UNA INTRODUZIONE A BITCOIN

Milano, febbraio 2016

che cosa è bitcoin

- quando parliamo di bitcoin parliamo in realtà di due cose distinte che, pur essendo nate e cresciute insieme
  - sono concettualmente separate
  - possono in parte esistere l'una indipendentemente dall'altra

- la prima cosa è bitcoin come "moneta elettronica"

- la seconda cosa è bitcoin come "sistema di transazioni" per lo scambio di questa moneta elettronica

bitcoin come moneta elettronica 1/2

- bitcoin ha tutte le caratteristiche di una moneta:
  - ha un valore
  - è negoziabile e convertibile con altre monete
  - viene accettata come mezzo di pagamento
  - è anonima (con alcune limitazioni)

- ma, a differenza delle monete cui siamo abituati
  - non esiste (ancora) fisicamente
  - non è emessa da alcun ente centrale (non esiste la banca centrale dei bitcoin)
  - ha un tetto alla circolazione (21 milioni bitcoin), per cui non è inflazionabile
  - questa ultima caratteristica la rende più simile ad una hard commodity (ad esempio all'oro) che ad una moneta

bitcoin come moneta elettronica 2/2

- la validità di bitcoin come moneta elettronica, nel senso descritto prima, è contestata e sotto attacco
- dal punto di vista teorico si contesta
  - la desiderabilità di una moneta non inflazionabile
  - la ingovernabilità di un sistema in cui la moneta viene creata in modo algoritmico (anzichè secondo le necessità dell'economia reale)
- dal punto di vista pratico si contesta
  - la eccessiva fluttuazione di valore che la rende poco interessante come "store of value" https://blockchain.info/charts/market-price
  - la eccessiva facilità di scambio e l'eccessivo livello di anonimato delle transazioni che permettono di eludere la maggior parte dei controlli doganali, valutari, fiscali, ecc
  - il fatto che proprio per queste ragioni bitcoin sia diventata la moneta di elezione per le transazioni illegali

bitcoin come sistema di transazioni 1/2

- è un sistema che veicola pagamenti senza necessità di un ente centrale, né come trusted party, né come arbitro di controversie
- è un sistema distribuito (peer-to-peer) costituito da un numero elevato di nodi di elaborazione
- assicura il controllo forte sulla proprietà della moneta attraverso un sistema crittografico di firme digitali
- rende impossibile il double-spend attraverso la creazione di un giornale pubblico, condiviso e univoco di tutte le transazioni avvenute nel sistema
- tutte le transazioni sono registrate nel giornale univoco in modo anonimo
- il giornale univoco è replicato e memorizzato in ciascun nodo che partecipa alla rete
- le rete dei nodi non è strutturata gerarchicamente e robusta nella sua semplicità
- ciascun nodo può abbandonare la rete e riconnettersi in qualsiasi momento: la ricezione della copia più aggiornata del giornale lo mette in grado di operare
- il sistema è sicuro fino a che una maggioranza dei nodi non coopera alla falsificazione del giornale univoco

bitcoin come sistema di transazioni 2/2

- questi principi sono stati incarnati in un software open-source (bitcoind) che definisce lo standard della moneta e dei protocolli di scambio in termini di algoritmi, protocolli e interfacce
- questo software svolge tutte le funzioni necessarie al funzionamento del sistema di transazioni e in particolare:
  - le funzioni di borsellino elettronico
  - le funzioni di creazione dei blocchi
  - le funzioni di concatenazione dei blocchi e di pubblicazione del giornale condiviso
- esistono ad oggi numerosi software derivati dall'originale bitcoind che svolgono alcune di queste funzioni in modo specializzato, ad esempio:
  - borsellini per dispositivi mobili
  - POS
  - miners (vedi più avanti)

