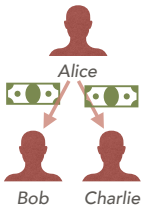
Blockchain

- Una ***blockchain*** è un *registro* (***ledger***) distribuito, simile a un *database*, *non* controllato da un'*autorità centrale*, duplicato su server (**peer**, o **nodi**) sparsi nel mondo. I dati possono essere aggiunti al registro attraverso un ***consenso*** dei singoli server. Una volta che i dati sono stati aggiunti *non* possono essere *eliminati o modificati*
- Un blocco (***block***) è una lista di dati registrati, e la *catena* (**chain**) è la pila di blocchi che cresce nel tempo
- Perché le blockchain?
  - Alice vuol mandare 10 coin a Bob, tipicamente la richiesta (***transazione***) è gestita da vari operatori e da una banca, che verifica l'autenticità della transazione e che Alice abbia credito sufficiente. La banca è l'autorità centrale
  - Negli anni 2000 un problema affrontato è stato quello di ***evitare che vi fosse un'autorità centrale*** quando si usa una moneta digitale, risolvendo il problema della spesa multipla (***double spending***)

Cosa È Il Double Spending

- Con una moneta fisica, Alice compra un bene e paga con una banconota. Dopo aver pagato, Alice non ha più la banconota iniziale da poter spendere nuovamente
- Con una moneta digitale, Alice potrebbe usare 10 coin digitali per pagare Bob, e subito dopo gli stessi 10 coin digitali per pagare Charlie



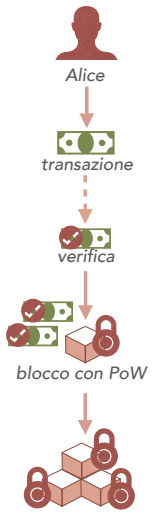
- Con una banca che verifica il credito disponibile e le spese effettuate da Alice, il problema può essere risolto facilmente, ma come fare senza un'autorità centrale?
  - Come fa Charlie a capire che Alice ha già speso 10 coin digitali? **Se** si usasse un codice per i coin, il codice dei coin sarebbe corretto sia prima che dopo averli spesi
- Ecco che è necessaria una blockchain

Blocchi Della Blockchain

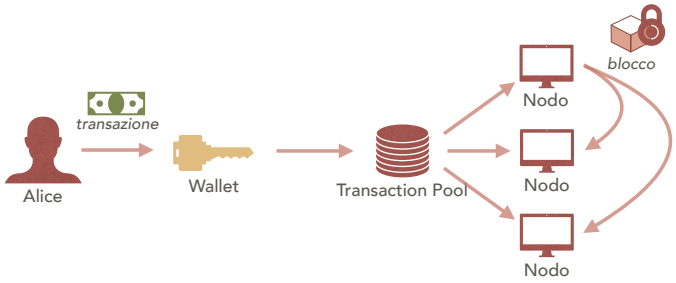
- In una blockchain, i dati relativi a ***transazioni*** sono raggruppati in ***blocchi***, replicati sui ***nodi*** (***peer***) della rete
- Un blocco contiene i dettagli di un certo numero di **transazioni** *(Tx: A manda 1 coin a B)*, una firma crittografica (**hash)** del blocco precedente, una ***nonce***
- L'**hash** generato per il blocco vale unicamente per i suoi dati, e la modifica dei dati produrrà un hash diverso
- Solo un **blocco** di dati alla volta può essere aggiunto alla blockchain (ovvero, l'insieme dei blocchi, *concatenati* dagli hash, e duplicati in ciascun peer)
- L'hash del blocco fa sì che una transazione già registrata nel blocco precedente non sia alterabile
- Le blockchain forniscono informazioni in modo ***consistente*** (ogni nodo ha gli stessi dati) e ***non-ripudiabile*** (i dati registrati non possono essere alterati o cancellati), e garantiscono l'***impossibilità di double spending***

