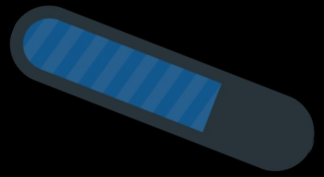
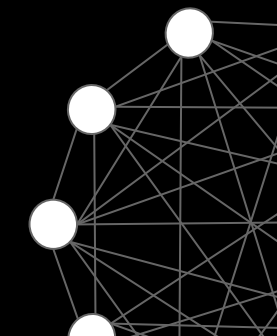
₿6.15

@anilsaidso

Bitcoin

Terminology

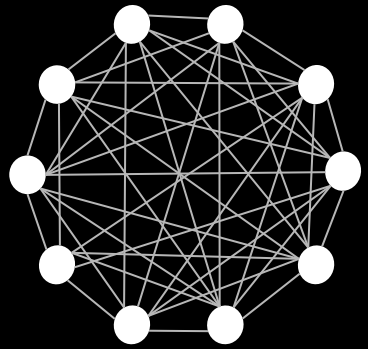


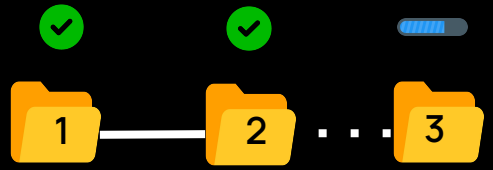


Contents

- Bitcoin
- Lightning Network
- N.O.S.T.R.

₿6.15





bitcoin

money

the network

connected nodes

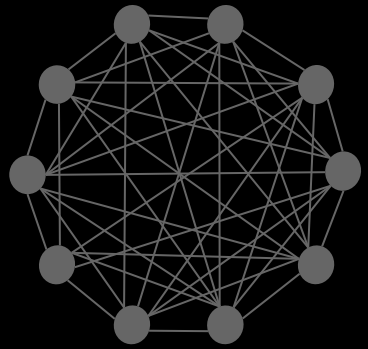
the blockchain

linked record of verified tx's

₿6.15

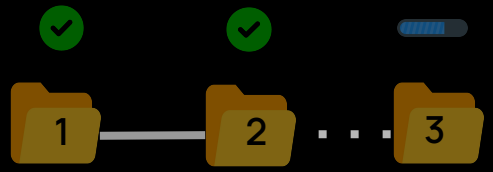
bitcoin

money



the network

connected nodes



the blockchain

linked record of verified tx's

bitcoin

unit of
account

native to the
bitcoin blockchain

@anilsaidso

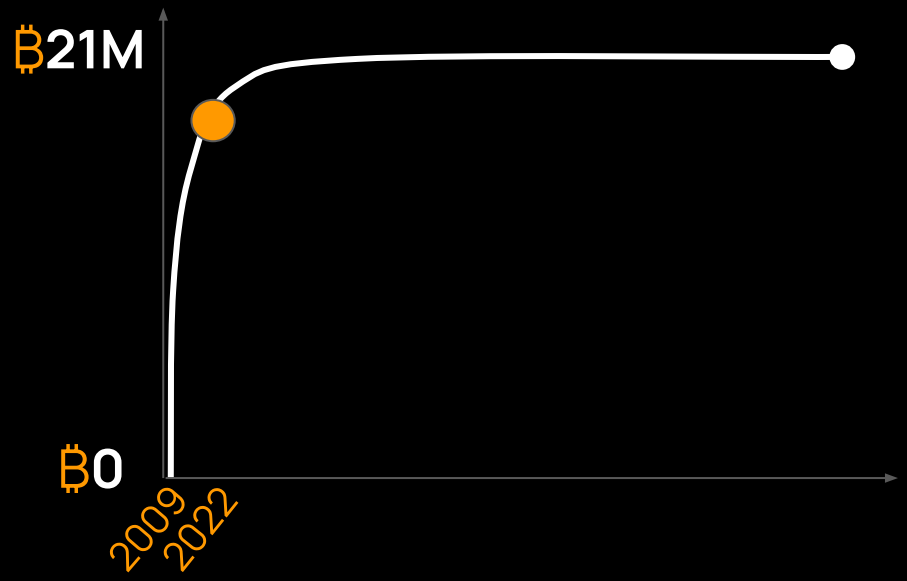
satoshi

A bitcoin is divisible into 100 million smaller units called satoshis (or *sats*)

