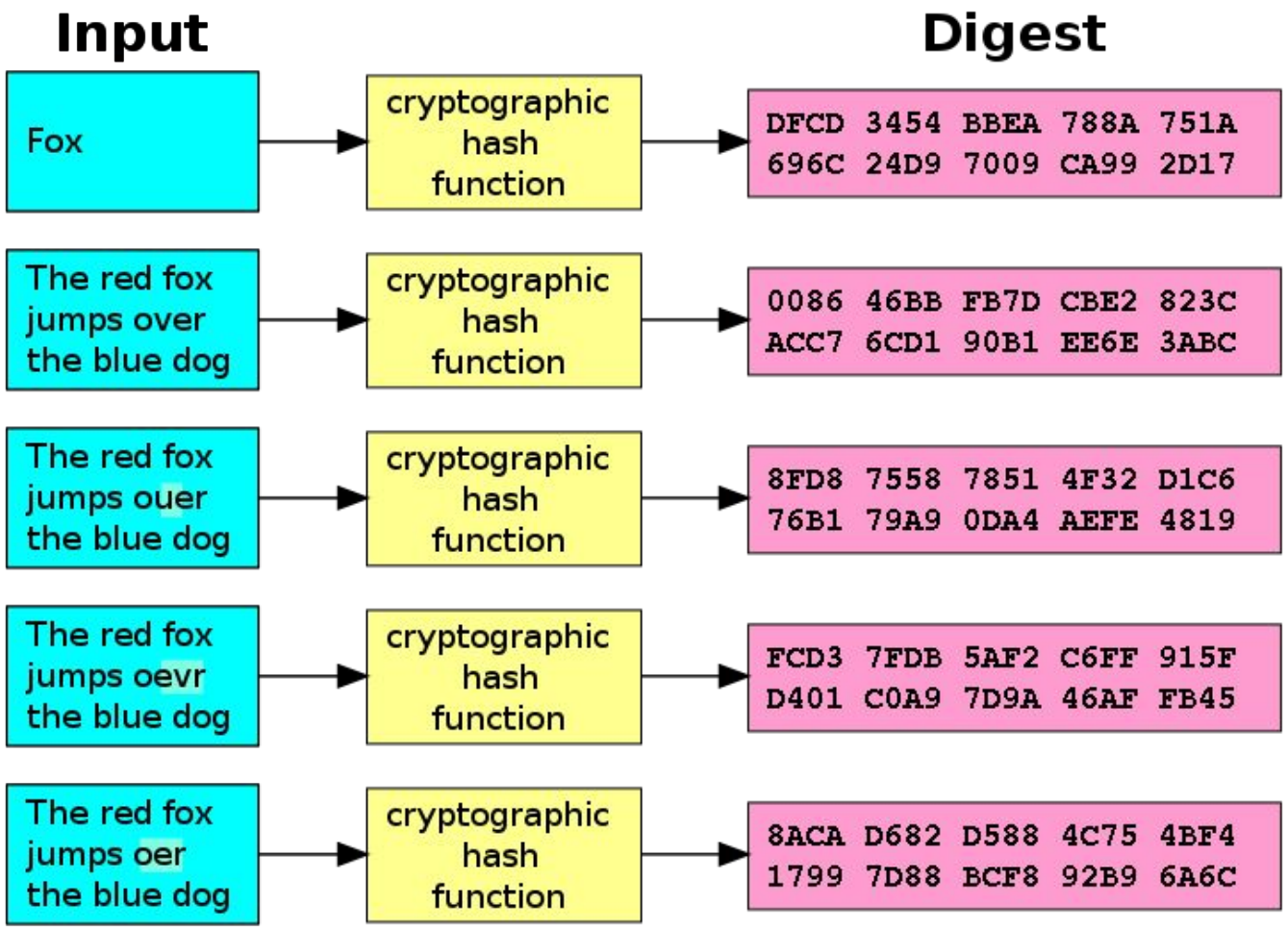
Come raggiungere il consenso in una rete distribuita?

Problema dei Generali Bizantini



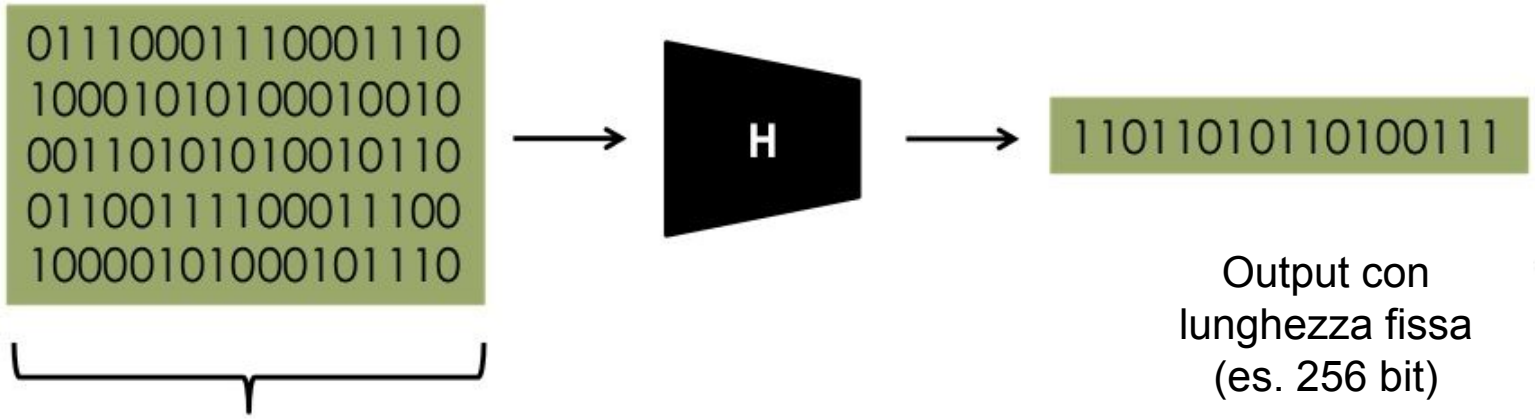
Blockchain for the win

Hash e Controllo di Integrità



[https://en.wikipedia.org/wiki/Cryptographic_hash_function]

Hash e Controllo di Integrità



- Una modifica di 1 bit in input produce grandi (impredicibili) effetti in output
- Trovare l'inversa è matematicamente non fattibile
- Trovare delle collisioni è matematicamente non fattibile

[https://www.slideshare.net/philippecamacho/how-to-explain-bitcoin-to-your-mother]

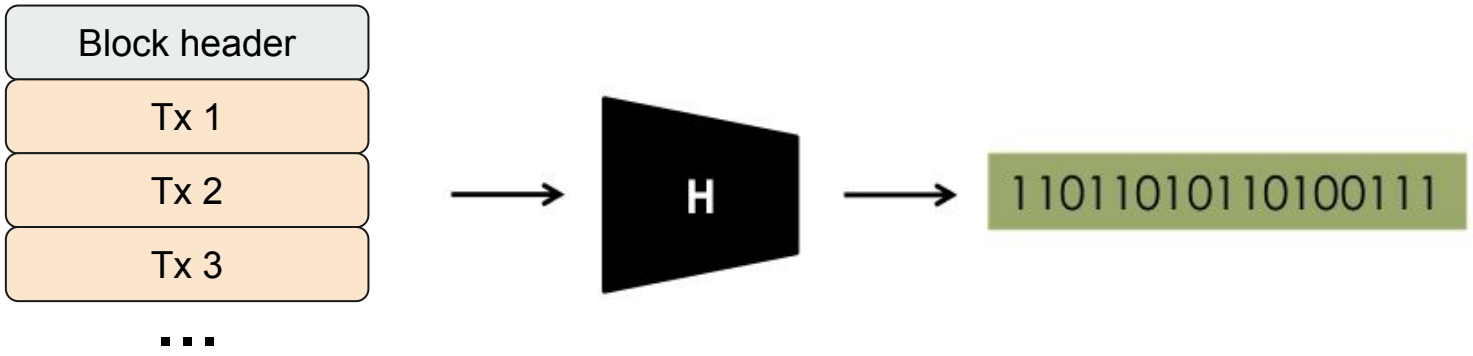
“if every computer ever made by humanity was computing since the beginning of the entire universe, up to now, the odds that they would have found a collision is still infinitely small.

So small that it’s way less than the odds that the Earth will be destroyed by a giant meteor in the next two seconds.”

Blocco

Mettiamo tutte le transazioni in un blocco ...

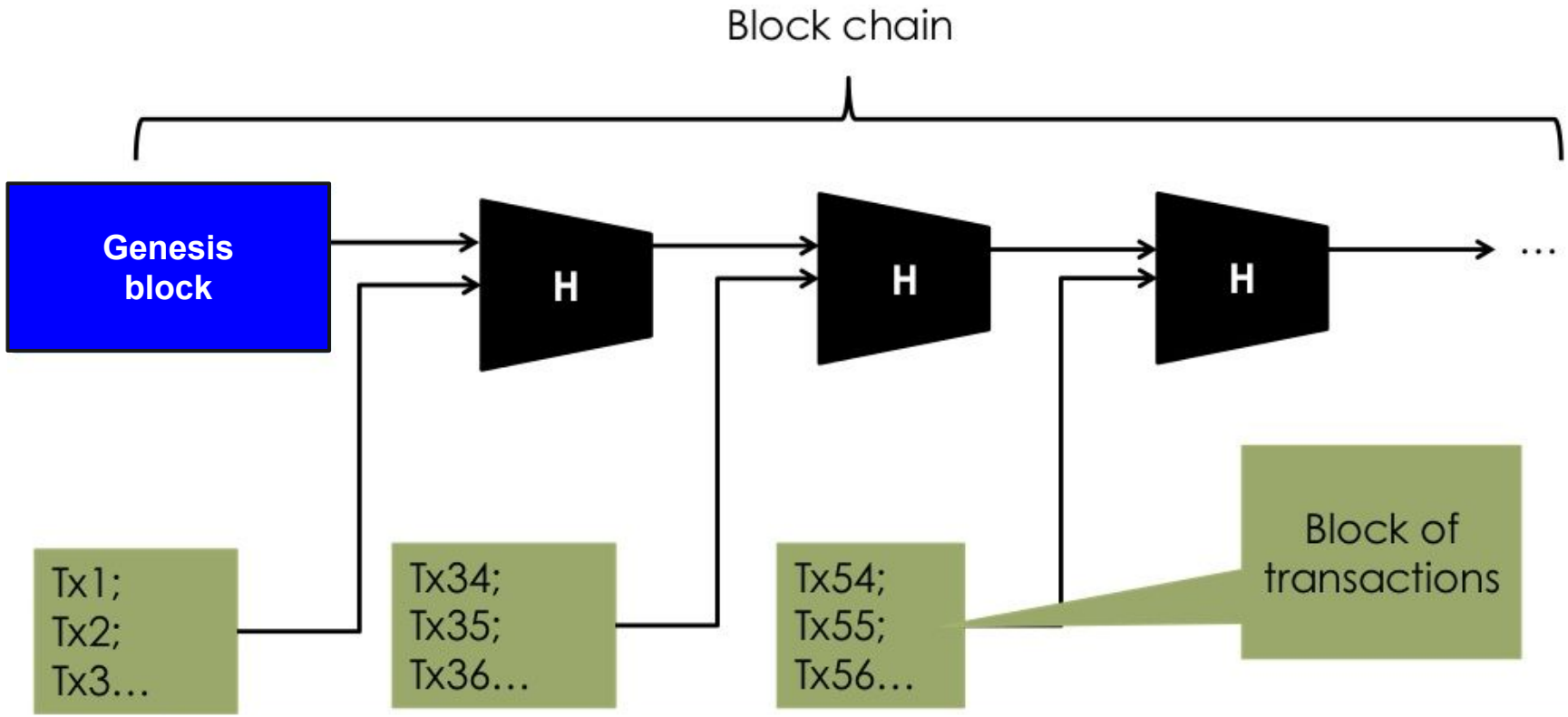
... e usiamo questo come input della funzione hash



Blocco di transazioni

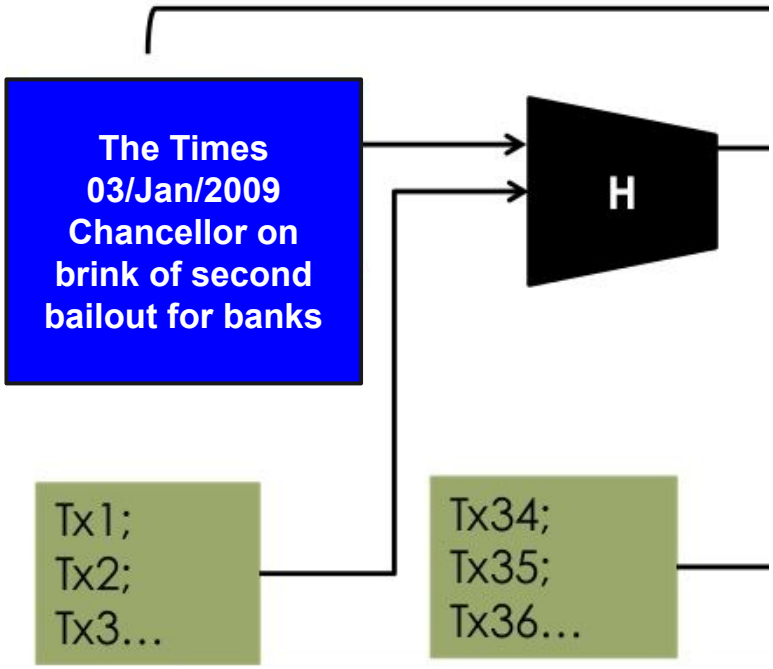
https://blockchain.info

Blockchain



[https://www.slideshare.net/philippecamacho/how-to-explain-bitcoin-to-your-mother]

Bitcoin Genesis



THE TIMES

Max 5C, min -5C | Saturday January 3 2009 timesonline.co.uk No 69523 | £1.50

Eat Out from £5

More than 900 great restaurants, including four **Gordon Ramsay** favourites from £15

Start collecting tokens today Pullout inside

Israel prepares to send tanks and troops into Gaza

Israel allowed foreigners to flee the Gaza Strip as it prepared for a ground offensive. At least 430 Palestinians were killed in a week of airstrikes News, page 3

Chancellor on brink of second bailout for banks

Billions may be needed as lending squeeze tightens

Francis Elliott Deputy Political Editor
Gary Duncan Economics Editor

Alistair Darling has been forced to consider a second bailout for banks as the lending drought worsens.

The Chancellor will decide within weeks whether to pump billions more into the economy as evidence mounts that the £37billion part-nationalisation last year has failed to keep credit flowing. Options include cash injections, offering banks cheaper state guarantees to raise money privately or buying up "toxic assets", The Times has learnt.

The Bank of England revealed yesterday that, despite intense pressure, the banks curbed lending in the final quarter of last year and plan even tighter restrictions in the coming months. Its findings will alarm the Treasury.

The Bank is expected to take yet more aggressive action this week by cutting the base rate from its current level of 2 per cent. Doing so would reduce the cost of borrowing but have little effect on the availability of loans.

Whitehall sources said that ministers planned to "keep the banks on the boil" but accepted that they need more help to restore lending levels. Formally, the Treasury plans to focus on state-backed guarantees to encourage private finance, but a number of interventions are on the table, including further injections of taxpayers' cash.

Under one option, a "bad bank" would be created to dispose of bad debts. The Treasury would take bad loans off the hands of troubled banks, perhaps swapping them for government bonds. The toxic assets, blamed for poisoning the financial system, would be parked in a state vehicle or "bad bank" that would manage them and attempt to dispose of them while "detoxifying" the mainstream banking system.

The idea would mirror the initial proposal by Henry Paulson, the US Treasury Secretary, to underpin the American banking system by buying

Continued on page 6, col 1
Leading article, page 2

99p

Pub chain cuts the price of a pint from £1.69 to 1989 levels
Business, page 47

Michael Sheen
Frost, Nixon and me
Magazine

Working mums
So that's how she does it
Body&Soul

Detox in style
The best spas on the planet
Travel

Salmon Rushdie
I Won't Marry Again
Pages 22, 23

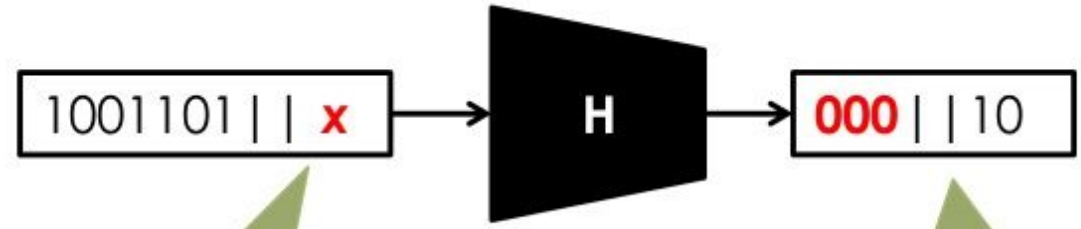
Giant Killing?
Guide to the FA Cup Third Round
Sport

[https://www.slideshare.net/philippecamacho/how-to-explain-bitcoin-to-your-mother]

Come ordinare le transazioni?

