Blockchain e tutela della creatività: Inquadramento tecnico

Marcello Esposito
Ceo & founder, CreativitySafe

CREATIVITYSAFE
PROTECT YOUR IDEAS

Università Bocconi
12 dicembre 2019

Che cosa è la blockchain

Un registro digitale e distribuito di transazioni dove l'inserimento di dati può avvenire solo attraverso il consenso dei partecipanti alla rete, seguendo un protocollo condiviso e senza quindi un ente centrale che coordini o certifichi le modifiche al database.

- Per funzionare, è necessario che il registro possieda le seguenti caratteristiche:
  - «**inalterabile**»: impossibile modificare/cancellare dati pre-esistenti
  - «**mono-verso**»: solo additivo, cresce in un'unica direzione temporale
  - «**consensuale**»: solo le transazioni approvate dalla collettività possono essere inserite nel registro
- Nelle blockchain pubbliche, la raccolta del consenso collettivo avviene attraverso il processo di «**mining**». Ad esempio, nella blockchain di bitcoin:
  - un sapiente dosaggio di incentivi e costi consente alla «mano invisibile» del libero mercato di svolgere il proprio dovere, mantenendo l'integrità del database
  - ogni 10 minuti si svolge una gara crittografica dove chi riesce ad aggiungere un nuovo blocco di dati alla catena si aggiudica 12,5 bitcoin (incentivo). Per partecipare, è necessario impiegare tanta energia elettrica e hardware.

Per capire la blockchain dobbiamo capire l'idea di «cripto» valuta

L'obiettivo della crittografia non è rendere anonime le transazioni, ma rendere possibile una moneta digitale in un ambiente decentralizzato

- Per replicare una moneta "fisica" bisogna possedere abilità metallurgiche o tipografiche. Per replicare un file basta schiacciare un bottone.
- Una moneta digitale può senz'altro esistere in forma centralizzata (come oggi le monete *fiat,* quelle cioè a corso legale) ma bisogna avere regolamentazioni, apparati giudiziari e forze di polizia.
- Creare una moneta digitale che possa esistere in forma decentralizzata è una sfida che ha richiesto la convergenza tra tecnologie di trasmissione e di condivisione *peer-to-peer*, applicazione di teoria dei giochi e le più moderne tecniche di crittografia.

I pilastri crittografici della blockchain

- La blockchain è fondata sulla crittografia, in particolare su tre funzioni matematiche :
  - **Chiavi asimmetriche**: identificare i soggetti (e aprire/chiudere i rispettivi «conti»)
  - **Hashing** : identificare oggetto della transazione (e imbullonare i blocchi tra di loro)
  - **Merkle Tree**: aggregare le transazioni in blocchi
- L'algoritmo di hashing è usato anche per gestire la dimensione di una transazione e quindi la dimensione del database.

La struttura a blocchi e il «mono-verso» della blockchain rendono possibile attribuire data certa alle transazioni registrate su di essa.

Il primo pilastro crittografico:
la crittografia a chiave pubblica

- A partire da Giulio Cesare e fino agli anni ‘70, la crittografia era sempre stata di tipo **simmetrico**: il destinatario e il mittente dovevano condividere la stessa chiave per decifrare il messaggio.
- Negli anni ’70, nasce la crittografia a **chiavi asimmettriche**: il mittente può cifrare il messaggio usando le chiavi pubbliche del destinatario, ma solo quest’ultimo (grazie alla chiave privata con cui ha forgiato le chiavi pubbliche) può decifrarlo.
- **In un colpo solo, il destinatario può non solo decifrare il messaggio ma dimostrare anche di essere il proprietario legittimo delle chiavi pubbliche**. Tutti infatti sono a conoscenza delle chiavi pubbliche, ma solo chi conosce la chiave privata associata ad esse può decifrare il messaggio.

Le chiavi crittografiche non servono per nascondere l’identità del soggetto, al contrario servono per :

1. identificare la paternità di una transazione
2. proteggere la proprietà dell’oggetto digitale

Il secondo pilastro crittografico:
l'algoritmo di hashing

L'hash identifica univocamente un file ...
... come l' impronta digitale un uomo o la targa un veicolo ...

