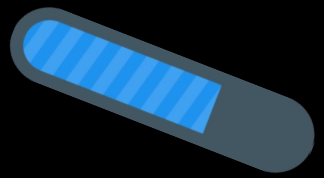
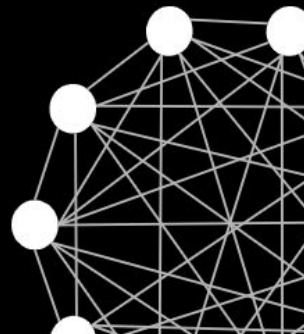
₿6.15

Terminologia Bitcoin

@anilsaidso



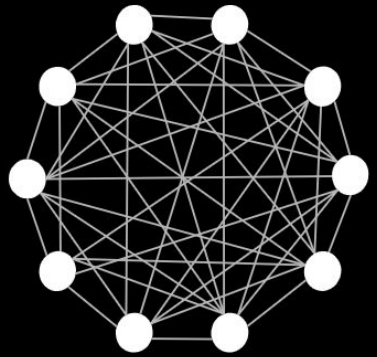


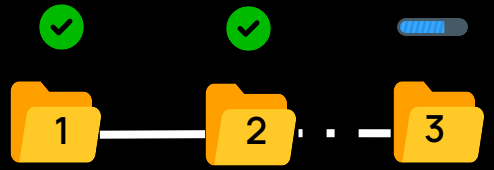
Traduzione a cura di @loop_btc

Indice

@anilsaidso

₿6.15





bitcoin

moneta

la rete

nodi interconnessi

*la timechain**

registro collegato
di transazioni verificate

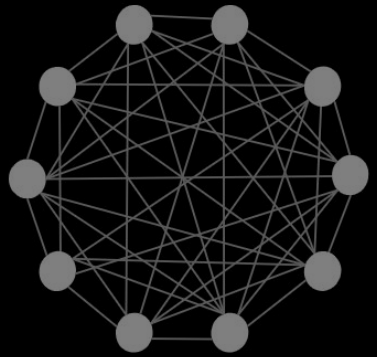
*NdT: nota ai più come “blockchain” anche se Satoshi nel codice la chiama *timechain* (e, in altri casi, “*Proof-of-work chain*”).

Traduzione a cura di @loop_btc

₿6.15

bitcoin

moneta



la rete

nodi interconnessi

la timechain

registro collegato
di transazioni verificate

@anilsaidso

su un totale
di **21 milioni**

₿6.15

=15,000,000
di satoshi (sats)

bitcoin

unità di
conto
nativa della
timechain

@anilsaidso

satoshi

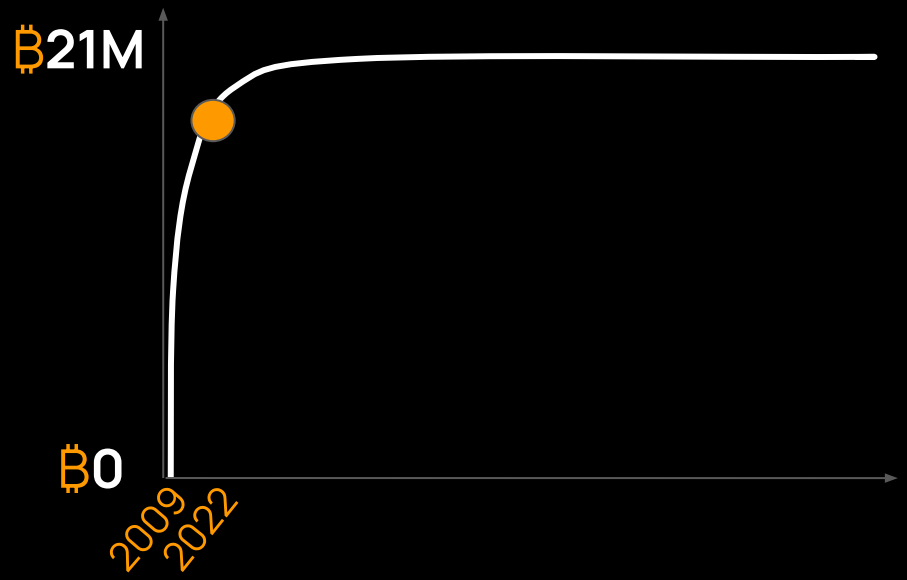
Un bitcoin è divisibile in 100 milioni di unità chiamate *satoshi* (o *sats*).

offerta limitata

₿0 ₿21M

La quantità massima di bitcoin che potrà esistere una volta che saranno stati tutti emessi (minati).

