Bitcoin

Il peso delle monete (1)

- Popoli primitivi usavano monete di pietra, del peso di decine di chili.
  - Tuttora in uso per scopi ostentativi/rituali.
- Nelle società antiche le monete valevano per il loro contenuto di metallo prezioso.
  - Chi non poteva utilizzare oro o argento aveva a che fare con monete inevitabilmente più pesanti: il 10 daler svedese del 1658, in rame, pesava 19 kg.
- La moneta (teoricamente) circolante di maggior peso fu emessa nel 1997 dall'Austria: 31 kg di oro (solo 15 pezzi coniati).
- A scopo celebrativo/pubblicitario sono state coniate monete enormi, che però non hanno mai realmente circolato.
  - Il record è dell'Australia, con una moneta da una tonnellata (d'oro puro), coniata nel 2011.

Il peso delle monete (2)

- La cartamoneta sostituì il valore reale con uno simbolico, perché rappresentava, all'inizio, un valore in metallo prezioso custodito dallo stato.
  - Pochi grammi potevano rappresentare un grande valore (non a caso la Svezia fu la prima nazione a usarla).
- Ora siamo arrivati alla moneta fatta di pura informazione, di peso nullo.

Bitcoin: una valuta eterea

Cosa sono i bitcoin

- Una criptovaluta, ossia una valuta che non necessita di supporto fisico.
  - La sicurezza e le transazioni sono basate su metodi crittografici.
  - La conoscenza di chiavi crittografiche è tutto quanto necessario per controllarli e scambiarli.
  - La gestione è distribuita, basata su una logica “peer to peer”; nessun singolo individuo od organizzazione può controllarli.

I precedenti

- L’idea comparve nel 1998 (Wei Dai); i bitcoin furono la prima implementazione pratica.
- Vi sono stati alcuni predecessori, ma non piacquero perché gestiti in modo centralizzato e quindi vulnerabili, sia fisicamente, sia soprattutto politicamente.

La storia dei bitcoin

- Furono messi in circolazione nel 2008 da Satoshi Nakamoto.
  - Nessuno sa chi si celi sotto quello pseudonimo.
  - Data la vastità delle competenze richieste dal sistema, l'opinione prevalente è che si tratti di un piccolo gruppo di esperti.
  - Lentamente si sono diffusi e hanno guadagnato popolarità in tutto il mondo.
    - BTC è diventata un'abbreviazione ufficiale di valuta.
    - Il simbolo dei Bitcoin è un carattere ufficiale UNICODE dal 2015.

Uso dei bitcoin (1)

- L'uso dei bitcoin si sta diffondendo rapidamente:
  - moltissime fondazioni (p. es. Wikimedia Foundation) accettano donazioni in bitcoin;
  - dal 2013 le tasse dell'università di Nicosia possono essere pagate in bitcoin;
  - dal 2016 a Zugo (Svizzera) sanità e trasporti possono essere pagati in bitcoin;
  - dal 2013 (in Italia dal 2014) esistono ATM (Bancomat) che permettono di versare denaro, convertito in bitcoin, in un proprio wallet o di prelevare bitcoin, convertendoli in contante che viene erogato.

Uso dei bitcoin (2)

- Molti esercizi commerciali nel mondo li accettano.
  - A Berlino tutti i negozi di un'intera via accettano bitcoin.

Il codice

- Satoshi mise in rete tutto il codice necessario alla loro gestione.
  - Il codice è scritto in C e indipendente dalla macchina su cui gira.
  - Oggi è disponibile sia come sorgente, che già compilato per diverse architetture.
  - Una comunità di volontari si occupa di (minimi) aggiornamenti.

Il valore dei bitcoin (1)

- Il loro valore non dipende da alcun bene materiale, né è garantito da alcuna riserva fisica di materiali preziosi.
  - Il loro valore è quello che le persone attribuiscono loro.
  - Del resto, senza più la convertibilità aurea, anche il valore delle altre valute è puramente convenzionale e riflette la fiducia nell'ente che le emette.