- E' l'output di una speciale funzione matematica applicata ai bit di un file che deve avere le seguenti caratteristiche:
  - produrre sempre lo stesso numero di caratteri (16, 32, 64 ...)
  - deve generare una «impronta» (hash) che sia imprevedibile e diversa al seppur minimo cambiamento del file in input
- Un algoritmo di hashing deve inoltre produrre output che siano:
  - **non invertibili**, **cioè dall'hash non deve essere possibile risalire all'originale**
  - distribuiti uniformemente su un range molto ampio di valori, di modo che attacchi a «forza bruta» siano impossibili.
- Esistono diversi algoritmi e metodologie di hashing. Quelli più utilizzati sono pubblici e approvati dal NIST. Lo SHA256 è uno di questi.

Esempi

SHA256: genera un'impronta di 64 caratteri in esadecimale (0,1,2 ... a,b,c,d,e,f)

SHA256(«ciao»):

`b133a0c0e9bee3be20163d2ad31d6248db292aa6dcb1ee087a2aa50e0fc75ae2`

SHA256(«Ciao»):

`25c73520e69f4bf229811e8e46ffe7d80471544b9bee15ed25044b86be4115ad`

SHA256(«O bella Ciao»):

`1fe6b9559e05ff00fa173efe28127fe646edf3eb9f28fd4a079cb72a24afeed9`

SHA256(zip intero album «The Wall»)

`31b3c8bd2227768346bd5288cb65398ae1599aad4ba9f689e571001f7078d2d2`

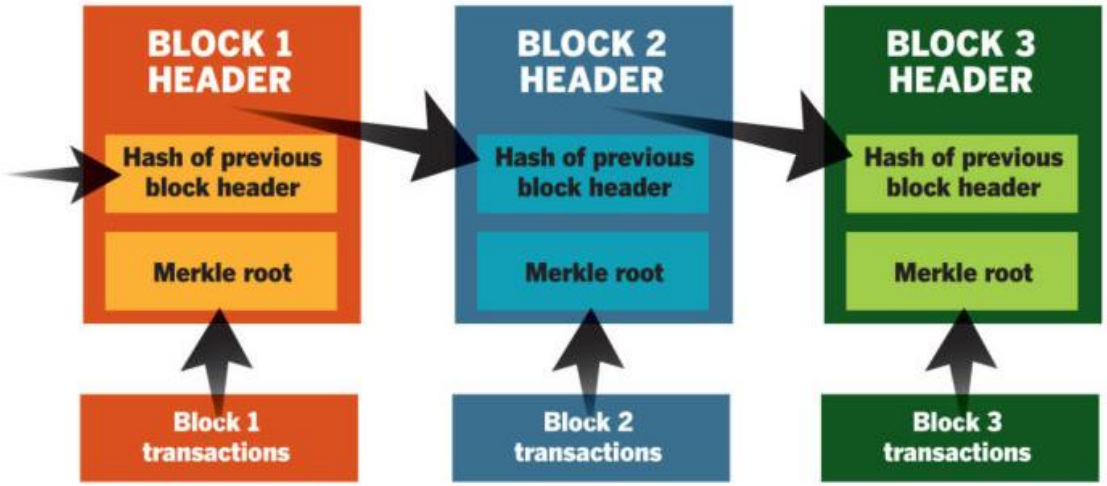
Il co-dominio della funzione SHA256 è enorme: 2^256 ~ 10^77
circa pari al numero di atomi presenti nell'universo:

1. La probabilità di trovare due file con lo stesso hash è «fisicamente» zero.

2. Un attacco di tipo «forza bruta» richiederebbe in media l'età stimata dell'universo usando la GPU di un computer da gaming.

Il «mono-verso» della catena dei blocchi

Nella blockchain di bitcoin le transazioni vengono raggruppate in blocchi di 1.000-3.000 transazioni utilizzando un'altra funzione crittografica (Merkle Tree)



Il registro distribuito delle transazioni viene reso **inviolabile e immutabile** concatendo le transazione un blocco dopo l'altro. Ancora una volta entra in gioco l'algoritmo di hashing: è il giunto matematico che collega un blocco a quello successive.