₿0 ₿21M

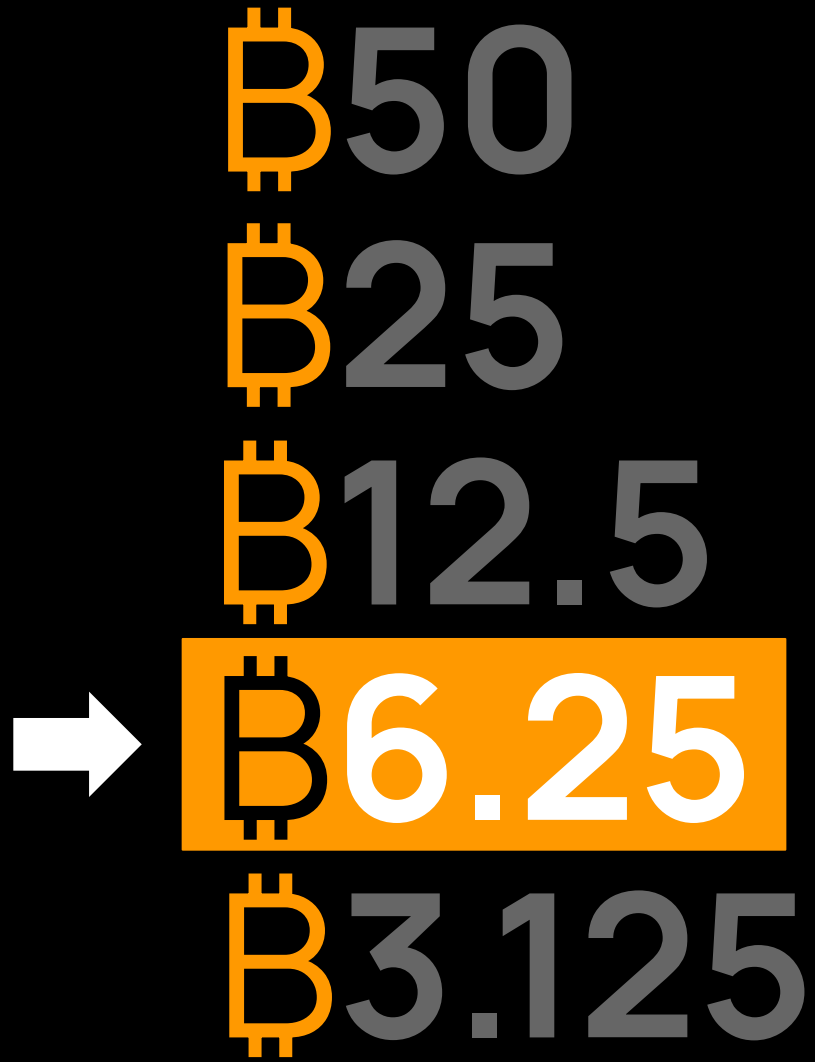
terminal supply

The maximum amount of bitcoin that will ever exist once all has been mined



supply schedule

pre-programmed timetable for issuance of new bitcoin



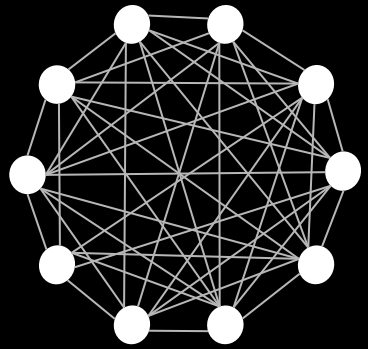
halving

every 210,000 blocks (~4yrs), the rate of new bitcoin issued per block is reduced by 50%

