Blockchain - PDT

SANDRO VECCHIARELLI

COO POMIAGER

MERCOLEDI 25 NOVEMBRE 2020

Blockchain

AT A GLANCE

Cos’è una blockchain

- Una tecnologia che permette di memorizzare informazioni che nel tempo non potranno mai più essere modificate

Cos’è una blockchain

- Perché le informazioni non possono essere modificabili?
- Dobbiamo parlare di Hash

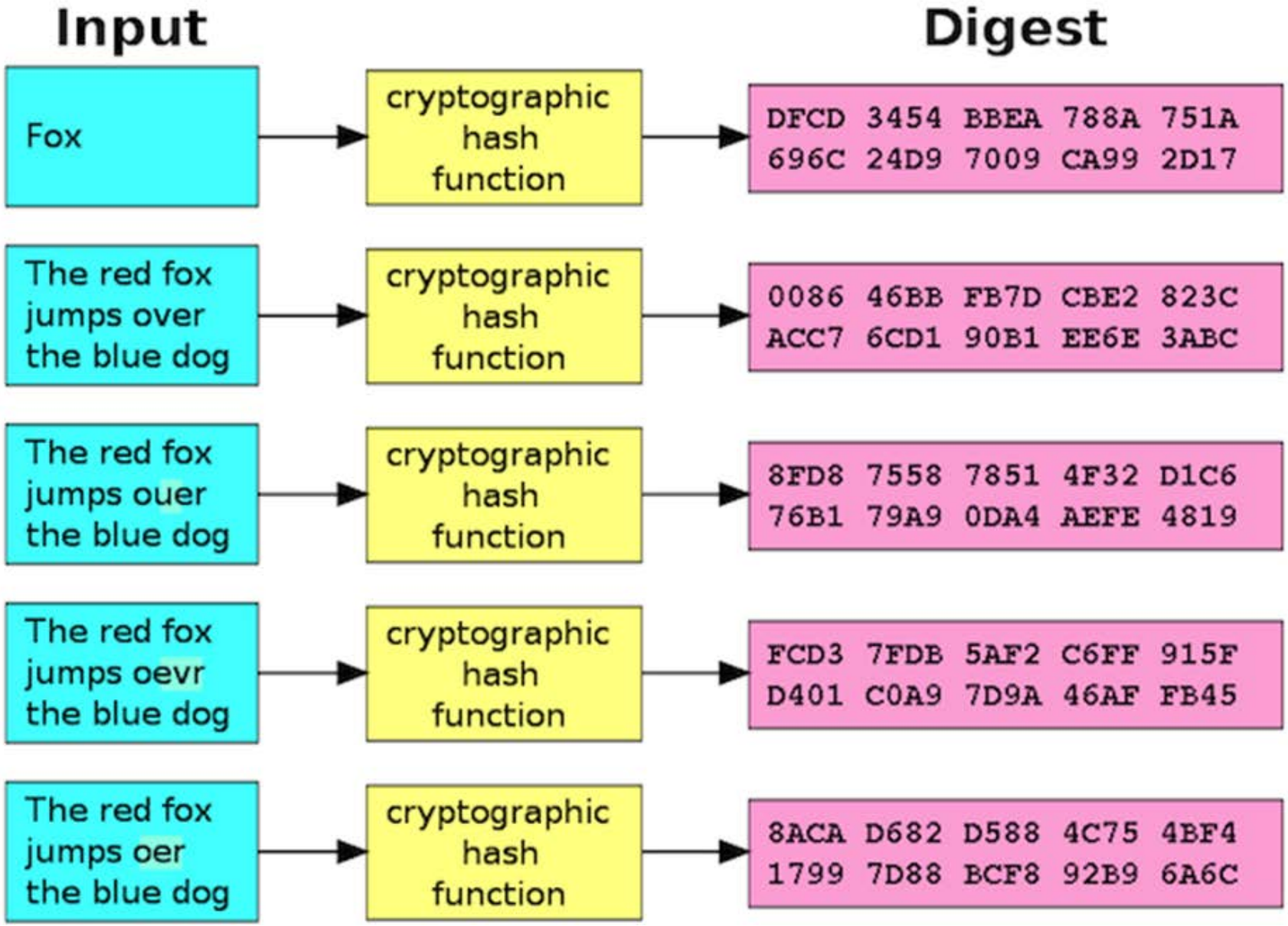
Hash

- E’ una funzione matematica
- permette di ricavare l’impronta digitale elettronica di un qualsiasi numero di byte.