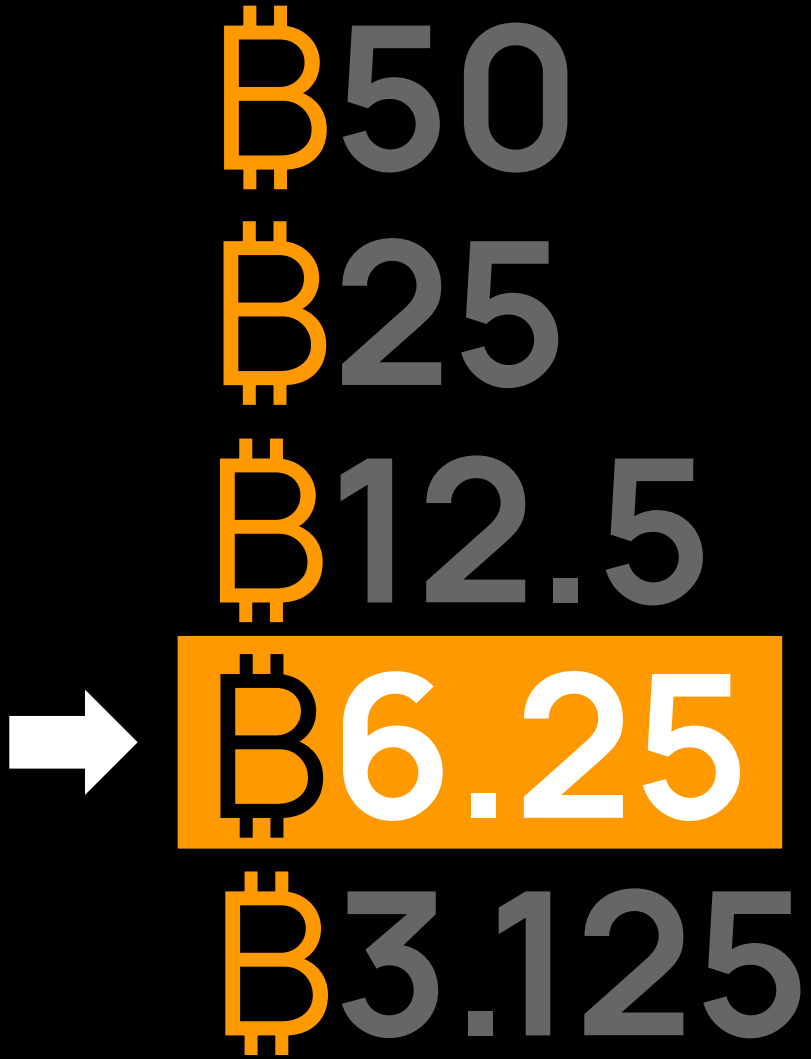
@anilsaidso



supply programmata

emissione pre-programmata di nuovi bitcoin

@anilsaidso



@anilsaidso

halvening

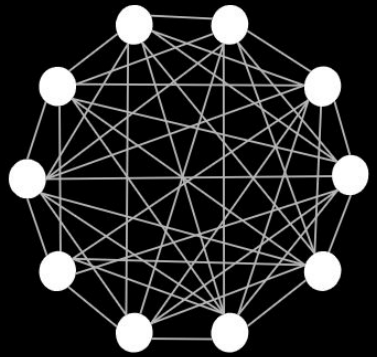
NdT: noto anche come "*halving*" = dimezzamento

Ogni 210,000 blocchi (~4 anni), il tasso di emissione di nuovi bitcoin per blocco si riduce del 50%.