Interazioni Della Blockchain

- Alice chiede di effettuare una transazione (ovvero un trasferimento di una quantità di moneta digitale) firmandola con la **chiave privata** del suo **wallet**, tramite una ***wallet app*** che calcola un hash per la transazione
- La wallet app manda la transazione a un *pool di transazioni non confermate* (ci sono vari pool), detto ***mempool***
- Ciascun nodo della blockchain estrae varie transazioni dalla mempool, le verifica (l'account sorgente ha la somma da trasferire?), e forma un blocco
- Ciascun nodo forma il suo blocco, potrebbe prelevare transazioni diverse. Il nodo calcola un hash particolare per il blocco, un hash con certe proprietà, e l'hash trovato costituisce la ***proof-of-work***, *PoW*
- Il nodo che ha trovato l'hash del blocco, si chiama ***miner***, manda il risultato a tutti gli altri nodi, che lo verificano e lo registrano come blocco successivo. Il miner riceve un **compenso**



Interazioni

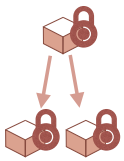


Compenso

- Sulla blockchain Bitcoin, durante la creazione di un blocco, si creano nuovi bitcoin il cui ammontare è fissato e decrescente
- Ogni blocco, creato mediamente ogni 10 minuti, contiene nuovi bitcoin creati dal nulla. La prima transazione registrata in ciascun blocco è una transazione da **coinbase** al miner di massimo 12,5 bitcoin (attualmente)
- Ogni 210.000 blocchi, approssimativamente ogni 4 anni, l'ammontare di nuovi bitcoin, quindi il compenso per il miner, diminuisce del 50%
- Per i primi 4 anni ogni blocco conteneva 50 nuovi bitcoin, a novembre 2012 l'ammontare è stato fissato a 25 bitcoin per blocco, da luglio 2016 si hanno 12,5 bitcoin per blocco. Al blocco 630.000, in qualche mese del 2020, si avranno 6,25 bitcoin per blocco
- Il dimezzamento continuerà fino al blocco 6.720.000 (circa nel 2137), quando arriverà a 1 satoshi (10^{-8} bitcoin). Quindi, dopo 6,93 milioni di blocchi (circa nel 2140), i blocchi non conterranno nuovi bitcoin

Mining, Proof Of Work

- Il processo che trova l'hash si dice ***mining*** o ***Proof of Work (PoW)***
- Ciascun nodo calcola l'hash del blocco che vuole aggiungere alla blockchain. Il nodo che trova l'hash per primo vince. L'hash cercato è quello che risolve un ***puzzle*** computazionale costoso, es. *un hash che ha un certo numero di zeri iniziali*. Si risolve a tentativi
- Poiché le transazioni e l'hash del blocco precedente sono fissati, per poter risolvere il puzzle si varia in modo random il ***nonce***
- Sulla blockchain *Bitcoin* si trova *mediamente* **un blocco ogni 10 minuti**. La difficoltà del puzzle è aggiustata ogni **due settimane** così che al variare dell'hardware globalmente presente il tempo di mining rimanga invariato
- Il nodo vincente annuncia la soluzione alla rete di peer, questi verificano che la soluzione sia corretta e registrano il blocco nella copia locale (la verifica che l'hash trovato sia corretto è veloce)
- 10 minuti permettono a nodi distanti di poter ricevere il nuovo blocco



Proof Of Work

- La proof of work per essere risolta impiega tante risorse computazionali per tanti minuti, questo dissuade attacchi distribuiti tipo denial of Service (DoS)
- Un attaccante che dedica risorse computazionali per tanto tempo, compete con i vari nodi per trovare l'hash, e solo qualche volta vince (circa proporzionalmente alle risorse impegnate)
- Vincendo solo ogni tanto non riesce ad alterare i dati presenti su un blocco già registrato, sprecando quindi risorse computazionali ed energia elettrica

Nonce

- Il nonce prende uno fra 4 miliardi di valori ($4 * 10^9$ valori)
- I miner potrebbero provare tutti i 4 miliardi di valori senza trovare il blocco
- Si riprova modificando il timestamp del blocco (la granularità del timestamp è 1 secondo)
- Attualmente, la potenza di calcolo dei miner eccede 4GH/sec quindi in meno di un secondo si riescono a provare tutti gli hash
- I miner (con potenze di hashing superiori a 4GH/sec) variano il contenuto del campo coinbase, che ha solo i primi byte fissati, per trovare l'hash che soddisfa i vincoli

