Introduzione alle Blockchain

Vincenzo Ciaschini

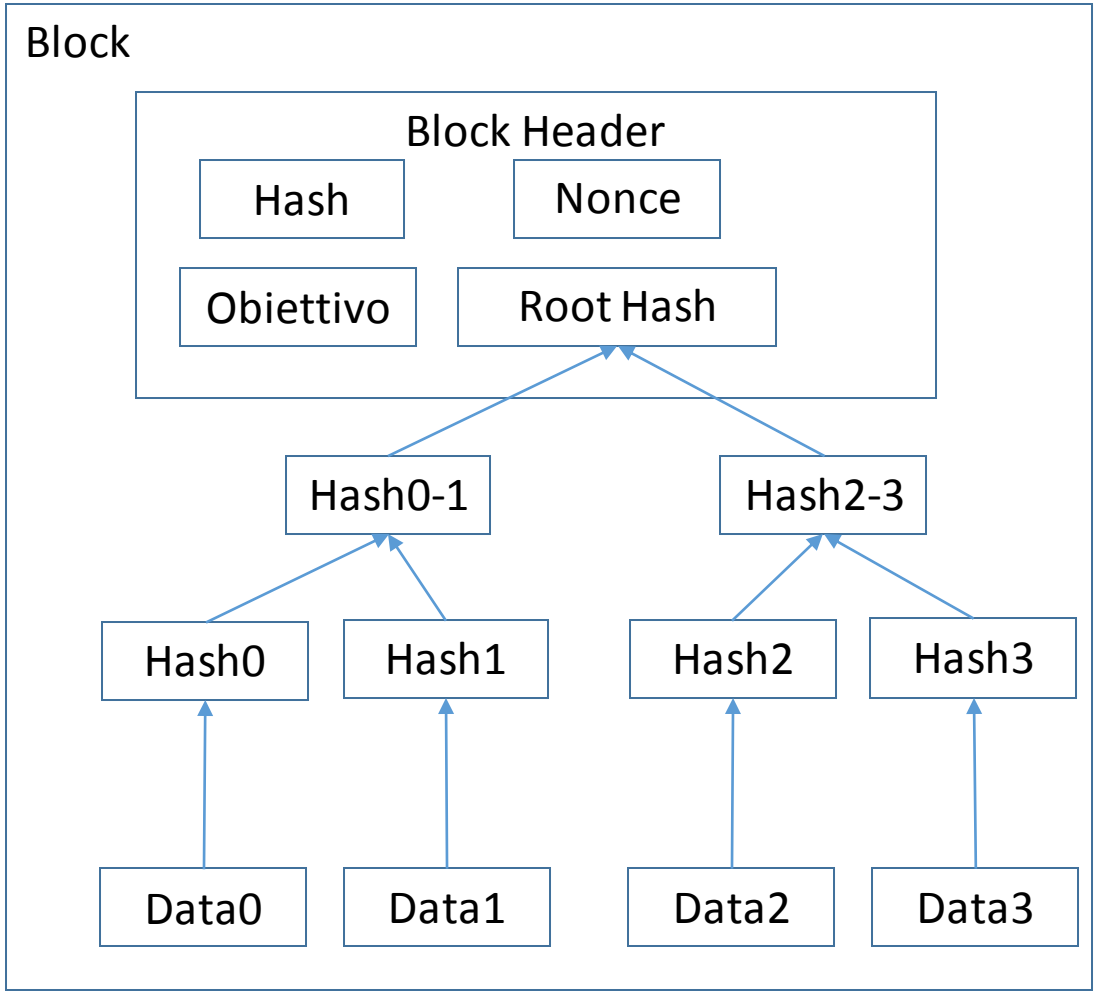
CNAF, 12/4/2018

Cos’e’ una blockchain

- Una block chain è un libro mastro distribuito su una rete di computer (miner)
- Il contenuto del libro mastro è irrilevante per ciò che riguarda la struttura della blockchain
- La blockchain è organizzata in blocchi distinti collegati tra di loro
- Esiste un modo per pubblicare informazioni di pura configurazione per tutti i miner
  - “Obiettivo”, vedi in seguito
- Ogni blocco può contenere uno o più set di informazioni
- Ogni miner ha una copia della blockchain. Queste copie non sono necessariamente coerenti.
- Esiste un algoritmo di convergenza per eliminare le incoerenze
  - La maggioranza dei miner decide
- È praticamente impossibile da falsificare
  - A meno che la maggioranza dei miner (intesi come potenza di calcolo) si metta d’accordo