Rallentando la generazione dei blocchi

Proof-of-Work (PoW)



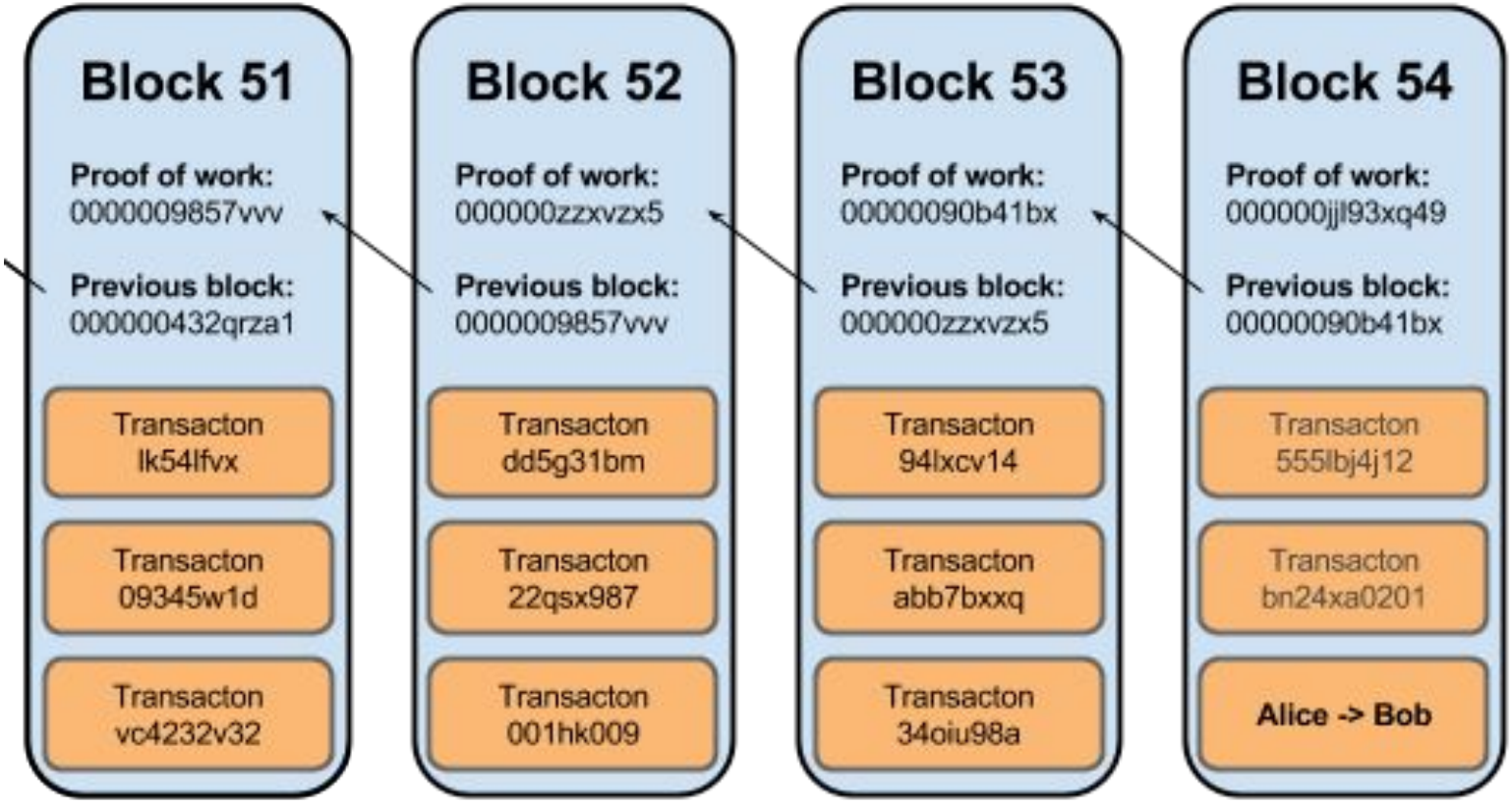
Trova il numero casuale (nonce) x tale per cui l'output inizi con n zeri

L'unico modo (*) per trovare una x per cui l'output inizi con n zeri è quello di provare circa 2^{n-1} possibilità

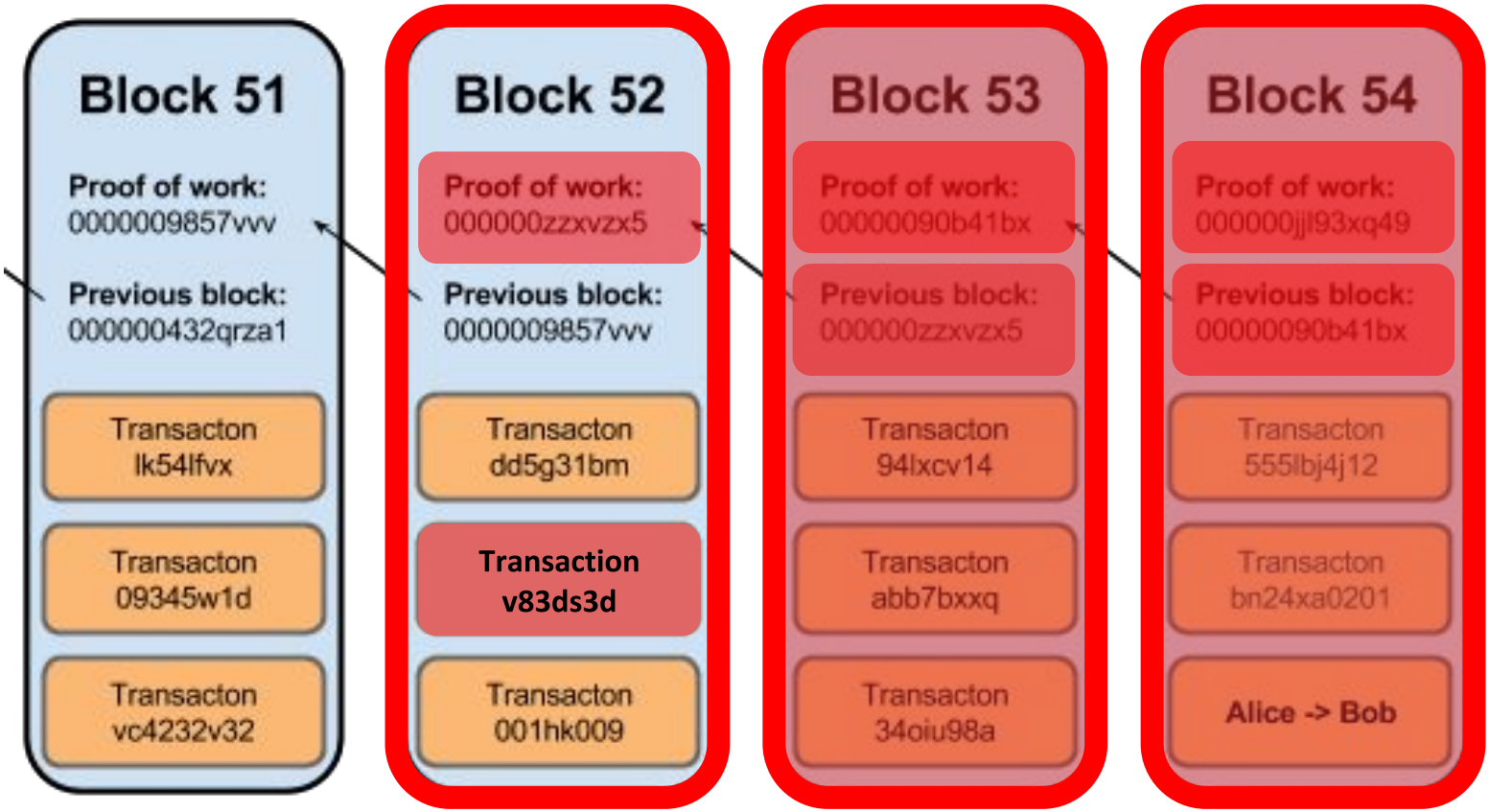
(*) se trovate una soluzione migliore potreste (1) diventare ricchi, (2), diventare famosi (Turing award), o (3) entrambi.

[https://www.slideshare.net/philippecamacho/how-to-explain-bitcoin-to-your-mother]

Blockchain = block chain



Blockchain = block chain



La blockchain **non è modificabile** (*a meno di ri-eseguire il Proof-of-Work*)

Bello in teoria,

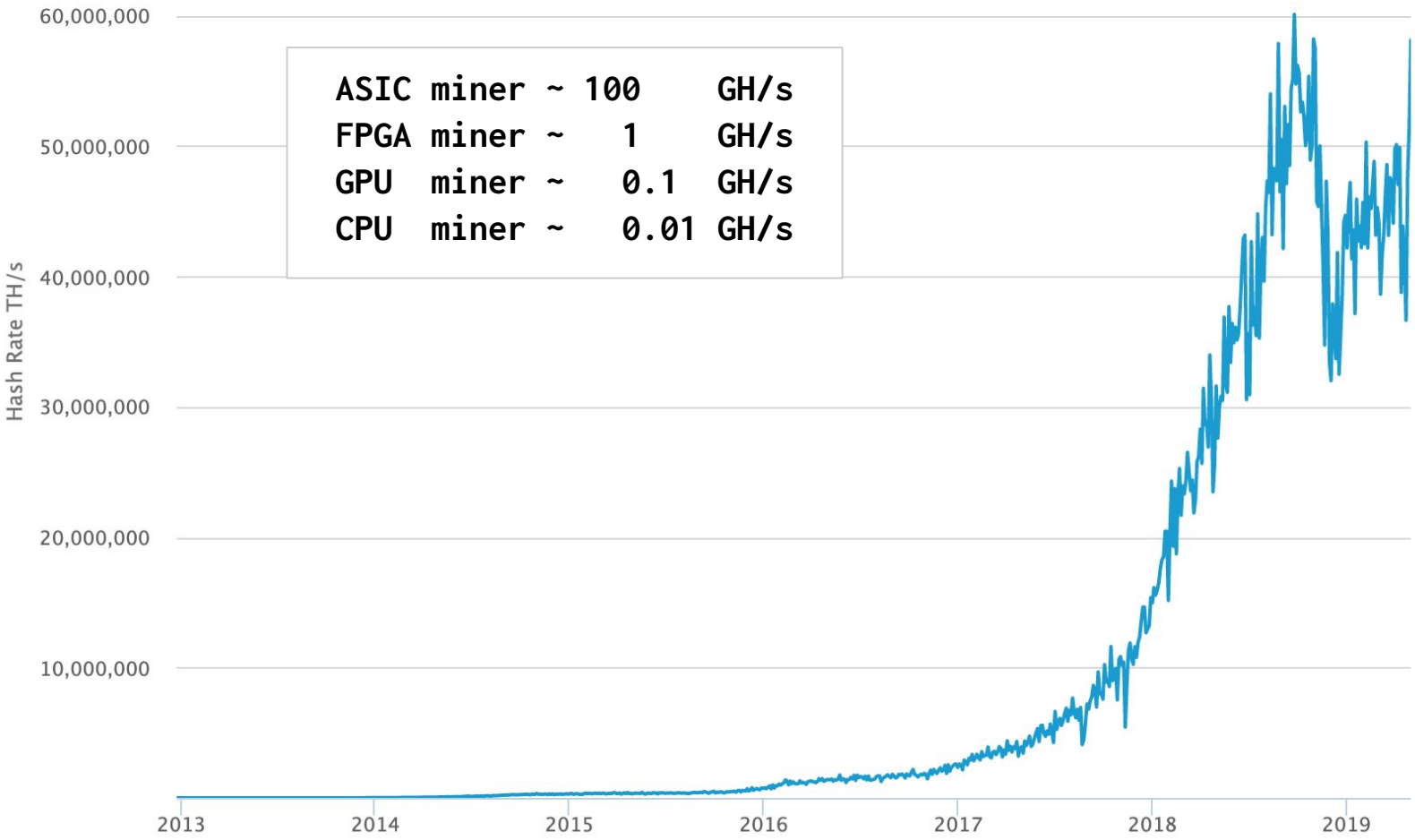
Ma chi butterebbe
della potenza di calcolo
per non avere nulla in cambio?

Bitcoin Mining

Bitcoin Mining

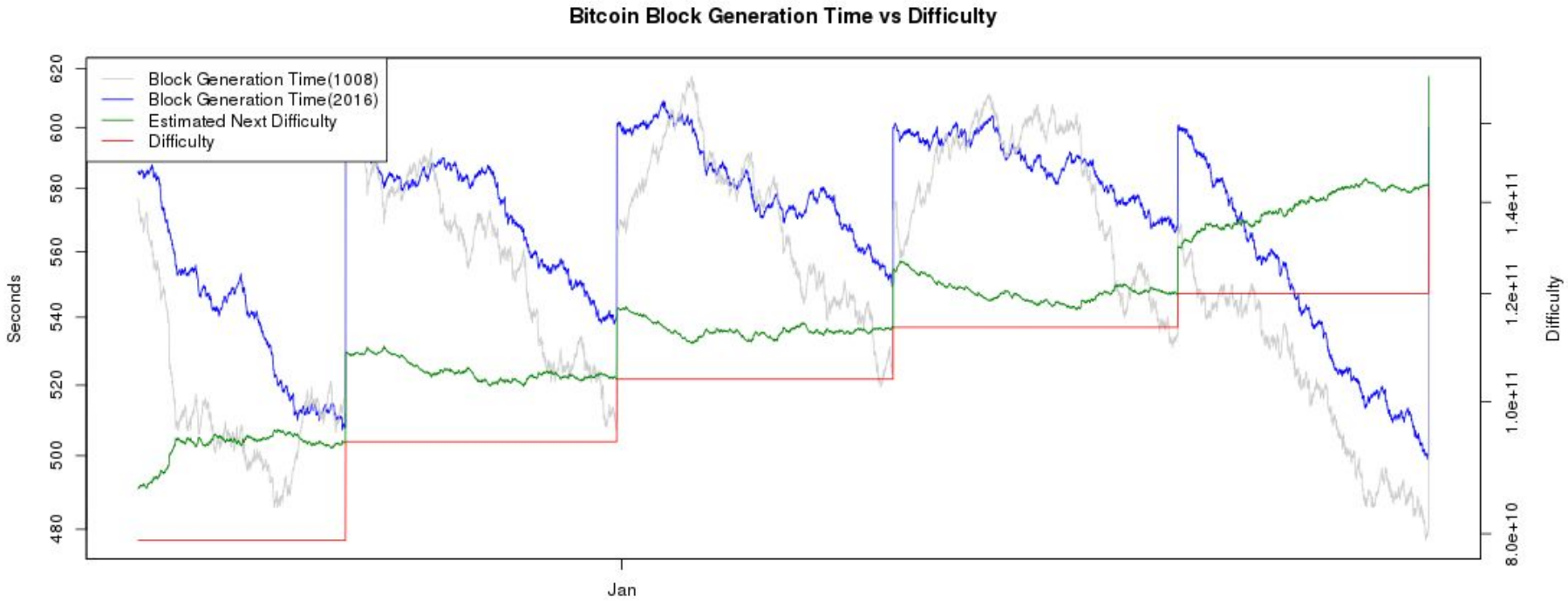
- Chi risolve il blocco è ricompensato con dei Bitcoin
  - Il miner aggiunge una transazione a sé stesso (coinbase) al blocco
  - Tutti i bitcoin sono creati in questo modo
- Qualsiasi abuso è protetto grazie al consenso
- La difficoltà del Proof-of-Work (numero di zeri iniziali nell'hash) viene concordata dai miner in modo da produrre un nuovo blocco ogni 10 minuti.

Hash Rate



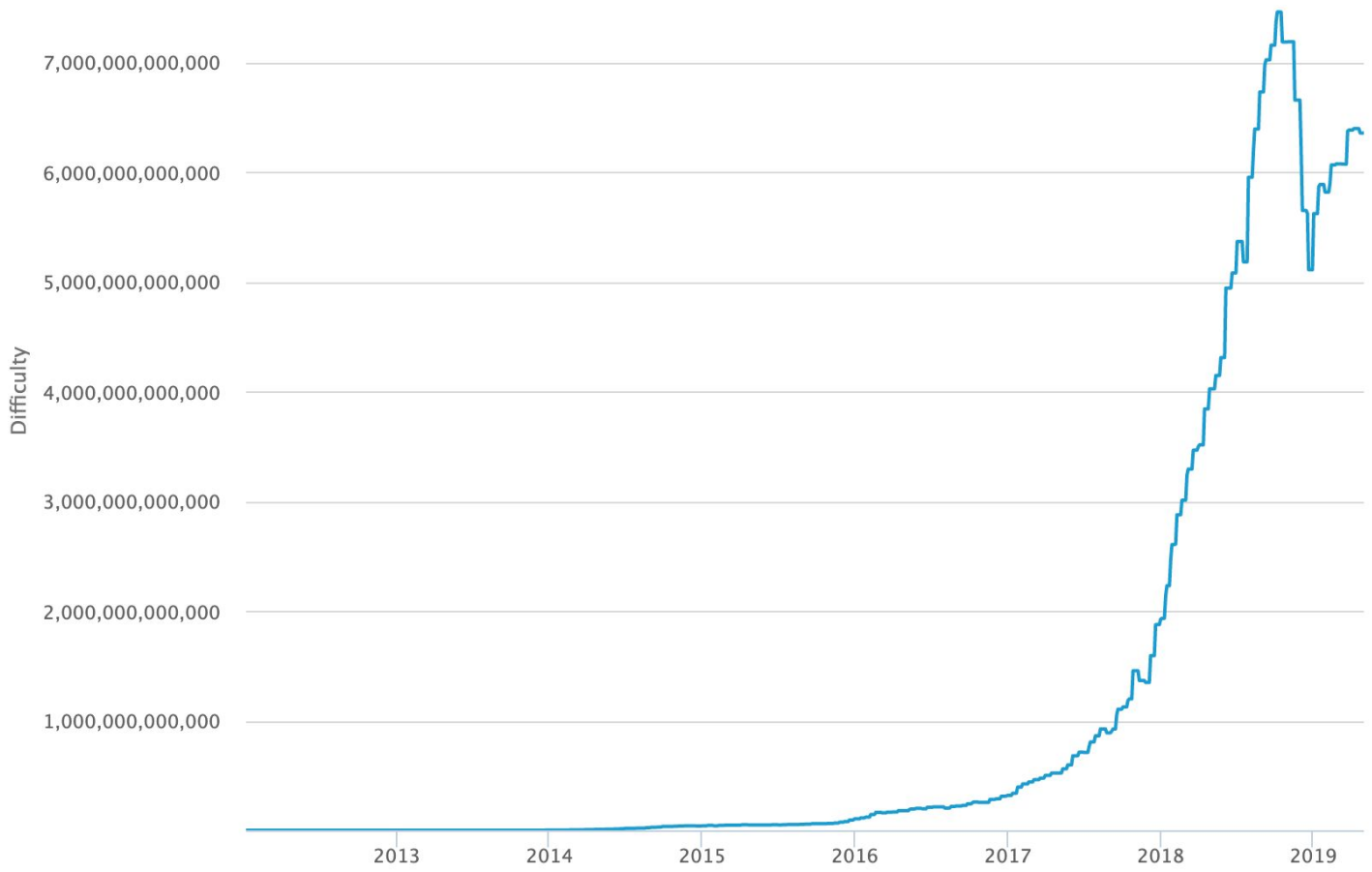
[https://blockchain.info/charts/hash-rate]

Difficoltà del Proof-of-Work



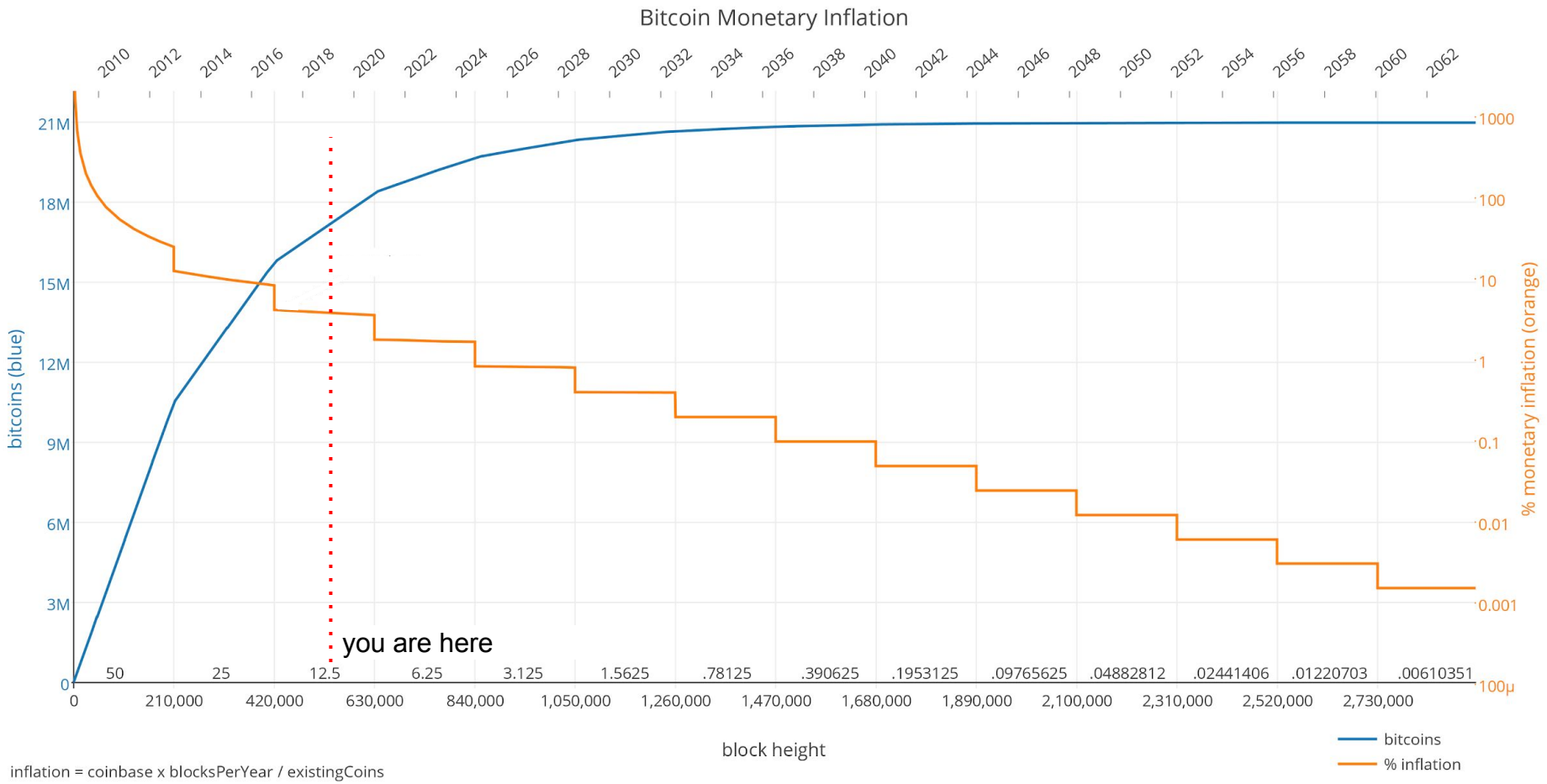
[https://plot.ly/~BashCo/5.embed]