sistema: il borsellino elettronico

- le principali funzioni del borsellino elettronico sono:
  - tenere traccia di tutte le transazioni dare/avere in entrata e in uscita
  - evidenziare in ogni momento il saldo disponibile
  - generare e conservare le coppie di chiavi privata/pubblica che servono per autenticare le transazioni in uscita
  - creare le transazioni di pagamento e trasmetterle ai nodi più vicini della rete
  - le transazioni contengono obbligatoriamente almeno
    - l'importo della transazione (fino all'ottavo decimale di bitcoin)
    - l'indirizzo elettronico del destinatario
    - la provenienza dei fondi (una o più transazioni in entrata)
    - la chiave crittografica del mittente (che rende non ripudiabile la transazione stessa)
  - le transazioni possono essere n-to-m, cioè possono combinare bitcoin provenienti da n incassi diversi per pagare m percettori diversi

sistema: la creazione dei blocchi

- una volta firmata crittograficamente nel borsellino e inviata la transazione entra a far parte del giornale condiviso ed è visibile a tutti
- riporta in chiaro la chiave pubblica del pagatore e del percettore, quindi la privacy è garantita solo fintanto che non diventi noto il proprietario della chiave pubblica
- le transazioni vengono poi raggruppate in blocchi che vengono sigillati crittograficamente e diventano immodificabili da quel momento in poi
- i blocchi sigillati vengono inoltrati a tutti i nodi della rete
- ciascun nodo verifica che la operazione di sigillatura sia stata compiuta correttamente e che quindi il blocco sia valido
- mentre questa operazione di verifica è banale in termini di risorse computazionali, l'operazione di creazione del sigillo è volutamente onerosa per scoraggiare ulteriormente tentativi di falsificazione
- i nodi che collaborano alla creazione dei sigilli vengono remunerati attraverso la assegnazione di un certo numero di bitcoin (è il cosiddetto "mining")
- una volta sigillata in un blocco una transazione viene considerata confermata, viene poi considerata sicura dopo sei successive conferme

sistema: la concatenazione dei blocchi

- la chiave crittografia che sigilla ciascun blocco punta univocamente al blocco precedente, creando una catena ininterrotta (come la successione di pagine del giornale univoco: non si possono aggiungere, né strappare pagine)
- in questo modo viene garantita la completezza del giornale univoco sin dalla sua origine
- ciascun nodo propaga ciascun blocco sigillato a tutti i nodi limitrofi collegati
- esistono meccanismi per ridurre le dimensioni del giornale univoco e altri meccanismi consentono la verifica semplificata dei pagamenti

sistema: vantaggi della block-chain

- le idee che stanno alla base della blockchain stanno incontrando vivo interesse nella comunità finanziaria e attirano investimenti crescenti
- piacciono in particolare:
  - anonimato e non ripudiabilità delle transazioni
  - tracciabilità totale delle transazioni stesse
  - garanzia di completezza cronologica
  - pubblicità delle informazioni
  - bassissimi costi operativi (un ventesimo circa di un tradizionale sistema di carte di credito)

- questi vantaggi non sfuggono più al pubblico e agli investitori ed esistono letteralmente centinaia di start-up e molte grandi banche che vogliono replicare le logiche della block-chain
- il motto potrebbe essere: “come funziona bene questo sistema aperto e decentralizzato - facciamone una versione chiusa e centralizzata”

il bitcoin mining

- come già anticipato il lavoro (oneroso) di sigillatura dei blocchi viene remunerato assegnando un certo numero di bitcoin a chi lo svolge con successo
- attualmente la sigillatura di un blocco viene remunerata con 25 bitcoin
- questo è l'unico meccanismo attraverso il quale vengono generati nuovi bitcoin e si chiama mining (se il bitcoin è assimilabile all'oro, allora il lavoro speso per creare nuovi bitcoin è assimilabile al mining)
- poiché si tratta di un'attività remunerata, è nata tutta un'industria, dapprima domestica e quindi sempre più complessa e sofisticata
- oggi esistono chip e calcolatori specializzati per il mining, datacenter ad hoc, fondi di investimento, ecc. che hanno come scopo la sigillatura sempre più efficiente dei blocchi
- sofisticati meccanismi statistici di regolazione del sistema pero garantiscono che non si possa sigillare più di un blocco ogni 10 minuti circa
- questo è il meccanismo di base attraverso cui si mette un tetto al numero di bitcoin creati https://en.bitcoin.it/wiki/Controlled_supply

in sintesi

- personalmente non sono qualificato per discutere degli aspetti sociologici e di teoria monetaria di bitcoin come “moneta” e in particolare della sua validità come moneta universale alternativa (come viene talvolta proposta)