Struttura di un blocco

- Un blocco è composto da:
  - Un set di oggetti
    - Organizzati in un merkle tree
  - Un header che contiene:
    - L'hash del blocco precedente
      - Hash *crittografico*
    - Un nonce
    - Un obiettivo (descritto in seguito)
    - Un root hash del Merkle Tree
    - Varie ed eventuali



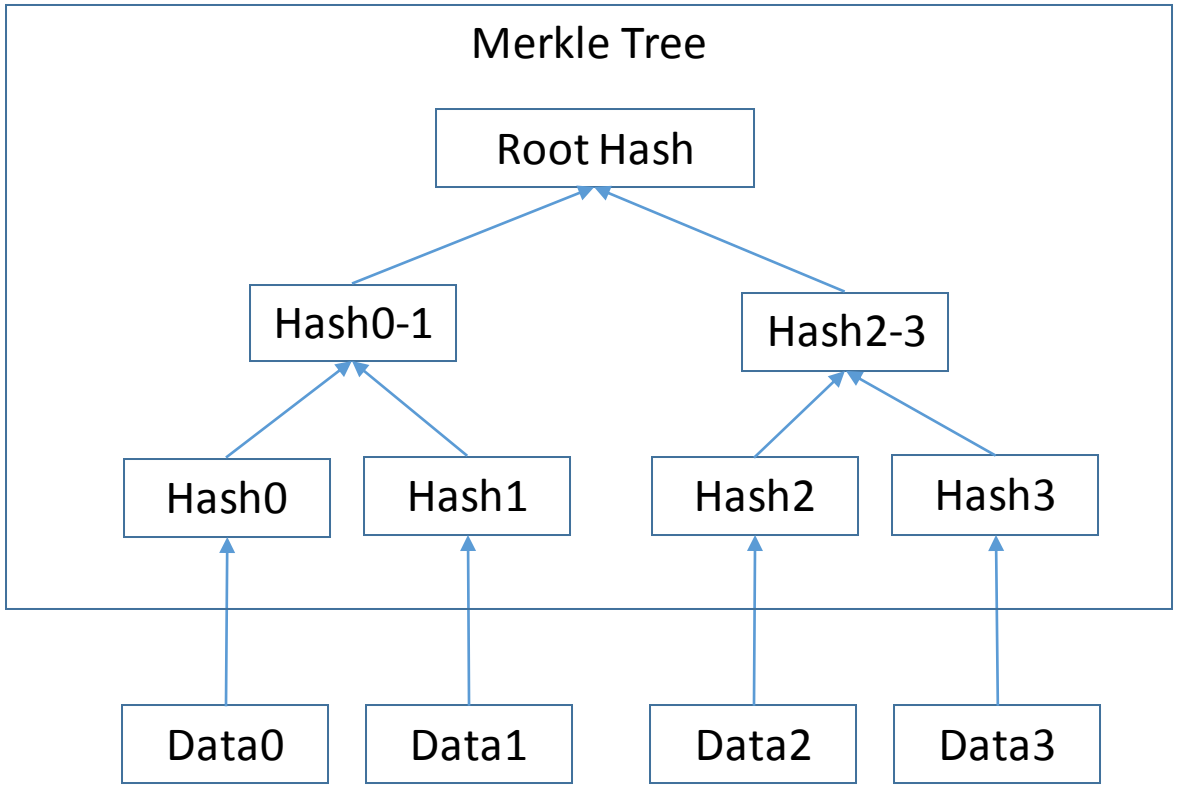
Digressione: hash crittografico

- Un hash crittografico è una funzione di hash realizzata in modo che:
  - Sia estremamente improbabile aver due input diversi con lo stesso hash
  - Deve essere deterministica
  - Deve essere semplice e rapida da calcolare
  - Piccole modifiche nell'input generano hash senza relazioni col valore precedente
  - Deve essere praticamente impossibile, dato un valore di hash, ricostruire un input che generi quello stesso valore di hash se non per forza bruta
    - i.e: provando in sequenza tutti gli input possibili
  - Deve essere praticamente impossibile trovare due differenti input che generino lo stesso hash. (Di nuovo, a meno della forza bruta)
- L'output è un numero intero