₿6.15

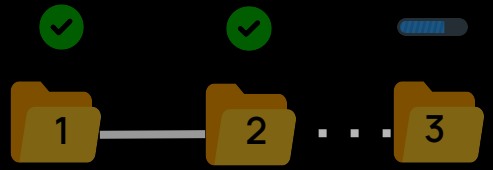
bitcoin

money



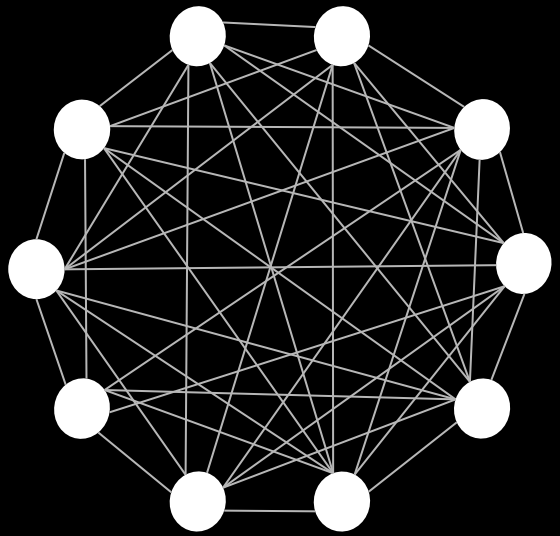
the network

connected nodes



the blockchain

linked record of verified tx's

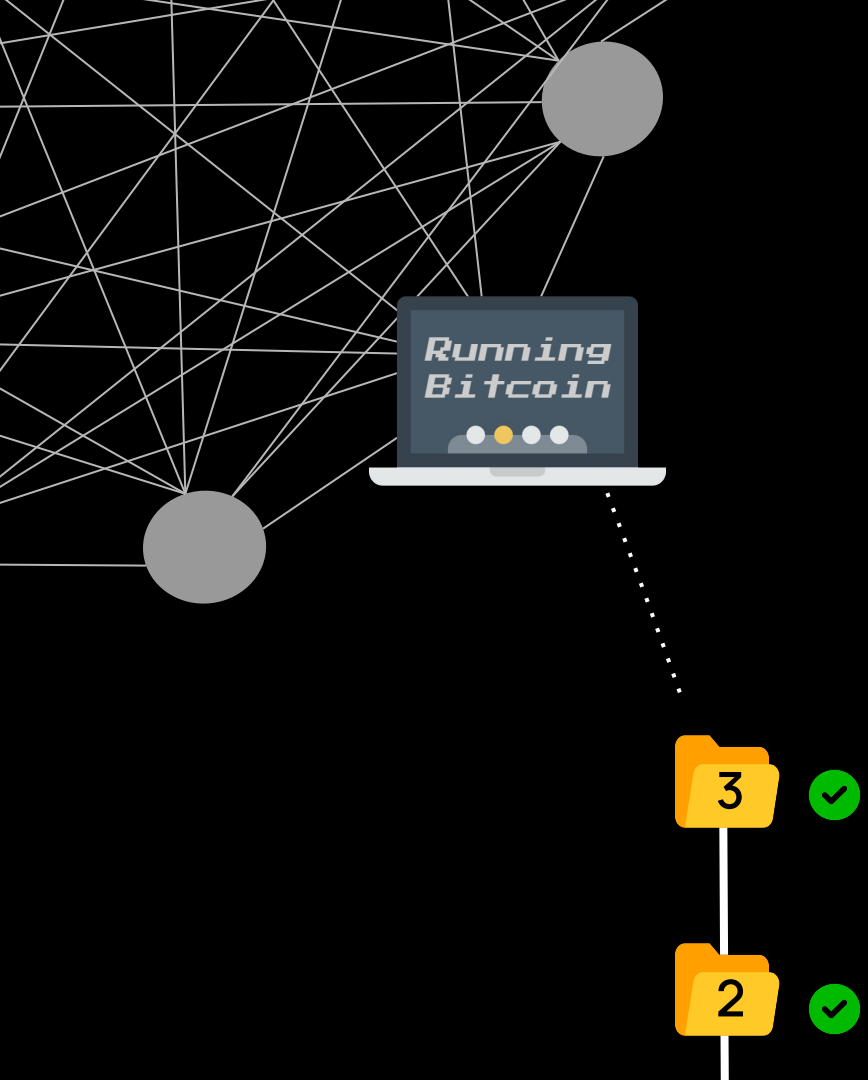


bitcoin's network

connected nodes following a common set of rules

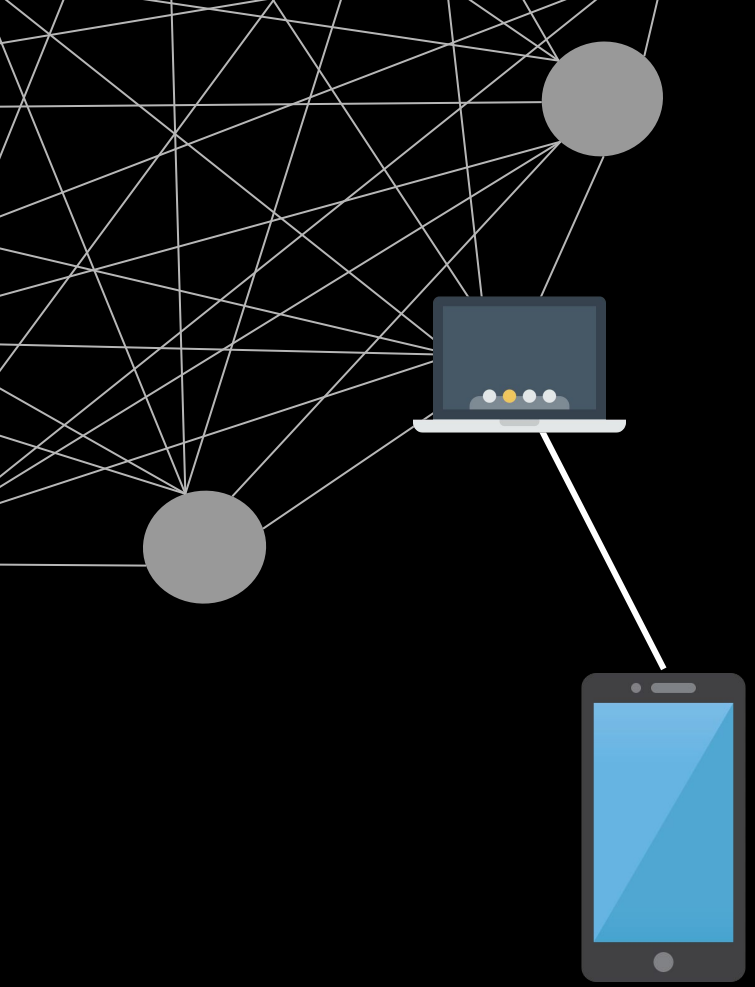
bitcoin software

open-source software that codifies the ruleset



full node

- runs bitcoin software
- maintains a complete copy of the blockchain
