Abilità Informatiche

Blockchain e Monete Digitali

(Bitcoin)

A.A. 2020/2021

Blockchain

- Cos'è questa tecnologia?
- Internet non può trasferire una proprietà, un bene, una cosa preziosa, ma solo copie.
- Anche i sistemi di web banking in realtà utilizzano un intermediario. Posso considerare questo un limite?
- Nel 2008 compare un articolo di un tal Satoshi Nakamoto la cui identità non è ancora individuata con certezza, articolo che può essere considerato il documento fondativo.
- Ha illustrato un insieme di teorie crittografiche alla base di un sistema basato sul peer-to-peer, un particolare utilizzo dell'architettura distribuita.

"Bitcoin: un sistema di moneta elettronica peer-to-peer"

Blockchain

- L’identità del suo inventore, Satoshi Nakamoto, è avvolta ancora nel mistero. Sembra che sia Craig Wright, informatico australiano che afferma di essere l’inventore della tecnologia che sta dietro i bitcoin, ma ancora non si sa se sia una persona o un insieme di programmatori
- È interessante leggere quanto avvenuto nel 2019 (*)per comprendere come la nascita del bitcoin sia ancora non chiaramente identificata se non per quanto riguarda gli aspetti algoritmici, matematici e procedurali.

(*) https://iusletter.com/oggi-sulla-stampa/bitcoin-linventore-deve-pagare-5-miliardi/

Blockchain: concetti chiave (1)

- Blockchain è utilizzato in molteplici applicazioni, tra cui ***anche*** le criptovalute
- Concetti chiave:
  - **Rete e Nodi**
  - **Transazione**
  - **Ledger**
  - **Blocco**
  - **Funzione di Hash**
  - **Miner (mining)**
  - **Proof of Work (PoW)**
  - **Ricompensa (Reward)**
  - **Portafoglio (Wallet)**
  - **Chiave privata e chiave pubblica**

Blockchain (2)

Rete e Nodi: disponiamo di un database distribuito su tutti i nodi appartenenti alla rete

Transazione:

- Verificata
- Validata
- Confermata

Blocco di informazioni che comprende anche la marca temporale, Timestamp

Ledger: (Libro mastro distribuito) per registrare ogni transazione ogni volta che questo interviene in un cambio di proprietà; ogni nodo ha esattamente lo stesso archivio, lo stesso libro mastro contenente ***tutte*** le transazioni

Funzione di Hash, cioè trasformare le informazioni in un numero contenuto in uno specifico intervallo

Blockchain (3)

Miner (mining), to mine, scavare, andare al di la di quello che è già noto

Proof of Work (PoW): algoritmo di consenso, utilizzato per confermare le transazioni e generare i successivi blocchi della catena.

Ricompensa (Reward): tramite PoW i miner sono incentivati a competere tra loro nella verifica della transazione

Portafoglio (Wallet)

Chiave pubblica e chiave privata (v. slide sicurezza)

Sicurezza e immutabilità del dato

- È molto meno vulnerabile, sono decine di migliaia di nodi sparpagliati in giro per il mondo
- In caso di alterazione di un nodo tutti gli altri nodi hanno la stessa copia.
- Trasparenza e visibilità; in ogni nodo è possibile vedere il contenuto della transazione, partecipando così al ***"modello di consenso"***

Modello di consenso cioè un algoritmo, una regola matematica, come indicato nell'articolo di Nakamoto che lo rende possibile.

Come si scrive questa nuova transazione?

Sicurezza e immutabilità del dato

- Si costruisce il blocco che contiene un'informazione sintetica ed allo stesso tempo completa
- Si aggiunge alle informazioni il Timestamp, data e ora
- Si aggiunge il numero di Hash del blocco precedente
- La complessità dell'algoritmo garantisce che la formula sia sufficientemente complessa per tutelare il principio sul quale si fonda la blockchain
- Aggiungendo alle transazioni timestamp ed hash opero la **concatenazione** dei vari blocchi tra loro.
- Ogni blocco che viene creato contiene una informazione univoca del blocco precedente, come un'impronta digitale.
- ***Garantiamo così l'immutabilità del dato***