Traduzione a cura di @loop_btc

@anilsaidso

₿6.15



bitcoin

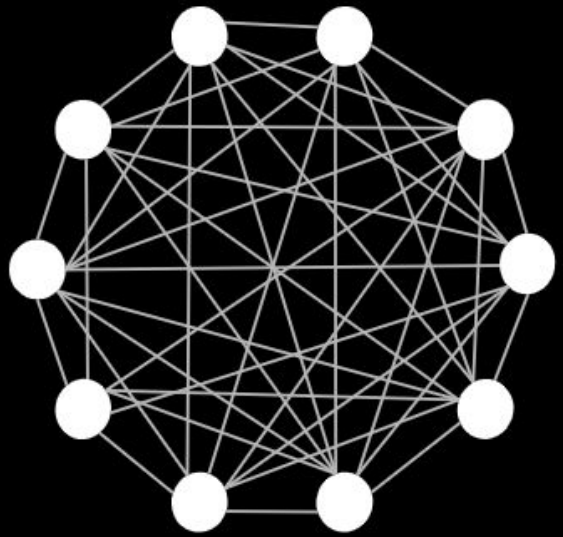
moneta

la rete

nodi interconnessi

la timechain

registro collegato
di transazioni verificate



la rete Bitcoin

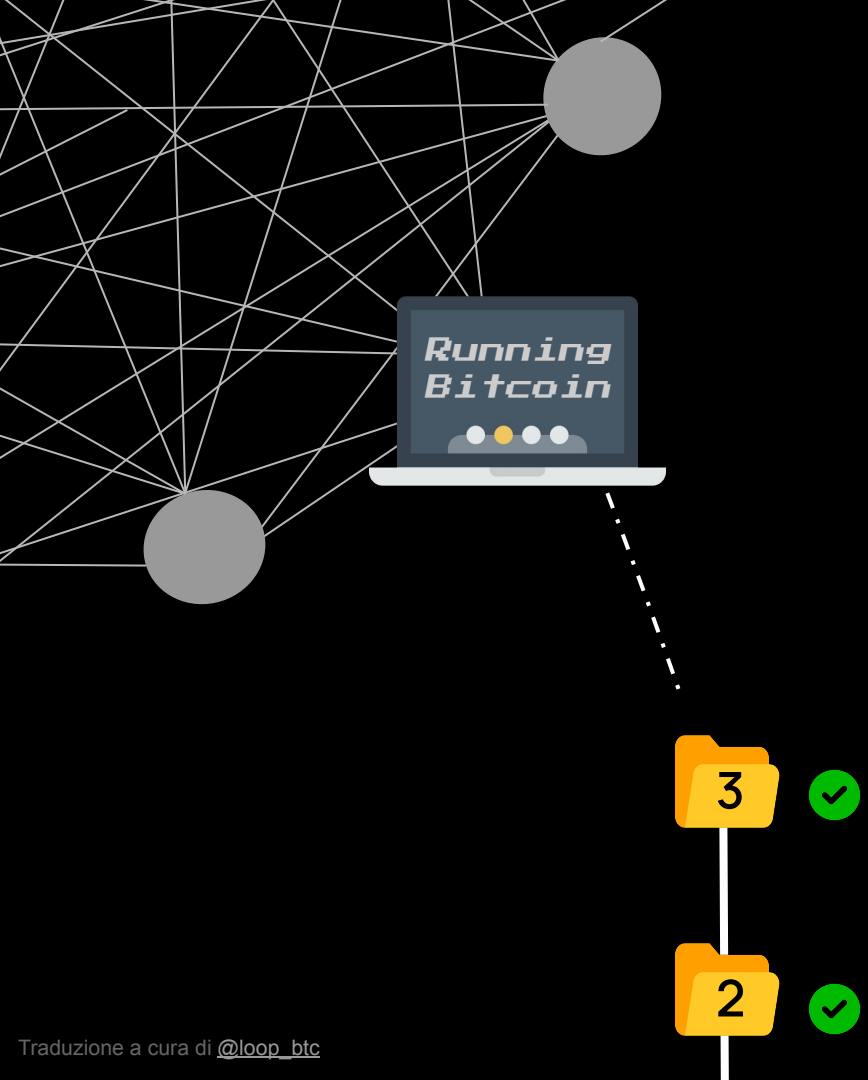
nodi interconnessi che rispettano un insieme condiviso di regole

@anilsaidso

software Bitcoin

software
open-source che
codifica le regole

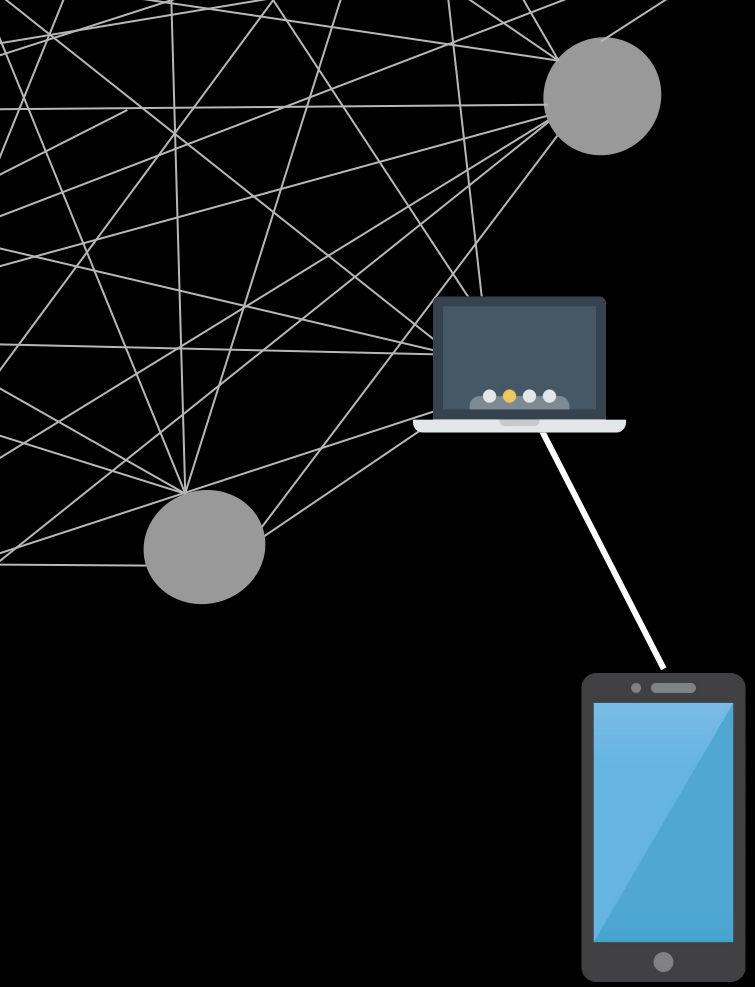
@anilsaidso



nodo completo

- esegue il software Bitcoin
- conserva una copia completa della *timechain*
- fa rispettare le regole della rete