- viceversa come “sistema di transazioni” bitcoin è un algoritmo brillante e tradotto brillantemente in software, che permette di:
  - abbattere drasticamente i costi di transazione
  - annullare completamente i costi di riconciliazioni, dispute, contestazioni

- resta da vedere se e come potrà svilupparsi

la storia di bitcoin

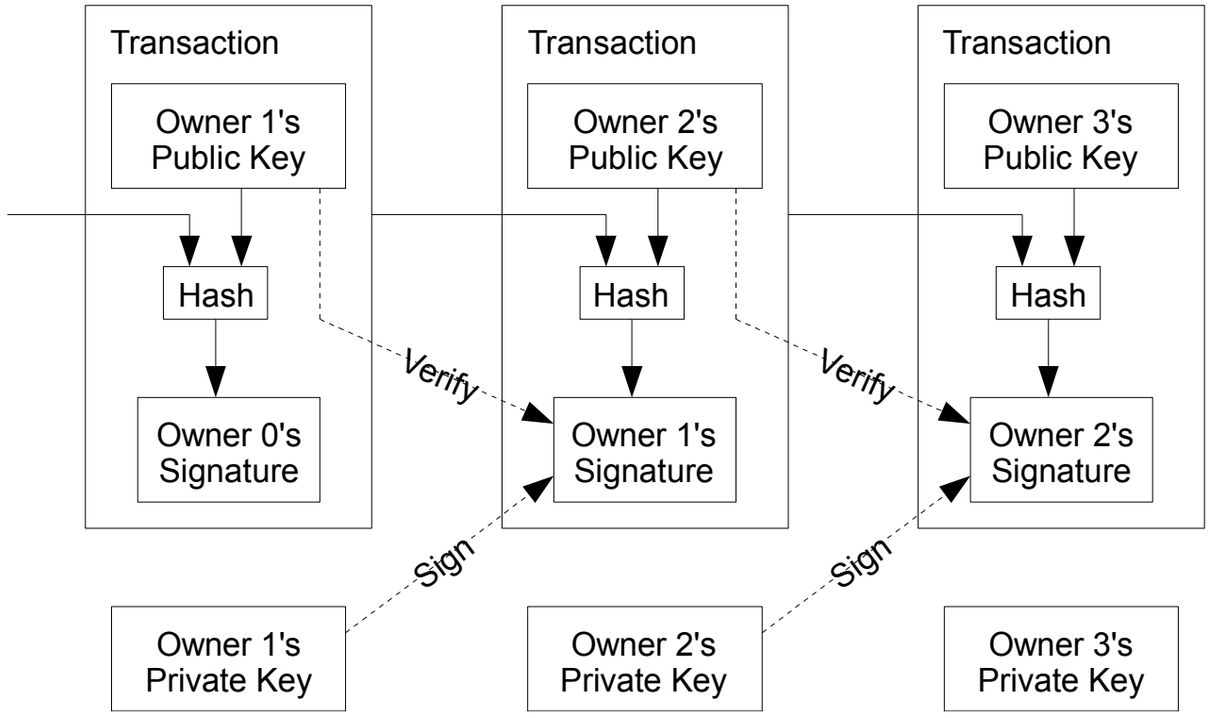
- bitcoin nelle sue due accezioni è stato descritto originariamente in un breve documento firmato Satoshi Nakamoto
- Satoshi Nakamoto è un nom-de-plume; il vero autore del documento è sconosciuto a tutt'oggi
- la prima release pubblica del software è del gennaio 2009
- la versione originaria del software risulta scritta da Satoshi Nakamoto e da alcuni riconosciuti esperti di crittografia
- il primo blocco è stato sigillato il 9 gennaio 2009; conteneva una sola transazione di 50 bitcoin per l'acquisto di una pizza
- ad oggi (febbraio 2016)
  - la block-chain è lunga un po' meno di 400.000 blocchi https://blockchain.info
  - sono collegati alla rete circa 6.000 nodi https://bitnodes.21.co
  - vengono elaborate più di 200.000 transazioni al giorno https://blockchain.info/charts/n-transactions
  - il sistema ha funzionato ininterrottamente per sette anni e non è mai stato violato

