

# La Blockchain

Valerio Vaccaro

Thursday 29<sup>th</sup> February, 2024



- 1 Struttura del Blocco
- 2 Genesis Block: analisi approfondita e particolarità
- 3 Le Blockchain di test di Bitcoin
- 4 Bibliografia

# Meme



\* entro la fine del corso capirete tutti i meme.

# Riassunto

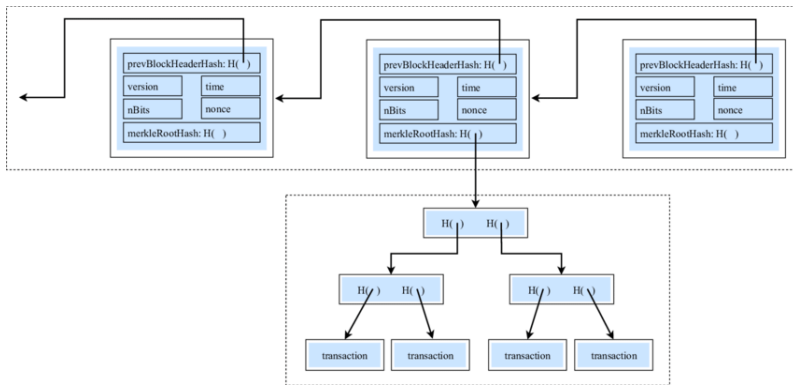
Nella scorsa lezione abbiamo parlato di:

- Cosa è Bitcoin
- Caratteristiche e funzionalità di un nodo
- Full node, SPV, Bloom Filters
- Tor e transportv2
- Mempool

Oggi invece approfondiremo cosa è la **blockchain**.

# Definizione

La blockchain è strutturata come un'ordinata lista di blocchi di transazioni back-linked ovvero in cui ogni blocco è collegato al blocco precedente.



# La catena

La catena è sempre una?

Che succede se due miner trovano un blocco nello stesso istante?

In Bitcoin conta il **lavoro** fatto all'interno di un blocco.

(Se il fork è dettato da una modifica al consenso questo split potrebbe essere insanabile!)

# Come è fatto un blocco?

Il blocco ha questa struttura:

Dimensioni	Campo	Descrizione
4 byte	Block Size	La dimensione del blocco in byte
80 byte	Header	Campi dell'header del blocco
1-9 byte	Transaction Counter	Numero di transazioni presenti nel blocco
Variabile	Transactions	Transazioni registrate nel blocco

# Header

L'header del blocco (80 byte) ha questa struttura:


Dimensioni	Campo	Descrizione
4 byte	Version	Numero di versione del protocollo
32 byte	Previous Block Hash	Hash del blocco precedente (block id)
32 byte	Merkle Root	Radice dell'albero di merkle delle transazioni
4 byte	Timestamp	Orario del blocco (approssimato)
4 byte	Difficulty Target	Target dell'algoritmo di mining
4 byte	Nonce	Campo usato per il mining (ormai è troppo piccolo)



# Riassumendo

version	02000000
previous block hash (reversed)	17975b97c18ed1f7e255adf297599b55 330edab87803c81701000000000000000
Merkle root (reversed)	8a97295a2747b4f1a0b3948df3990344 c0e19fa6b2b92b3a19c8e6badc141787
timestamp	358b0553
bits	535f0119
nonce	48750833
transaction count	63
coinbase transaction	
transaction	
...	