Il valore dei bitcoin (2)

- Il valore di un bitcoin è andato costantemente (e molto irregolarmente) aumentando, da pochi centesimi l'uno, all'inizio, a oltre 12000 euro attualmente.
  - Sono fortemente soggetti alla speculazione, il loro valore a volte raddoppia o si dimezza nell'arco di un paio di giorni.
  - Nessun ente o persona controlla o regola gli scambi, per essi vige la legge della domanda e dell'offerta, nel modo più selvaggio.

I bitcoin esistenti

- Il numero di bitcoin che possono esistere è limitato a 21 milioni.
  - A oggi ne sono stati creati circa 3/4.
  - Entro il 2140 circa saranno stati creati tutti e da quel momento non ne saranno creati di nuovi.
  - Questo garantisce che non vi sarà inflazione per l'aumento di unità circolanti.
- Ogni bitcoin ha però un sottomultiplo, detto "Satoshi" che è di fatto la vera unità minima di scambio.
  - Un bitcoin equivale a 100 milioni di Satoshi.

Il possesso di bitcoin

- I bitcoin si conservano in “portafogli” (wallet) puramente virtuali, l’accesso ai quali è consentito tramite una coppia di chiavi.
  - Il contenuto di ogni wallet è attestato da un immenso database distribuito in rete (in pratica un file, detto “blockchain”), che contiene la storia di tutte le transazioni che hanno avuto luogo.
  - Chiunque può scaricarne una copia, esaminarlo e, con semplici programmi disponibili gratuitamente, verificare il contenuto di ogni wallet.

I wallet

- I wallet possono essere generati tramite un semplicissimo programma, disponibile gratuitamente, che genera una chiave casuale (privata) e una pubblica, legate tra loro.
  - La chiave privata va mantenuta segreta, quella pubblica può essere divulgata.
    - La chiave privata è una sequenza di lettere e cifre, lunga in media 33 caratteri.
  - Assolutamente nulla collega un wallet al suo proprietario: l'anonimità è totale.

Le chiavi

- La conoscenza della **chiave pubblica** è necessaria e sufficiente per **versare** bitcoin in un wallet.
- La conoscenza della **chiave privata** è necessaria e sufficiente per **prelevare** bitcoin da un wallet.

La crittografia a chiave pubblica

- La crittografia a chiave pubblica prevede l'uso di due chiavi, legate tra loro.
  - La chiave pubblica (da divulgare) serve per criptare un messaggio, quella privata (da tenere segreta), per decifrarlo.
  - Dalla chiave pubblica non si può risalire a quella privata, se non impiegando risorse di calcolo immense.

La crittografia RSA

- Fu il primo meccanismo di crittografia a chiave pubblica, è tuttora largamente impiegato.
- La chiave privata è costituita da due grandi numeri primi (di almeno 100 cifre, spesso di più), quella pubblica dal loro prodotto.
  - Per scomporre il prodotto anche con i migliori algoritmi noti possono servire secoli di calcolo da parte di migliaia di calcolatori che lavorino insieme (dipende dalle dimensioni dei numeri primi).

L’algoritmo di Shor

- L’algoritmo di Shor (Peter Shor, 1994), permette in teoria scomporre un numero n nei suoi fattori primi, in un tempo proporzionale a $\log^2 n \cdot \log\log n \cdot \log\log\log n$, quindi polinomiale rispetto al numero di cifre, disponendo di un grande calcolatore quantistico
  - Serve un calcolatore quantistico con un numero di qbit uguale al doppio delle cifre nella rappresentazione binaria di n.
  - Ha una piccola probabilità di errore, che può essere ridotta arbitrariamente ripetendolo.
- Lascia incertezze sul futuro a lungo termine della crittografia RSA.