Difficoltà del Proof-of-Work



[https://blockchain.info/charts/difficulty?timespan=all]

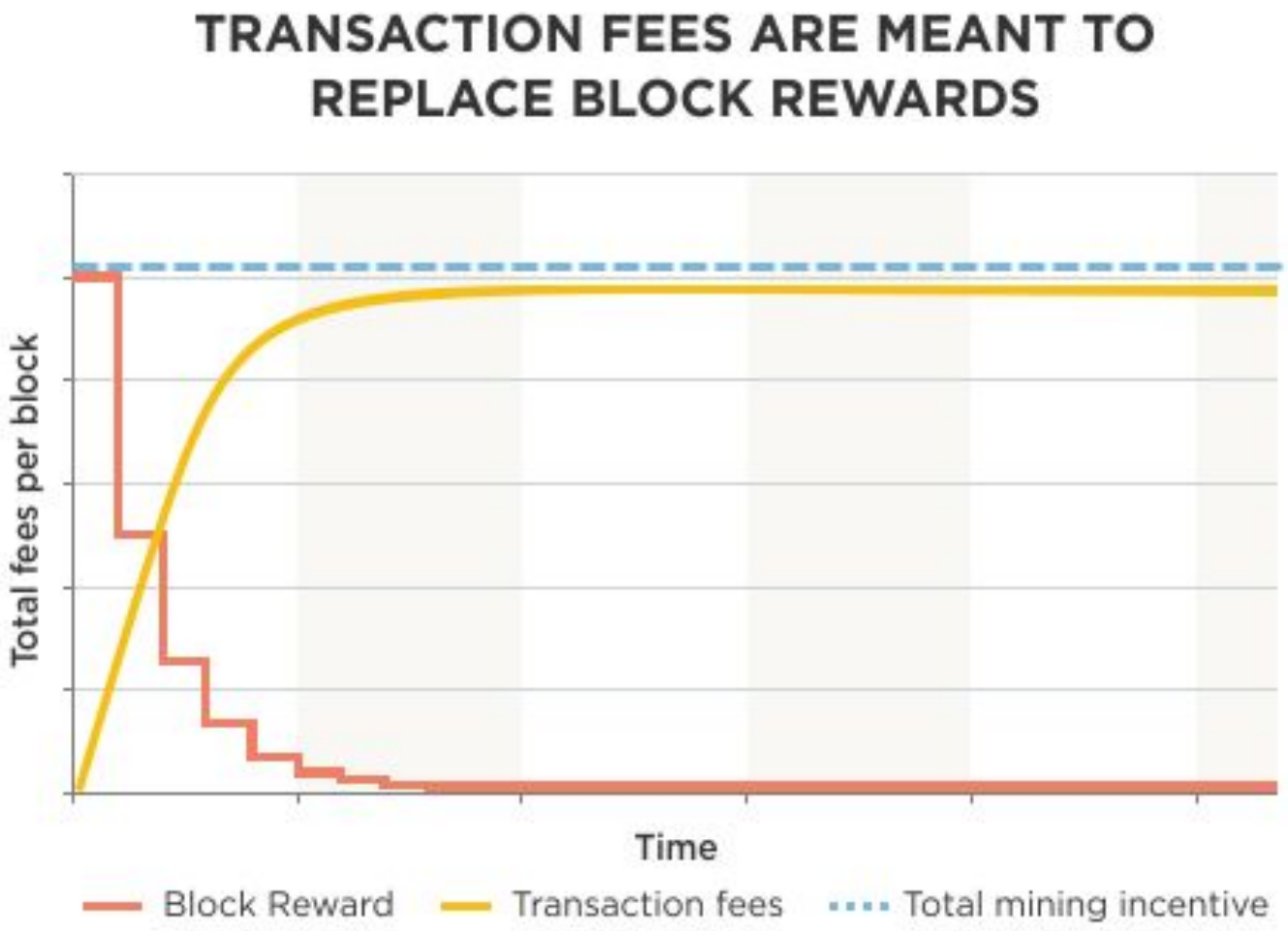
Block Reward - Inflazione controllata



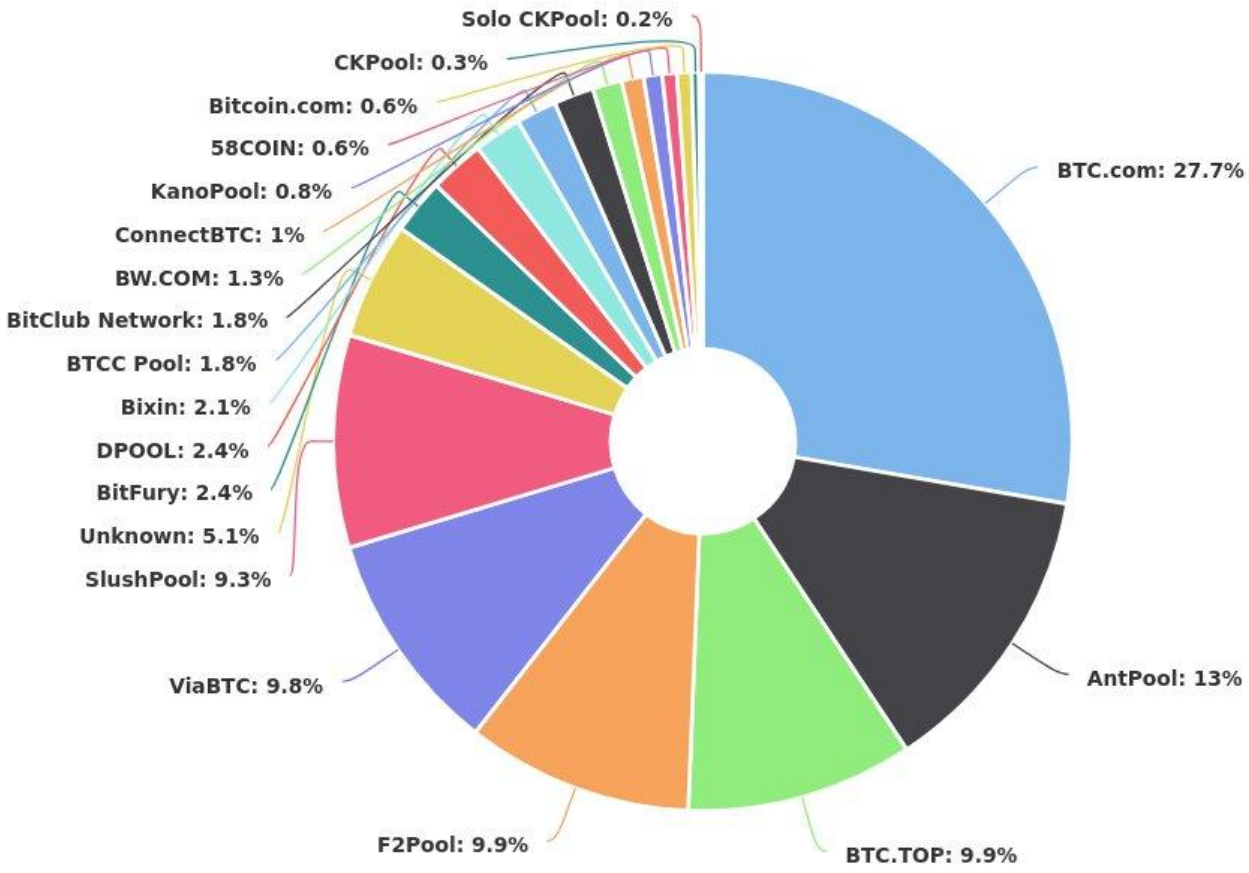
inflation = coinbase x blocksPerYear / existingCoins

[https://plot.ly/~BashCo/5.embed]

Transaction Fees



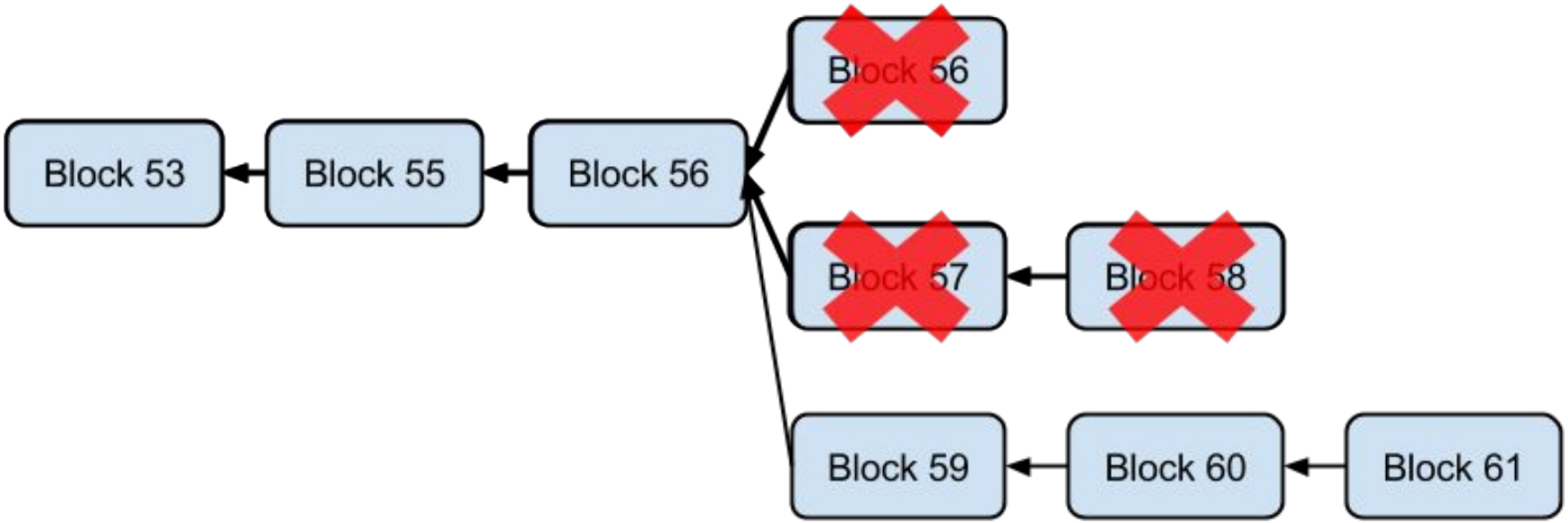
Pool Mining



[https://blockchain.info/pools]

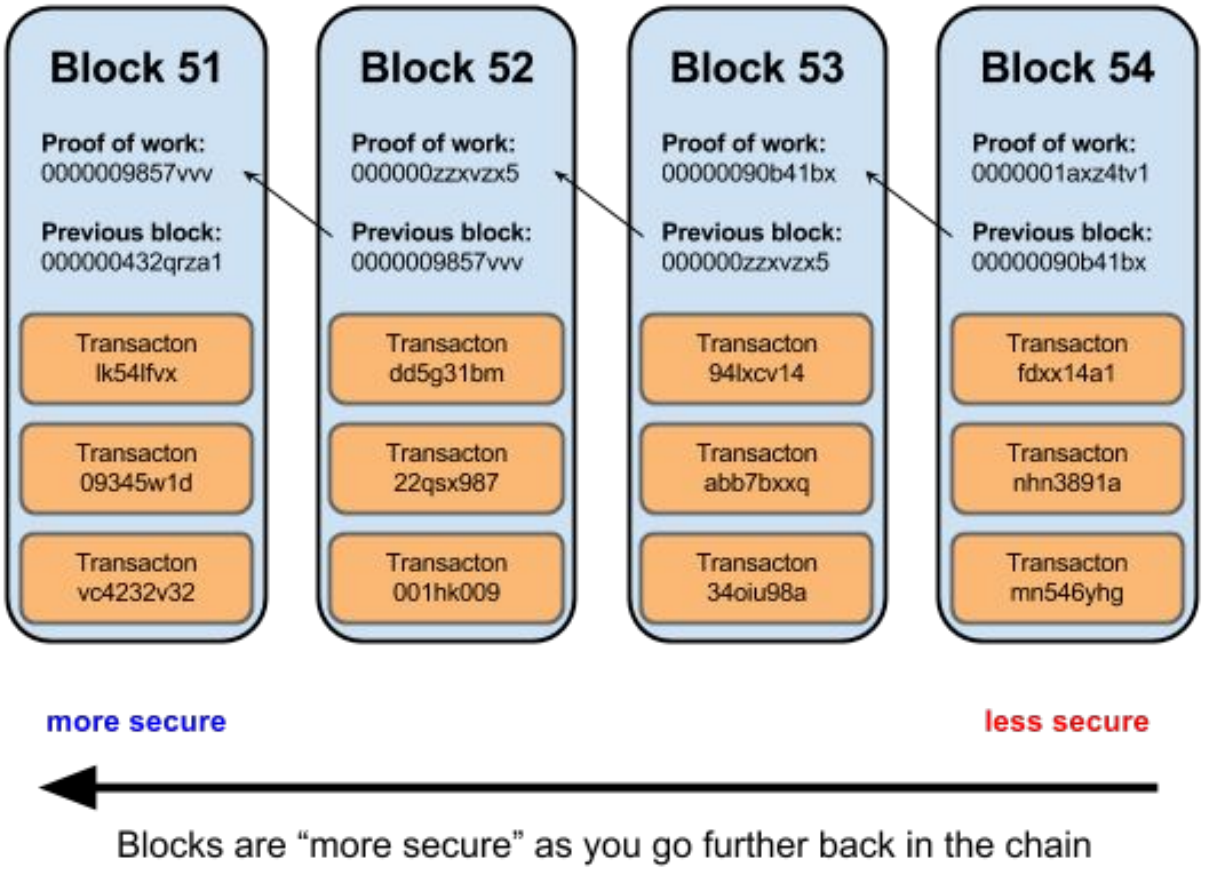
Cosa succede se due miners producono un blocco nello stesso momento?

Regola della catena più lunga



[https://www.ybrikman.com/writing/2014/04/24/bitcoin-by-analogy/]

Double Spending



[https://www.ybrikman.com/writing/2014/04/24/bitcoin-by-analogy/]

Cosa è Bitcoin?

un libro mastro pubblico e distribuito basato sul consenso

Parte II

Punto di vista pratico e finanziario

DISCLAIMER

Questa lezione non costituisce consiglio finanziario / legale.

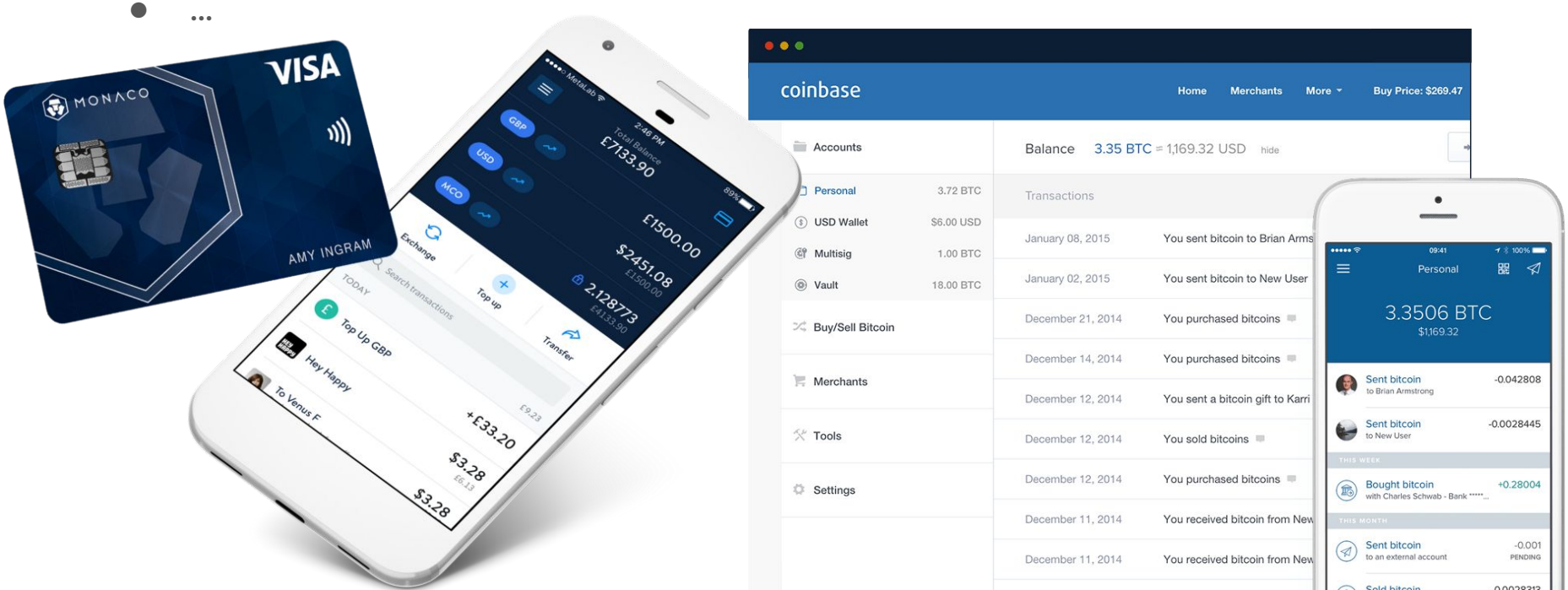
Possesso e gestione di Bitcoin

Tipi di Wallet

- App wallet
- Exchange wallet
- Paper wallet
- Hardware wallet

App Wallet

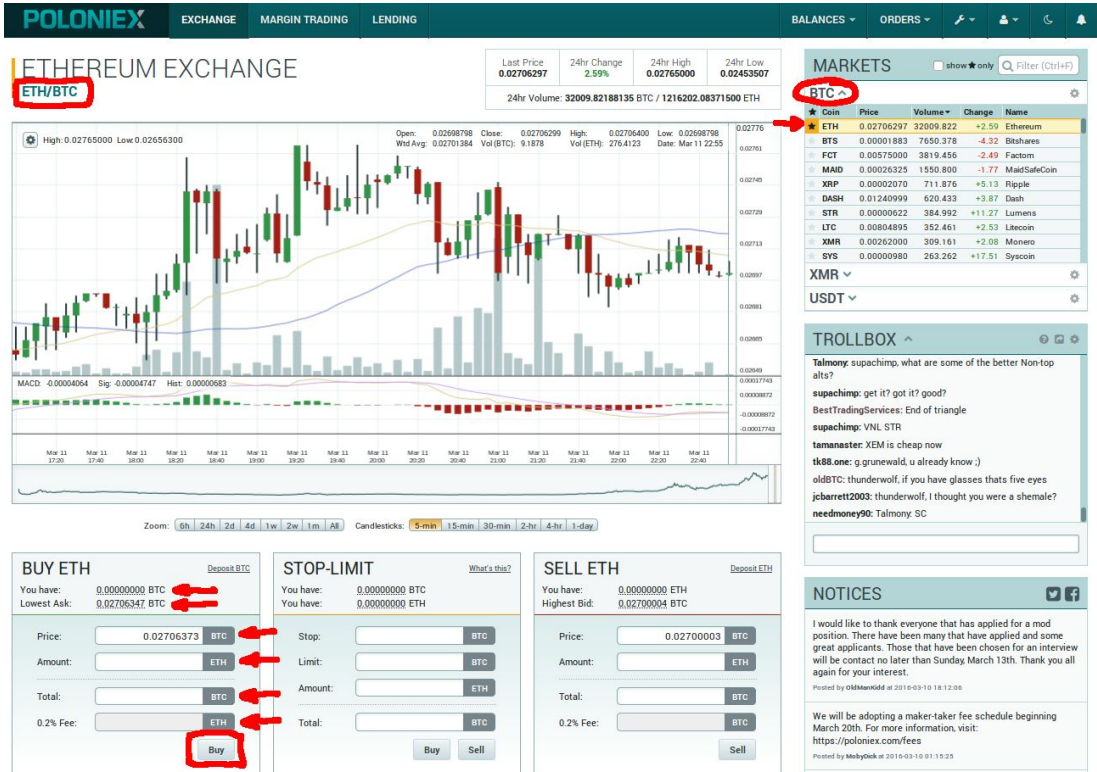
- Online e mobile
- In molti casi offrono carte di debito associate
- Accettano fiat currency
- Coinbase
- BitPay
- Monaco
- ...