- Esempio: SHA2 (massima lunghezza dell'input: 2^{128} -1 bit = 2^{125} -1 bytes

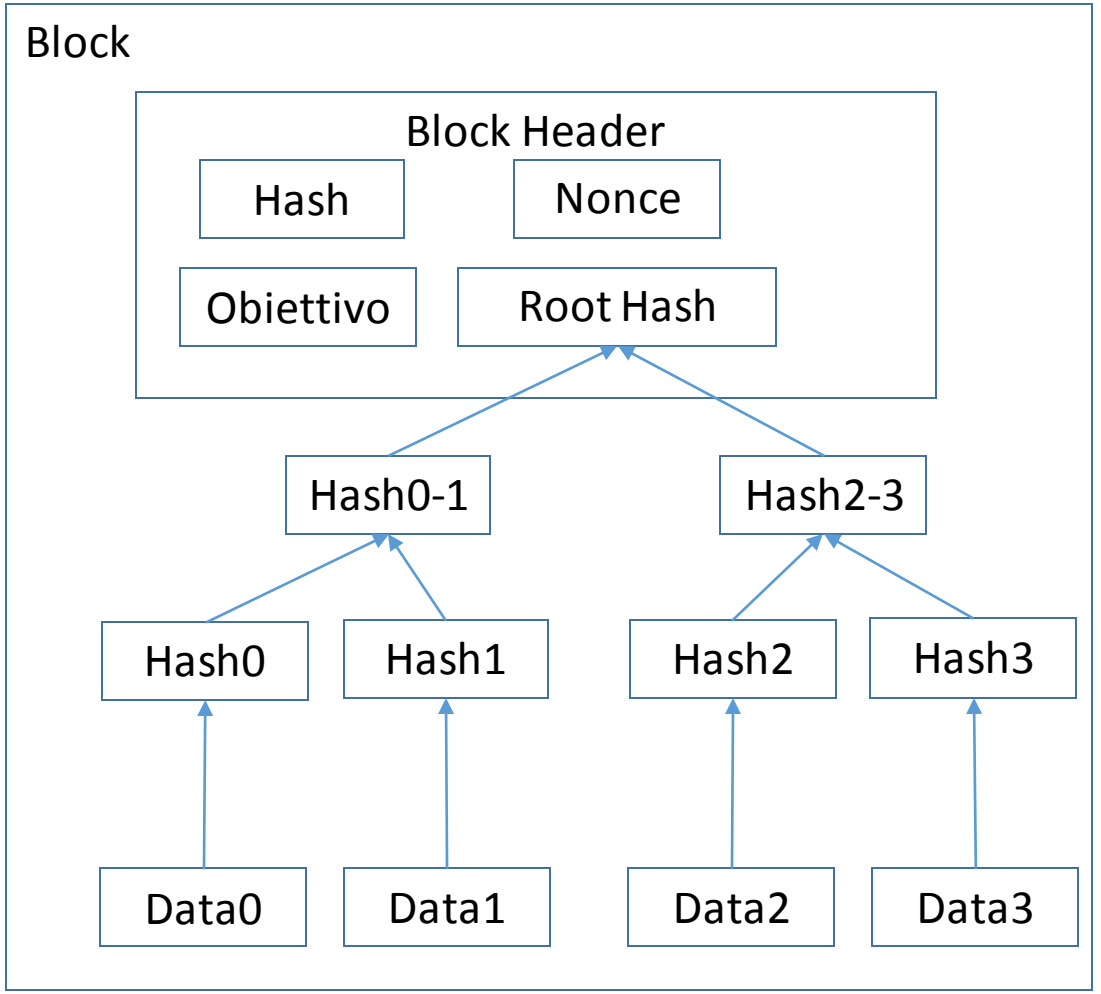
Digressione: Merkle Tree

- Un Merkle Tree è una struttura ad albero in cui ogni nodo foglia è un hash di un dato, ed ogni altro nodo è l'hash della concatenazione degli hash dei nodi figli.
- Generalmente è un albero binario.
- Garantisce la correttezza dei dati in maniera rapida ed efficiente.
- La modifica di un qualunque dato cambia il suo hash, che a cascata cambia tutti gli hash padre fino al root hash.