La crittografia dei bitcoin (1)

- Nel caso dei bitcoin il metodo crittografico è basato sulle proprietà delle curve ellittiche.
  - Per la precisione, è l'Elliptic Curve Digital Signature Algorithm (noto come ECDSA, proposto da Scott Vanstone nel 1992), standard ISO dal 1998.
    - E' analogo alla crittografia RSA, ma richiede chiavi pubbliche più corte a parità di sicurezza (p. es 160 bit invece di 1024 perché siano necessari 2^{80} operazioni per decifrare un messaggio) ed è ritenuto più robusto.
    - Per ora è immune da un attacco tramite calcolatore quantistico.

La crittografia dei bitcoin (2)

- Il movimento di bitcoin funziona in un certo senso al contrario della crittografia RSA, o meglio, come la "firma" nel caso della crittografia RSA: tramite la chiave privata viene crittografata una stringa che descrive la transazione, mentre la chiave pubblica permette di decifrarla.
  - Solo chi conosce la chiave privata può inserire nella rete una transazione crittografata correttamente.
  - Chiunque, tramite la chiave pubblica, può decifrarla e verificarne la correttezza.

Chiavi multiple

- Sono possibili più chiavi per uno stesso wallet.
  - Per autorizzare l'uscita dei bitcoin possono essere richieste tutte le chiavi o un numero prefissato, p. es. 5 su 7.
  - Questo permette di gestire wallet di società, in modo che serva una certa maggioranza per autorizzare una transazione, senza rendere indispensabile ciascun possessore di chiave.
  - Il meccanismo serve anche alle piattaforme di scambio, che gestiscono wallet molto ricchi, per evitare che un singolo individuo possa rubarli.

Le transazioni con i bitcoin (1)

- Per trasferire bitcoin da un wallet a un altro, il cedente mette in rete la transazione, che autorizza l'uscita dei bitcoin dal suo wallet.
  - La transazione contiene l'ora in cui è stata effettuata, è "firmata", ossia crittografata, mediante la chiave privata, e usa la chiave pubblica del wallet ricevente per l'accredito.

Le transazioni con i bitcoin (2)

- Vari programmi permettono di semplificare la gestione delle chiavi, sia tramite PC, che tramite telefoni cellulari, memorizzando su essi le chiavi.
  - In alcuni esercizi pubblici che accettano bitcoin vicino alla cassa è esposto un QR-code con la chiave pubblica del negozio: basta inquadrarla col telefono e digitare l'importo e un PIN di poche cifre, per effettuare il trasferimento.

La validazione delle transazioni

- La validazione delle transazioni è effettuata dai “minatori” (miner), che a caccia di “pepite”, costituite da bitcoin, validano blocchi di transazioni, ricavandone un guadagno.
  - Il meccanismo è basato sulla cooperazione volontaria, ma è molto robusto: per validare una transazione fraudolenta servirebbe la cooperazione di oltre la metà dei miners.

L’attività dei miner

- Un miner:
  - preleva dalla rete e aggrega transazioni in attesa di validazione, costruendo un blocco;
  - verifica la loro validità tramite le chiavi pubbliche;
  - aggiunge in testa una transazione che crea alcuni bitcoin (che andranno a lui) e un hash crittografato dell’ultimo blocco valido a lui noto.
  - cerca di rendere valido il blocco.

Il guadagno dei miner

- Per un miner vi sono due fonti di guadagno:
  - la prima transazione del blocco, che crea alcuni bitcoin per lui;
  - una piccolissima commissione incamerata su ogni transazione validata.
- Il numero di bitcoin creati per ogni blocco valido era inizialmente di 50 e diminuisce nel tempo, dimezzandosi ogni 4 anni; dal 2016 è di 12.5.
  - E' previsto che verso il 2140 si annulli; alla fine resterà solo la percentuale.

Le commissioni

- Chi effettua una transazione vi aggiunge una commissione (arbitraria), destinata a chi valida la transazione stessa.
  - Commissioni alte fanno sì che la transazione sia tra le prime prese in considerazione dai miner.
  - Commissioni troppo piccole (inferiori a 0.0001 bitcoin nel 2013) rischiano di non var mai validare la transazione.