Exchange Wallet

- Il metodo più semplice
- Accettano fiat currency (non tutti)
- Utili per trading
- Kraken
- Poloniex
- eToro
- Gemini
- ...

kraken
bitcoin exchange



eToro
Trading Starts Here

Paper Wallet

- Coppia di chiavi generata localmente e stampata su carta
- Si possono solo fare trasferimenti
- Sicuri
- bitaddress.org

Hardware Wallet

- Metodo più sicuro
- Trezor
- Ledger Nano S
- KeepKey
- ...

Ledger
AUTHORIZED Reseller

TREZOR

Buy Bitcoin

Oltre ai metodi appena visti ne esistono altri in cui le valute vengono acquistate “di persona”

- ATM (coinatmradar.com)
- localbitcoins.com

LocalBitcoins.com
Bringing Bitcoin Everywhere

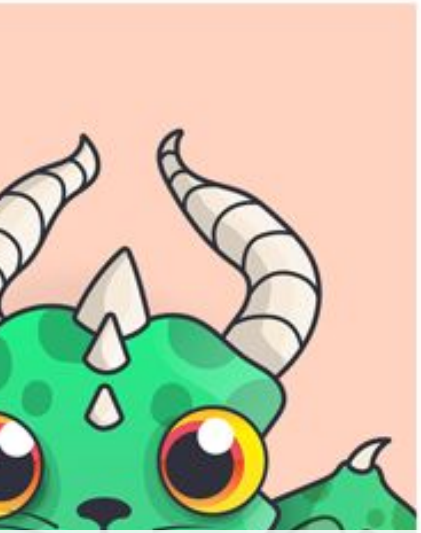
Rischi

- Hacking
  - Mt.Gox
  - Bitfinex
  - BitGrail
  - ...
- Truffe
  - Bitconnect
  - OneCoin
  - ...

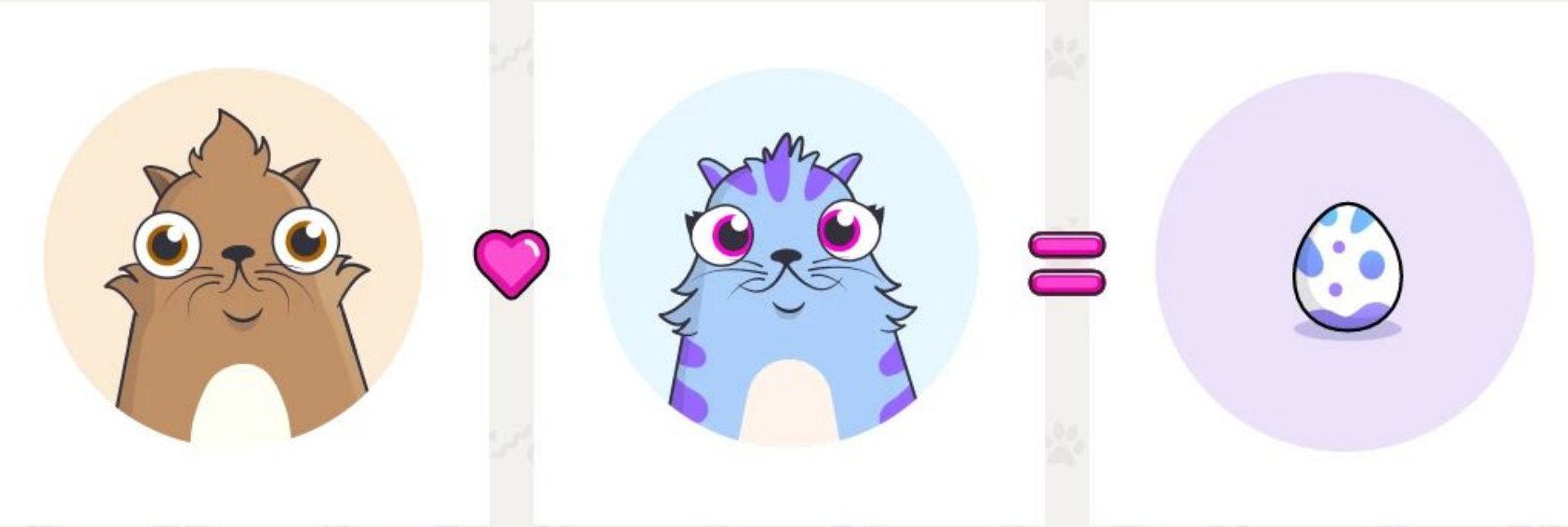
Conseguenze

- Nessun risarcimento
- Crollo del prezzo
- Fork?

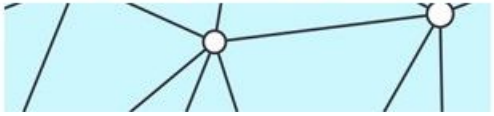
CryptoKitties



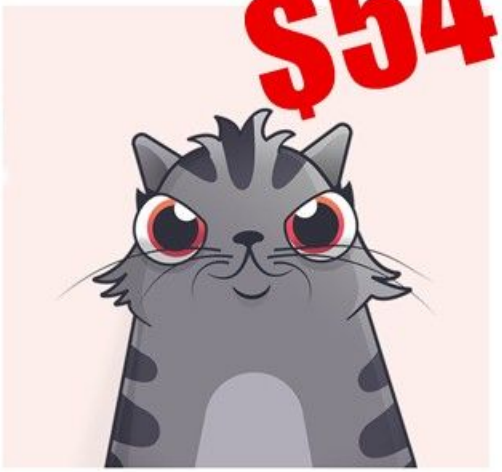
E poi ci sono
I criptogattini ...




$2500




$115,000


$54

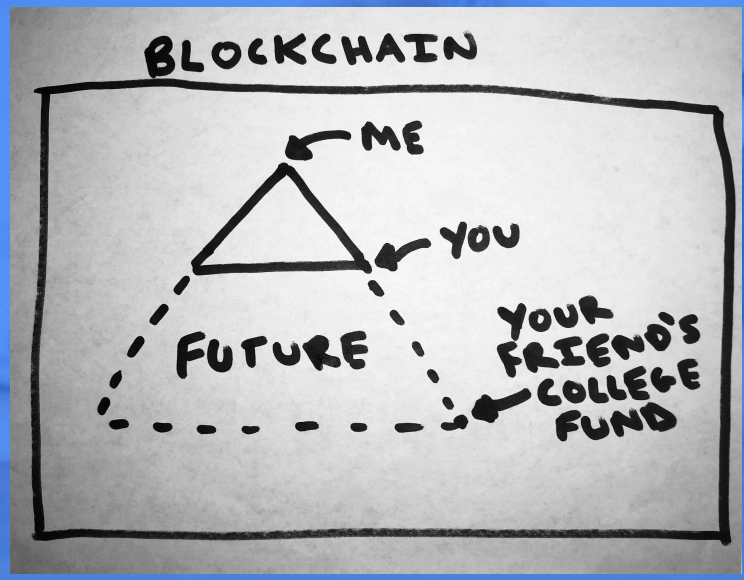

LIVE San Francisco
Jackson Palmer
DOGECOIN CO-CREATOR
Bloomberg
DOGECOIN: THE $2 BILLION "JOKE" CRYPTO

PonziCoin Home My Coins Source White Paper

The World's First Legitimate Ponzi Scheme

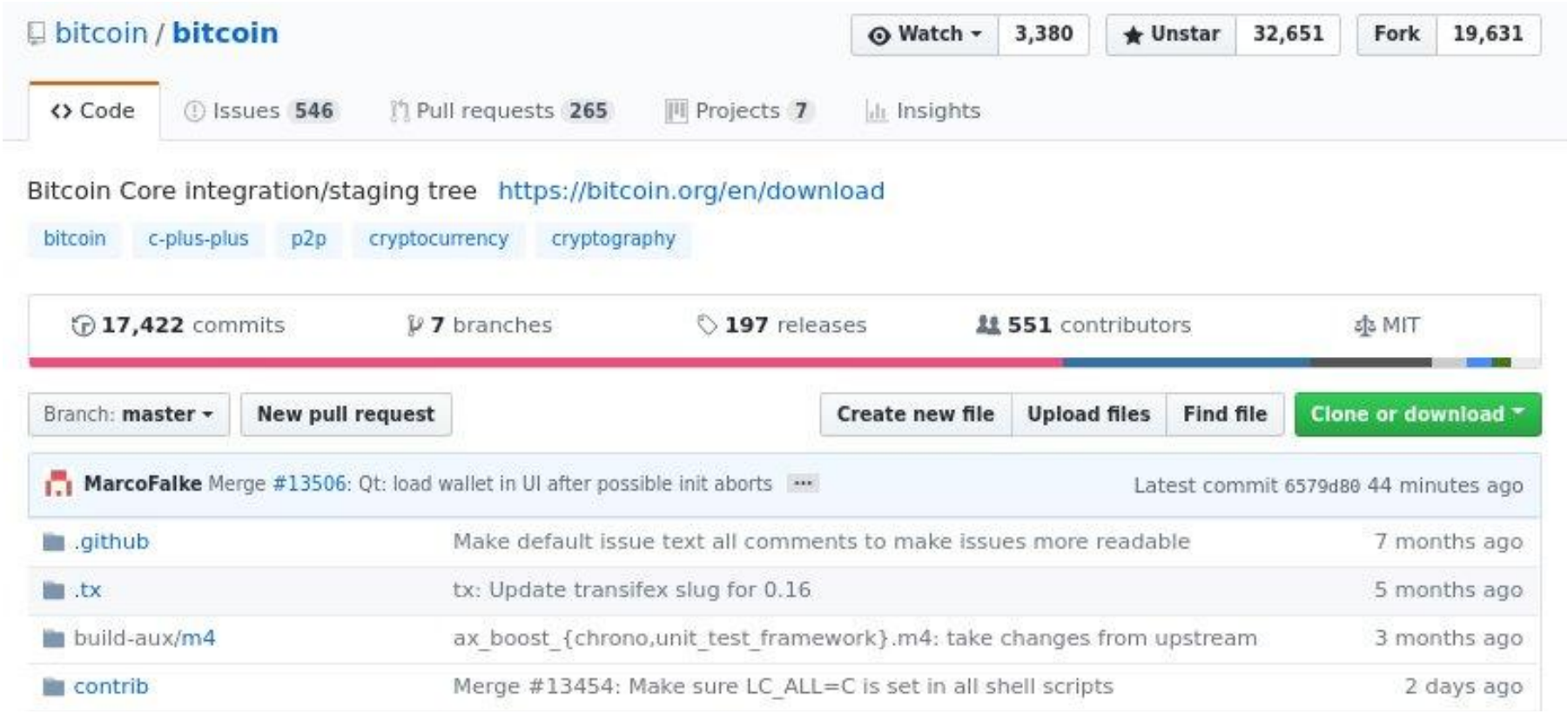
Because money doesn't grow on trees... unless you're BitFinex

Learn More



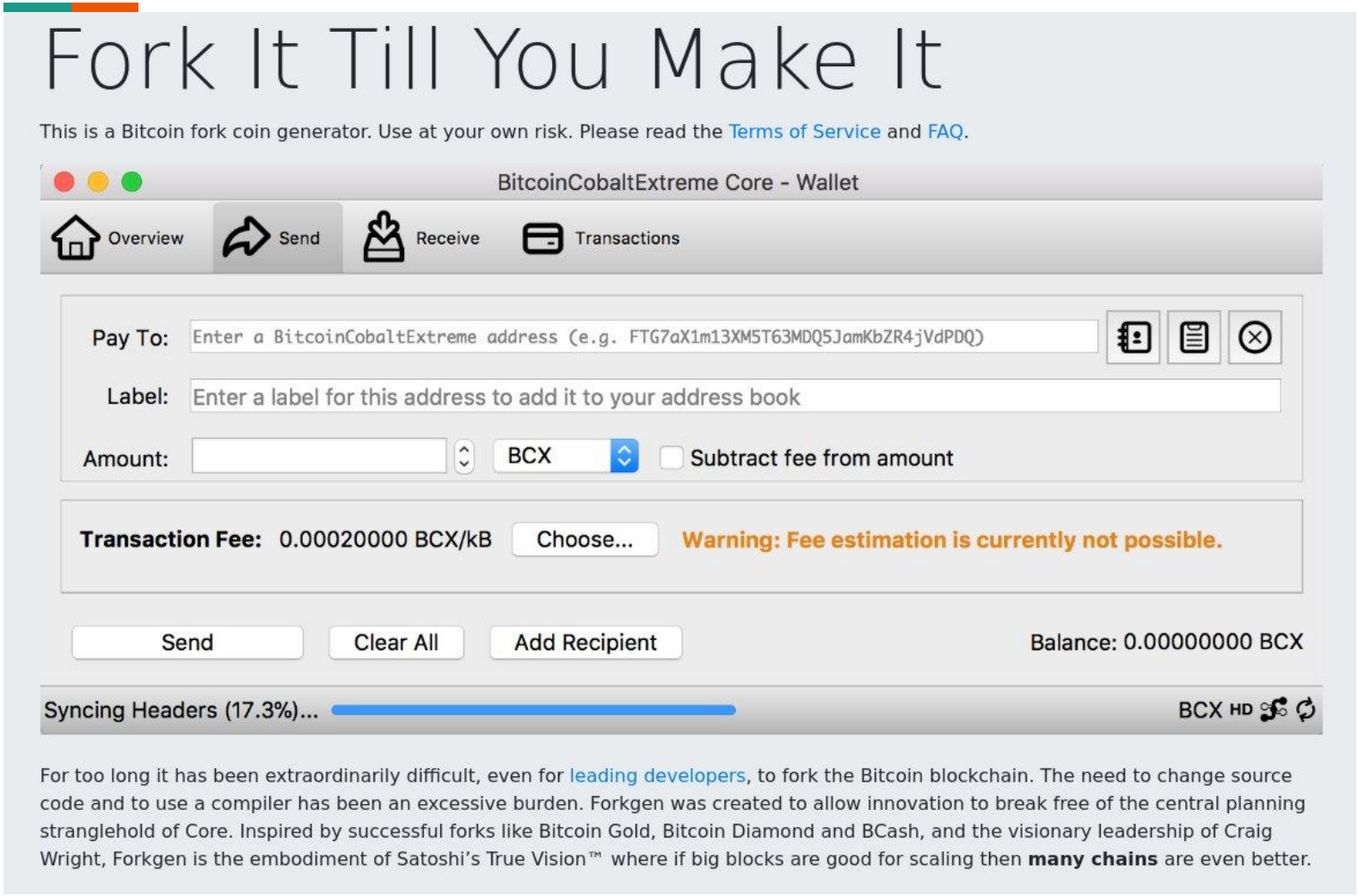

HOW TO:
MAKE A
BITCOIN
FORK
BTCMANAGER

Create your own coin! (i.e., attenti alle truffe)



[https://github.com/bitcoin/bitcoin]

Create your own coin! (i.e., attenti alle truffe)

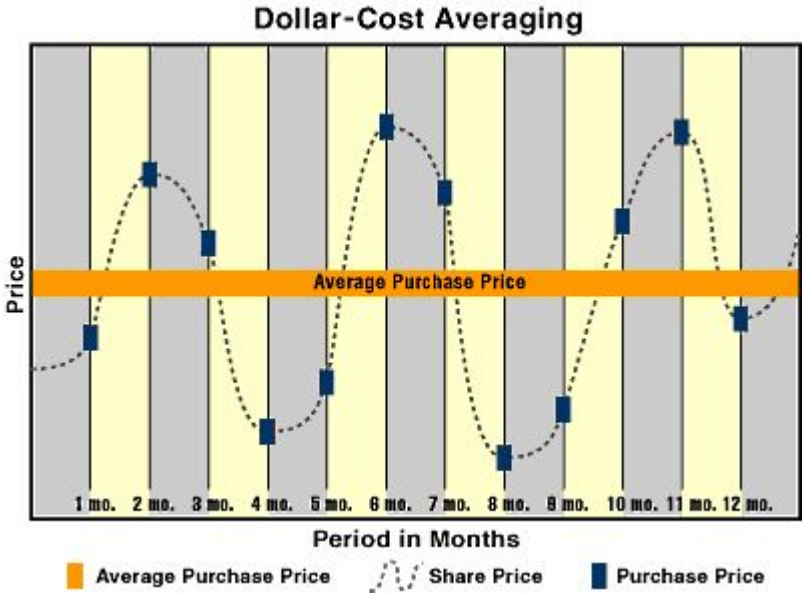


[https://forkgen.tech]

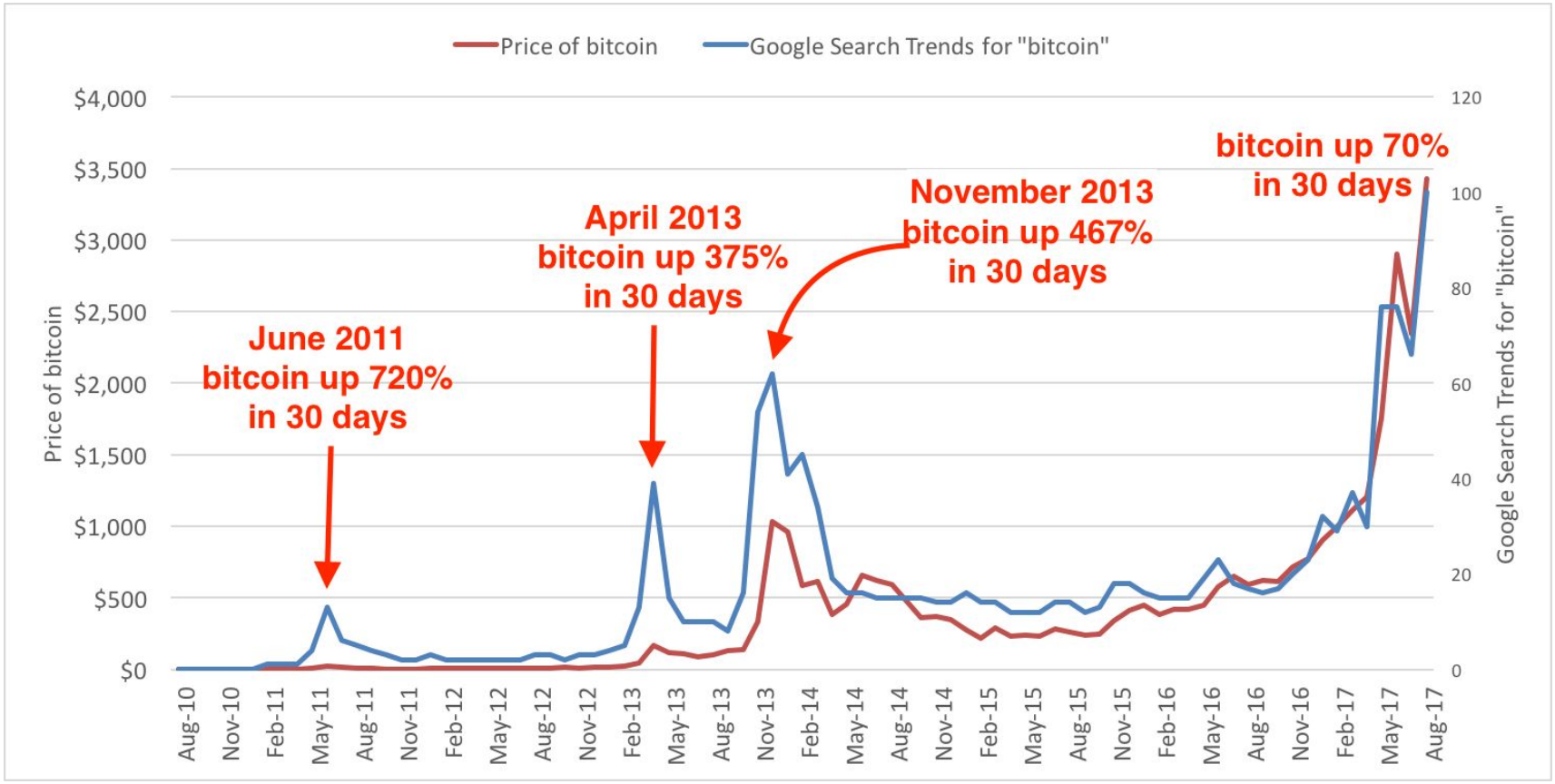
Utilizzi di Bitcoin

Trading finanziario

- Facile usando gli exchange
- Forex
  - Strategie applicate a valute reali
  - Cost averaging
  - Buy limit/Sell limit
  - Stime (AI?)
- Prezzi diversi su exchange diversi (arbitraggio)
  - cryptocompare.com
  - coinmarketcap.com