Hash

- Preso un insieme di byte qualsiasi
  - un’immagine
  - un audio
  - un video
  - un file .txt, .pdf, .doc
- la funzione di Hash riesce a ricavare una successione di caratteri sempre della stessa dimensione che rappresenta univocamente l’insieme di byte di partenza

Hash


Input
Digest
Fox
cryptographic hash function
DFCD 3454 BBEA 788A 751A 696C 24D9 7009 CA99 2D17
The red fox jumps over the blue dog
cryptographic hash function
0086 46BB FB7D CBE2 823C ACC7 6CD1 90B1 EE6E 3ABC
The red fox jumps ouer the blue dog
cryptographic hash function
8FD8 7558 7851 4F32 D1C6 76B1 79A9 0DA4 AEFE 4819
The red fox jumps oevr the blue dog
cryptographic hash function
FCD3 7FDB 5AF2 C6FF 915F D401 C0A9 7D9A 46AF FB45
The red fox jumps oer the blue dog
cryptographic hash function
8ACA D682 D588 4C75 4BF4 1799 7D88 BCF8 92B9 6A6C

Hash

- La funzione di Hash è ‘a senso unico’, cioè è facile produrre l’Hash dall’input di partenza ma non potremo mai risalire dall’Hash all’insieme dei dati che l’ha prodotto
- Modificando un singolo bit dall’insieme di partenza ottengo un Hash (Digest) completamente diverso

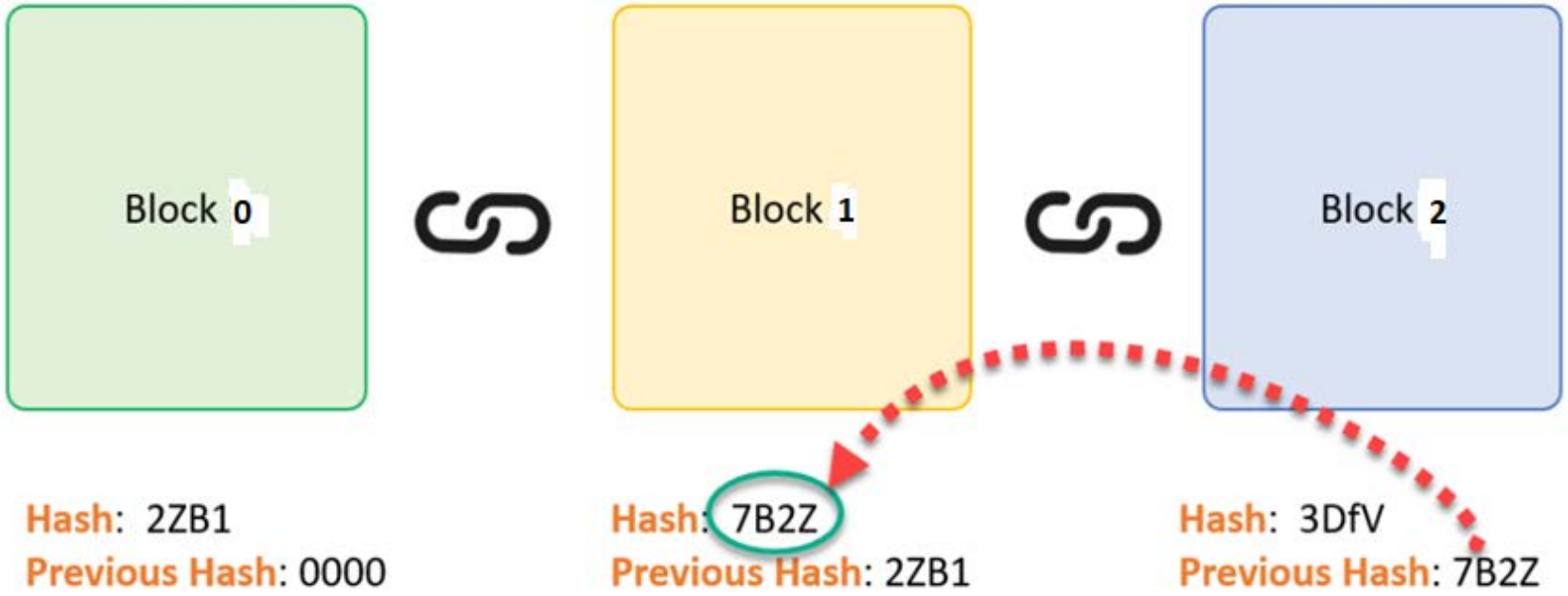
Blockchain

- La Blockchain è formata da **due** entità.
- La prima è rappresentata dalla **concatenazione dei blocchi**
- La seconda dagli **Smart Contract**
- Entrambi residenti all’interno della Blockchain (Quindi nascosti e intoccabili direttamente)