Cosa accade se…

- Ipotizziamo di voler modificare le informazioni, devo non solo incidere sul blocco corrente, ma anche su quello superiore ed ancora superiore.
- Questo processo dal punto di vista computazionale è (quasi?) impossibile.
- Nessuno è mai riuscito a violare questo tipo di meccanismo.
- In supersintesi: **è una catena di blocchi, leggibile da tutti e scrivibile da tutti, garantendo sempre l'immutabilità del dato**

alcune applicazioni……

- Garantire la proprietà intellettuale, il contenuto creativo che voglio registrare (es LIRAX.org)
- Reti elettriche: La direttiva 2001/2018/UE, L'art. 21 parla di autoconsumo elettrico **collettivo**. Esiste però un problema di misurazione, registrazione, vendita distribuita ecc. .. La blockchain permette di fissare le regole per rispondere a queste problematiche.
- Un articolo apparso qualche tempo fa "È italiano il primo cane su blockchain contro abbandono e commercio illegale" riporta "il progetto potrà garantire in prospettiva l'unificazione a livello nazionale dell'anagrafe canina (oggi organizzata su base regionale)…
- **W**orld **F**ood **P**rogramme, l'agenzia delle Nazioni Unite che si occupa della fame nel mondo. Il progetto si chiama Building Blocks (*).
- .. e molto altro

(*) https://innovation.wfp.org/project/building-blocks

Bitcoin in (super) sintesi

- Bitcoin può essere definita come una *cripto-moneta open source*
  - Non esiste un'autorità centrale.
  - Non dipende dalla fiducia in una particolare "istituzione"
- Equivalente al contante (non è una carta di credito!) ma "circolante" su Internet
- Non è la prima moneta digitale!
  - Fin dal 1982 erano state poste (da Chaum) le basi per il *cash* digitale
- Creata da Satoshi Nakamoto
  - Pseudonimo di Craig Wright?
  - Rivelato in un'intervista alla BBC (vedi giornali del 2 maggio 2016)
- Basata su una rete *peer-to-peer* di computer che eseguono il software *bitcoin*
  - Le transazioni sono verificate tramite un *proof-of-work* (la risoluzione di un problema) da sistemi che eseguono un software di *mining.*

Il successo di Bitcoin

Dipende da tre tipi di *consenso:*

1. Consenso sulle **regole**: i partecipanti concordano sui criteri che determinano quali transazioni sono valide;
   - Problema sociale
2. Consenso sullo **stato**: i partecipanti concordano su chi è il proprietario di quale (bit)coin in un qualsiasi momento;
   - Problema tecnologico
3. Consenso sul **valore**: i partecipanti concordano nell'accettare i bitcoin come forma di pagamento
   - Problema comune a tutte le valute!

Cosa è una moneta?

La moneta è un mezzo di scambio

- Rappresenta una forma alternativa, ampiamente accettata, di baratto
- Una moneta **dovrebbe** essere
  - Riconoscibile
  - Divisibile
  - Trasportabile
  - Trasferibile
  - Utilizzabile
  - Difficile da contraffare
  - Durevole nel tempo
- La quantità totale di moneta dovrebbe essere controllabile

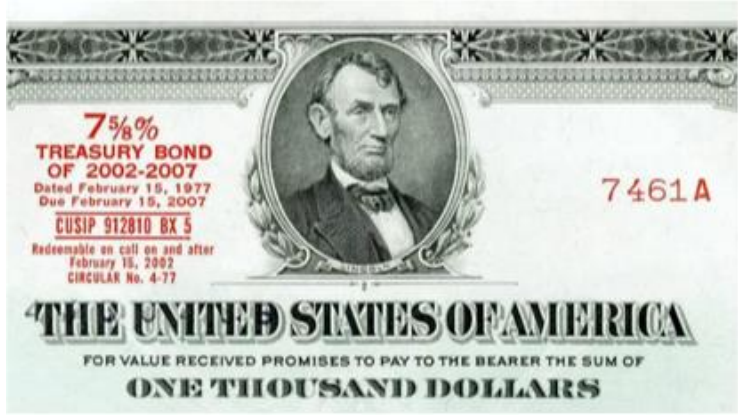
Cosa è una cripto-moneta?

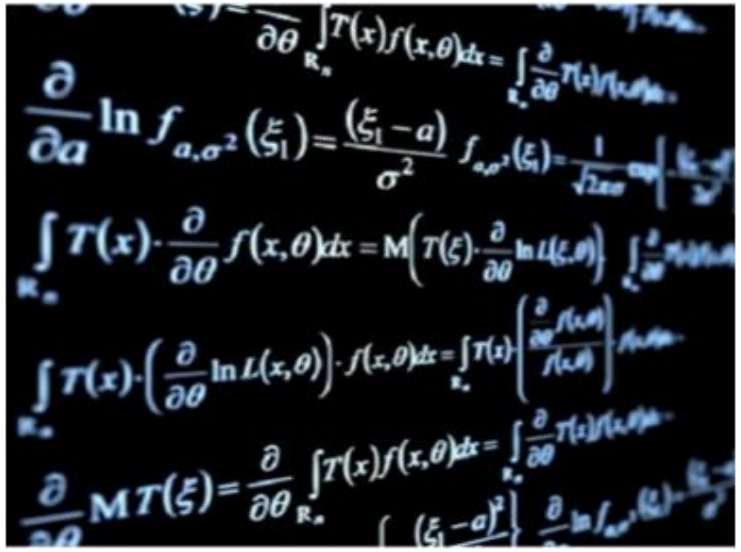
- È una moneta le cui proprietà
  - sicurezza
  - difficoltà di sostituzione

  derivano non da proprietà chimico fisiche ma matematiche:
  - basata su primitive crittografiche note e già ampiamente utilizzate

Nessuna legge (almeno al momento) regola la creazione e l'utilizzo delle cripto-monete.