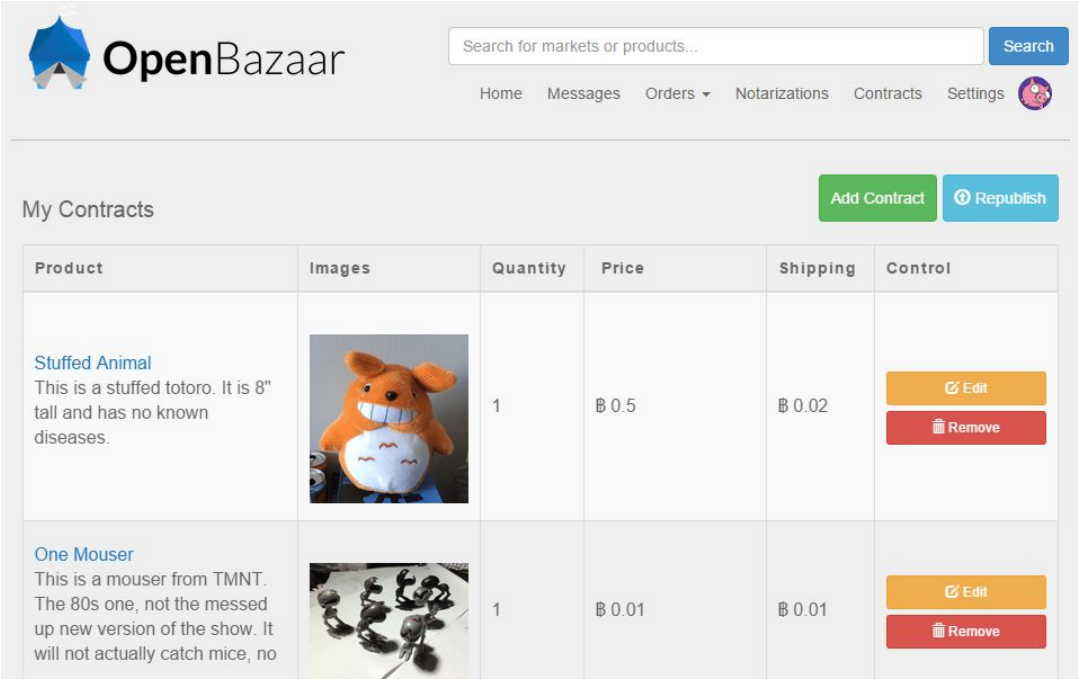


Google Trends



Acquisto di beni

- Shopping Online
  - Shopify
  - Expedia/Microsoft/...
  - Openbazaar.org
- On site
  - Negozi che accettano bitcoin
  - Coinmap.org
- Attività ludica
  - Giochi (Cryptokitties, ...)
  - Scommesse (Bitcoin Lotto, ...)
  - Gioco d'azzardo (BitCasino, ...)

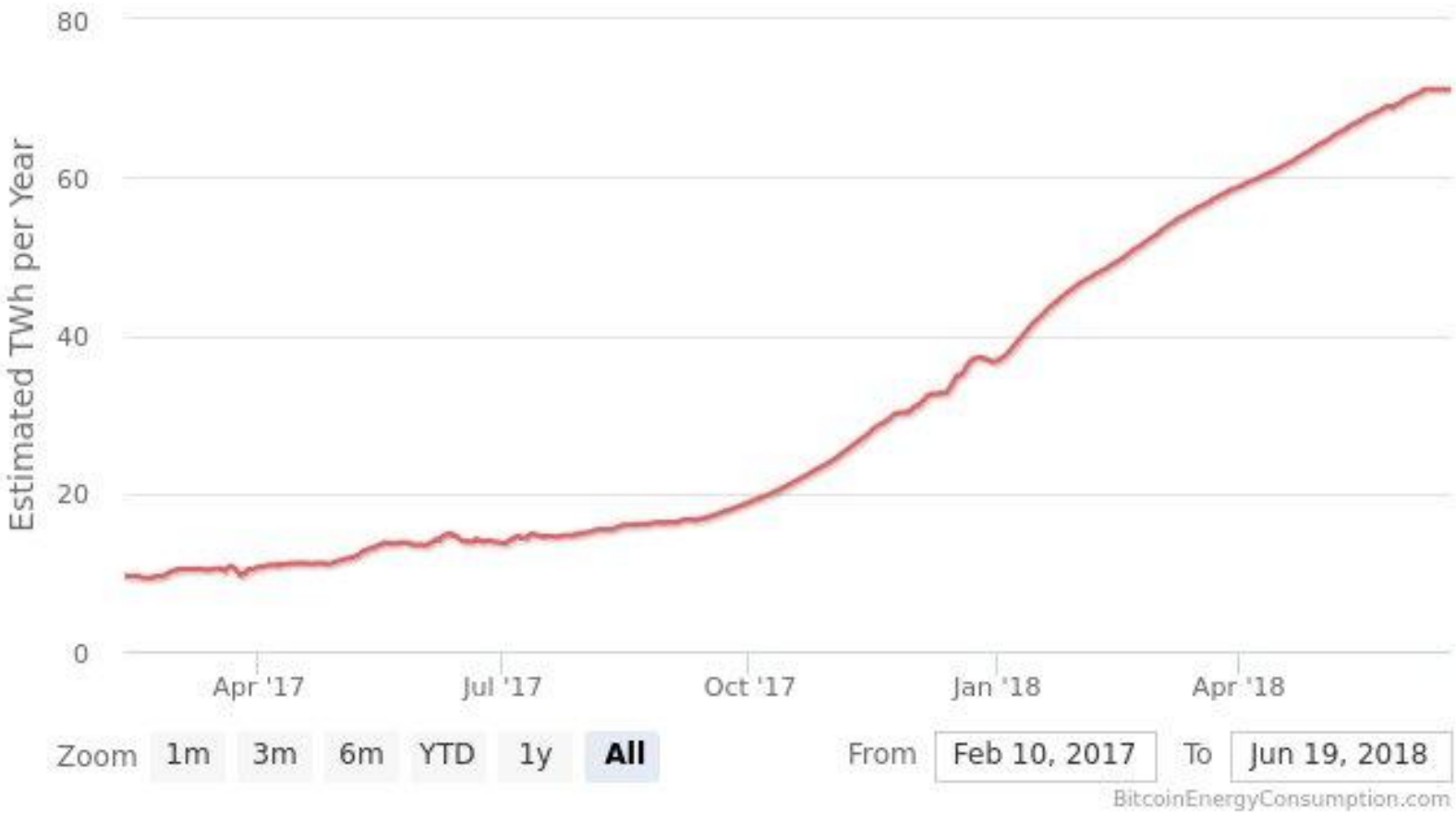


Attività Illegali

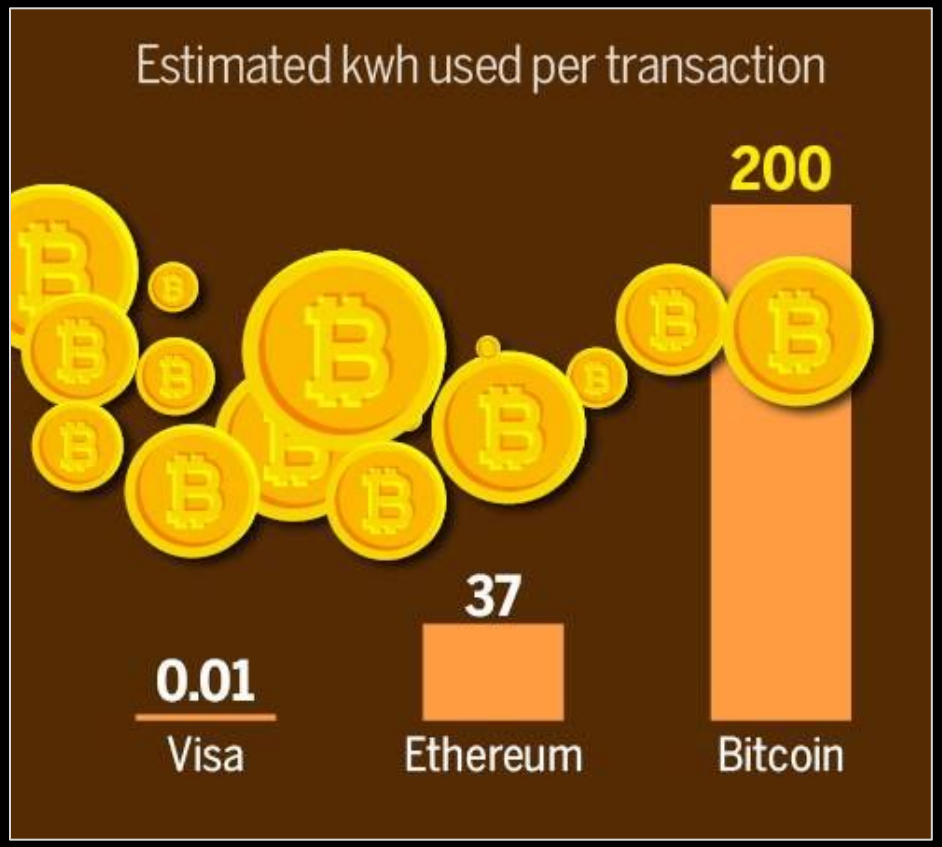
- Commercio illegale
  - Silkroad
  - Empire Market
  - …
- Malware
  - Ransomware (Cryptolocker, WannaCry, …)
  - Crypto mining (ads, estensioni, app, …)

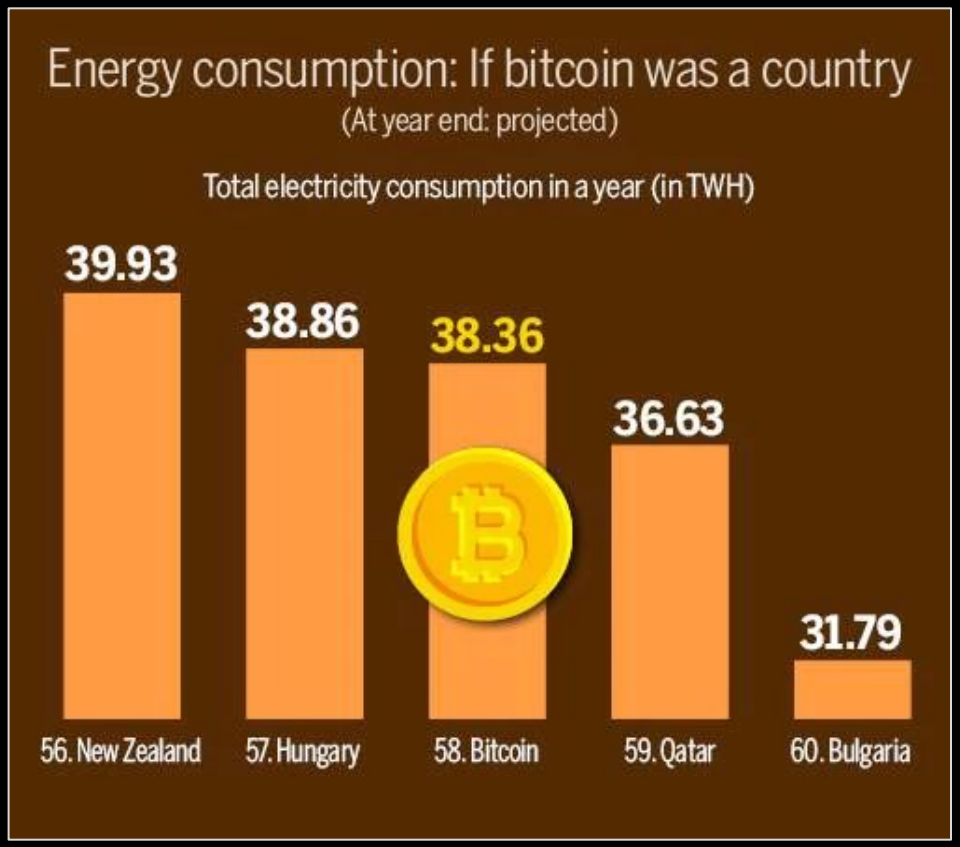
I Problemi di Bitcoin

Energia consumata



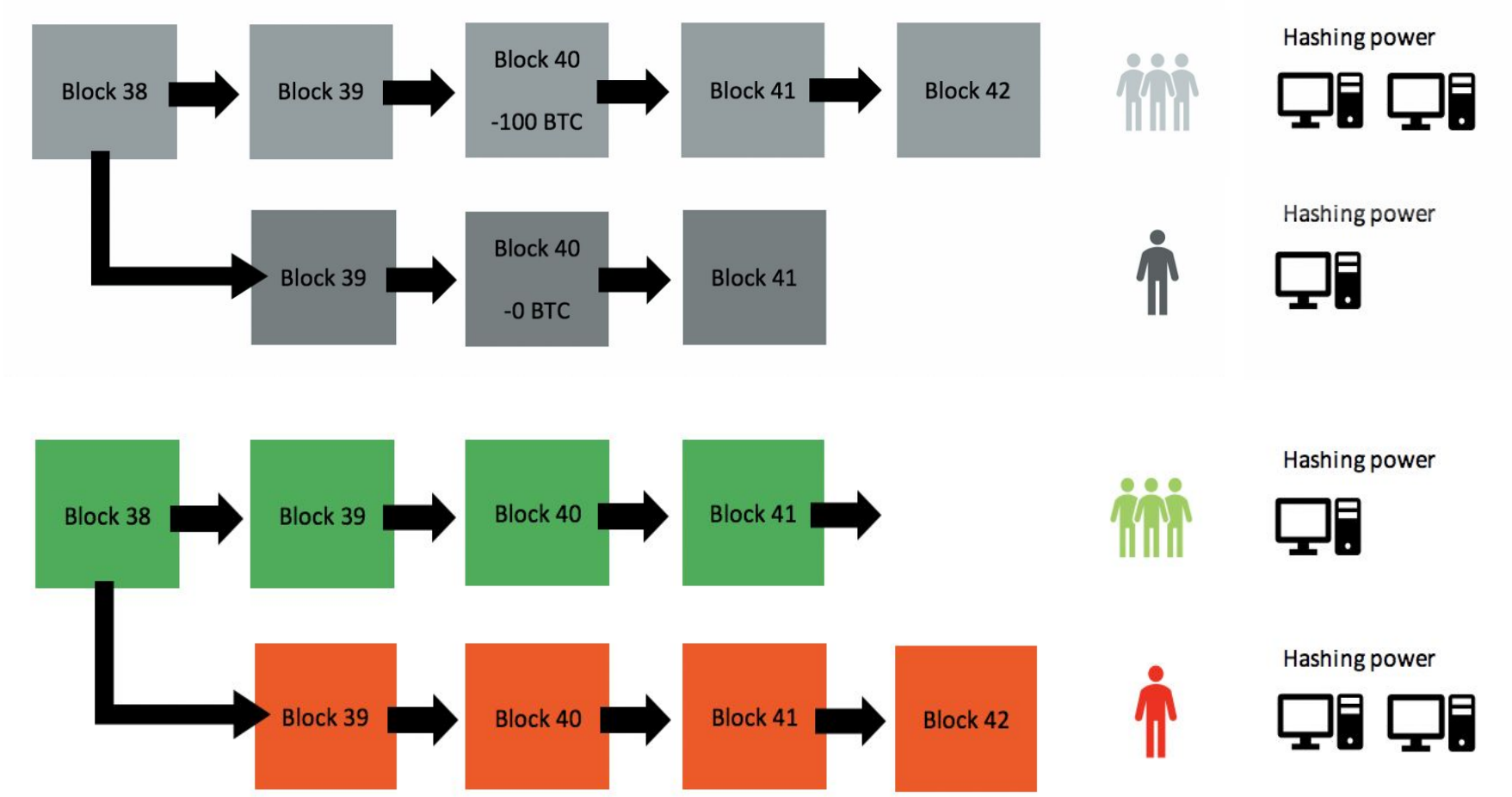
[https://digiconomist.net/bitcoin-energy-consumption]


Estimated kwh used per transaction
200
37
0.01
Visa
Ethereum
Bitcoin


Energy consumption: If bitcoin was a country
(At year end: projected)
Total electricity consumption in a year (in TWH)
39.93
38.86
38.36
36.63
31.79
56. New Zealand
57. Hungary
58. Bitcoin
59. Qatar
60. Bulgaria