La creazione di un blocco valido (1)

- Un miner pone in testa a ogni blocco un numero casuale di 64 bit e calcola una funzione di hash del blocco, tramite un algoritmo apposito (SHA-256).
- Se il valore della funzione termina con un certo numero di bit a zero, il blocco è convalidato, altrimenti riprova con un altro numero.

La creazione di un blocco valido (2)

- Non esiste alcun metodo per scoprire, dato un blocco di transazioni, quali numeri soddisferanno il requisito.
  - Se sono richiesti *n* bit finali a zero, un numero scelto a caso ha una probabilità di essere corretto pari a $1 / 2^n$.
- Il numero di bit a zero richiesti viene aggiornato ogni due settimane, in modo da avere una frequenza media di creazione di blocchi di uno ogni 10 minuti.
  - In questo modo si annullano gli effetti della variazione del numero di miner e dell'aumento della velocità dei calcolatori, rendendo statisticamente prevedibile il processo di creazione di nuovi bitcoin.
- Il numero di bitcoin che il miner guadagna viene dimezzato ogni 4 anni, per compensare l'aumento del loro valore.

La validazione di un blocco (3)

- I miner lavorano in concorrenza tra loro, perché il primo che valida un blocco si accaparra i bitcoin relativi, rendendo inutile il lavoro degli altri su quel blocco e costringendoli a provare con un altro blocco.
  - All'aumentare del numero di scambi, i blocchi da validare non mancano.
- Il miner che valida un blocco lo distribuisce ai nodi più vicini della rete, che lo verificano e diffondono.
  - La diffusione di un blocco fraudolento sarebbe immediatamente bloccata.

La validazione delle transazioni (1)

- Quando una transazione entra in un blocco, riceve una prima conferma.
- Quando alla catena che inizia con un blocco valido ne viene aggiunto un altro, il primo riceve una ulteriore conferma.
- Alla sesta conferma tutte le transazioni del blocco sono considerate confermate.
  - Un ipotetico attaccante per far sparire una transazione dovrebbe costruire una catena di almeno altrettanti blocchi, senza quella transazione, tutti validi, e diffonderla.

La validazione delle transazioni

- Il tentativo di “spendere” due volte lo stesso bitcoin viene facilmente scoperto e rifiutato dalla rete.
- Tramite la blockchain è possibile ricostruire ogni transazione e il contenuto di ogni wallet.
  - Vari strumenti permettono di esaminaresolo una parte della blockchain, per ricostruire, per esempio, la storia di un singolo wallet.

Il “mercato” delle validazioni (1)

- Inizialmente i miner lavoravano con comuni PC, con la speranza di poter validare anche più blocchi al giorno (servivano in media milioni di tentativi).
- Poi sono state utilizzate le GPU per calcolare la funzione di hash, sfruttandone l’elevato parallelismo.
- In seguito, all’aumentare del numero di tentativi richiesti e del guadagno in caso di successo, è nato un mercato di componenti hardware appositi.
  - Sono stati sviluppati chip specializzati, che possono essere inseriti nei PC su apposite schede, che permettono di calcolare la funzione di hash miliardi di volte al secondo.

Il “mercato” delle validazioni (2)

- A un certo punto il costo dei chip, dei calcolatori e dell’energia elettrica richiesta ha reso meno conveniente l’attività.
  - Sono stati pubblicati studi sulla convenienza dell’attività in funzione del costo dell’energia elettrica nei vari paesi, sugli investimenti richiesti e sul relativo ROI.