Il protocollo di bitcoin calibra la "gara" crittografica che i miners devono vincere per aggiudicarsi i bitcoin disponibili di modo che **ogni 10 minuti** venga aggiunto un nuovo blocco alla catena.

Applicazione alla tutela della creatività
step 1 – identificazione univoca dell'opera

Logo da proteggere

SHA256

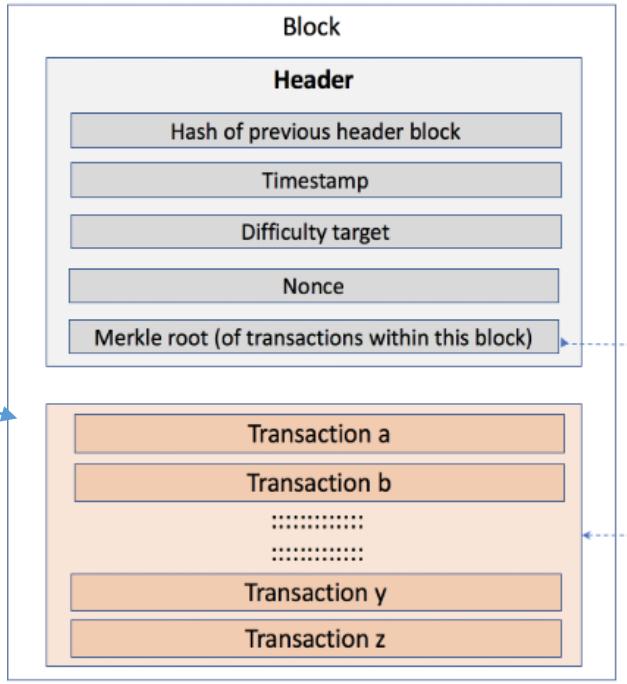
2c27a61aa289aafe42c61ff92c6dcfea621accfcdf24318201f6b1f0d0f2c20e

Applicazione alla tutela della creatività
step 2 – attribuzione della data certa

SHA256

`2c27a61aa289aafe42c61ff92c6dcfea621accfcdf24318201f6b1f0d0f2c20e`

TRANSAZIONE SU BLOCKCHAIN



Quale? PUBBLICA: BITCOIN, ETHEREUM ...

PRIVATA: HYPERLEDGER, CORDA ...

Ricapitolando

1. Si calcola l'hash dell'opera. L'hash identifica l'opera
2. Si registra sulla blockchain l'hash (del file) dell'opera
3. La registrazione attribuisce la data certa all'opera

Da quel momento, l'hash viene cristallizzato per sempre all'interno della blockchain:

- Non può essere cancellato
- Non può essere alterato
- Non può essere modificata la data di registrazione

Volendo si può effettuare una seconda registrazione, ma la data sarebbe comunque successiva alla prima.

E a ben vedere il mono-verso temporale della blockchain può risultare molto utile in tutti i casi (uso nel tempo del marchio, reiterazione delle minacce, etc etc) dove è necessario fornire una rappresentazione dinamica e non statica del fenomeno.

Ultime considerazioni

La scelta della blockchain di bitcoin

La scelta della blockchain dipende dagli obiettivi.

Nel caso della tutela degli IP rights

- **Durata**: le blockchain possono «morire» per disinteresse
- **Notorietà**: l'uso in ambiti non finanziari è agli albori
- **Diffusione**: la knowledge economy non ha confini spaziali