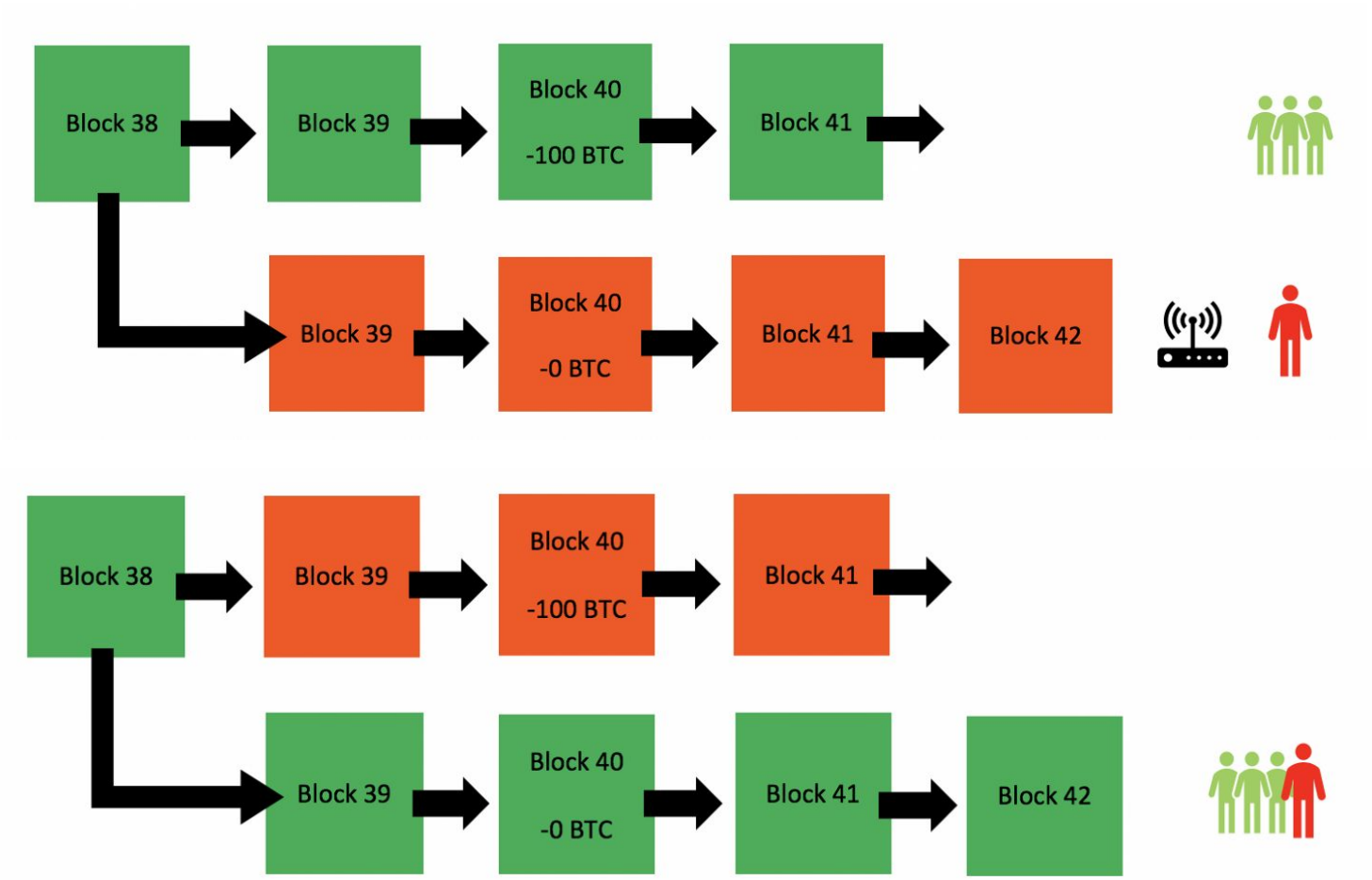
51% Attack

51% Attack



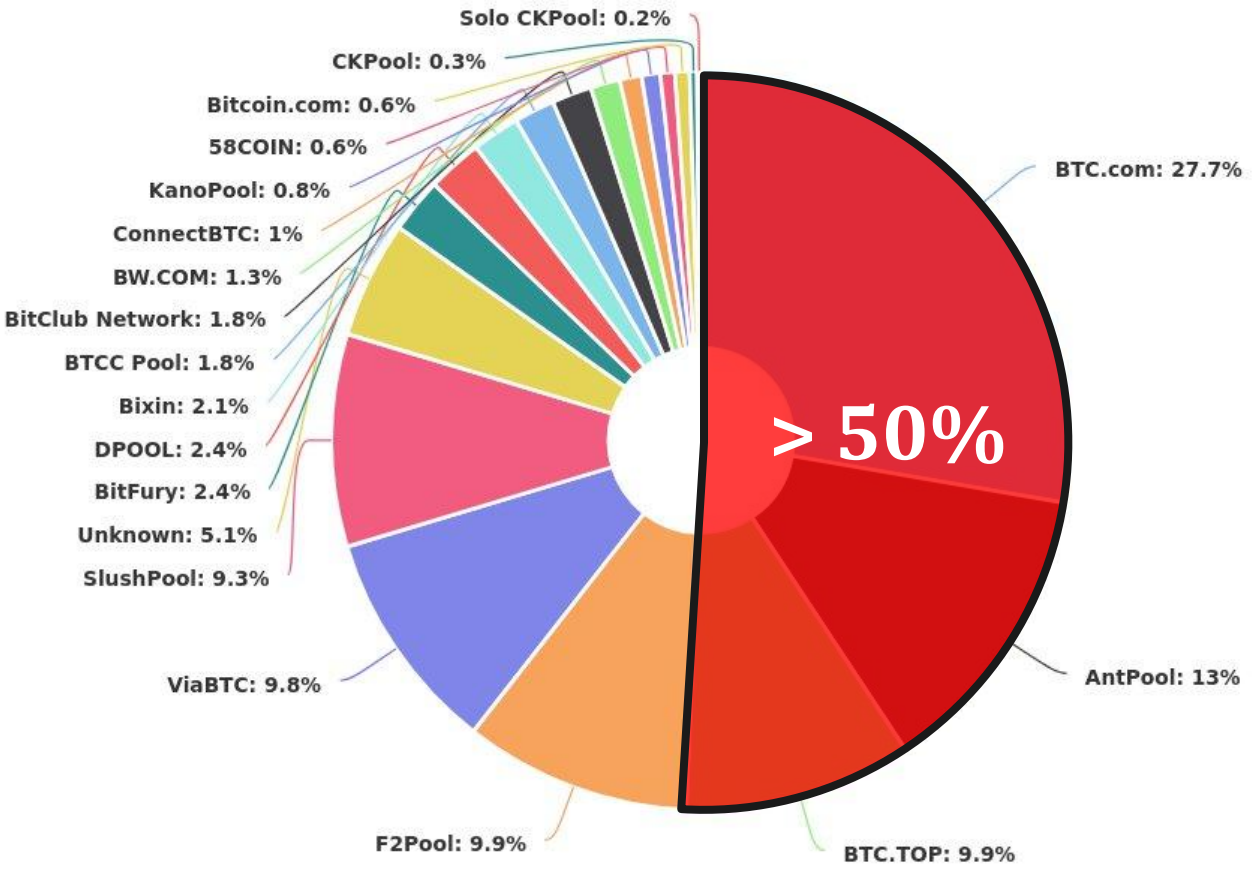
[https://medium.com/coinmonks/what-is-a-51-attack-or-double-spend-attack-aa108db63474]

51% Attack



[https://medium.com/coinmonks/what-is-a-51-attack-or-double-spend-attack-aa108db63474]

Mining Pool - 51% Attack



[https://blockchain.info/pools]

PoW 51% Attack Cost

This is a collection of coins and the theoretical cost of a 51% attack on each network.

Learn More ⚡ Tip

Name	Symbol	Market Cap	Algorithm	Hash Rate	1h Attack Cost	NiceHash-able
Bitcoin	BTC	$106.49 B	SHA-256	48,136 PH/s	*$451,284*	0%
Ethereum	ETH	$18.60 B	Ethash	137 TH/s	*$90,971*	5%
BitcoinCashABC	BCH	$5.39 B	SHA-256	2,254 PH/s	*$21,134*	2%
Litecoin	LTC	$4.82 B	Scrypt	350 TH/s	*$51,437*	3%
Monero	XMR	$1.20 B	CryptoNightR	314 MH/s	*$5,574*	5%
Dash	DASH	$1.10 B	X11	3 PH/s	*$4,761*	15%

Come risolvere questi problemi?

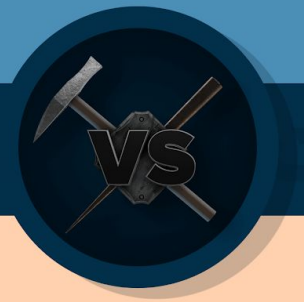
Proof-of-Work → Proof-of-Stake

PROOF OF WORK

The probability of mining a block depends on the amount of work a miner does

Takes more energy than Proof of Stake

One example is Mining, which uses computer cycle time to validate new transactions



Stakeholders validate new blocks by utilizing their share of coins on the network

The first example of Proof of Stake was Peercoin

A user would need to own a majority of all coins in order to attack the network

PROOF OF STAKE

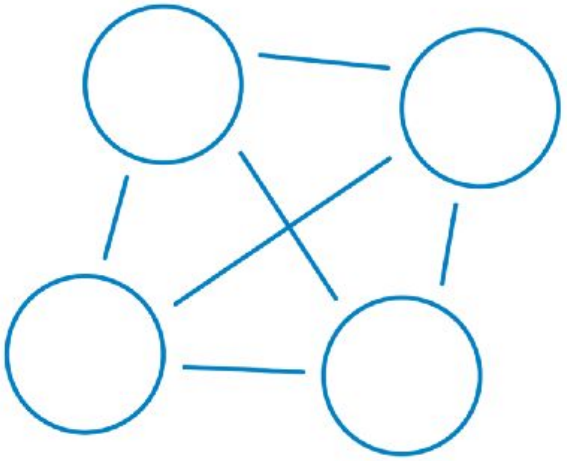
COMPARING PROOF ALGORITHMS

Proof of work & Proof of stake are methods of verifying the authenticity of transactions, without the need for a centralized third party.

WHAT ARE THEIR MAIN DIFFERENCES?

HolyTransaction

PROOF OF WORK



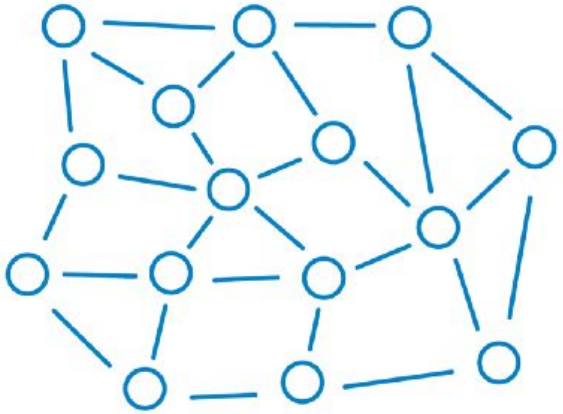
Centralized

Users organize in
mining pools

Hardware tools
ASICS and CPUs

Energy
high consumption
Unsustainable concept

PROOF OF STAKE



Decentralized

Users remain in control
of their tokens

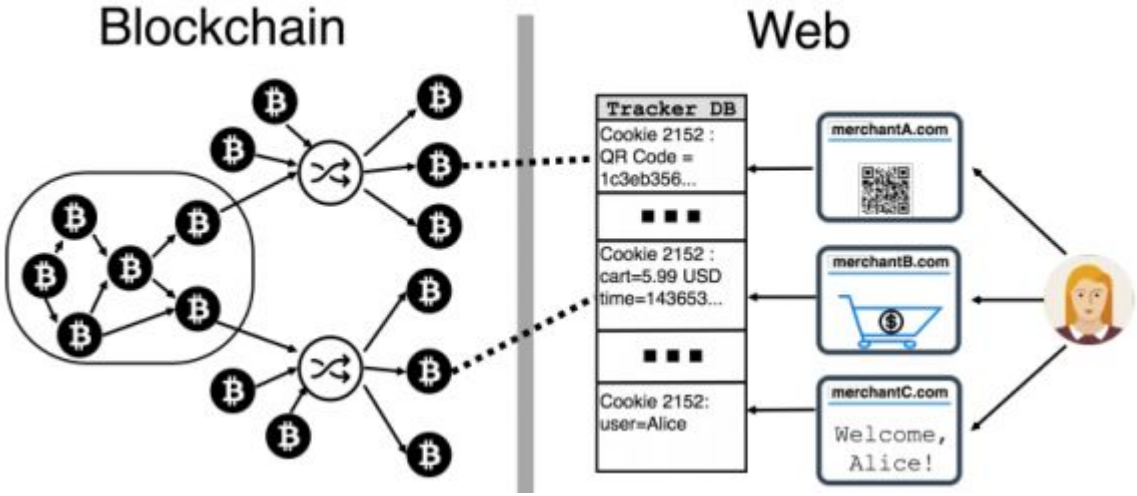
Hardware tools
no necessary

Energy
low consumption
Sustainable concept

[https://cryptocurrencyhub.io/an-introduction-to-consensus-algorithms-proof-of-stake-and-proof-of-work-cd0e1e6baf52]

Realmente Anonimo?

- Indirizzo IP
- Credenziali su app ed exchange wallet
- Storia delle transazioni
- Bitcoin mixer
- Altcoin anonime (Monero)



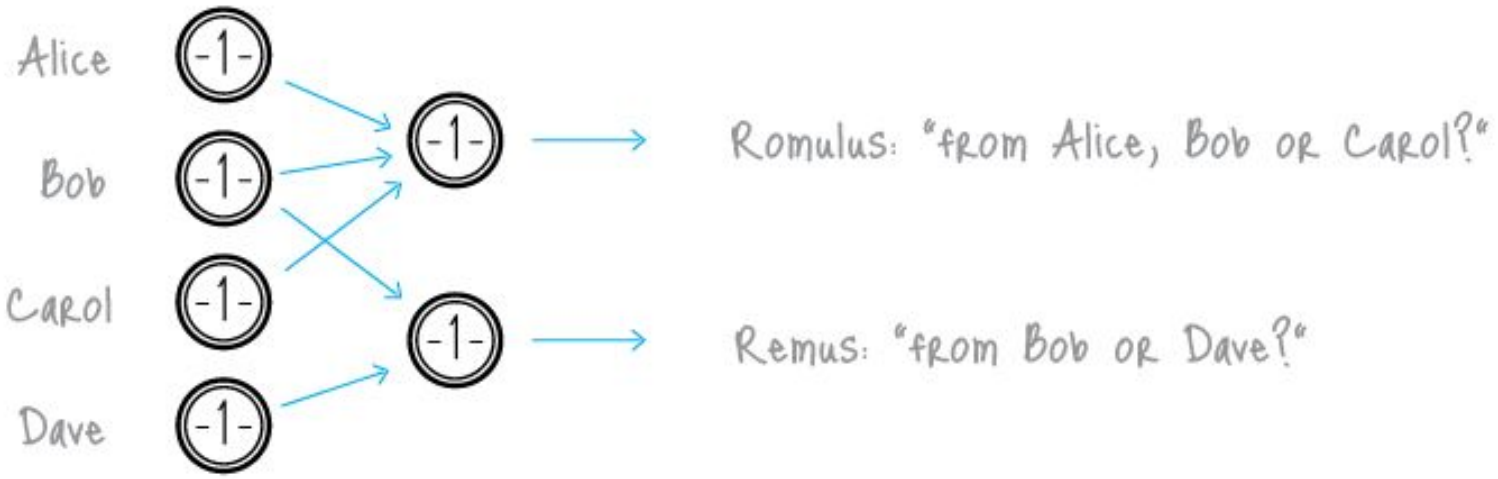
Untraceable payments

Bitcoin payment

Monero payment

[https://bitcointalk.org/index.php?topic=583449]

Untraceable payments



[https://bitcointalk.org/index.php?topic=583449]

Daily Meme Supply @DailyMemeSupply · 16h

buys 0.000001 bitcoin

changes bio

investor & entrepreneur 💰 $BTC 💵 living life in the sky ✈️ ☁️ eat, sleep, bitcoin

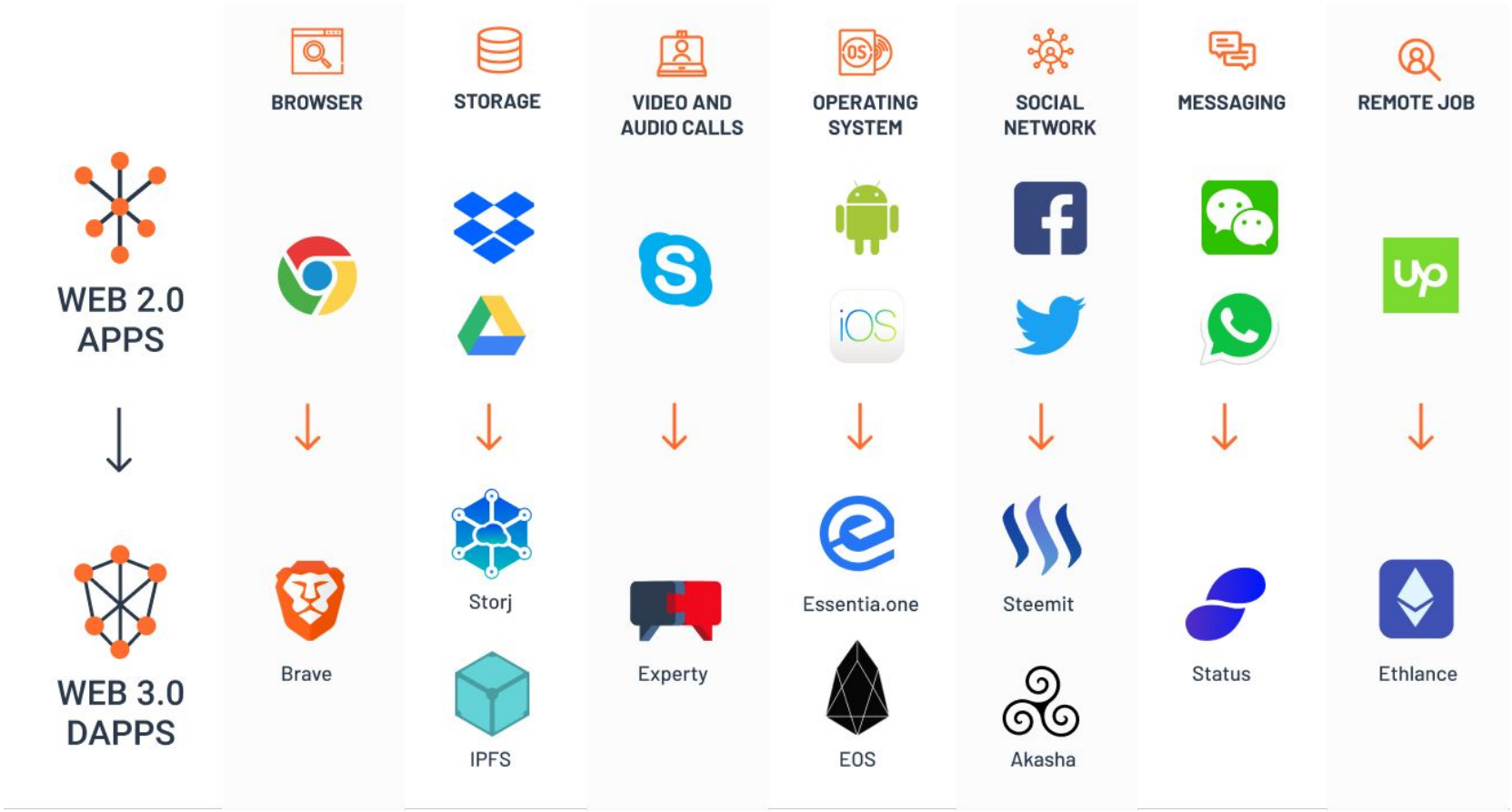
69 2.6K 10.1K

Parte III

Prospettive future

Altcoins e Internet 3.0

Internet 3.0


WEB 2.0 APPS
WEB 3.0 DAPPS
BROWSER
Brave
STORAGE
Storj
IPFS
VIDEO AND AUDIO CALLS
Experty
OPERATING SYSTEM
iOS
Essentia.one
EOS
SOCIAL NETWORK
Steemit
Akasha
MESSAGING
Status
REMOTE JOB
Ethlance

Smart Contracts

(programming the blockchain)

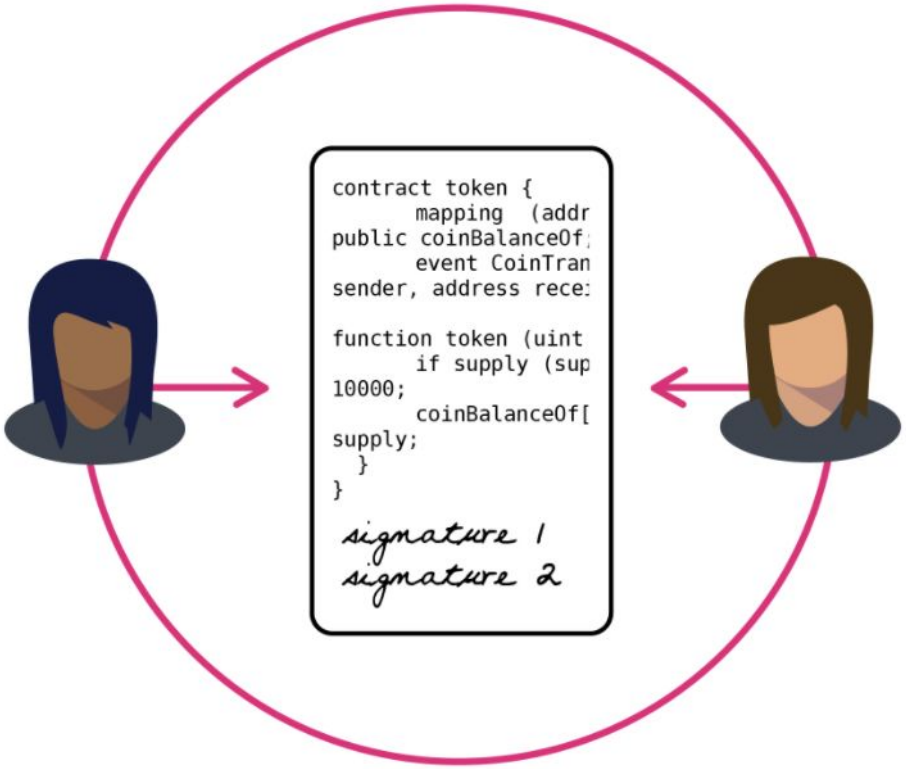
Smart Contracts

Attraverso gli smart contract si possono **automatizzare** le **clausole** contrattuali in modo parziale o completo.