Blockchain – Concatenazione dei Blocchi

- Nella blockchain le informazioni vengono memorizzate in Blocchi
- Tali blocchi sono concatenati e da qui il nome appunto Blockchain o catena di blocchi
- Nel singolo blocco viene memorizzato, oltre alle informazioni, anche l'Hash (il digest) del blocco precedente

Blockchain – Concatenazione dei Blocchi

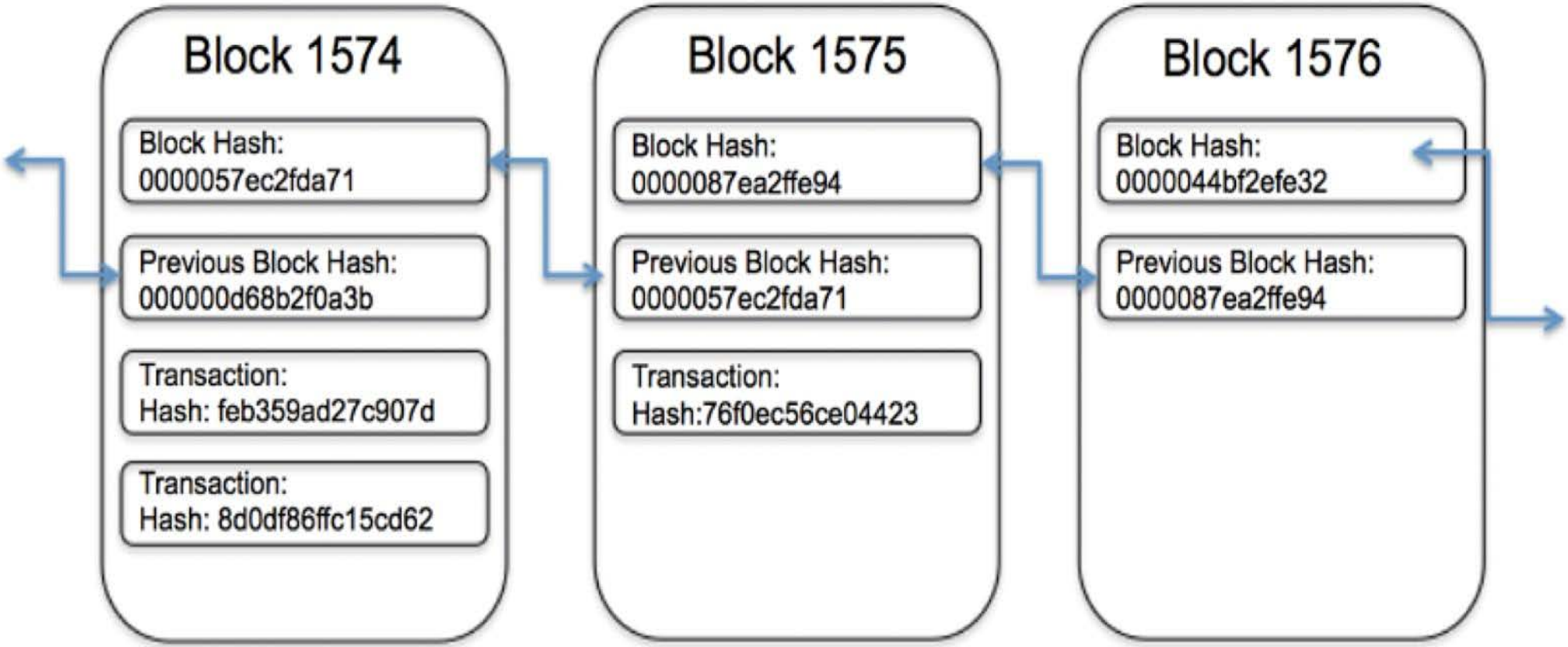


In questo modo la modifica di un singolo bit all'interno del blocco invaliderà le informazioni dell'intera catena a ritroso

Blockchain – Concatenazione dei Blocchi

- Le informazioni che sono memorizzate dentro i blocchi si chiamano **transazioni**
- Sono delle lunghe stringhe di caratteri (ovviamente univoci all'interno di tutti i blocchi della Blockchain) che rappresentano, per esempio come nel nostro caso, il fatto che qualcuno ha creato uno **Smart Contract**