Esistono molte (centinaia!) varianti di criptomonete.





Cosa rende bitcoin diversa?

Bitcoin è decentralizzata, distribuita, basata sul principio del *volunteer computing*

- Nessuna autorità centrale di emissione o controllo
  - Non esiste (almeno non è nota…) nessuna *Bitcoin corporation*
  - *Bitcoin foundation* (**bitcoinfoundation.org**)
  - Un numero crescente di imprese accettano o basano nuovi modelli di affari (più o meno leciti) su *bitcoin*
- Rispetto ad altri "strumenti al portatore"
  - Più facile da "trasportare" ovunque nel mondo
  - Più facile da rendere "sicura" (vedremo come)
- Rispetto ad altre monete elettroniche
  - Immune a leggi e/o confische
  - Immune dall'inflazione e dai fallimenti delle banche

Cosa serve per partecipare a bitcoin?

- Ogni *account* consiste di una chiave pubblica (indirizzo *bitcoin*) e di una chiave privata
  - Per ricevere bitcoin è sufficiente che il mittente conosca la chiave pubblica del destinatario
  - Per spendere bitcoin è necessario conoscere la propria chiave privata

Vari modi di mantenere

i bitcoins

Paper Bills

Canascius Physical Bitcoins

Indirizzi e chiavi bitcoin

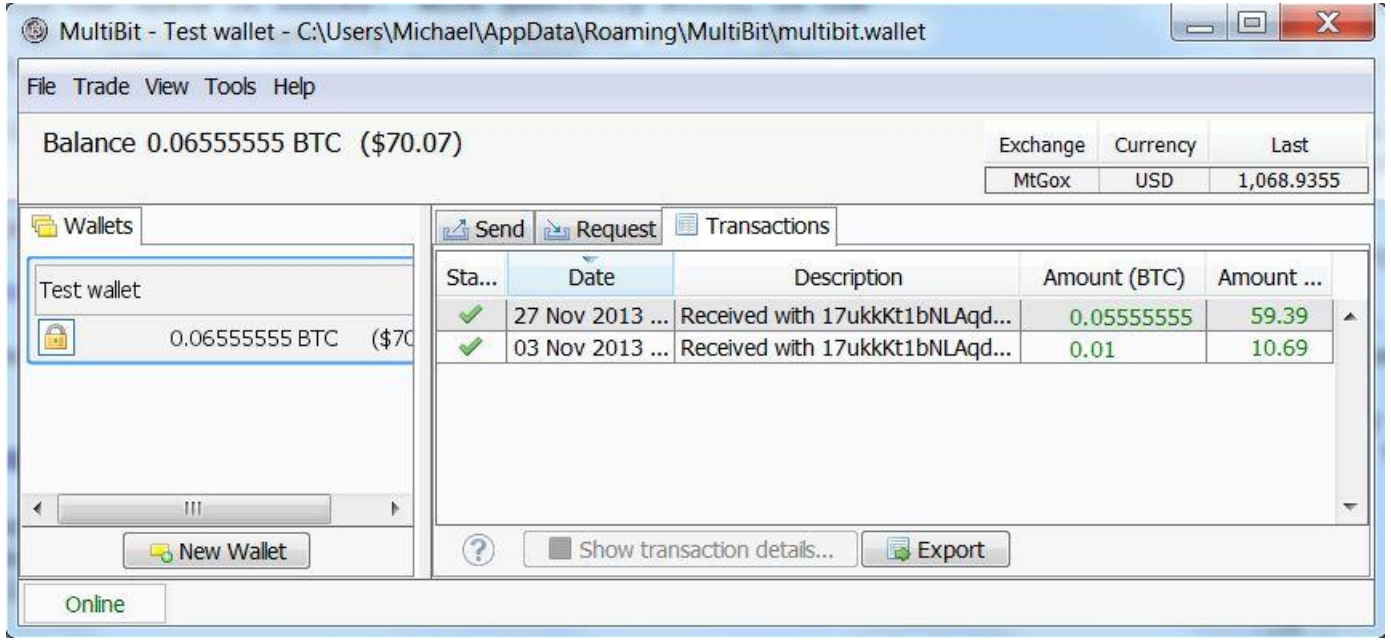
- Esempio di indirizzo bitcoin

  14nRKoXJAUpKYYbzw6Yrqh9gW2p26zerpW
  - **34 caratteri che iniziano con 1 oppure 3**
  - 2^{160} (circa10^{48}) possibili indirizzi
- La corrispondente chiave privata è 5HuEupX3DNFJ7UypjFtXDTm4BVuAwZtAgYf94sMALPyakgafVnU
  - **51 caratteri che iniziano sempre con un 5**
  - 256 bits
  - Circa 10^{77} possibili chiavi private
- Tecnicamente si usa una firma digitale