Si tratta di contratti digitali atti a scambiare proprietà, denaro, azioni o altri asset di valore in modo trasparente, sicuro e senza intermediari.

Ethereum

ethereum



Ethereum - MyCoin

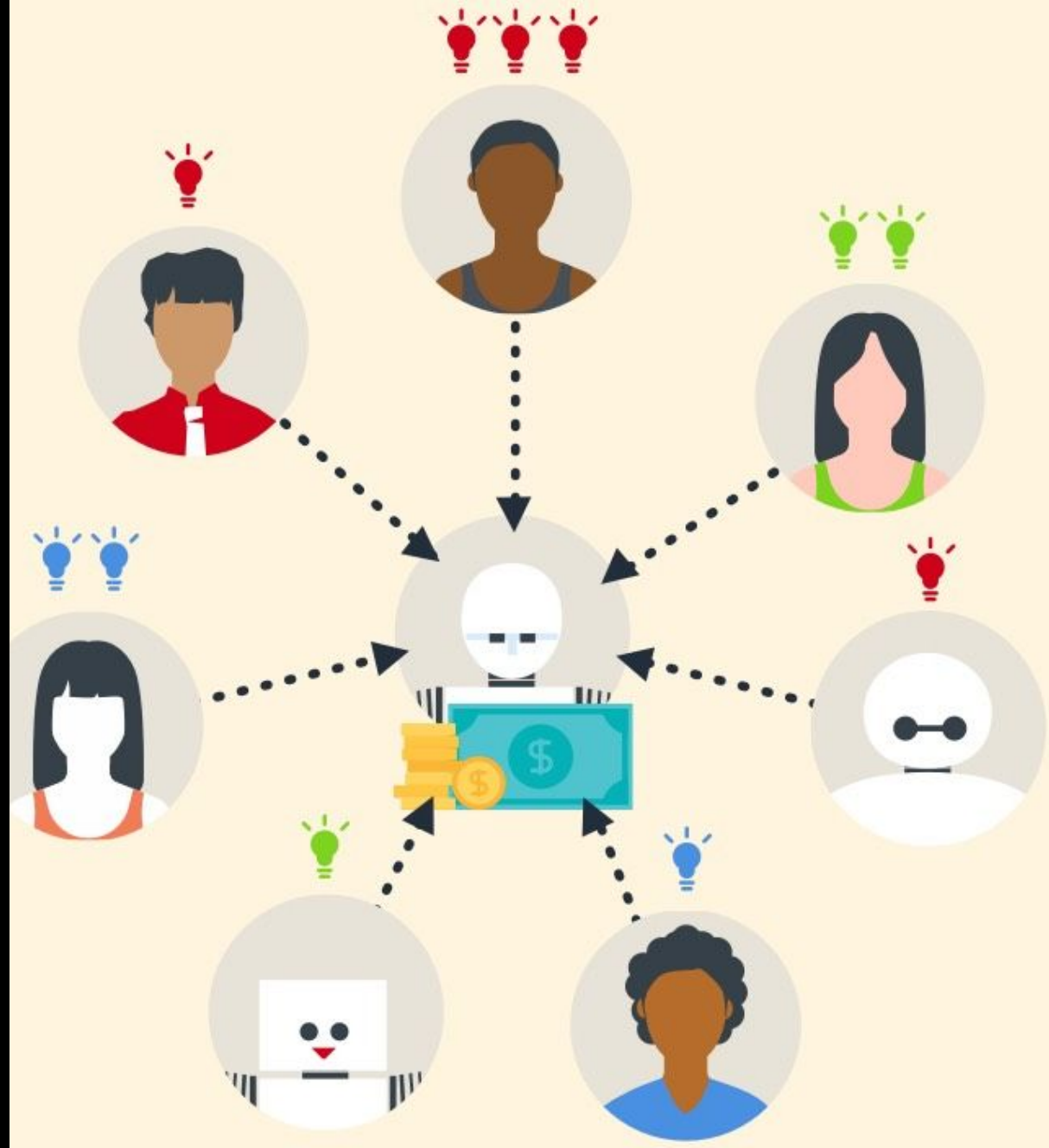
```
contract MyCoin {
    /* This creates an array with all balances */
    mapping (address => uint256) public balanceOf;

    /* Initializes contract with initial supply coins to the creator of the contract */
    function MyCoin(
        uint256 initialSupply
        ) public {
        balanceOf[msg.sender] = initialSupply;
    }

    /* Send coins */
    function transfer(address _to, uint256 _value) public {
        require(balanceOf[msg.sender] >= _value);           // Check if the sender has enough
        require(balanceOf[_to] + _value >= balanceOf[_to]); // Check for overflows
        balanceOf[msg.sender] -= _value;                    // Subtract from the sender
        balanceOf[_to] += _value;                           // Add the same to the recipient
    }
}
```

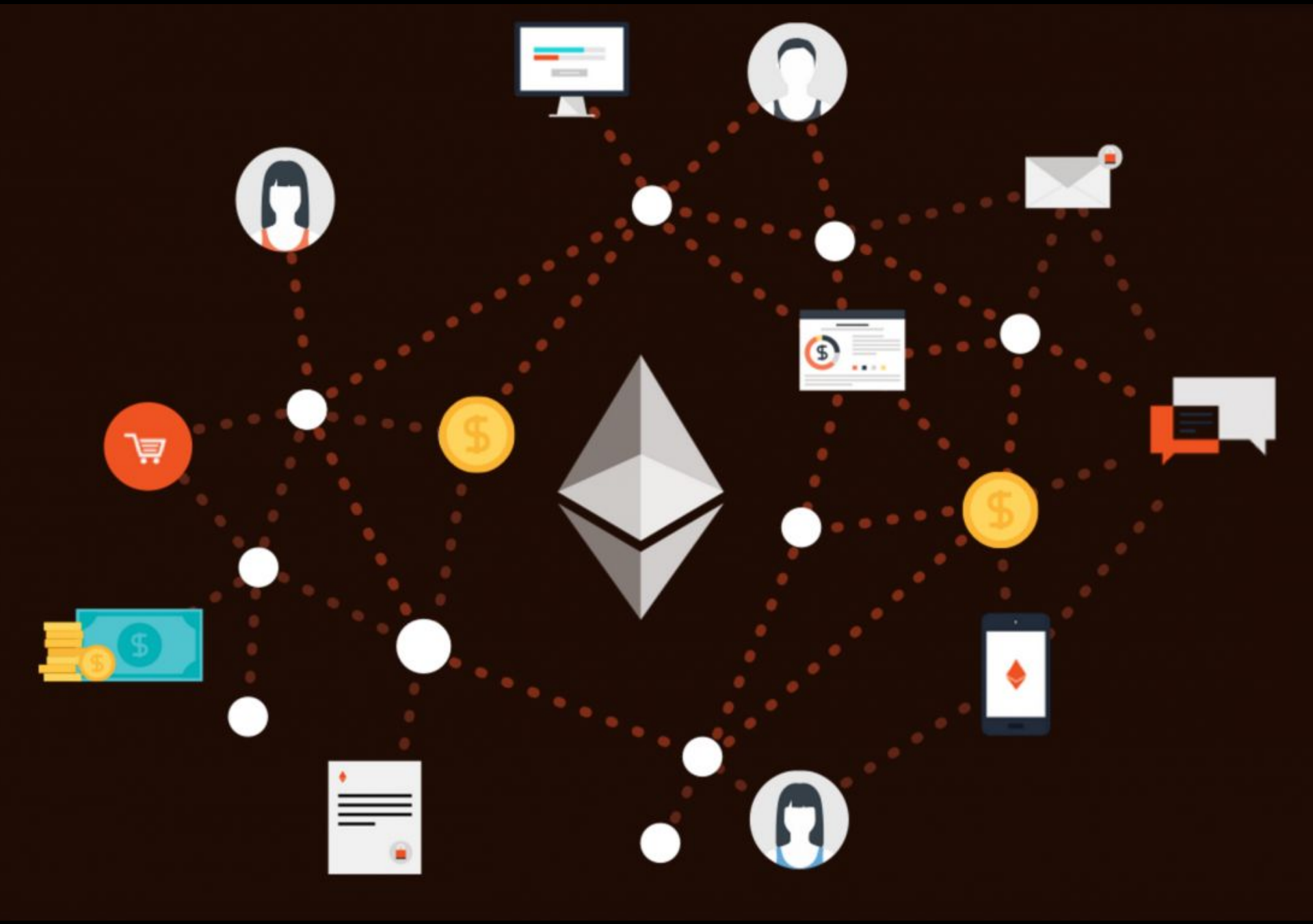
[https://www.ethereum.org/token]

Decentralized Autonomous Organization

Sarebbe possibile creare una democrazia digitale basata sul consenso?

https://www.ethereum.org/dao





CryptoZombies

CryptoZombies è un corso di programmazione interattivo e gratuito che ti insegna a creare giochi su Ethereum.

Viene utilizzato il linguaggio Solidity per creare smart contracts.

Il corso è progettato per partire dalle basi assolute.

cryptozombies.io

Cosa è ERC-20?

- Prima che venisse creato lo standard dell'ERC-20, si erano verificati diversi problemi di compatibilità tra le varie forme di token di Ethereum. **Ogni token possedeva uno smart contract completamente unico.**

- ERC-20: **Standard** per la creazione di token Ethereum.

- I token possono fungere da quote in un progetto, certificati di proprietà di asset, punti fedeltà o persino criptovalute vere e proprie (hanno indirizzi ETH).

- Facili da creare: https://coinlaunch.market/coincreator

- **Contro**: porta ad un'abbondanza di token molto simili e rende il processo di selezione da parte di possibili investitori più complesso e confusionario.

[https://it.ihodl.com/tutorials/2018-03-26/token-erc-20-guida-ico-ethereum-tutorial]

Initial Coin Offering / Token Sale

ICO

Its a bit like a mix between an IPO and Online Crowdfunding, but for Cryptocurrency.

History of ICOs

Mastercoin
$500 000
July 2013

Maidsafe
$7 Million
April 2014

EOS
$185 Million
Ongoing

Ethereum
$18 Million
July 2014

Tezos
$232 Million
July 2017

Waves
$16 Million
June 2016

Bancor
$156 Million
June 2017

TheDAO
$150 Million
April 2016

Status
$100 Million
June 2017

Qtum
$15,5 Million
March 2017

Gnosis
$13 Million
April 24, 2017

Gnosis Dutch Auction:
4,17% of tokens sold to investors.
95,83% kept by the Gnosis team.
Total market cap: $312 Million

BlockchainHub

ParkinGO lancia GOT: il suo Token Digitale!

Il GOToken è una moneta che permette di acquistare tutti i servizi offerti dalla piattaforma ParkinGO.
È partita la token sale pubblica che si concluderà il 3 luglio.

Dal **04 luglio 2018**, potrai pagare i servizi ParkinGO con i GOToken usufruendo di esclusivi vantaggi.

Permissionless

Vs

Permissioned

Le reti Blockchain possono essere categorizzate in due classi:

- **Permissionless**: Tutti possono partecipare alla rete ed inviare le transazioni. La fiducia è garantita dal protocollo crittografico.

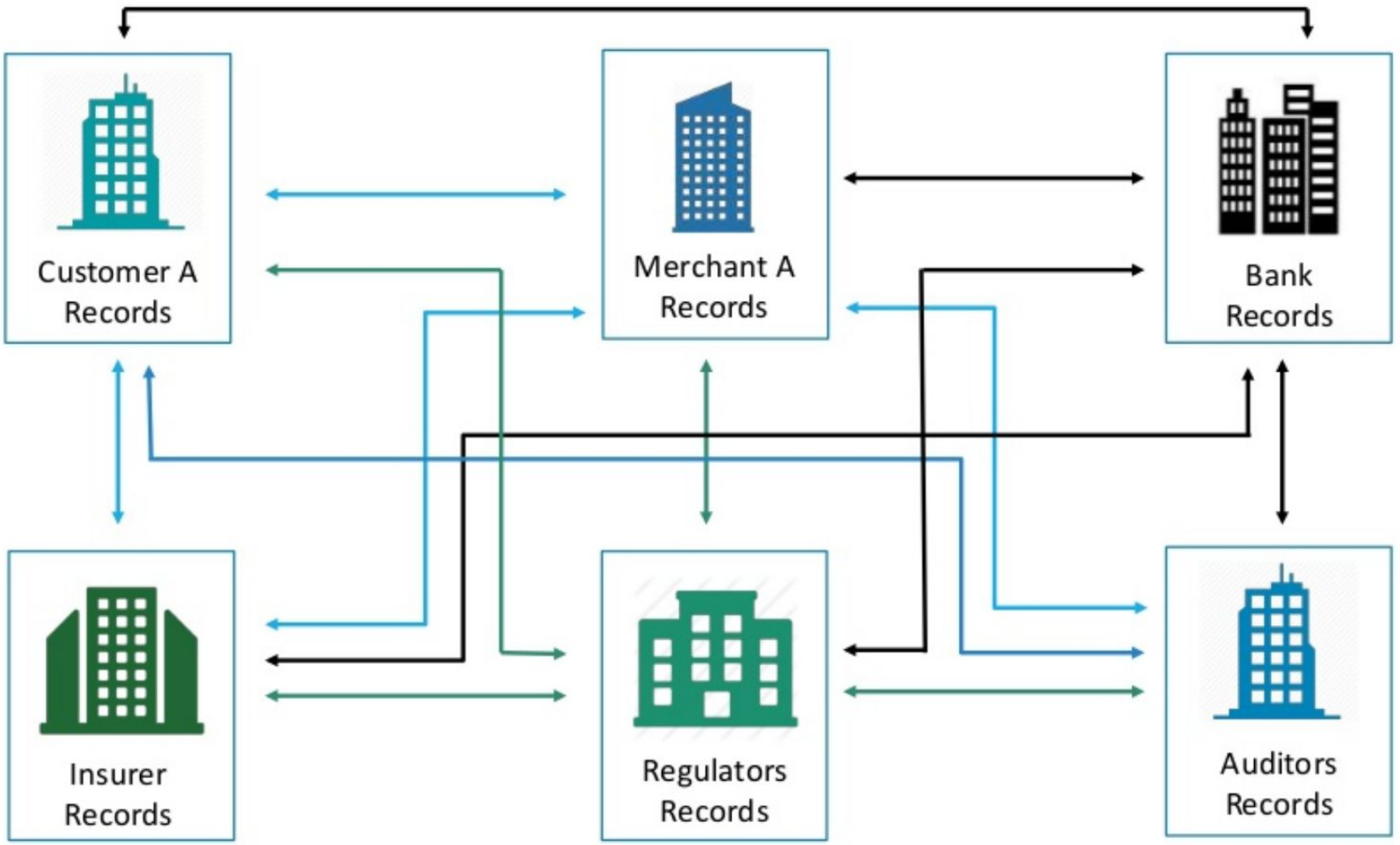
  Esempio: bitcoin

- **Permissioned**: Un membro ha bisogno di essere autenticato per partecipare alla rete e sottomettere delle transazioni.

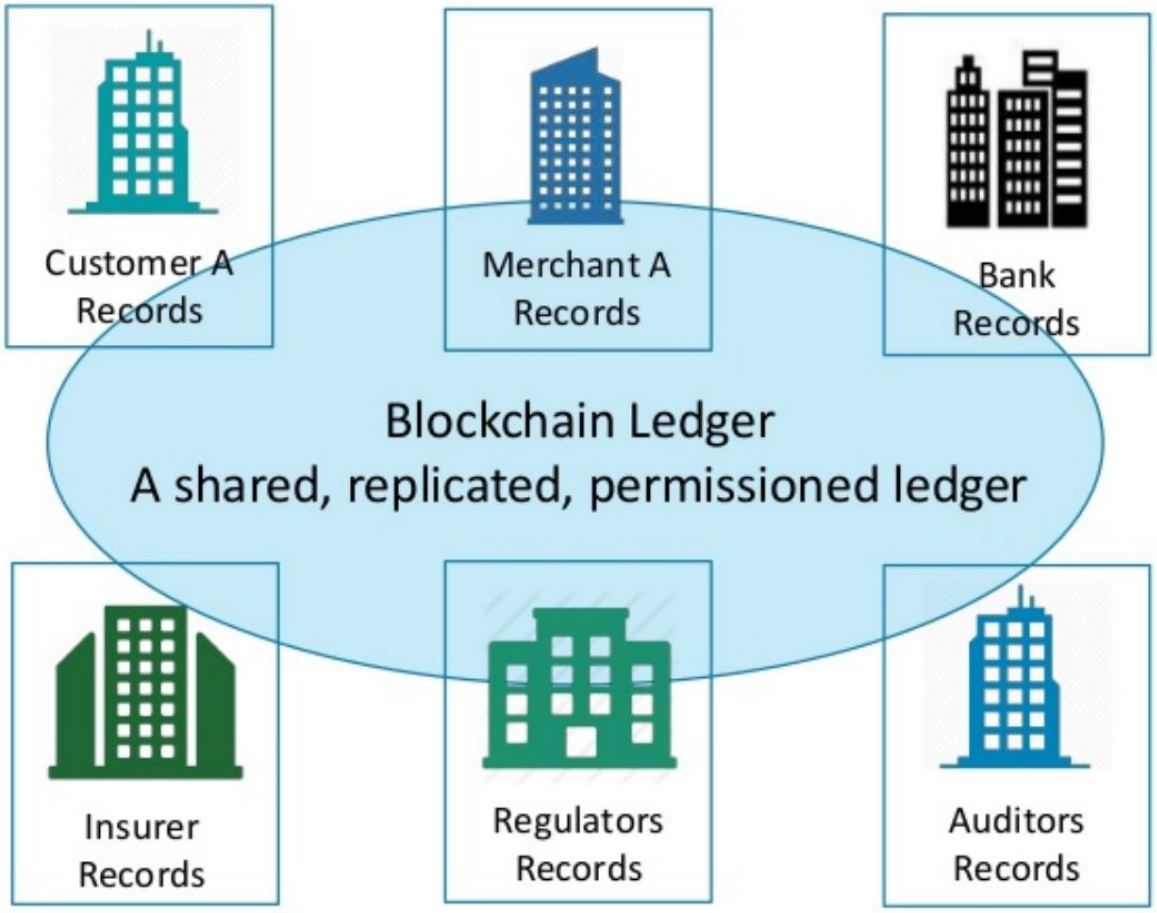
  Esempio: Hyperledger fabric

Hyperledger

Problema

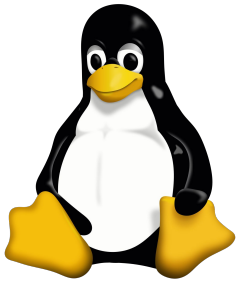

Customer A Records
Merchant A Records
Bank Records
Insurer Records
Regulators Records
Auditors Records