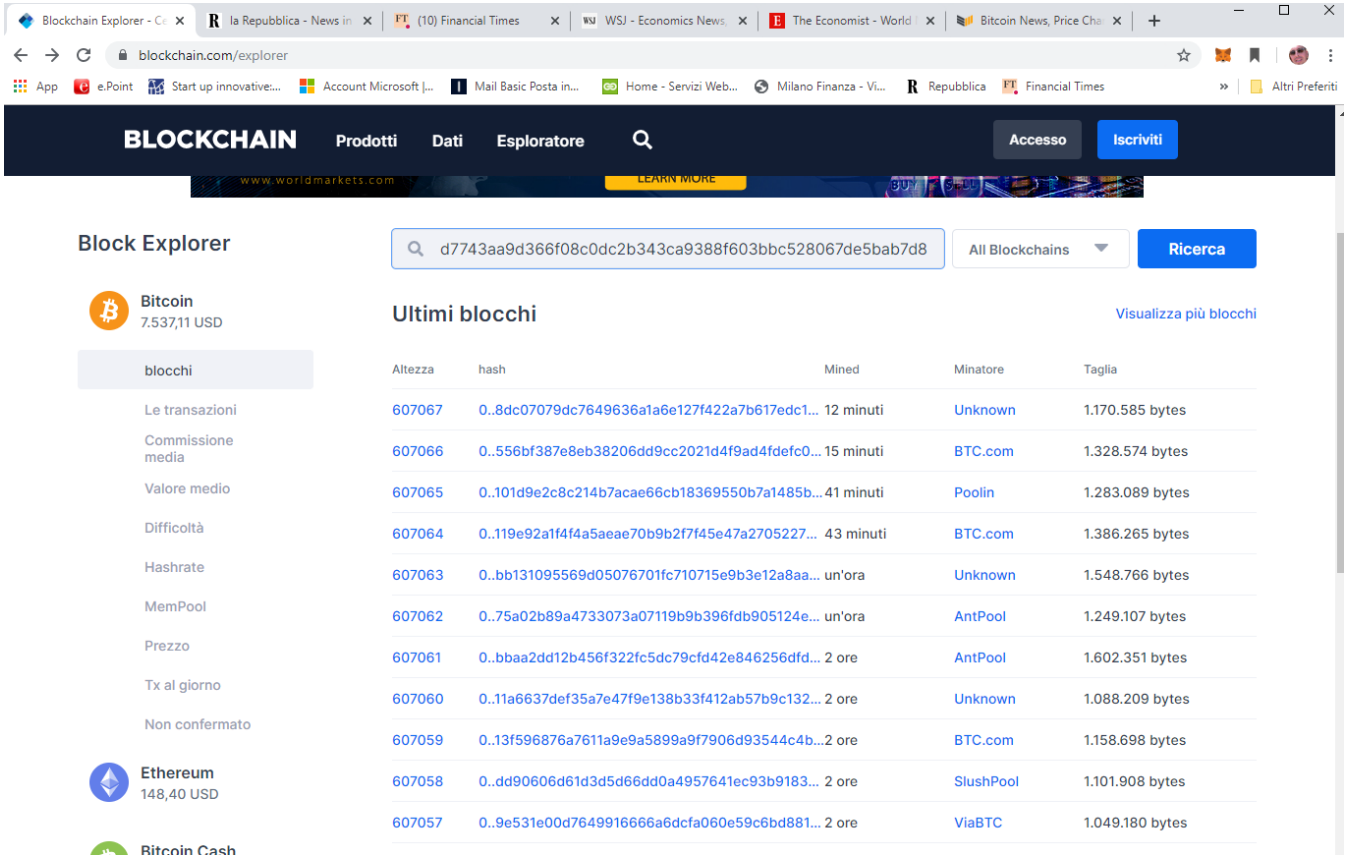
Latenza, programmabilità sono meno importanti