Transazioni

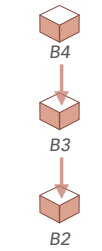
- Alice vuol pagare Bob con bitcoin, e usa una applicazione wallet per leggere il QR code del prodotto in vendita da Bob
- Il QR code contiene l'indirizzo bitcoin del destinatario, l'ammontare richiesto, e una descrizione
- Alice aveva ricevuto bitcoin con una precedente transazione. La transazione con Bob fa riferimento alla precedente transazione come input e crea nuovi output per pagare Bob e per dare il resto ad Alice
- Alice fornisce la chiave privata per sbloccare l'output della precedente transazione, provando quindi alla rete che ha i bitcoin
- La transazione registrata farà sì che Bob riceva un ammontare e Alice riceva un resto
- Alice potrebbe far riferimento a più transazioni precedenti che hanno un output verso Alice (**UTXO**, ***unspent transaction output***) per indicare una quantità di bitcoin da spendere sufficienti al pagamento

Costo Della Transazione

- Ogni transazione ha un costo (tassa, **fee**), che è il compenso per il miner che trova la PoW per il blocco che registra la transazione
- Tale costo rende economicamente non fattibile per un attaccante inondare la rete di transazioni
- Il costo è calcolato in base alla dimensione in byte della transazione (una transazione consiste di circa 250 byte)
- Attualmente il costo minimo della transazione è 0,00001 bitcoin per kilobyte (circa 8 centesimi di euro al cambio attuale)
- Il costo vero dipende dalle transazioni che competono, più basso è il costo e meno probabile sarà la registrazione. Quindi ci sono costi della transazione per alta priorità, media priorità o bassa priorità
- Alice vuole pagare a Bob 0,015 bitcoin; con un costo di transazione di 0,001 bitcoin, Alice deve avere almeno 0,016 bitcoin. Se Alice ha 0,2 bitcoin, la transazione creerà un output per Bob di 0,015 bitcoin, un output di 0,184 bitcoin per Alice e lascerà 0,001 bitcoin non allocati, che sono il costo della transazione

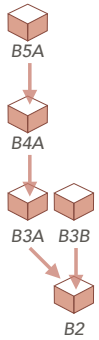
Registrazioni Immutabili

- Il processo di mining è stato progettato per assicurare che si raggiunga un **consenso** su ciascun blocco della blockchain e che nessun dato (o blocco) precedente sia alterato da una singola parte
- Poiché ciascun blocco contiene l'hash del blocco precedente, la modifica di un dato su un blocco registrato sarebbe scoperta, poiché chiunque può verificare che l'hash non corrisponde
- Supponiamo che Eve modifichi una transazione presente in un blocco 3 (B3) registrato (es. la transazione in cui Alice ha mandato 10 coin sarebbe modificata per dire che Alice ha mandato 1 coin). Eve deve avere la chiave privata di Alice per codificare la transazione di Alice
- L'hash del B3 modificato (B3M) sarà diverso da quello del B3 originario, e presente in B4 (successivo a B3). Quindi il B3M sarebbe rifiutato, poiché esiste un B4, più recente di B3M, contenente l'hash, già accettato, di B3
- Per far accettare B3M, Eve dovrebbe trovare gli hash di B3M e di B4M, prima che altri trovino l'hash di B4, così Eve darebbe i blocchi B3M e B4M a tutti i nodi. Che un singolo nodo calcoli l'hash di più blocchi consecutivi (prima quindi di tutti gli altri nodi) è altamente improbabile