I pool (1)

- Per chi non dispone di grandi potenze di calcolo fare il miner è diventata un'attività troppo aleatoria.
  - Si finisce con l'investire denaro per comprare l'energia, in cambio di una piccola probabilità di un forte guadagno.
- Per rendere più uniforme il guadagno sono nati i "pool" di miner, consorzi di miner che si suddividono l'onere di calcolo e i guadagni

I pool (2)

- Chi fa parte di un pool mette a disposizione del tempo di calcolo di macchine connesse alla rete.
- Il gestore del pool ripartisce i calcoli tra i partecipanti e, in caso di successo, i guadagni, in proporzione al numero di valori di hash calcolati, indipendentemente da chi effettivamente abbia avuto successo.
  - Il gestore trattiene per sé una piccola percentuale degli utili, come compenso per la sua attività.

I pool (3)

- Naturalmente il tutto è automatizzato e gestito da programmi gratuitamente disponibili.
  - In pratica basta iscriversi e lasciare acceso il calcolatore il più possibile.

Il “mercato nero” delle validazioni (1)

- Si è anche assistito a un grande aumento di furti di tempo di calcolo.
  - Alcuni miner hanno prodotto “virus”, che inseriti in PC altrui lavorano freneticamente e incessantemente al calcolo di funzioni di hash, mandando al miner il numero giusto, quando lo trovano.
  - Altri utilizzavano banalmente i calcolatori aziendali.

Il “mercato nero” delle validazioni (2)

- Recentemente si è scoperto che qualcuno ha trovato modo di rubare il tempo di calcolo di dispositivi di vasta diffusione, dotati di una sia pur minima potenza di calcolo, come le webcam e i dispositivi di sorveglianza.

Le piattaforme di scambio

- Esistono siti che permettono di effettuare compravendita di bitcoin e di depositarli.
  - Con una semplice registrazione e qualche password ci si libera dal problema di custodire la chiave privata e si può fare speculazione.
- Il volume delle transazioni è ragguardevole: solo su Kraken, la piattaforma più nota, in un mese sono stati comprati e venduti bitcoin per oltre 2.5 miliardi di euro.

Le frodi (1)

- Come tutte le valute, i bitcoin si prestano a vari tipi di frodi.
  - In fondo, sono tutte l'analogo informatico di raggiri che hanno origini antichissime.

Le frodi (3)

- La frode più comune consiste nel carpire la chiave privata di un wallet, per poi trasferirne il contenuto in un altro.
  - Sono stati usati programmi che intercettano, copiano e trasferiscono altrove le sequenze di tasti premuti sulla tastiera, a caccia di password e chiavi.
  - Quando sono in ballo milioni di euro, anche l'intercettazione di messaggi sulla connessione di rete non è da escludere.

Le frodi (3)

- In alcuni casi sono state create piattaforme di scambio, incoraggiando la gente a depositare bitcoin per la compravendita.
  - Un giorno poi il gestore della piattaforma sparisce con la cassa.
- In altri casi le piattaforme stesse non erano abbastanza sicure, qualcuno è riuscito a intrufolarsi, rubare le chiavi e asportare il contenuto.

Le limitazioni dei bitcoin (1)

- Il sistema ha varie limitazioni, una delle quali è l'esistenza di un numero non enorme di bitcoin.
  - Anche considerando la suddivisione in Satoshi, non sarebbero in grado di supportare l'economia mondiale, perché il Satoshi finirebbe con l'avere un valore eccessivo per fungere da unità.

Le limitazioni dei bitcoin (2)

- Un grande numero di bitcoin è andato irrimediabilmente perduto.
  - Sono state perse le chiavi private, magari per distruzione dei calcolatori che li contenevano.
  - Nel 2013 un utente si sbarazzò accidentalmente di un hard disk, che conteneva l'unica copia della chiave privata di un wallet con 7500 bitcoin (vari milioni di dollari al valore di allora).

Le limitazioni dei bitcoin (2)

- Il sistema è nato per fare concorrenza ai pagamenti tramite banca, rispetto ai quali è più veloce.
  - Oggi una transazione viene validata in media in 14 minuti: può sostituire un bonifico, ma il tempo è inadeguato per sostituire i pagamenti in un negozio.