- per saperne di più:
  - http://en.wikipedia.org/wiki/Elliptic_Curve_DSA

Usare bitcoin (1)

1. Si installa un *wallet* (portafoglio)
   - ne esistono diversi tipi (desktop, mobile, web)
   - reperibili da https://www.bitaddress.org/ o http://blockchain.info/
   - Il *wallet* va protetto (cifrato)



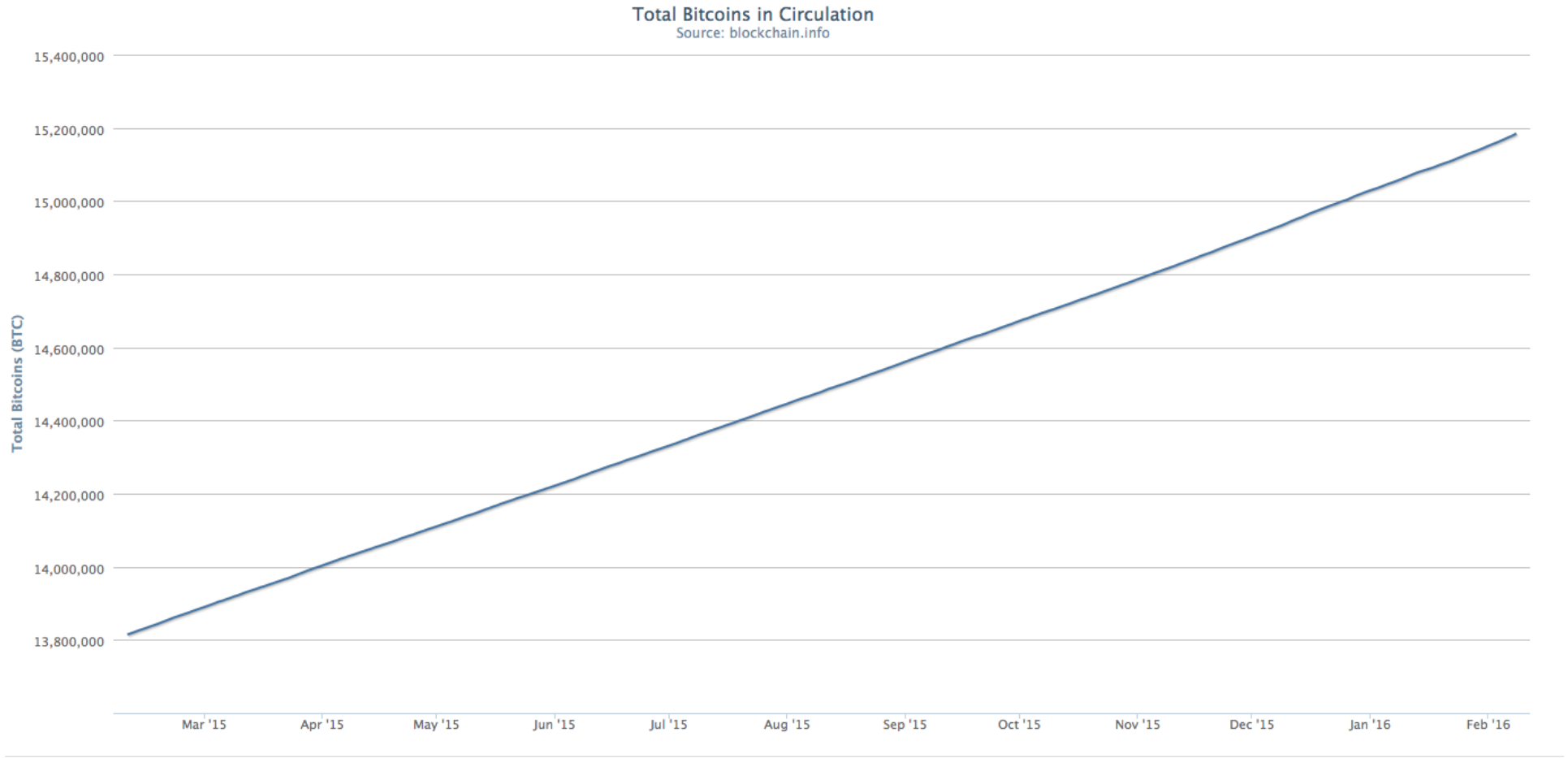
Usare bitcoin (2)

2. Ci si *procura* i bitcoins
   - Accettando bitcoin in cambio di ”merce” o servizi
   - Comprandoli da altri partecipanti
   - Comprandoli da un *punto di scambio (exchange)*
     http://howtobuybitcoins.info/it.html
   - Creandoli con il processo di validazione (*mining)*
3. Si spendono i bitcoin
   - Cosa si può comprare
     - Libri
     - Computer, elettronica *consumer,* software ma anche gioielli o cibi *on line*!