Fork

- La propagazione della soluzione (blocco successivo) fra i vari nodi non è istantanea, parti distanti e connesse con un canale lento, potrebbero aver registrato blocchi diversi (o qualche nodo potrebbe non essere onesto)
- Ciascun nodo sceglie da un pool di transazioni, potenzialmente diverso, le transazioni non confermate che formano il blocco. Quindi ciascun nodo fa mining del proprio blocco (B3A), che è possibilmente diverso dai blocchi (B3B) di altri miner
- Quindi, con bassissima probabilità, alcuni nodi potrebbero registrare un blocco diverso, rispetto a quello registrato da altri nodi, come successivo alla catena di blocchi in comune
- In presenza di più blocchi nuovi da aggiungere, un nodo sceglie quale blocco successivo prendere, secondo un processo **democratico**, ovvero si adegua alla blockchain più lunga, quest'ultima ha richiesto più potenza computazionale delle altre, e quindi si assume che rappresenti la maggioranza dei nodi
- Un blocco che non appartiene alla catena più lunga verrà scartato
- Più è profondo un blocco, più è probabile che le transazioni registrate siano permanenti. Per transazioni registrate recentemente vi è una piccola probabilità che non siano definitive (potrebbero essere annullate)



Cenni Sulla Storia Di Bitcoin

- Bitcoin è stato inventato nel 2008 con il paper "Bitcoin: A Peer-to-Peer Electronic Cash System" da Satoshi Nakamoto
- L'innovazione principale fu di usare un sistema distribuito di elaborazione (chiamato algoritmo di Proof-of-Work) per far sì che ci fosse una "elezione" globale ogni 10 minuti, che permette alla rete distribuita di arrivare a un consenso sullo stato delle transazioni. Questo risolve il problema del double-spend, che non era stato ancora risolto (in assenza di un'autorità centrale)
- La rete bitcoin è stata fatta partire nel 2009, basandosi su una implementazione pubblicata da Nakamoto (l'implementazione è stata migliorata mano a mano)
- Il valore totale di bitcoin in alcuni momenti ha superato 35 miliardi di dollari americani (dipende dal cambio)
- La più grande transazione gestita dalla rete è stata di 150 milioni $ US
- La Proof-of-Work permette di ottenere un consenso nei sistemi distribuiti, al di là della moneta, può essere usata per elezioni, lotterie, registri, etc.

Mining Power

- La potenza di hashing è cresciuta esponenzialmente ogni anno. Dal 2010 al 2011, il passaggio dall'uso delle CPU alle GPU ha causato un salto. Nel 2013, grazie agli ASIC (circuiti dedicati all'hashing) vi è stato un altro salto
- Hashing power totale dell'intera rete
- 2009 0,5 MH/sec 8 MH/sec
- 2010 8 MH/sec 16 GH/sec
- 2011 16 GH/s 9 TH/sec
- 2012 9 TH/sec 23 TH/sec
- 2013 23 TH/sec 10 PH/sec
- 2014 10 PH/sec 300 PH/sec
- 2015 300 PH/sec 800 PH/sec
- 2016 800 PH/sec 2,5 EX/sec

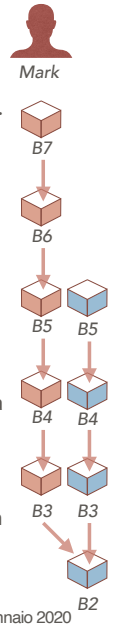
Mining Pools

- Un hardware che ha una potenza di hashing di 14 TH/sec costava circa 2500 US $ nel 2017
- L'hardware consuma 1375 watt, 32 kWh al giorno, al costo di 1$ o 2$ al giorno
- Con la difficoltà corrente, il miner potrà trovare un blocco ogni 4 anni, ottenendo 12,5 bitcoin

Double Spending (1)

- Problema: Alice usa 10 bitcoin per pagare Bob, inoltre usa 10 bitcoin per pagare Charles
- Nelle blockchain, tutte le transazioni sono annunciate in modo pubblico a tutti i nodi
- I nodi raggiungono un accordo sull'ordine in cui le transazioni sono state ricevute, e avendo un ordine per le transazioni, i tentativi di double spending sono subito risolti: la transazione che viene eseguita è la prima, la successiva viene annullata se Alice non ha sufficiente UTXO
- Per capire l'ordine delle transazioni, il blocco ha un timestamp e un hash calcolato su quelle transazioni
- Inoltre, tramite il timestamp si prova che i dati (corrispondenti all'hash) non siano stati creati dopo che l'hash era stato reso pubblico, ovvero i dati non sono stati alterati