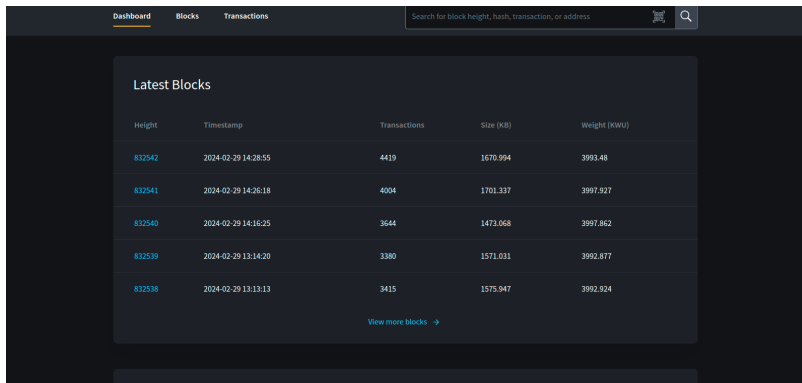
Block hash



```
0000000000000000  
e067a478024addfe  
cdc93628978aa52d  
91fabd4292982a50
```

# Altezza o identificativo del blocco?

L'altezza non è un dato univoco mentre lo è il block id che è ottenibile come hash (SHA256) dell'header del blocco.



The screenshot shows a blockchain explorer interface with a dark theme. At the top, there are tabs for 'Dashboard', 'Blocks', and 'Transactions'. A search bar is located on the right side of the top bar. The main content area is titled 'Latest Blocks' and contains a table with the following data:

Height	Timestamp	Transactions	Size (KB)	Weight (KWU)
832542	2024-02-29 14:28:55	4419	1670.994	3993.48
832541	2024-02-29 14:26:18	4004	1701.337	3997.927
832540	2024-02-29 14:16:25	3644	1473.068	3997.862
832539	2024-02-29 13:14:20	3380	1571.031	3992.877
832538	2024-02-29 13:13:13	3415	1575.947	3992.924

Below the table, there is a link that says 'View more blocks →'.

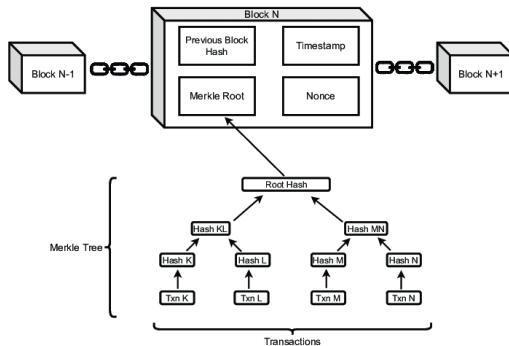
# Altezza o identificativo del blocco?

L'altezza non è un dato univoco mentre lo è il block id che è ottenibile come hash (SHA256) dell'header del blocco.

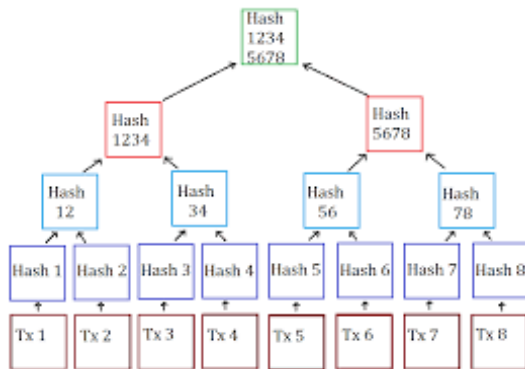
The screenshot shows a blockchain explorer interface with a dark theme. At the top, there are tabs for 'Dashboard', 'Blocks', and 'Transactions'. A search bar is located on the right side of the top navigation bar. The main content area displays 'Block 832542' with a Bitcoin icon. Below the block number is the block hash: '00000000000000000000000235ac398dc2426bf51487aba7d55cf9b8099e10aad35'. A 'PREVIOUS' button with a left arrow is visible. Below this is a table of block details. A 'DETAILS +' button is in the top right corner of the table.