Come funziona bitcoin (1)

- Bitcoin è un **protocollo** (https://en.bitcoin.it/wiki/Protocol_specification) che regola operazioni di un network di partecipanti (utilizza la porta TCP 8333)
  - Chiunque può implementarlo come vuole purché rispetti il protocollo
  - È disponibile un'implementazione di riferimento
- L'unita della valuta sono i *bitcoins*
- Ogni transazione, firmata digitalmente, è inviata in *broadcast* al network bitcoin
  - Le transazioni sono pubbliche ma non facilmente riconducibili alla reale identità dei partecipanti al network
- I partecipanti al network "confermano" le transazioni e mantengono un "libro mastro" delle transazioni in quella che viene chiamata *block chain*
- Un trasferimento di bitcoins non implica un "movimento" ma l'aggiunta e **l'accettazione** di una nuova transazione alla *block chain*
- È molto difficile creare un nuovo blocco valido ma è molto facile per ogni partecipante controllare la validità di un nuovo blocco (*hash chain)*
- L'algoritmo distribuito garantisce che la creazione di *nuovi* bitcoin permetterà di raggiungere il limite asintotico di 21 milioni di unità (*bitcoins).*

Numero di bitcoin in circolazione



Come funziona bitcoin (2)

- L'algoritmo distribuito *controlla* quanta potenza di calcolo è necessaria per validare un blocco in modo che la creazione di un nuovo blocco richieda (in media) circa 10 minuti
- I partecipanti guadagnano un premio in bitcoin quando riescono a validare un blocco. L'ammontare del premio diminuisce con il tempo
  - Il premio originale era 50 Bitcoin ed è stato dimezzato a 25 nel Novembre 2012 quando è stato validato il blocco 210000
  - Tende ad azzerarsi man-mano che ci si avvicina ai 21 milioni di bitcoins circolanti
- Ma cosa vuol dire *validare un blocco?*
- Perché è importante e merita un premio *la validazione*?

Il problema della *doppia spesa* (1)

- Uno dei principali problemi di sicurezza delle cripto monete è la possibilità di effettuare una *doppia spesa*, spendere cioè più di una volta gli **stessi** *bitcoin*
  - Alice compra qualcosa da Bob (cedendo quindi la proprietà di alcuni bitcoin)
  - Alice compra qualcosa da Charlie usando gli ***stessi*** bitcoin utilizzati per acquistare da Bob.
- È soprattutto per eliminare questa possibilità, senza dover ricorrere ad un'autorità centrale, che *bitcoin* utilizza il concetto di *block chain*
  - Ogni nodo della rete ha una copia di tutti i blocchi di transazioni

Il problema della *doppia spesa* (2)

- Supponiamo, per una volta…, che Alice sia la “cattiva”
  - Alice invia due messaggi
  1. ”Io, Alice, sto cedendo a Bob un bitcoin con numero seriale 1234567”
  2. ”Io, Alice, sto cedendo a Charlie un bitcoin con numero seriale 1234567”
- Sia Bob che Charlie ricevono il messaggio, controllano che il bitcoin con numero seriale 1234567 appartiene ad Alice, accettano la transazione e inviano in broadcast a tutti, il messaggio di Alice e la loro accettazione della transazione.
- A questo punto gli altri partecipanti quale delle due transazioni devono considerare valida?

Soluzione al problema della *doppia spesa* (1)

Una possibile soluzione è che Bob non tenti di verificare la transazione da solo ma chieda a tutti di partecipare alla verifica.

In sostanza Bob:

- può fare un broadcast della possibile transazione e chiedere l'aiuto per determinare se la transazione è legittima.
- Quando un numero *sufficiente* di partecipanti al network ha diffuso in broadcast la conferma che quel bitcoin appartiene a Alice, allora si assume che la transazione è accettabile,
- Bob accetta il bitcoin e tutti aggiornano la *block chain*.

- Se Alice tenta di spendere lo stesso bitcoin con Charlie, altri utenti lo noteranno ed indicheranno che c'è un problema con quella transazione.
- Sembra fatta ma…

Soluzione al problema della *doppia spesa* (2)

Ci sono almeno due problemi con questa soluzione

1. Quando è che il numero di partecipanti è sufficiente?
2. Cosa succede se Alice crea uno zilione di identità fittizie che comunicano sia a Bob sia ad Charlie che la transazione è valida?