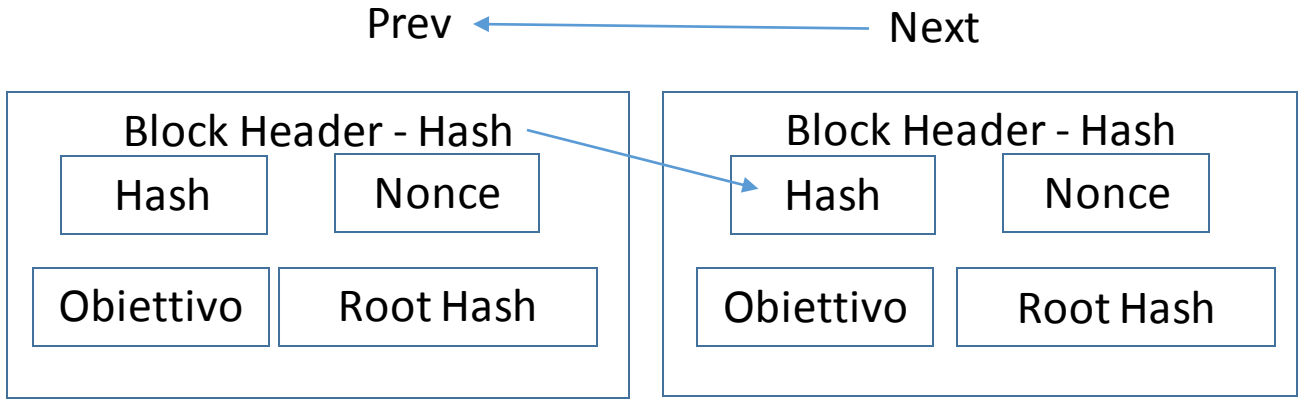
Struttura di un blocco

- La presenza nell'header del root hash del Merkle Tree lega univocamente l'header al contenuto dell'albero.



Blockchain

- Una blockchain è una catena di blocchi collegati dai loro hash
- Il campo hash di un blocco contiene l'hash del block header del blocco precedente

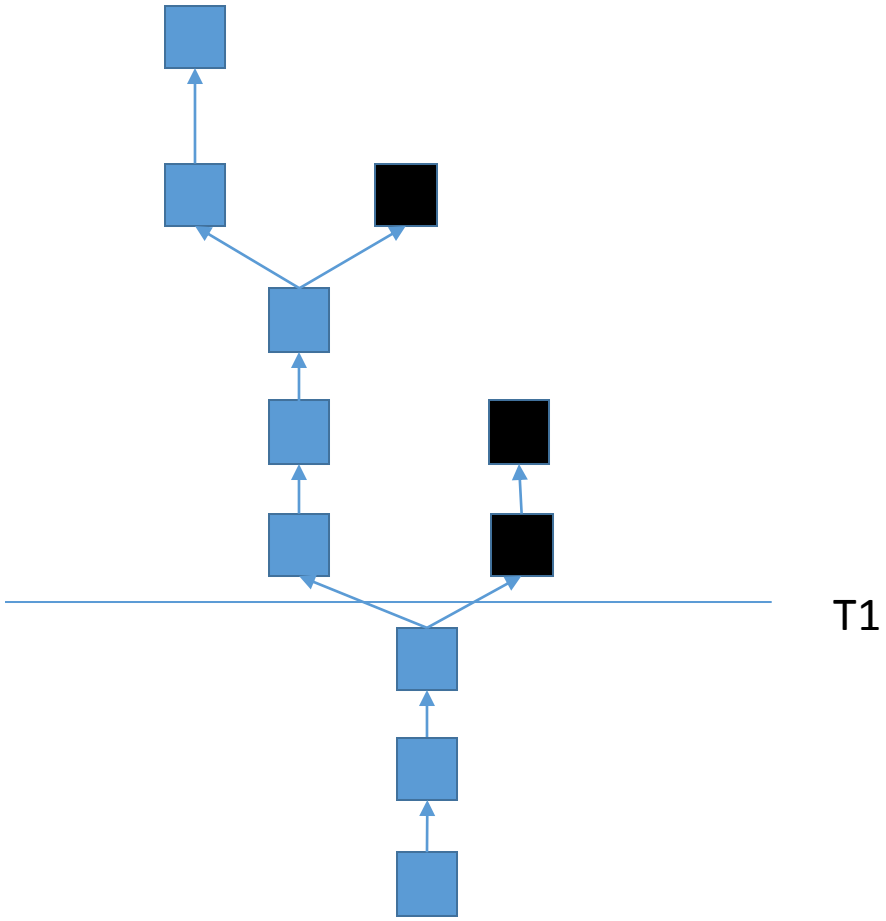


Creazione della blockchain (1/)

- Un nuovo item viene annunciato alla rete
- I componenti della rete (miners) lo ricevono e lo inseriscono in un merkle tree.
- Quando ci sono sufficienti nuovi item, viene creato un nuovo blocco, che viene aggiunto alla visione della catena di un singolo miner
- Il nuovo blocco viene annunciato alla rete
  - Nota: più miner possono annunciare il blocco col nuovo item (fork). Solo uno può entrare a far parte della chain “definitiva”
- I miner aggiungono il blocco alla propria blockchain e cominciano a lavorare sul successivo