Double Spending (2)



- Un miner malevolo (Mark) potrebbe creare un catena derivata (offspring) evitando di mandare alla rete i blocchi che ha trovato. Ci sarebbero quindi due versioni della blockchain: una versione *veritiera*, che hanno tutti, e la versione che ha solo Mark
- Mark richiede una sua transazione, spendendo i suoi coin, e la transazione è registrata sulla blockchain veritiera, supponiamo che sia registrata su B3; Mark non include questa transazione sulla sua versione della blockchain
- Mark fa crescere la sua versione di blockchain per superare la lunghezza di quella veritiera, quindi rivela al resto dei nodi la sua versione della blockchain
- Il resto della rete si adegua alla versione più lunga, quindi cancella B3 della versione veritiera, e Mark ha nuovamente i coin che aveva speso
- E' riferito come attacco 51%

Attacco 51%

- Per imporre i suoi blocchi, un'organizzazione dovrebbe controllare il 51% dei nodi (è detto 51% attack), per avere potenza di calcolo sufficiente a produrre (con buona probabilità) catene di blocchi lunghe prima di tutti gli altri nodi, ciò è altamente improbabile

Alcune Statistiche

- Attualmente (Gennaio 2020)
  - Il valore di 1 Bitcoin è 7919 Euro
  - Ci sono circa 10800 nodi connessi alla rete blockchain Bitcoin
  - Le prime nazioni per quantità di nodi connessi alla blockchain Bitcoin sono: US (2352), Germania (1912), Francia (605), Netherlands (483), Singapore (347), UK (333), Canada (325)

Introduzione A Ethereum

- Ethereum è stato creato per dare agli utenti una piattaforma generale che può eseguire smart contract.
- Ethereum è un sistema di transizioni di stati distribuito, dove lo stato consiste nei conti correnti (account), e le transizioni di stato sono trasferimenti diretti di valori e di informazioni fra account
- Per proteggere la blockchain da attacchi e abusi, Ethereum ha un protocollo di pagamento, per mezzo del quale si paga una tassa (detta gas) per ciascun memoria usata o computazione eseguita in un contratto o transazione
- I miner che eseguono, verificano, e propagano le transazioni, collezionano le tasse. Le transazioni hanno un campo gas limit per specificare l'ammontare massimo che il mandante può pagare. Se il gas usato in una transazione eccede questo limite la computazione viene bloccata

Cosa È Ethereum

- Ethereum è una macchina a stati deterministica consistente di uno stato singleton accessibile globalmente e una macchina virtuale che applica cambiamento allo stato
- Dal punto di vista pratico, Ethereum è una infrastruttura globale decentralizzata che esegue programmi chiamati *smart contract*. Usa una blockchain per sincronizzare e immagazzinare i cambiamenti di stato e una moneta (cryptocurrency) chiamata ***ether*** per limitare i costi di esecuzione
- Come Bitcoin usa una rete peer-to-peer di partecipanti, un algoritmo di consenso per la sincronizzazione degli aggiornamenti dello stato, firme digitali, hash e una moneta digitale
- Ethereum è progettata per essere una blockchain programmabile general-purpose. Il linguaggio Ethereum è Turing complete

Una Blockchain Generale

- La blockchain originaria è la blockchain di Bitcoin, che traccia lo stato di unità di bitcoin e il loro possesso. Bitcoin è una macchina a stati con consenso distribuito dove le transazioni causano una transizione di stati, alterando il possesso di coin
- Ethereum è una macchina a stati distribuita che traccia lo stato di transizioni di dati di uno store (deposito), ovvero uno store che può tenere dati esprimibili come tuple chiave valore

Decentralised Application

- Ethereum è diventata una piattaforma per programmare Applicazioni Decentralizzate (DApp), ovvero al minimo uno smart contract e una interfaccia utente come frontend web
- Altri componenti della DApp sono: un protocollo e una piattaforma di storage decentralizzati P2P; un protocollo e una piattaforma di messaggistica decentralizzati P2P
- Anziché DApp Si può trovar ÐApp, dove il primo carattere Ð è il carattere latino chiamato ETH