principali riferimenti

- introduzione
  http://en.wikipedia.org/wiki/Bitcoin
- il paper original di Satoshi Nakamoto (8 pagine!)
  http://bitcoin.org/bitcoin.pdf
- il software (open source, licenza MIT)
  https://github.com/bitcoin/bitcoin
- il sito ufficiale
  http://bitcoin.org/
- il wiki con gli approfondimenti tecnici
  https://en.bitcoin.it/wiki/Category:Technical
- una descrizione esaustiva con enfasi sulle vulnerabilità (tesi di dottorato)
  https://dl.dropbox.com/u/3658181/PiotrPiasecki-BitcoinMasterThesis.pdf
- un paper sulla moneta elettronica virtuale della BCE (ottobre 2012)
  http://www.ecb.int/pub/pdf/other/virtualcurrencyschemes201210en.pdf
- il sistema in azione
  http://blockchain.info/
- per navigare in tempo reale blocchi, transazioni e indirizzi
  http://www.blockexplorer.com/

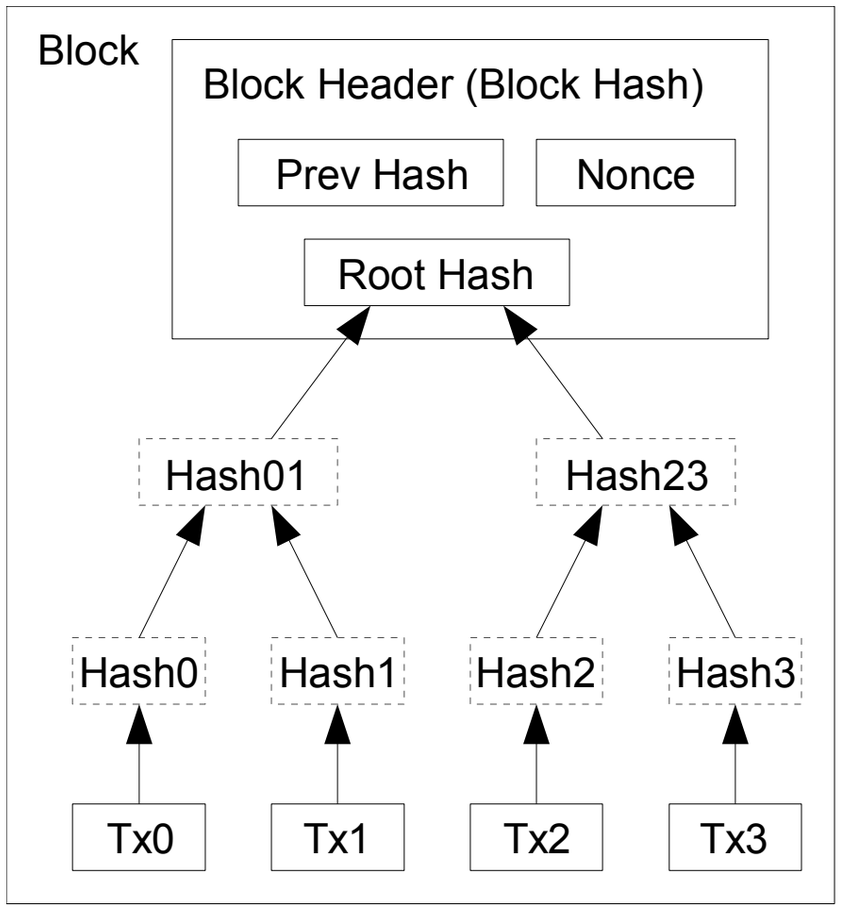
allegati: cambio USD/bitcoin

allegati: struttura di una transazione



Fonte: paper originale di Satoshi Nakamoto

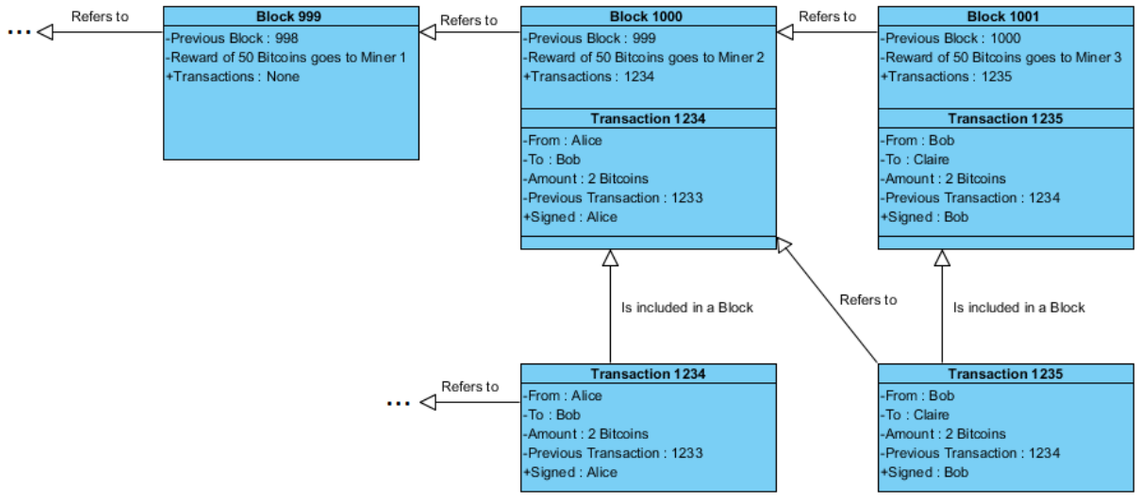
allegati: struttura di un blocco



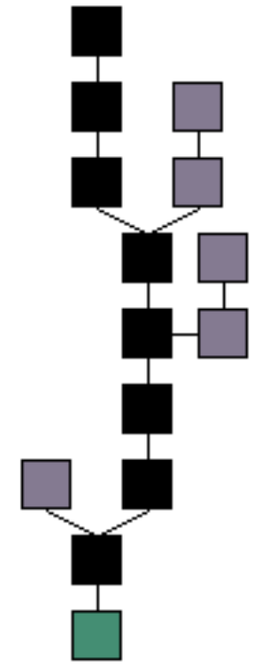
Transactions Hashed in a Merkle Tree

Fonte: paper originale di Satoshi Nakamoto