HEIGHT	832542
STATUS	In best chain (1 confirmation)
TIMESTAMP	2024-02-29 14:28:55 GMT +1
SIZE	1670.994 KB
VIRTUAL SIZE	999 vKB
WEIGHT UNITS	3993.48 KWHU

# Merkle tree



# Merkle tree



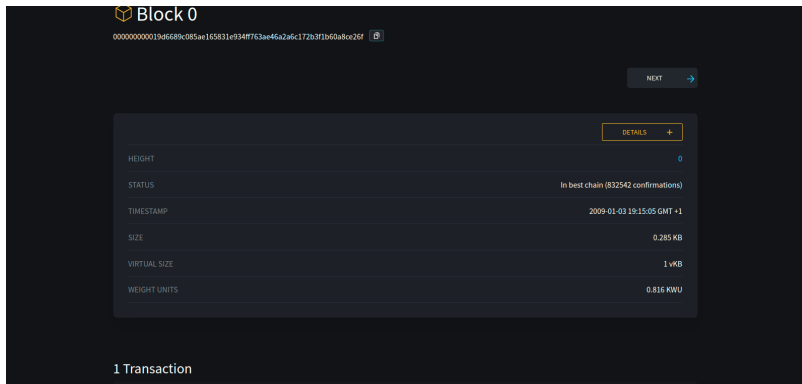
# Pausa



# Genesis Block

Blocco zero o

000000000019d6689c085ae165831e934ff763ae46a2a6c172b3f1b60a8ce26f.



The screenshot displays a web interface for a Bitcoin block explorer. At the top, it shows 'Block 0' with its hash '000000000019d6689c085ae165831e934ff763ae46a2a6c172b3f1b60a8ce26f'. Below this is a table with the following data:

	DETAILS +
HEIGHT	0
STATUS	In best chain (832542 confirmations)
TIMESTAMP	2009-01-03 19:15:05 GMT +1
SIZE	0.285 KB
VIRTUAL SIZE	1 vKB
WEIGHT UNITS	0.816 KWH

At the bottom of the interface, it indicates '1 Transaction'.

# Coinbase

La prima transazione (inspendibile).

1 Transaction

4a5e1e4baab89f3a32518a88c31bc87f6187f6673e2cc77ab2127b7afdeda33b

DETAILS

Coinbase		P2PK	
SCRIPTSIS (ASM)	OP_PUSHBYTES_4 ffffff00 OP_PUSHBYTES_1 04 OP_PUSHBYTES_50 54685205468d6572283032f4a616e2f32383039284368614e63656c6c6f72286f6e284272696e6b286f66287365636f6e64286261696c6f757428666f722862616e6b73	TYPE	P2PK
SCRIPTSIS (HEX)	04ffff00100104455468520546966573203032f4a616e2f32383039284368614e63656c6f72286f6e284272696e6b286f66287365636f6e64286261696c6f757428666f722862616e6b73	SCRIPTPUBKEY (ASM)	OP_PUSHBYTES_65 04678afdb8fc548271967f1a67130b7105cc0a828e39896a7962e0ea1f61deb648f30c3f4cef38c4f35584e51ec112ae5c384df7ba8b4d578a4c702b6df11d5f OP_CHECKSIG
NSEQUENCE	0xffffffff	SCRIPTPUBKEY (HEX)	4104678afdb8fc548271967f1a67130b7105cc0a828e39896a7962e0ea1f61deb649f6bc3f4cef38c4f35584e51ec112ae5c384df7ba8b4d578a4c702b6df11d5fac
		PENDING TX	Unspent