@anilsaidso



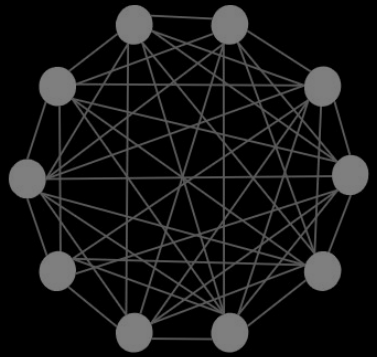
client leggero

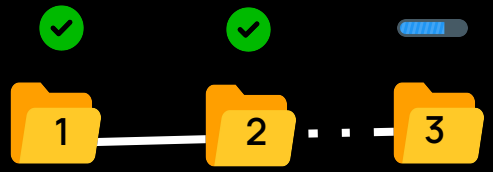
si connette ad un nodo completo per interagire con la rete

archivia solo record parziali per risparmiare spazio

@anilsaidso

₿6.15





bitcoin

moneta

la rete

nodi interconnessi

la timechain

registro collegato
di transazioni verificate

@anilsaidso

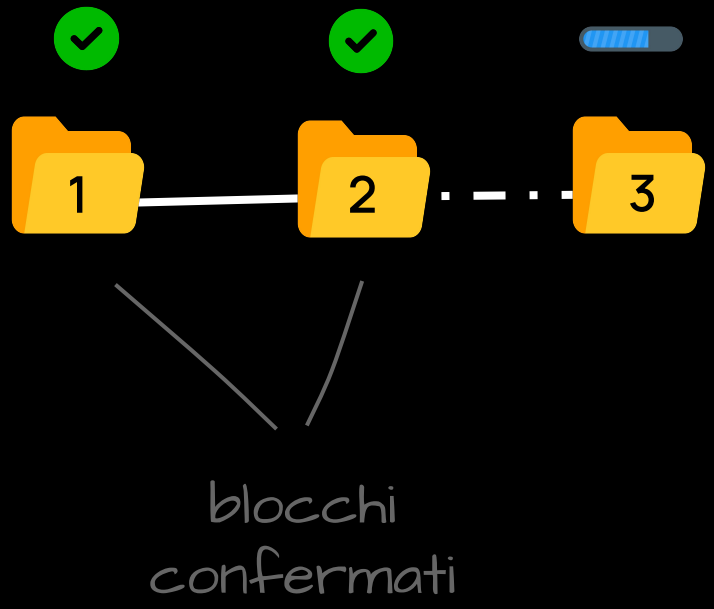
Transazione 1
Transazione 2
Transazione 3

blocco

insieme marcato temporalmente (tramite *timestamp*) di transazioni confermate
in media uno ogni 10 minuti