La soluzione è in realtà la combinazione di due idee:

1. Rendere (artificialmente) costoso, dal punto di vista computazionale, validare le transazioni
2. Premiare i partecipanti che validano le transazioni.

Soluzione al problema della *doppia spesa* (3)

Supponiamo Alice invi il solito messaggio:

- ”Io, Alice, sto cedendo a Bob un bitcoin con numero seriale 1234567*”

Ogni partecipante lo aggiunge alla coda delle transazioni.

- Ad esempio l’utente Davide potrebbe avere in coda tre transazioni:
  1. Io, Tom, sto cedendo a Sue un bitcoin con numero seriale 1201174
  2. Io, Sidney, sto cedendo a Paul un bitcoin con numero seriale 1398482
  3. Io, Alice, sto cedendo a Bob un bitcoin con numero seriale 1234567
- David controlla che tutte le transazioni siano valide, però prima di inviare la conferma a tutto il network deve risolvere un *puzzle* ed inviare la soluzione
  - Senza la soluzione, gli altri partecipanti non accettano la sua validazione delle transazioni.
- Ma in cosa consiste effettivamente il *puzzle* da risolvere?

*__Attenzione:__ in realtà un bitcoin non ha associato un numero di serie. Si tratta di una semplificazione a scopo illustrativo. In Bitcoin il ruolo del numero di serie è giocato dai *transaction hashes.*

Soluzione al problema della *doppia spesa* (4)

In maniera (abbastanza) semplificata David deve calcolare una funzione di *hash (SHA-256)* fino a quando l'*hash* risultante non soddisfa un requisito.

1. Si parte da un blocco di dati (relativo ad attività sul network di Bitcoin) a cui si aggiunge un numero arbitrario da usare una sola volta (*nonce*)
2. Si calcola l'hash del blocco+*nonce,* se l'hash risultante ha valore inferiore ad un dato valore di soglia, il criterio è soddisfatto
   - In sostanza l'hash risultante deve avere un certo numero di zeri all'inizio.
3. Se il criterio non è soddisfatto, si incrementa il *nonce* di un'unità e si ricalcola l'hash.
   - Esiste un limite superiore al numero possibili di tentativi (attualmente 4 miliardi di tentativi).
   - Superato il limite il partecipante richiede l'assegnazione di un nuovo *puzzle.*
4. Se David individua il *nonce* che soddisfa il criterio*,* invia in broadcast il blocco di transazioni ed il *nonce* così altri partecipanti possono controllare che è una soluzione valida al puzzle ed accettare il blocco di transazioni.

Soluzione al problema della *doppia spesa* (5)

- Un partecipante scorretto che volesse far accettare una transazione *maliziosa* dovrebbe risolvere il *puzzle* prima degli altri.
  - Fino a quando i partecipanti *onesti* hanno più **potenza di calcolo aggregata** è altamente improbabile che l'attacco abbia successo.
- Il meccanismo del *proof of work* può essere visto come una competizione per validare le transazioni
- La probabilità di un *miner* di essere il primo a validare una transazione è (rozzamente) uguale alla percentuale che possiede di tutta la potenza di calcolo coinvolta nel processo di validazione
- Spinge i partecipanti a cercare varie soluzioni per aumentare le loro chance di vincere la competizione
  - *Mining pools:* un numero (anche molto elevato) di partecipanti contribuisce alla validazione di **un** blocco. Il premio è quindi diviso tra i partecipanti al pool.
  - Maggiori probabilità di vincere la competizione ma premio **molto** ridotto

Oppure hardware dedicato!

Soluzioni *custom* (basate su speciali chip*)* con un costo nell'ordine di grandezza di qualche *K$*

http://www.theregister.co.uk/2014/01/17/ten_bitcoin_miners

Dettagli sulla conferma delle transazioni

- Durante il processo di *mining* tutte le transazioni sono raccolte in un blocco.
- La difficoltà è modificata nel corso del tempo in modo che la validazione richiede (in media) 10 minuti.
- Per piccoli pagamenti, oppure per transazioni con *peer* ritenuti "affidabili" non sono richieste conferme.
- Per transazioni rilevanti sono richieste 6 conferme per risolvere i problemi di possibili "biforcazioni" della *block chain*
  - Possibile quando due validazioni arrivano *quasi* contemporaneamente.
- Il numero totale di hash per secondo calcolato da tutti i partecipanti è (circa) **130 trilioni di hash**
  - (un trilione **equivale a mille miliardi** 1.000.000.000.000)