Problema



- ✓ Consensus
- ✓ Immutability
- ✓ Provenance
- ✓ Finality

HYPERLEDGER



CLOUDFOUNDRY

Hyperledger members

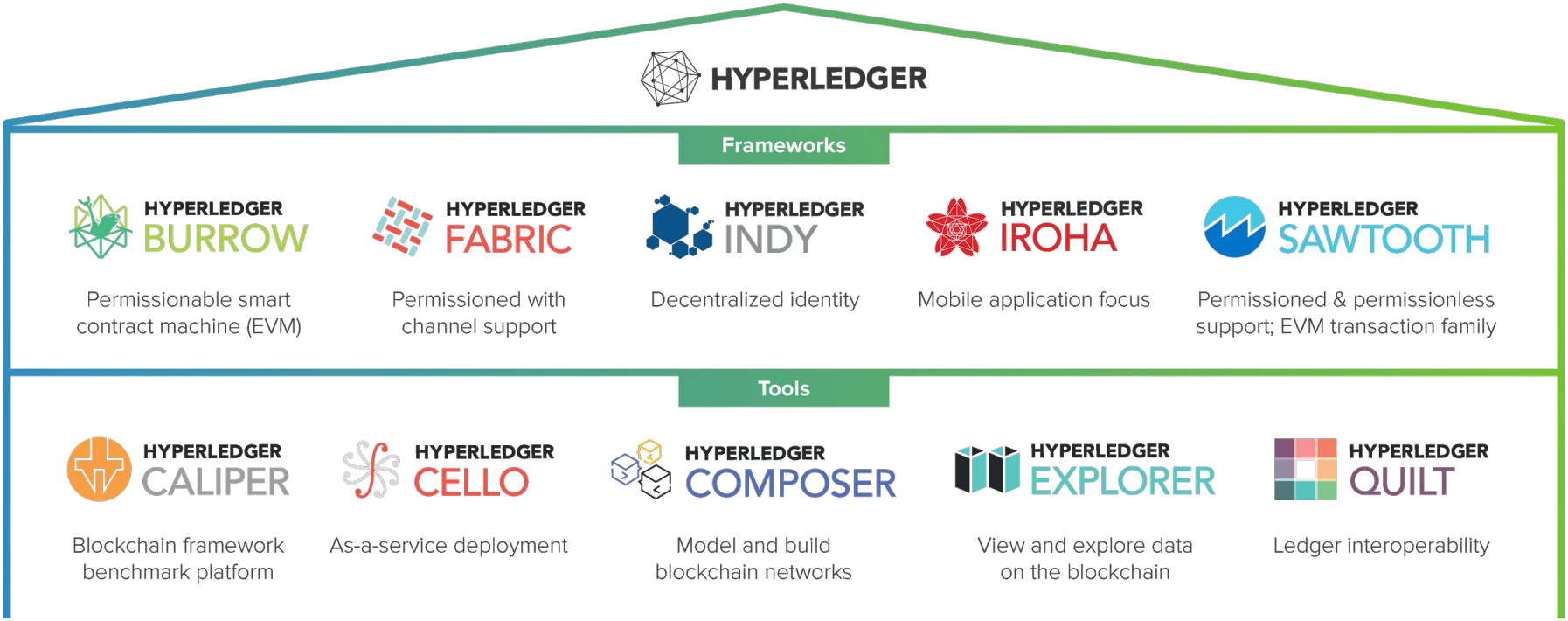
Premier

General

Associate

Source: https://www.hyperledger.org/about/members
Updated 14 February 2018

Hyperledger Foundation

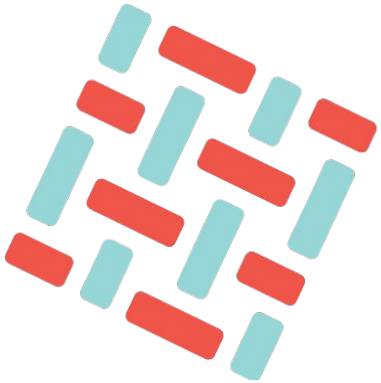


HYPERLEDGER

THE LINUX FOUNDATION

Hyperledger Fabric

- Permissioned Blockchain
  (utenti autorizzati - no PoW)
- Transazioni private
- Sevizio principale: distributed ledger e ordinamento delle transazioni
- Veloce e scalabile
- Nessuna criptovaluta associata
- Gestione di smart contracts

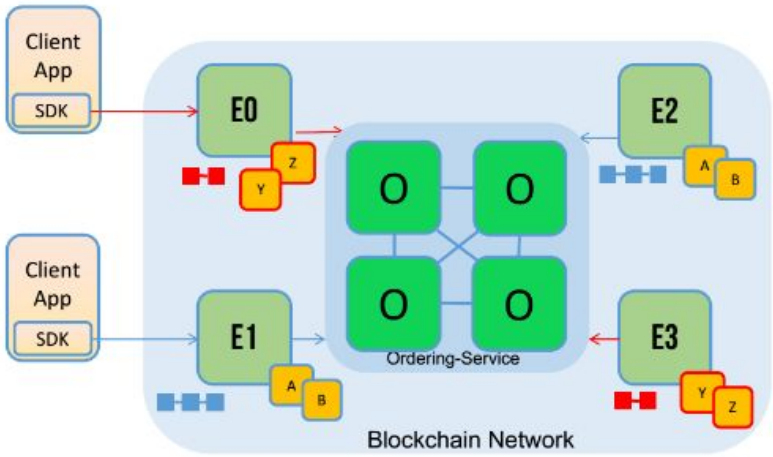


HYPERLEDGER
FABRIC

[https://vitalflux.com/hyperledger-fabric-channels-private-blockchain-deep-dive/]

Hyperledger Fabric - Canali privati

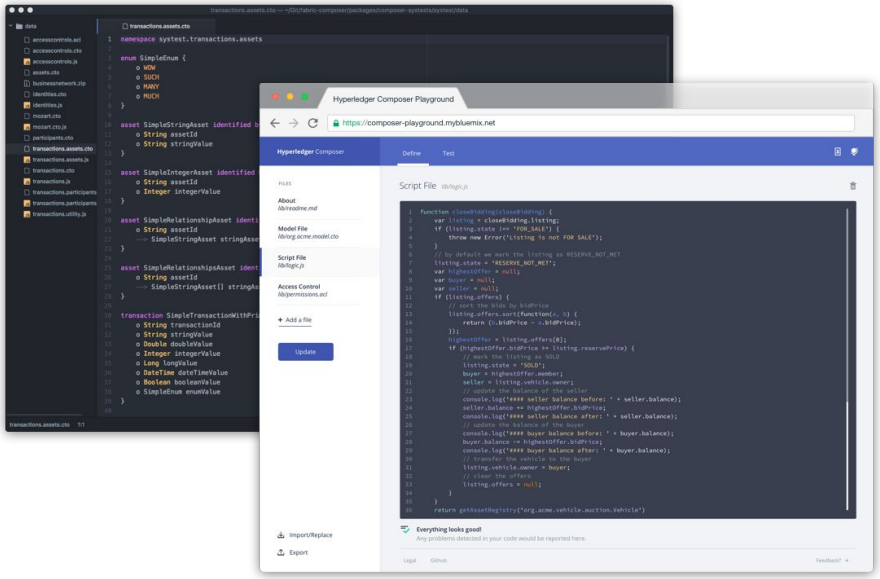
- Hyperledger Fabric è basata su canali (gruppi di due o più membri della blockchain).
- L'identità dei membri è verificata.
- I canali permettono di scambiare transazioni che sono validate e possono fare parte di smart contracts.
- Le transazioni nei canali rimangono private (ma con ordine definito e vincolanti).



[https://vitalflux.com/hyperledger-fabric-channels-private-blockchain-deep-dive/]

HYPERLEDGER FABRIC

Hyperledger Composer



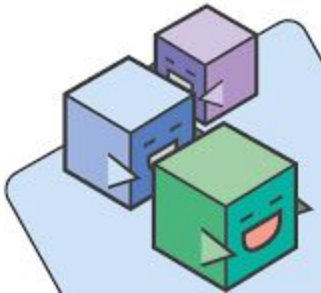
Hyperledger Composer è un framework che permette di comporre delle applicazioni su Hyperledger Fabric.

Guida l'utente nella modellazione del suo problema di business tramite la definizione di: **assets, partecipanti e transazioni**.

Permette di portare la propria soluzione in produzione in tempi rapidi.

https://hyperledger.github.io/composer

HYPERLEDGER
COMPOSER



50+ BLOCKCHAIN
REAL WORLD USES CASES

GOVERNMENT
Essentia develops world's first blockchain solution to manage international logistics hub together with Traffic Labs and the Finnish Government

essentia.one

IDENTIFICATION
Voter registration is being facilitated via a blockchain project in Switzerland spearheaded by **Uport**.

uport

MOBILE PAYMENTS
The blockchain ledger that **Ripple** uses has been latched onto by a group of Japanese banks, who will be using it for quick mobile payments.

ripple

INSURANCE
A smart contract-based blockchain is being used by Insurer **American International Group Inc** as a means of saving costs and increasing transparency.

AIG

ENDANGERED SPECIES PROTECTION
The protection of endangered species is being facilitated via a blockchain project that records the activities of these rare animals.

CARBON OFFSETS
IBM is using the Hyperledger Fabric blockchain in China to monitor carbon offset trading.

IBM HYPERLEDGER

ENTERPRISE
Ethereum's blockchain can be accessed as a cloud-based service courtesy of **Microsoft Azure.**

Microsoft Azure

BORDER CONTROL
Essentia has devised a border control system that would use blockchain to store passenger data in the Netherlands.

essentia.one

SUPPLY CHAINS
IBM and **Walmart** have partnered in China to create a blockchain project that will monitor food safety.

IBM Walmart

HEALTHCARE
A number of healthcare systems that store data on the blockchain have been pioneered including **MedRec.**

MEDREC

SHIPPING
Shipping is a natural fit for blockchain, and **Maersk** have been trialling a blockchainbased project within the maritime logistics industry.

MÆRSK

REAL ESTATE
Blockchain is now being used to complete real estate deals, the first of which was conducted in Kiev by **Propy.**

PROPY

ENERGY
Essentia is developing a test project that will help energy suppliers track the distribution of their resources in real time, whilst maintaining data confidentiality.

essentia.one

LAND REGISTRY
Land registry titles are now being stored on the blockchain in Georgia in a project developed by the **National Agency of Public Registry**.

NATIONAL AGENCY of PUBLIC REGISTRY

COMPUTATION
Digital Currency Group are helping Amazon Web Services examine ways in which the distributed ledger technology can help improve database security.

DIGITAL CURRENCY GROUP

ADVERTISING
New York Interactive Advertising Exchange has been experimen- ting with blockchain as a means of providing an ads marketplace for publishers.

NYIAX

BORDER CONTROL
Essentia is developing a blockchain project for border control that will allow customs agents to record passenger data from an array of inputs and safely store it.

essentia.one

JOURNALISM
Decentralized journalism, as enabled by blockchain technology, has the potential to prevent censorship and increase transparency, as **Civil** has shown.

CIVIL

WASTE MANAGEMENT
Waltonchain is using **RFID** technology to store waste management data on the blockchain in China.

ENERGY
Food importation is another industry where blockchain is proving its worth, with **Louis Dreyfus Co** trialling a soybean importation operation using this technology.

LDC. Louis Dreyfus Company

DIAMONDS
The **De Beers Group** is using blockchain to track the importation and sale of diamonds.

DE BEERS GROUP OF COMPANIES

FINE ART
By storing **certificates** of authenticity on the blockchain, it's possible to dramatically reduce art forgeries, as one blockchain project is proving.

NATIONAL SECURITY
For the past two years, the **US Department of Homeland Security** has been using blockchain to record and safely store data captured from its security cameras.

TOURISM
In a bid to boost its tourism economy, **Hawaii** is examining ways in which blockchain-based cryptocurrencies can be adopted throughout the US state.

TAXATION
In China, a tax-based initiative is using blockchain to store tax records and electronic invoices led by **Miaocai Network**.

ENERGY
Chile's National Energy Commission has started using blockchain technology as a way of certifying data pertaining to the country's energy usage as it seeks to update its electrical infrastructure.

CNE COMISIÓN NACIONAL DE ENERGÍA

RAILWAYS
Russian rail operator **Novotrans** is storing inventory data on a blockchain pertaining to repair requests and rolling stock

ДРУЗОВАЯ КОМПАНИЯ НОВОТРАНС

ENTERPRISE
Google is building its own blockchain which will be integrated into its cloud-based services, enabling businesses to store data on it, and to request their own white label version developed by **Alphabet Inc**

Google Alphabet

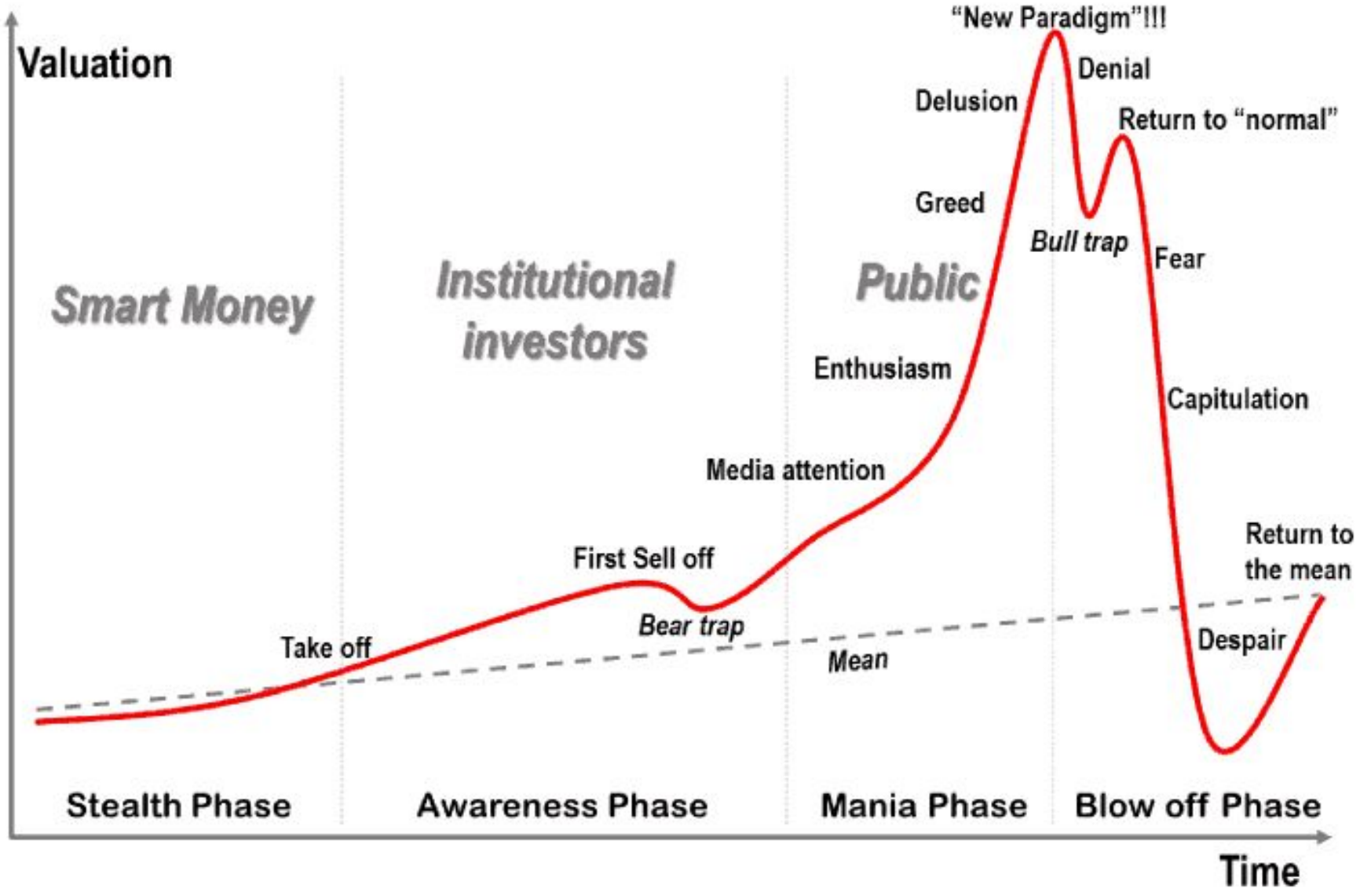
MUSIC
Arbit is a blockchain-based project led by former Guns N Roses drummer Matt Sorum seeking a fairer way to reward musicians for their creative efforts.

arbit

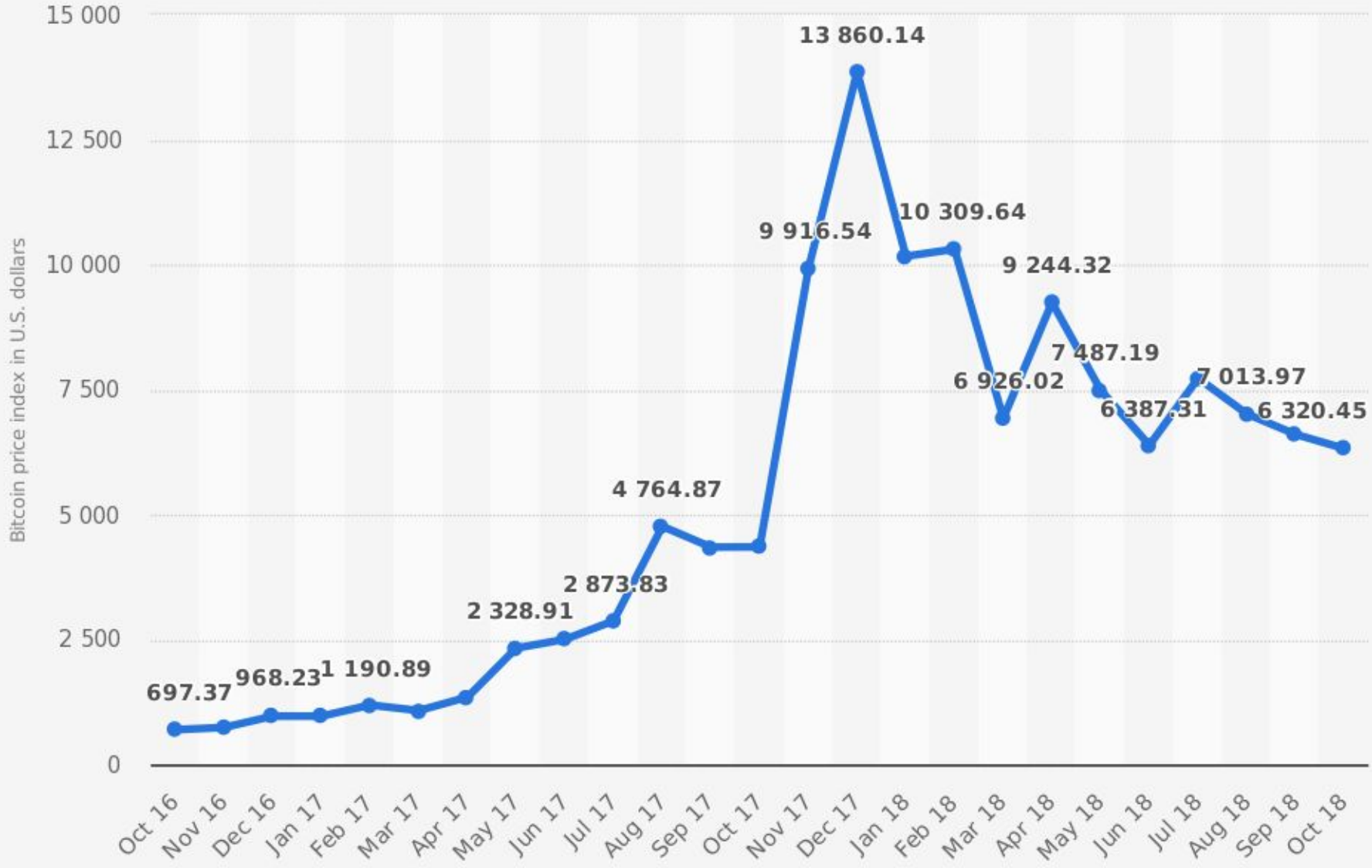
FISHING
Blockchain technology has been used to provide a transparent record of where fish was caught, as a means of ensuring it was legally landed.

THE INTERNET OF BLOCKCHAIN FOUNDATION

Is the Blockchain a bubble?


Valuation
"New Paradigm"!!!
Denial
Delusion
Return to "normal"
Greed
Bull trap
Fear
Smart Money
Institutional investors
Public
Enthusiasm
Capitulation
Media attention
Return to the mean
First Sell off
Bear trap
Take off
Mean
Despair
Stealth Phase
Awareness Phase
Mania Phase
Blow off Phase
Time

Bitcoin price index from October 2016 to October 2018 (in U.S. dollars)



Source
CoinDesk

Additional Information:
Worldwide; CoinDesk


Tulip price index 1636-37
200
150
100
50
25
Nov 12
Nov 25
Dec 1
Dec 12
Feb 3
Feb 5
Feb 9
May 1

Dot-com bubble

Demo Time

- https://anders.com/blockchain
- https://coindemo.io
- https://blockchaindemo.io

Thanks!

Enrico Bacis
enricobacis.com
enrico.bacis@unibg.it

Unibg Seclab
seclab.unibg.it
seclab@unibg.it