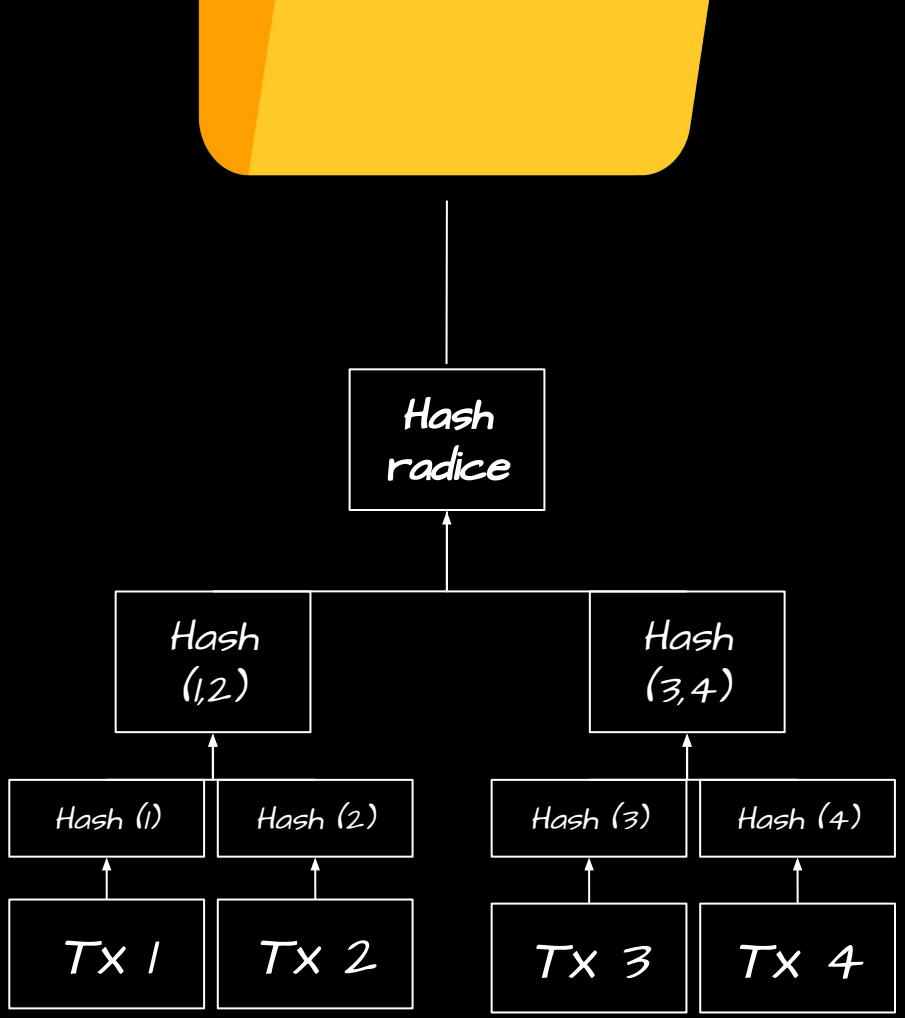
@anilsaidso

la timechain



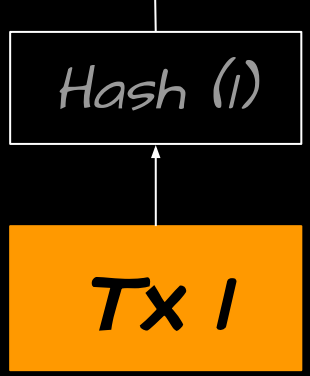
blocchi collegati in sequenza

registro storico di tutte le transazioni confermate



albero di Merkle

struttura di dati che aiuta a ridurre il consumo di spazio e facilita la prova di validità delle transazioni (tx)



transazione

trasferimento della proprietà di bitcoin tra partecipanti alla rete

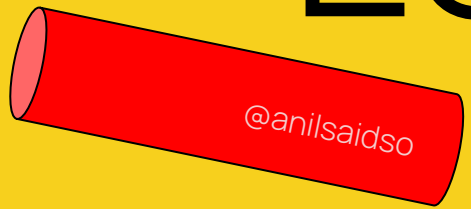
firmato crittograficamente dal mittente

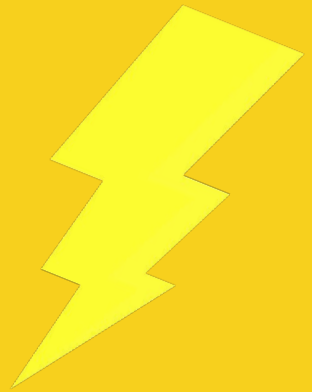
@anilsaidso

Traduzione a cura di @loop_btc

Lightning Network

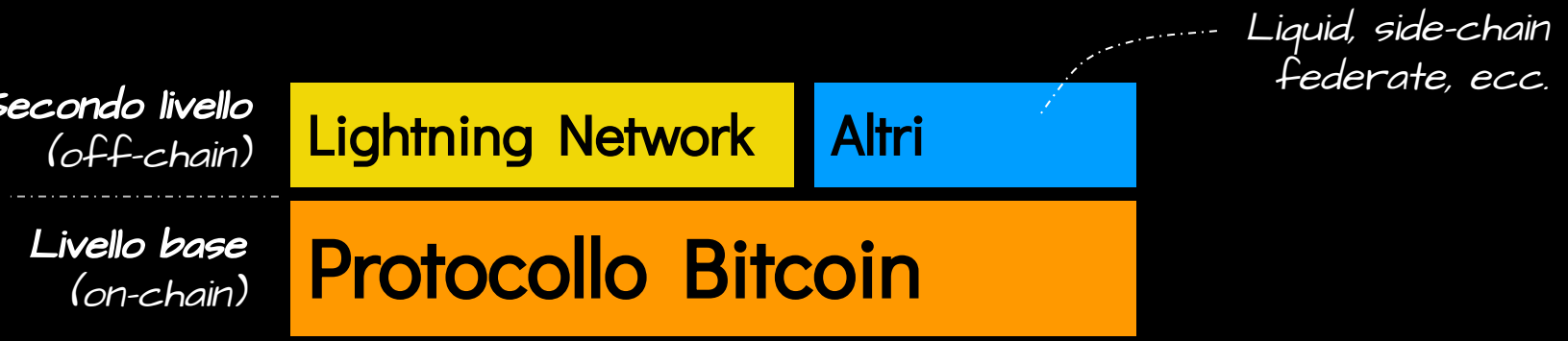
Le basi





Lightning Network

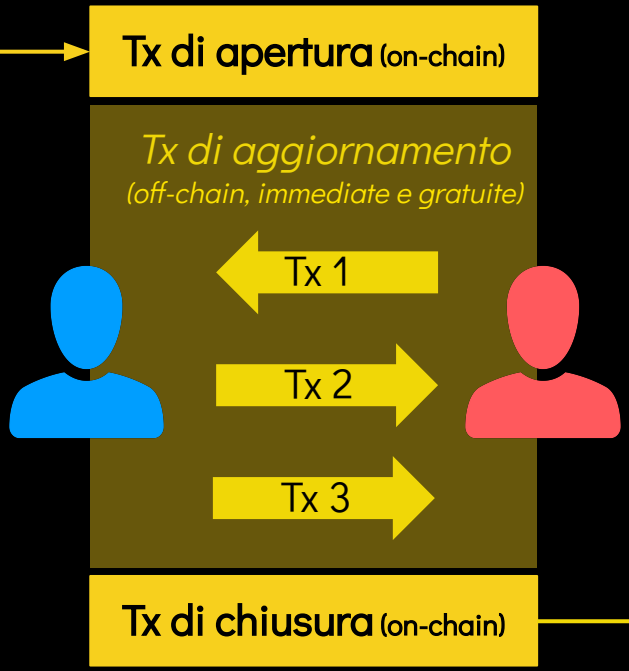
Protocollo che consente la scalabilità di Bitcoin attraverso pagamenti istantanei *off-chain*