Informazioni Essenziali Di Ethereum

- Moneta: la moneta digitale di Ethereum è chiamata *ether*, indicata con ETH o con il simbolo Ξ (dalla lettera greca Xi)
  - Un ether: 1 ether, 1 ETH, Ξ1
  - Un ether è diviso in unità più piccole, fino alla più piccola detta *wei*. 1 ether = 10^{18} wei
  - 1 ether = 142,95 US dollar (gennaio 2020)
- Un wallet di Ethereum è un componente software che tiene le chiavi private. E' usato per accedere agli account e interagire coi gli smart contract. Una chiave privata corrisponde a un account. I wallet non tengono i coin
  - Un wallet è un'applicazione per sistemi mobile, desktop, o web. Es. MetaMask (estensione del browser), Jaxx (per mobile e desktop)
  - Perdere le chiavi private significa perdere l'accesso ai propri fondi

MetaMask

- Una volta installato sul browser, MetaMask chiederà una password e mostrerà un insieme di 12 parole inglesi. Queste parole sono utili per recuperare l'accesso al wallet (e ai fondi) per mezzo di un altro computer
- MetaMask permette di scegliere fra varie reti Ethereum
  - Main Ethereum Network: la blockchain principale, con moneta digitale reale, ETH ha valore
  - Ropsten Test Network: la blockchain per i test, dove ETH non ha valore
  - Kovan Test Network (ETH non ha valore)
  - Rinkeby Test Network (ETH non ha valore)
  - Localhost 8545, connette a un nodo del computer locale (il nodo può essere parte di una blockchain principale o di test)
  - Custom RPC, connette a un nodo che ha un'interfaccia RPC compatibile Geth

Test

- Passare a Ropsten Test Network
- Andare sul sito faucet.ropsten.be (fornitore di ether), inserire l'indirizzo dell'account (copiandolo), click su Send me test Ether
- Apparirà un hash della transazione (per il pagamento richiesto)
- In pochi secondi la transazione viene accettata (mined) dalla rete Ropsten e il wallet MetaMask mostrerà il nuovo bilancio (di 1,5 ETH)
- Facendo click sull'id della transazione si potrà visualizzare l'hash, il timestamp, indirizzi mittente e destinatario, valore, il numero di blocco (block height)
- Chiunque tramite l'id della transazione può vedere tali dettagli

Gas

- Ogni transazione richiede il pagamento di una tassa che è presa dai miner per convalidare la transazione. La tassa in Ethereum è pagata attraverso una moneta virtuale chiamata *gas*. Si paga il gas tramite gli ether, come parte della transazione
- Il prezzo del gas è recentemente 3 gwei
- Il gas limit è impostato al costo di invio di una transazione base
- Un gas limit di 21000 unità = 3 * 21000 gwei = 6,3 * 10^4 * 10^9 wei = 6,3 * 10^{13} * 10^{-18} ether = 0,000063 ether

Account E Contratti

- L'account creato con il wallet MetaMask è detto account esterno (externally owned account, EOA)
- Gli account EOA sono quelli che hanno una chiave privata
- Un altro tipo di account è un contract account, che ha un codice di smart contract, e non ha una chiave privata. Questo account è controllato dalla logica dello smart contract, il programma che è registrato sulla blockchain al momento della creazione dell'account
- I contratti hanno indirizzi, come gli EOA, e possono mandare e ricevere ether, come gli EOA. Quando una transazione ha come destinazione un indirizzo di un contratto, la transazione fa sì che si adegua il contratto, usando i dati della transazione come input
- Oltre agli ether, le transazioni possono contenere dati che indicano quale funzione del contratto eseguire e quali parametri passare al contratto. Quindi la transazione chiama funzioni del contratto

EOA E Contratti

- Poiché un account con contratto non ha una chiave privata, esso non può iniziare una transazione. Solo EOA possono iniziare transazioni. I contratti possono reagire alle transazioni
- Generalmente, un EOA manda una richiesta di transazione a un wallet dello smart contract per mandare alcuni ETH a un altro indirizzo
- In una DApp tipicamente si ha un contratto A che chiama un contratto B per tenere uno stato condiviso fra gli utenti del contratto A