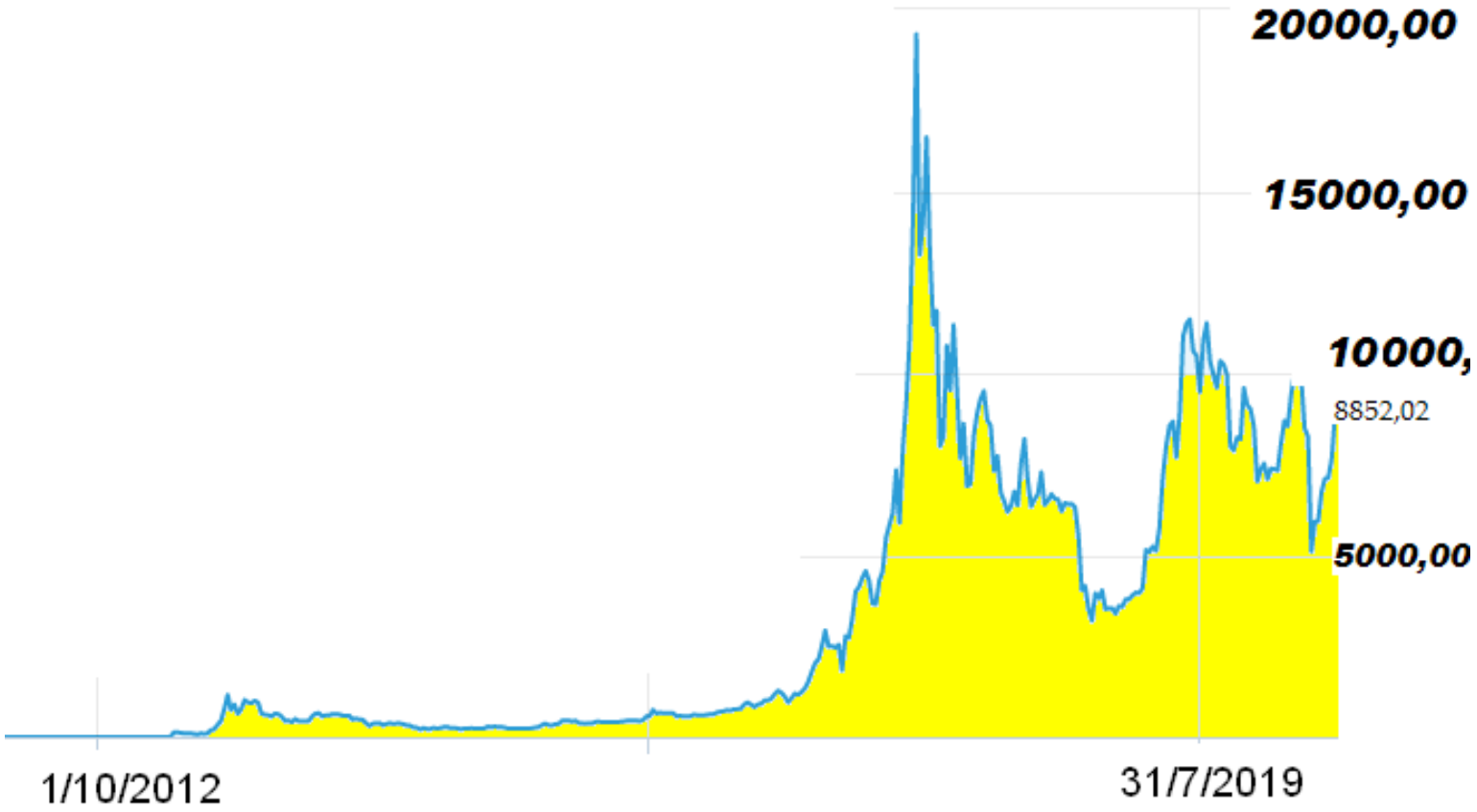
Possibili attacchi all'*equilibrio* di Bitcoin

- Formazione di un *cartello* di miner
  - Un gruppo che detenga > 50% della capacità di *mining* può sovvertire qualsiasi regola basata sul consenso
  - La formazione di un cartello è improbabile ma non impossibile
    - Si stima che http://www.btcguild.com controlli circa il 25% della capacità di mining
  - Un cartello potrebbe sfruttare la doppia spesa ma il guadagno sarebbe limitato perché il valore dei bitcoin diminuirebbe velocemente
- Attacco stile *Goldfinger*
  - I governi (e le loro istituzioni finanziarie) sono la più plausibile fonte di attacchi di questo tipo.