Creazione della blockchain (2/)

- La risoluzione contemporanea di più blocchi può causare forking della chain (T1)
- In caso di pari lunghezza dei rami, un miner può lavorare sul branch che preferisce
- Non appena un branch diventa più lungo degli altri, i branch più corti vengono abbandonati (in nero) e non si lavora più su di loro



Sicurezza della blockchain (1/)

- Cosa impedisce ad un miner di uscire rapidamente con sempre nuovi blocchi e così imporre la propria versione della chain?
- Non basta un hash qualunque.
- L'hash dell'header del nuovo blocco deve essere MINORE del valore "obiettivo."
  - Ricordate che un hash è un numero intero.
  - Il valore "obiettivo" varia nel tempo.
    - Generalmente diminuisce.
    - La diminuzione rende più difficile la creazione di un blocco ed è necessaria a causa dell'aumento delle capacità computazionali.
  - Questo è ottenuto manipolando il campo "nonce" fino a quando ciò è vero.
  - Fino a quando l'algoritmo di hash crittografico non viene infranto, questo è un processo computazionalmente pesante e fondamentalmente casuale.

Divagazione: Obiettivo

- Cos'è l'obiettivo?
- L'obiettivo di un blocco è il valore massimo che l'hash di quel blocco può assumere.
- Viene pubblicato da un servizio centrale e cambia col tempo. Generalmente in maniera descrescente.
- Dal momento della pubblicazione di un nuovo obiettivo dal servizio centrale, esso sarà quello usato da tutti i nuovi blocchi
- Il suo scopo è garantire che la creazione di un blocco richieda in ogni caso uno sforzo computazionale elevato (proof of work)

Sicurezza della blockchain (2/)

- Non repudiabilità:
  - Chiunque volesse falsificare un blocco in una blockchain dovrebbe ricostruire il blocco che lo contiene più tutti i blocchi successive nella rete. Ma nel frattempo gli altri miner hanno già allungato la catena. Questo compito è inoltre sempre più difficile man mano che passa il tempo
- Repudiabilità:
  - Qualunque dato contenuto in un blocco che faccia parte di un branch "ignorato" non esiste più.
    - Un blocco "ignorato" può venire "resuscitato" aggiungendo nuovo blocchi sopra
- È quindi necessario aspettare un adeguato allungamento della catena prima di aver fiducia nella sua non-repudiabilità
  - In pratica è sufficiente aspettare 6 blocchi dopo quello contenente il proprio item.
- Tutto si basa sul fatto che un nodo disonesto verrà superato dalla massa di quelli onesti.

Sicurezza della blockchain

- Casualità
  - Il requisito sul valore di hash non rende possibile prevedere quale miner creerà per primo il nuovo blocco
    - Tutti gli altri miner hanno sprecato il proprio lavoro
- Repudiabilità
  - Un numero sufficiente di miner (intesi come potenza di calcolo) che lavorino insieme può imporre la propria versione della blockchain.
    - Sufficiente -> > 50%
- La sicurezza e la corretta implementazione dell'algoritmo di hash sono FONDAMENTALI
  - Se l'algoritmo viene infranto, come fatto per esempio con MD5, l'affidabilità di tutta la blockchain decade

Utilità della blockchain

- Le blockchain sono utili quando le seguenti dichiarazioni sono tutte vere:
  - Si richiede una non-repudiabilità dei dati
  - Le modifiche sono concorrenti ed effettuate da entità che non si fidano l'una dell'altra
  - I miner sono numerosi, indipendenti e non c'è uno squilibrio esagerato di potenza di calcolo
  - Un registro centrale non è possibile o desiderabile
  - Esiste un modo sensato per ricompensare i miner

Praticalità della blockchain

- I miner fanno tantissimo lavoro
  - La maggior parte del quale sprecato
  - Ma che costa comunque denaro sonante
  - Occorre un incentivo per continuare a lavorare sulla chain
- Non è un caso se attualmente le implementazioni sono del tipo “x-coin”
  - L’incentivo classico è che la prima transazione di un nuovo blocco introduce la creazione di un coin che diventa proprietà del miner se il blocco viene creato con successo e accettato nella chain.

Praticalità della blockchain

- Implementazioni “centralizzate” sono possibili ma non hanno alcun senso
  - Bisognerebbe comunque pagare in qualche modo i miner
  - L’unico vantaggio sarebbe la distribuzione del libro delle transazioni
    - Esistono già soluzioni efficaci e a costo minore!
      - Spoiler: si chiamano DB