Cryptocurrencies ▾ Exchanges ▾ Watchlist

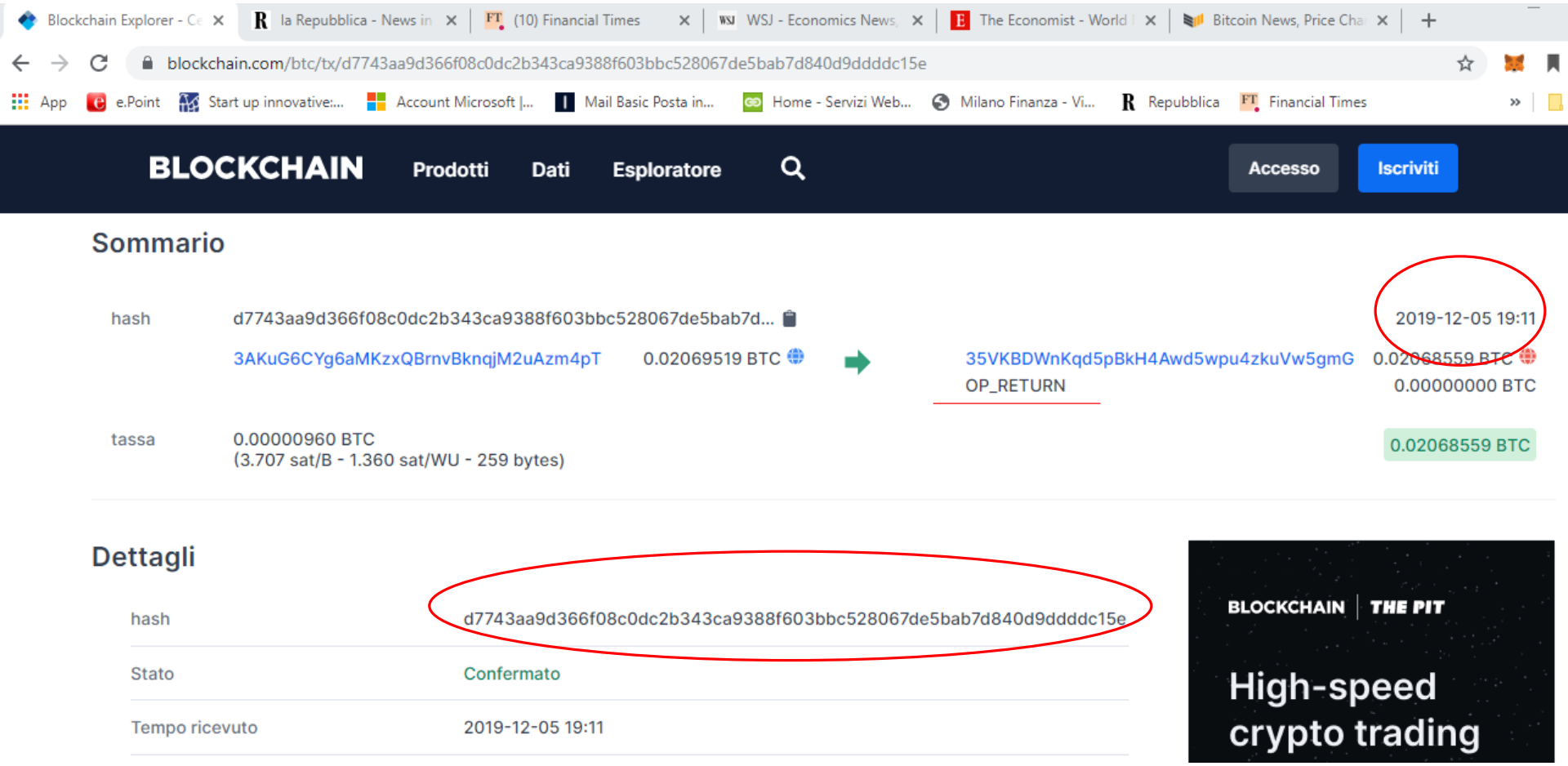
#	Name	Market Cap	Price	Volume (24h)
1	Bitcoin	$136.801.457.025	$7.562,99	$17.347.265.151
2	Ethereum	$16.240.091.536	$149,22	$6.302.942.592
3	XRP	$9.772.751.414	$0,225773	$1.175.243.084
4	Bitcoin Cash	$3.891.572.508	$214,37	$1.088.339.025
5	Litecoin	$2.924.289.527	$45,84	$2.553.258.917
6	EOS	$2.597.492.493	$2,75	$1.244.604.587

Verifica

- in Google cerca «blockchain explorer» e scegli quello che preferisci
- Inserisci il codice della transazione



Verifica



CREATIVITYSAFE
PROTECT YOUR IDEAS

Queste slide sono disponibili
https://creativitysafe.com/bibliografia-tecnica/