832542 CONFIRMATIONS 50.00000000 BTC



# Coinbase

Una nota di colore ...

```

00000000 01 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 .....
00000010 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 .....
00000020 00 00 00 00 3B A3 ED FD 7A 7B 12 B2 7A C7 2C 3E ....;fíýz{.²zÇ,>
00000030 67 76 8F 61 7F C8 1B C3 88 8A 51 32 3A 9F B8 AA gv.a.È.Ã^ŠQ2:Ÿ.a
00000040 4B 1E 5E 4A 29 AB 5F 49 FF FF 00 1D 1D AC 2B 7C K.^J)«_IŸŸ...¬+|
00000050 01 01 00 00 00 01 00 00 00 00 00 00 00 00 00 00 .....
00000060 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 .....
00000070 00 00 00 00 00 00 FF FF FF FF 4D 04 FF FF 00 1D .....ŸŸŸŸM.ŸŸ..
00000080 01 04 45 54 68 65 20 54 69 6D 65 73 20 30 33 2F ..EThe Times 03/
00000090 4A 61 6E 2F 32 30 30 39 20 43 68 61 6E 63 65 6C Jan/2009 Chancel
000000A0 6C 6F 72 20 6F 6E 20 62 72 69 6E 6B 20 6F 66 20 lor on brink of
000000B0 73 65 63 6F 6E 64 20 62 61 69 6C 6F 75 74 20 66 second bailout f
000000C0 6F 72 20 62 61 6E 6B 73 FF FF FF FF 01 00 F2 05 or banksŸŸŸŸ..ò.
000000D0 2A 01 00 00 00 43 41 04 67 8A FD B0 FE 55 48 27 *....CA.gŠŸ°pUH'
000000E0 19 67 F1 A6 71 30 B7 10 5C D6 A8 28 E0 39 09 A6 .gñ|q0°. \Ö"(à9. |
000000F0 79 62 E0 EA 1F 61 DE B6 49 F6 BC 3F 4C EF 38 C4 ybâê.ab¶IÖ¼?Lİ8Ă
00000100 F3 55 04 E5 1E C1 12 DE 5C 38 4D F7 BA 0B 8D 57 ÓU.ă.Ă.Đ\8M+²..W
00000110 8A 4C 70 2B 6B F1 1D 5F AC 00 00 00 00 00 00 ŠLp+kñ._¬....

```

# Coinbase



# Introduzione

Per provare non serve usare per forza bitcoin in main net ma ci sono delle "istanze" alternative della blockchain utilizzabili.

Tali reti sono state introdotte per dare la possibilità di testare software/procedure e per scopi didattici, le principali reti sono 3:

- Testnet
- Signet
- Regtest

# Testnet

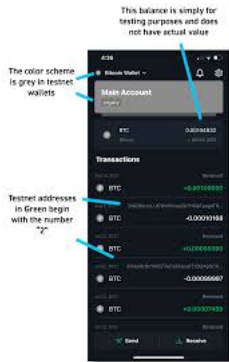
- I token hanno valore ZERO
- I blocchi sono generati con la stessa POW di Bitcoin
- Dopo 20 minuti senza blocchi la difficoltà precipita
- Tanti/tropi blocchi orfani
- Token quasi introvabili
- Molti wallet supportano testnet e ci sono servizi utili
- Ci sono molti wallet e block explorer che supportano testnet

# Signet

- I token hanno valore ZERO
- I blocchi sono firmati da una autorità (e sono regolari)
- Tanti token disponibili
- Poco usata
- Se l'autorità dovesse sparire ...

# Regtest

- I token hanno valore ZER
- Voi siete Satoshi
- Avete già 21.000.000 di token
- Minate con un comando (o anche con un miner)
- Non ci sono vincoli temporali sui blocchi
- Ovviamente vale solo sul vostro computer
- Facile cancellare tutto e simulare scenari complessi (ideale per CI)



Blockstream Green supporta testnet ed è disponibile per Android, iOS, Windows, Linux e MACOS.

# Bibliografia

- Andreas M. Antonopoulos, "Mastering Bitcoin", 2015
- Adam Back, "Hashcash-a denial of service counter-measure", 2002
- Satoshi Nakamoto, "Bitcoin: A Peer-to-Peer Electronic Cash System", 2008
- Hal Finney, "Reusable Proofs of Work", 2004



## Altre risorse

Tra le altre risorse utili mi piace citare:

- Ovviamente [BitPolimi](#) che ha organizzato queste lezioni.
- [Satoshi Spritz](#) - eventi serali a scadenze regolari per parlare di Bitcoin (a Milano ci incontriamo ogni mercoledì dalle 18).
- [Ventuno](#) - Podcast, raccolta di libri e materiali su Bitcoin.
- [Officine Bitcoin](#) - lezioni su telegram da 30 minuti per la risoluzione di problemi pratici.

# Domande





*"That's all Folks!"*