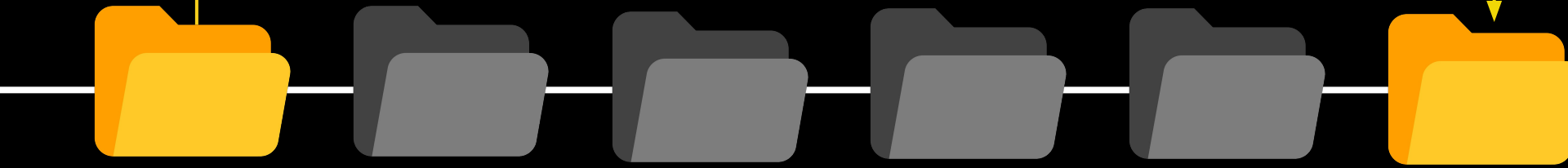


@anilsaidso

Transazioni off-chain

Le transazioni Lightning funzionano come un *conto* aperto tra due partecipanti, che ad un certo punto verrà chiuso e regolato sulla *timechain*.





@anilsaidso

Lightning Network

Il protocollo LN è costituito da **cinque strati**

Canale di pagamento

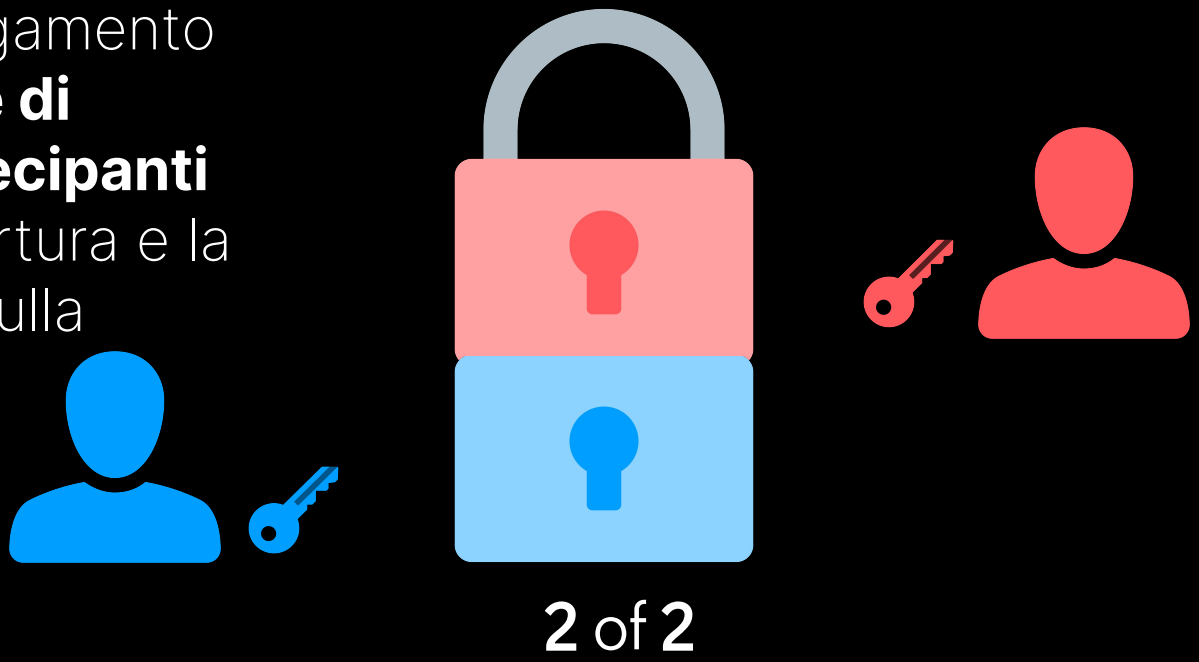
Relazione finanziaria tra **due** nodi

Capacità totale del canale:

150,000 sats

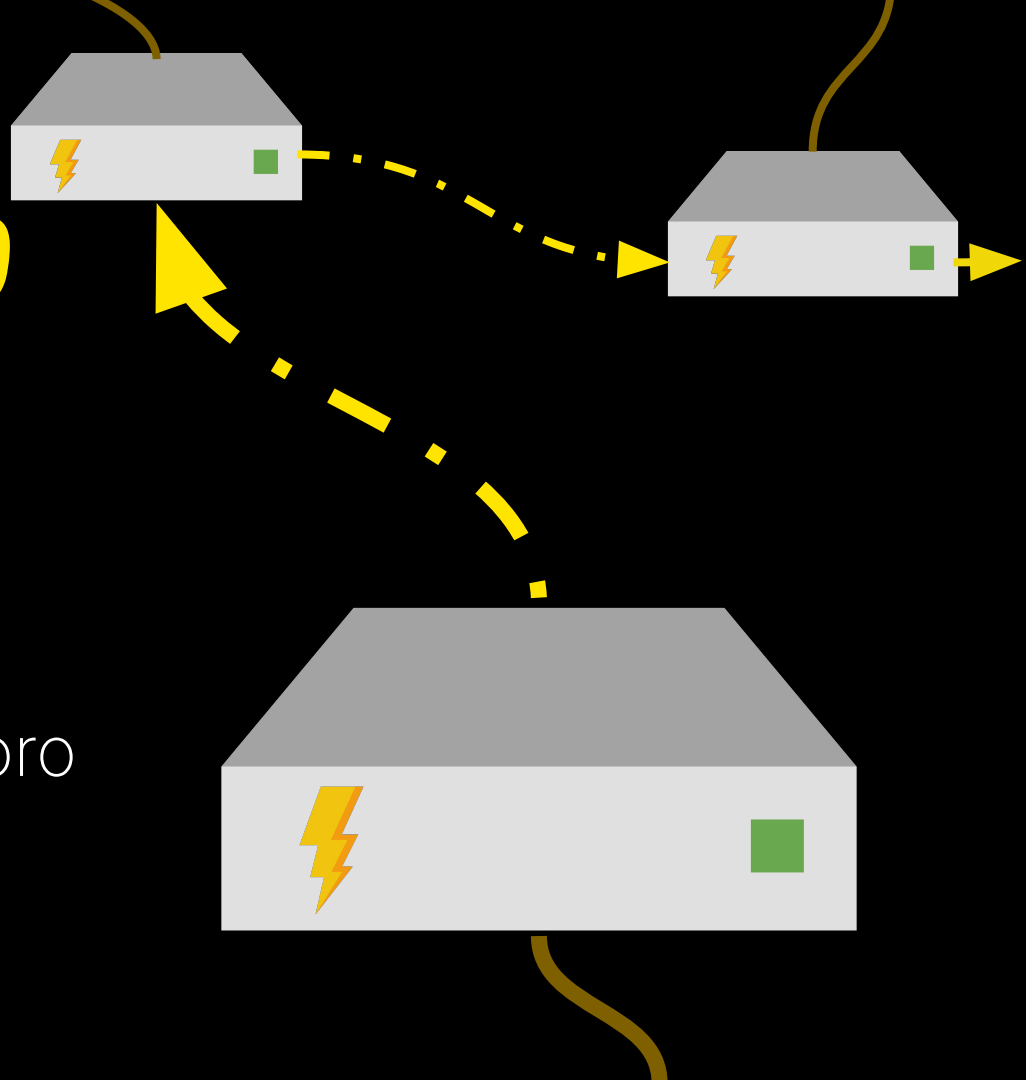
Multi-firma

Un canale di pagamento richiede le **firme di entrambi i partecipanti** (2 di 2) per l'apertura e la chiusura finale sulla *timechain*.



Instradamento dei pagamenti

I pagamenti Lightning avvengono off-chain, pertanto devono essere **inoltrati** (*instradati*) alla loro destinazione finale.



Wallet Lightning

Un wallet Lightning è **sempre online**. Pertanto non dovrebbe essere usato per grandi somme. Carica sul tuo wallet LN solo le somme che intendi spendere.

@anilsaidso

Traduzione a cura di @loop_btc

NOSTR

Fondamenti

@anilsaidso

N.O.S.T.R.

Notes and Other Stuff Transmitted by Relays

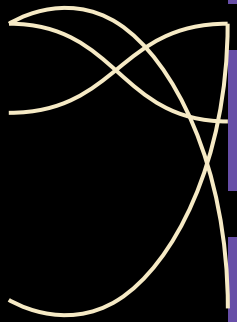
(Note e altre informazioni trasmesse da ripetitori)

Un **protocollo aperto** per reti di comunicazione resistenti alla censura creato da @fiatjaf

Traduzione a cura di @loop_btc

@anilsaidso

IN COSA CONSISTE NOSTR



- Utenti
- Eventi
- Ripetitori (Relays)
- Clients

Utenti

Analogamente a Bitcoin, NOSTR è **permissionless**.

Per utilizzare il protocollo, ogni utente genera una coppia di chiavi composta da una **chiave pubblica** e **una chiave privata.**

Chiave pubblica

Come un nome utente, è tramite essa che gli altri utenti ti trovano.