Le limitazioni dei bitcoin (3)

- Le grandi e rapide oscillazioni del valore rendono pericoloso per un negoziante accettarli in pagamento.
  - Sono però nate società che fungono da assicurazioni: garantiscono un cambio stabile (per un periodo limitato), accollandosi il rischio delle oscillazioni.
    - L'esercente può cambiare a fine giornata l'incasso in una qualsiasi valuta, senza incertezze sul valore.

Perché i bitcoin hanno avuto successo?

- Vi sono quattro motivi fondamentali:
  - anonimato;
  - indipendenza dai governi;
  - moda;
  - speculazione.
- L'ordine è, a mio parere, quello temporale di comparsa dei motivi, non quello di importanza attuale.

Anonimato

- L’uso di bitcoin garantisce il totale anonimato, quindi per anni l’uso principale è stato quello di transazioni illecite o riservate.
  - Su silkroad tutte le transazioni erano in bitcoin. Quando l’FBI chiuse il sito, sequestrò il wallet e il governo USA, sempre pragmatico, decise di mettere in vendita tutti i bitcoin. La minore domanda e la maggiore offerta fecero crollare il valore di oltre il 50%.
  - In molti casi il pagamento di un’estorsione è richiesto in bitcoin.

Indipendenza dai governi

- Accumulare bitcoin permette di creare una riserva al sicuro dalle pretese di uno stato.
  - Data l'assenza di una struttura centrale, nessun governo può sequestrare bitcoin senza le chiavi private;
  - Sembra che pochi siano disposti a fidarsi del proprio stato, sia come gestore di valuta, sia come esattore.
    - L'erba del vicino è sempre più verde, ma in molti stati la precauzione non è insensata.

Moda

- Andare in un bar e pagare in bitcoin fa “moda”, è divertente, permetteva di girare senza contanti anche prima che fossero diffusi i pagamenti tramite telefono cellulare.
  - Per i negozianti è un modo per attrarre clienti.

Speculazione

- Quando il valore di un bene tende mediamente a crescere e ha forti oscillazioni, diventa appetibile specularci sopra.
  - Molti effettuano transazioni frequenti, comprando e vendendo bitcoin nel giro di giorni, se non ore, speculando sulle fluttuazioni.
  - Altri sperano in un aumento sul lungo termine, conservandoli.
    - Chi avesse investito 100 euro all'inizio, conservandoli sino a oggi, sarebbe multimilionario.

I concorrenti dei bitcoin (1)

- Negli ultimi anni sono nate decine di criptovalute molto simili.
  - Copiare il meccanismo è semplice: i concetti sono noti, il codice è disponibile.
  - Mettere in giro una criptovaluta nuova può essere estremamente lucroso: chi lo fa generalmente tiene varie migliaia di unità per sé e se solo arrivano a valere un centinaio di euro l'una diventa ricco.

I concorrenti dei bitcoin (2)

- Alcune criptovalute si propongono di superare le limitazioni dei bitcoin:
  - permettendo di mettere in circolazione un numero di unità enormememente superiore.
  - permettendo tempi di transazione più rapidi.
    - In un caso la media è di 9 secondi per l'approvazione.

Il futuro dei bitcoin (1)

- Difficile prevederlo
  - c'è chi pensa a un'economia mondiale o almeno su vasta scala, basata su Bitcoin;
  - c'è chi prevede l'esplosione della bolla speculativa e la sparizione dal mercati.
- Le banche però li temono e stanno mettendo in circolazione metodi di pagamento veloci per somme piccole, (quasi) esenti da commissioni.
  - La concorrenza giova sempre all'utenza.

Il futuro dei bitcoin (2)

- Potrebbero diventare veramente la valuta del futuro.
- Molti governi stanno pensando a sistemi analoghi, sotto il loro controllo, per eliminare completamente il denaro contante.
  - Sarebbe sicuramente un grosso risparmio: produrre fisicamente il denaro ha un costo.
  - Diventerebbe possibile tracciare la più piccola transazione.
    - Il sogno di molti stati, non dei cittadini, però.


That's all Folks!