Blockchain – Concatenazione dei Blocchi



Blockchain – Smart Contract

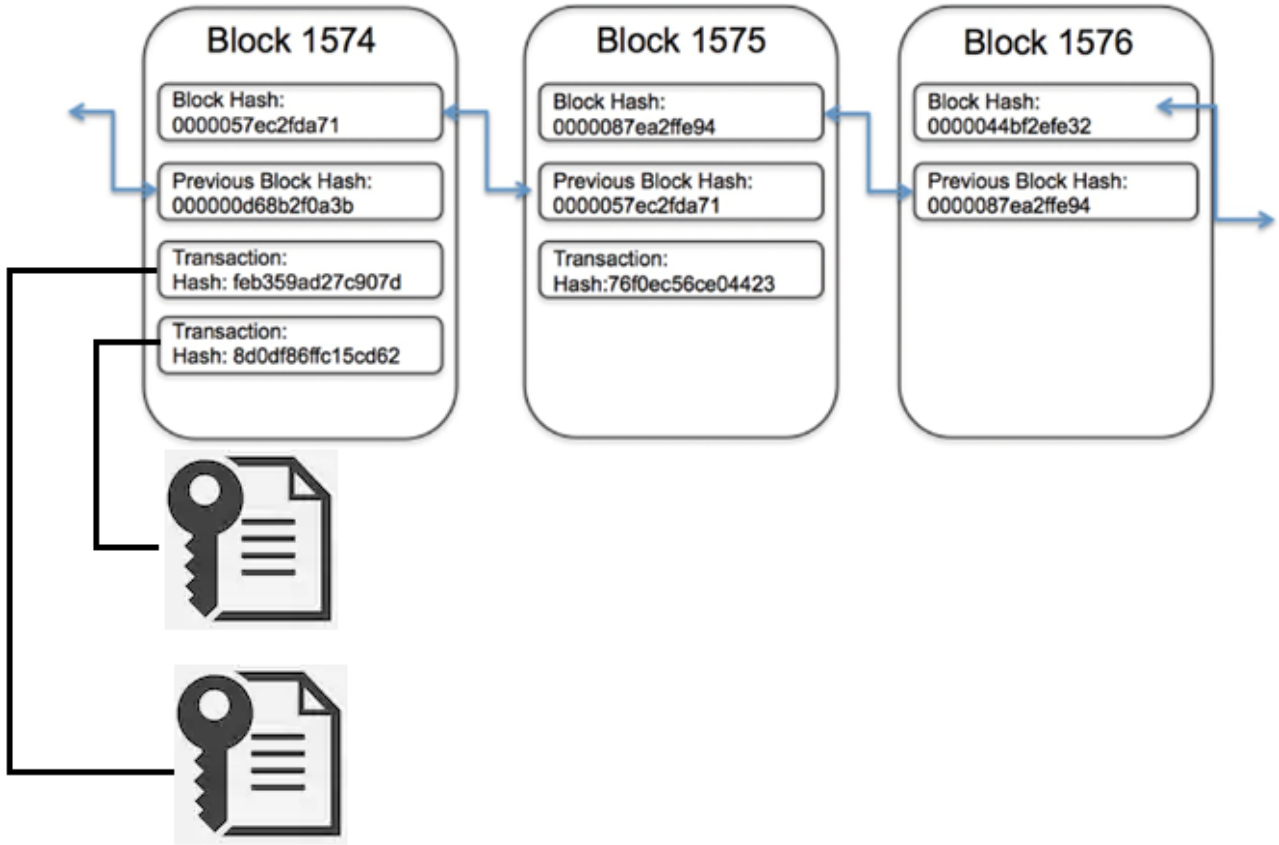
- Uno **Smart Contract** è un semplice ‘pezzettino’ di codice che può memorizzare dei dati o eseguire funzioni

Blockchain – Smart Contract

- Un **utente della blockchain** attraverso un **protocollo sicuro** crea uno **Smart Contract** inserendovi dentro un'informazione qualsiasi come per esempio
  - i dati di un conto corrente
  - i dati di un assegno
  - i dati prodotti da una macchina automatica
  - i dati di un evento accaduto durante il processo di supply-chain
  - i dati di un'operazione effettuata durante il processo di produzione di un alimento o di coltivazione di un prodotto alimentare

Blockchain – Smart Contract

- La creazione dello smart contract viene collegata a una **transazione** che viene inserita in un **blocco** e quest'ultimo concatenato al blocco precedente grazie alla funzione di **Hash** di cui abbiamo parlato prima.