Chiave privata

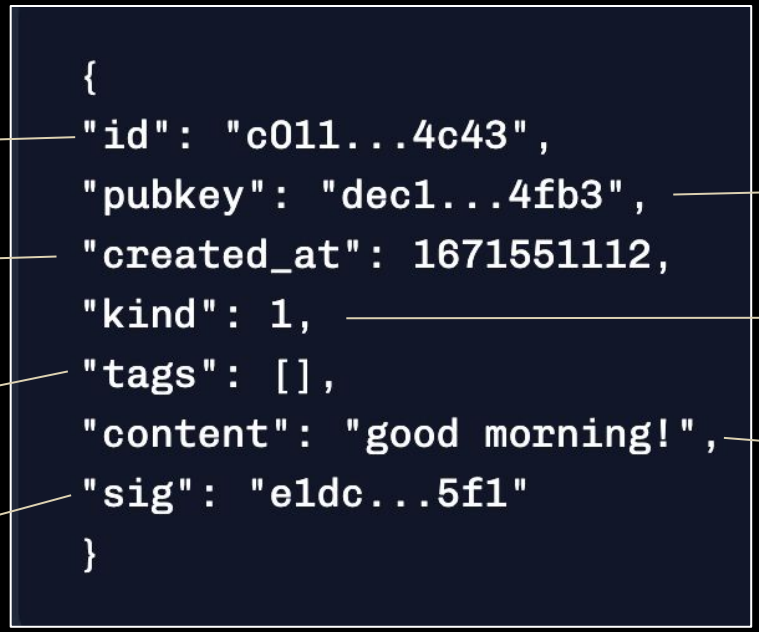
Come una password, è utilizzata per firmare i messaggi e provarne l'autenticità
NON CONDIVIDERLA!

Eventi

Nostr è un protocollo per **confezionare** dei semplici oggetti testuali: i cosiddetti *events*.


```
{
"id": "c011...4c43",
"pubkey": "dec1...4fb3",
"created_at": 1671551112,
"kind": 1,
"tags": [],
"content": "good morning!",
"sig": "e1dc...5f1"
}
```

Anatomia di un Evento



Identificatore univoco dell'evento

Timestamp

Tag
(ad es. indica che questa è una risposta al post XYZ)

Prova di autenticità
(firmato con la chiave privata)

Utente

Tipo di evento *(ad es. nota testuale, messaggio criptato, ecc.)*

Messaggio

💻 Relays

Pubblicare un contenuto non vuol dire renderlo disponibile a tutti gli utenti o inviarlo ad un destinatario in particolare (P2P).

Lo si invia ad un **relay (ripetitore)**, dove può essere letto da tutti gli altri utenti collegati al medesimo server.

I relay possono essere pubblici/privati, liberi/a pagamento o dedicati ad app specifiche.

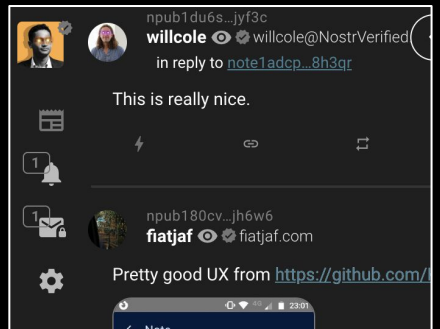
Client

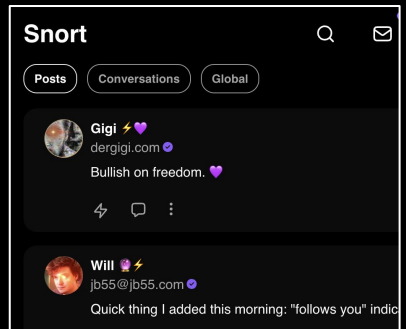
Gli utenti interagiscono con il protocollo NOSTR attraverso un *client*.

Puoi usare qualunque client desideri o persino creare il tuo.

Mobile

Web *(browser)*

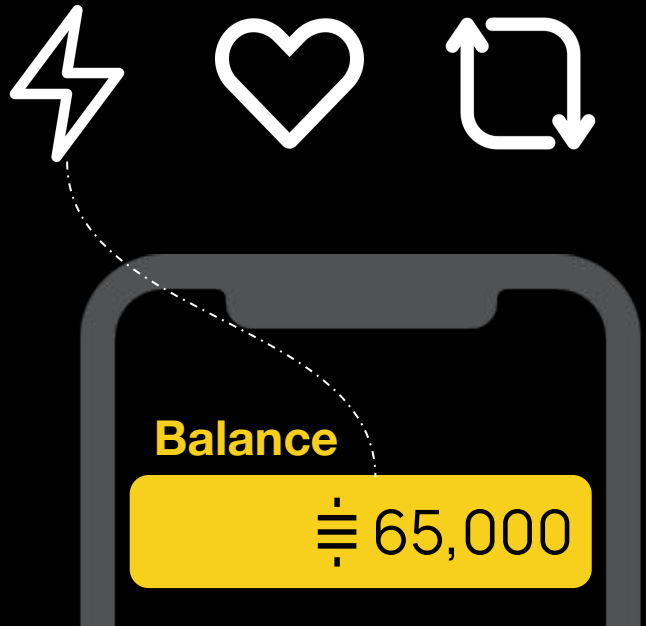




Zaps

Essendo un protocollo aperto, NOSTR dialoga con *altri* protocolli aperti come Lightning Network.

Utilizzando un client compatibile, gli utenti possono mostrare il loro apprezzamento per un contenuto lasciando una mancia in satoshi (bitcoin): ovvero tramite uno *zap*.



Anil

@anilsaidso