allegati: la catena più lunga fa testo

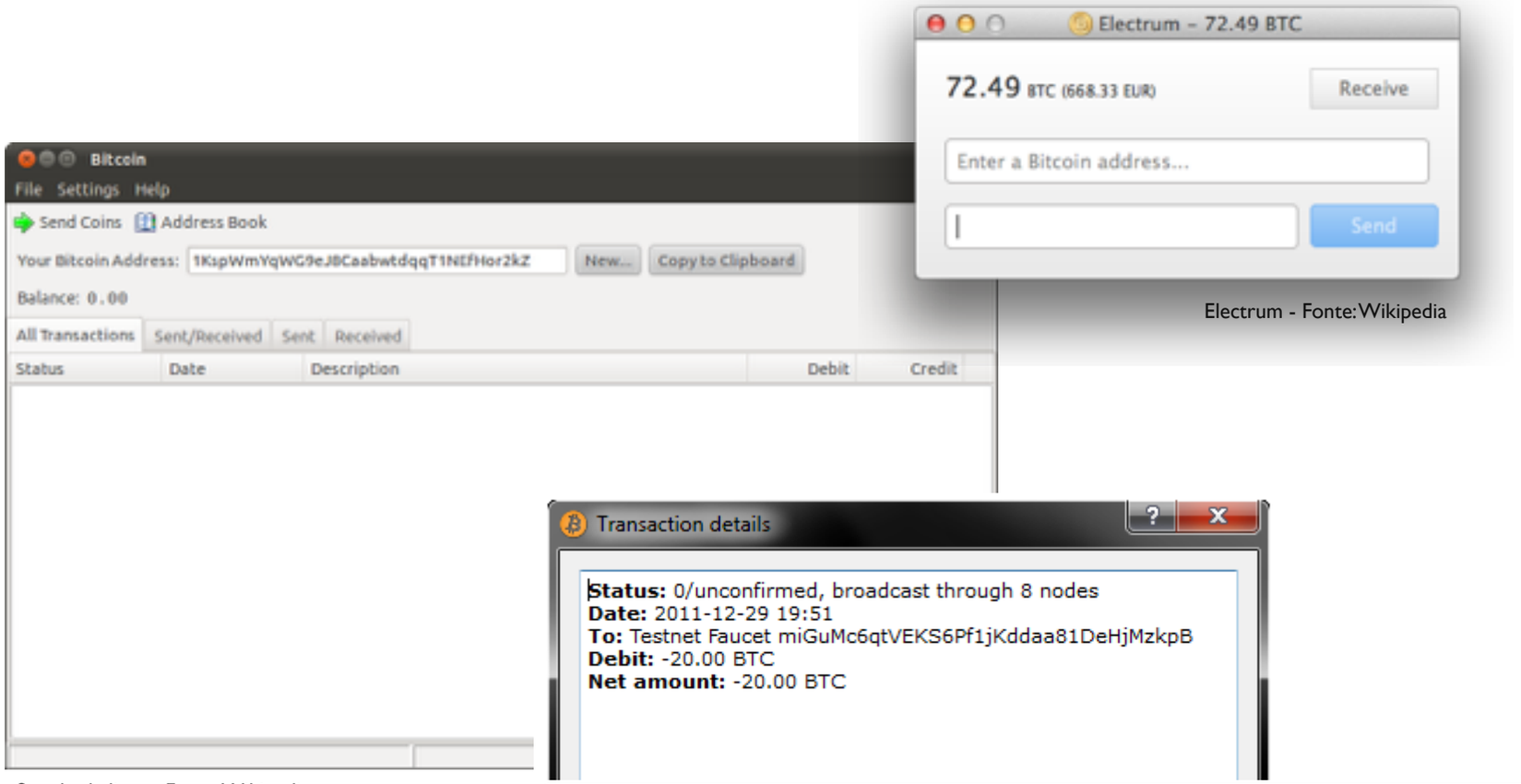


Fonte: tesi di dottorato di Piotr Piasecki



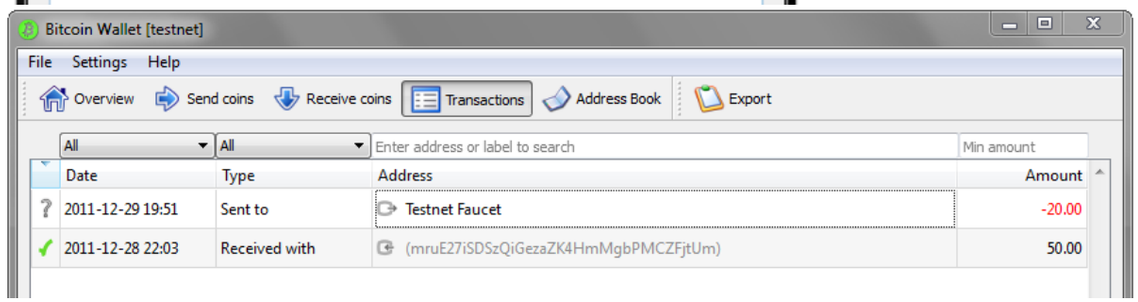
Fonte: Wikipedia

allegati: esempi di client



Electrum - Fonte: Wikipedia

Standard client - Fonte: Wikipedia



Standard Client (testnet) - Fonte: tesi di dottorato di Piotr Piasecki

élever - /ɛl.ve/
verbo francese
aumentare, incrementare, alzare

e•lever - /iˈliːvə/
nome inglese
crasi di electronic lever
leva elettronica

elever - /elever/
nome proprio italiano
il vostro partner per il digital