Blockchain – Smart Contract

- Gli Smart Contract sono assolutamente intoccabili per definizione (per come è strutturata fisicamente la Blockchain)
- Da fuori possiamo solo recuperare l’informazione contenuta nello Smart Contract grazie al legame con la transazione presente nel blocco

Blockchain – Smart Contract

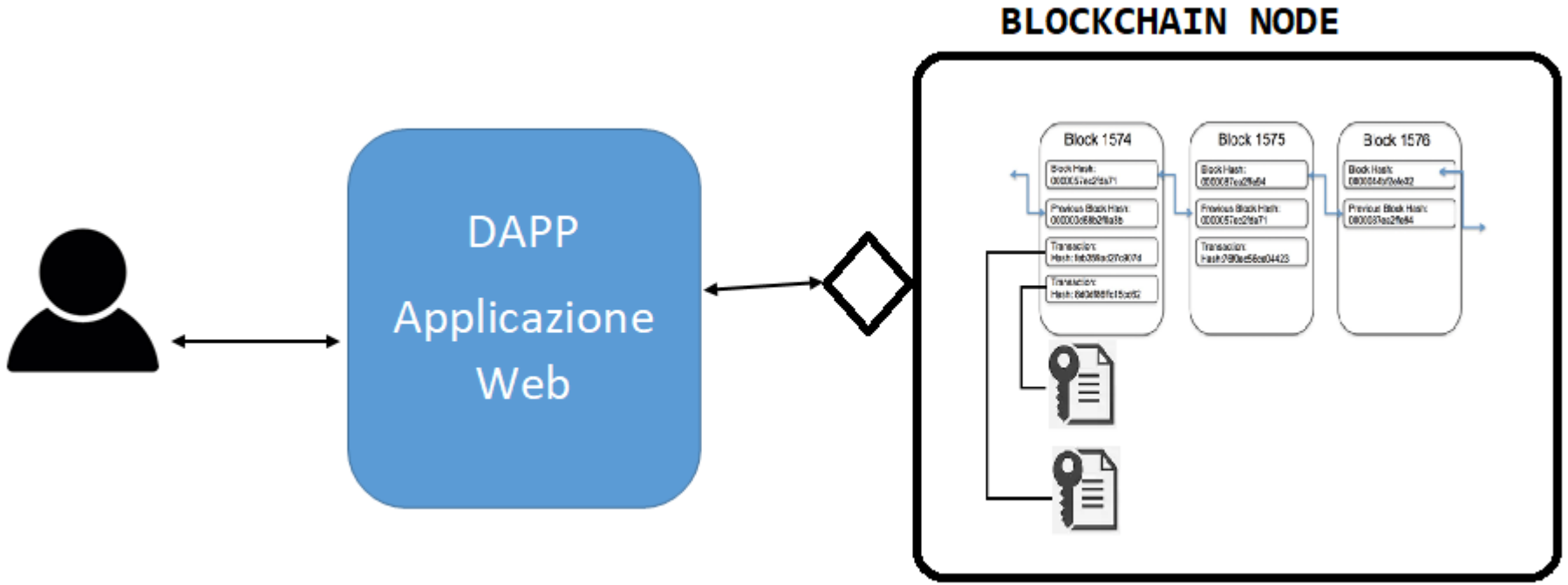
- A ciascuno Smart contract è associato un Identificativo all'interno della Blockchain chiamato **Address** (indirizzo) tipo questo: 0xF3da93e15Dad2976ccb02B79796373DD49ADCaDD
- Quando voglio recuperare l'informazione di uno Smart contract lo faccio fornendo in Input l'indirizzo dello smart Contract
- In Output ricevo l'informazione memorizzata nello Smart Contract al momento della sua creazione

Blockchain – Smart Contract

- Gli Smart Contract possono contenere qualunque tipo di informazione
- L'utente esterno può interagire con la Blockchain solamente attraverso un protocollo di comunicazione sicuro
- L'utente può effettuare solo alcune operazioni quali per esempio
  - **Creare uno Smart Contract** (solo del tipo ovviamente consentito, il cui modello è stato creato preventivamente e fatto 'conoscere' alla Blockchain)
  - **Recuperare i dati di uno Smart Contract** (tramite il suo indirizzo)

Blockchain

- Come si interagisce con la Blockchain?
- Attraverso le Dapp (Distributed Application)

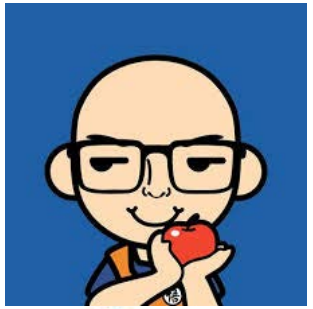


Dr. Sandro Vecchiarelli

Contatti

sandro.vecchiarelli@pomiager.com

http://blog.pomiager.com/



www.pomiager.com