Argomenti contro bitcoin

- Possono essere utilizzati per comprare droghe o armi
  - Anche la moneta tradizionale è usata per gli stessi scopi
  - Ad es. nel 2019 le segnalazioni all' Unità di Informazione Finanziaria per l'Italia della Banca d'Italia per operazione sospette sono cresciute del 140%
  - Si moltiplicano le modalità per garantire un maggior grado di anonimato, caratteristica peculiare delle transazioni
  - Il bitcoin risulta la prima moneta usata per pagamenti sul darknet (fonte: relazione della Procura nazionale del 2019 riferita a dati 2018)
- I primi partecipanti sono stati privilegiati
  - Più alto il valore del premio per l'attività di *mining*
  - Meno concorrenza tra *miners*
- Bitcoin non ha un valore "intrinseco"
  - Alta volatilità

Instabilità del valore



Instabilità del valore

- 2020 : da inizio anno il guadagno è stato del 180%
- Nel 2017 il valore era arrivato a circa 20.000 dollari, e in questi giorni (dicembre 2020) ha toccato un valore massimo di 20.800 dollari per poi attestarsi sui 20.000.
- Non si rilevano particolari motivazioni economico/finanziarie se non l'aumento di interesse da parte degli investitori che hanno fatto aumentare il valore, essendo legato alla domanda.
- Si ricorda che le teorie economiche tradizionali rapportano la costruzione del prezzo sulla base di valutazioni non solo della domanda ma anche dell'offerta.

Argomenti plausibili contro bitcoin

- Può essere una bolla?
  - L'attenzione dei *media* spinge le persone ad interessarsi e comprare bitcoins
  - L'attenzione dei *media* spinge le società ad accettare bitcoins
  - Il prezzo ("valore") dei bitcoins cresce ed aumenta l'attenzione dei media per il fenomeno
  - Il cerchio è completo…
- Fino a quando il prezzo (valore) cresce con l'uso non c'è (probabilmente…) pericolo di bolla
- Attenzione però perché la velocità di circolazione di bitcoin è bassa confrontata con quella delle valute tradizionali.

Argomenti plausibili contro bitcoin

- Bitcoin potrebbe essere sostituita da un'altra criptomoneta
  - Ad esempio http://litecoin.org che sfavorisce i *miner* dedicati
  - Libra (Facebook)
- Un governo potrebbe decidere o almeno provare a "spegnerla"
- Lentezza del processo di verifica delle transazioni
- Problemi di scalabilità
  - Se una frazione significativa di utenti di Internet si unisse al network dei partecipanti, l'attuale versione di bitcoin non reggerebbe il carico
- Trasparenza dei punti di scambio con la moneta ordinaria.

Bitcoin *pro*

- Nessun pericolo di inflazione tradizionale
  - Nessuno può “stampare più moneta”
- Praticamente zero costi di transazione
- Se si memorizza la password di protezione della chiave privata, l’unico modo di “rubare” bitcoin è torturare chi conosce la password…
- Facile da usare

Bitcoin *contro*

- Potenzialmente molto difficile da tracciare
- Bitcoin è ancora piuttosto nuova come moneta ed il suo ancora limitato
  - Valore dei bitcoins circolanti: ~ 5 miliardi di **€**
  - **€** tradizionali in circolazione: ~ 5000 miliardi
  - La conseguenza è un'alta volatilità
- È una moneta per Internet
  - Senza accesso ad Internet non si possono *spendere* bitcoins
- Se si perde la propria chiave privata si perdono i propri bitcoins!!!
- Potenzialmente molto difficile da tracciare
- Nessun meccanismo (noto) per cancellare transazioni!

Anonimicità dei bitcoin

- I Bitcoin sono considerati *ragionevolmente* anonimi perché gli indirizzi bitcoin derivano da chiavi pubbliche che potrebbero rappresentare chiunque in Internet
- In realtà i partecipanti potrebbero essere identificati
  - Seguendo l'andamento delle transazioni
  - Quando vengono utilizzati i punti di interscambio
- Recentemente sono state suggerite delle estensioni al protocollo Bitcoin per **garantire** l'anonimicità
  - I. Miers, C. Garman, M. Green, and A. D. Rubin. Zerocoin: Anonymous Distributed E-Cash from Bitcoin. IEEE Symposium on Security and Privacy, 2013.

Conclusioni e domande (1)

- Bitcoin è un esempio di successo per il concetto di cripto-moneta
  - Molte interessanti sfide per
    - Calcolo numerico
    - Scienze forensi
- Può essere la base per una nuova economia?
  - Definizione di un “modello”
    - Problema della tassazione
  - Stabilità del valore nel tempo
  - Una *software-based governance?*
- Si può diventare ricchi con bitcoin?
  - Un interessante problema dal punto di vista matematico

Conclusioni e domande (2)

Supponiamo che

- Il costo del processo di mining sia *C* (dollari o euro) al secondo
- Il numero delle possibili soluzioni calcolabili al secondo sia *P* (funzione di *C*)
- Il numero delle soluzioni da tentare (in media) per risolvere il puzzle sia *G*
- Il premio per l'individuazione della soluzione corretta sia *V*

Ha senso partecipare al processo di mining se

$$C \times G < P \times V$$