- enforces the network's rules

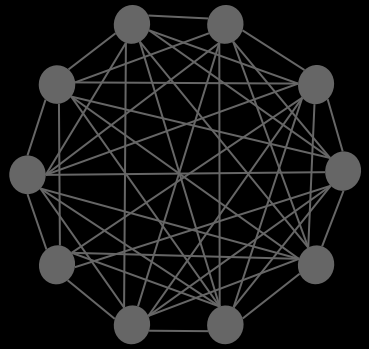


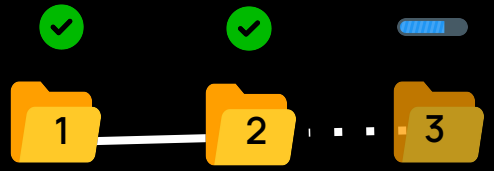
light client

connects to a full node to interact with the network

stores only partial records to save on disk space

₿6.15





bitcoin

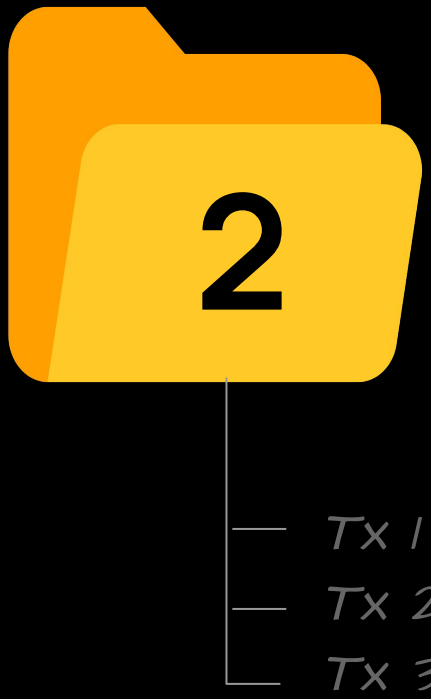
money

the network

connected nodes

the blockchain

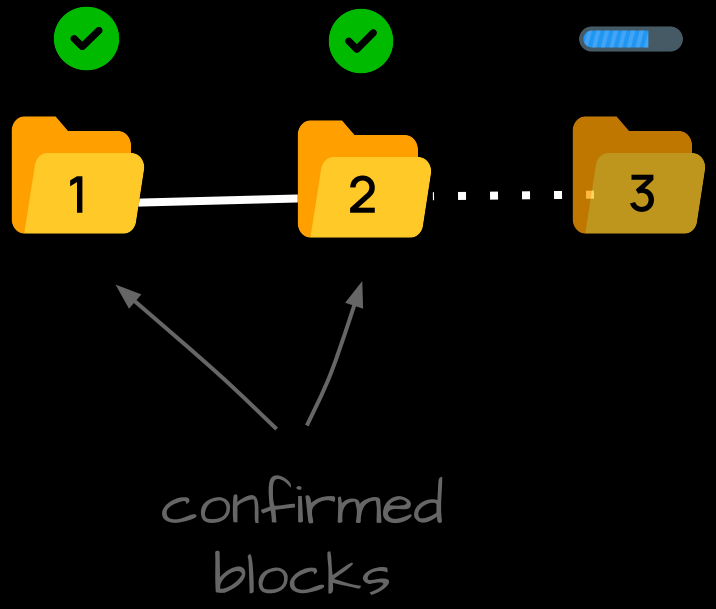
linked record of verified tx's



block

time-stamped
batch of confirmed
transactions

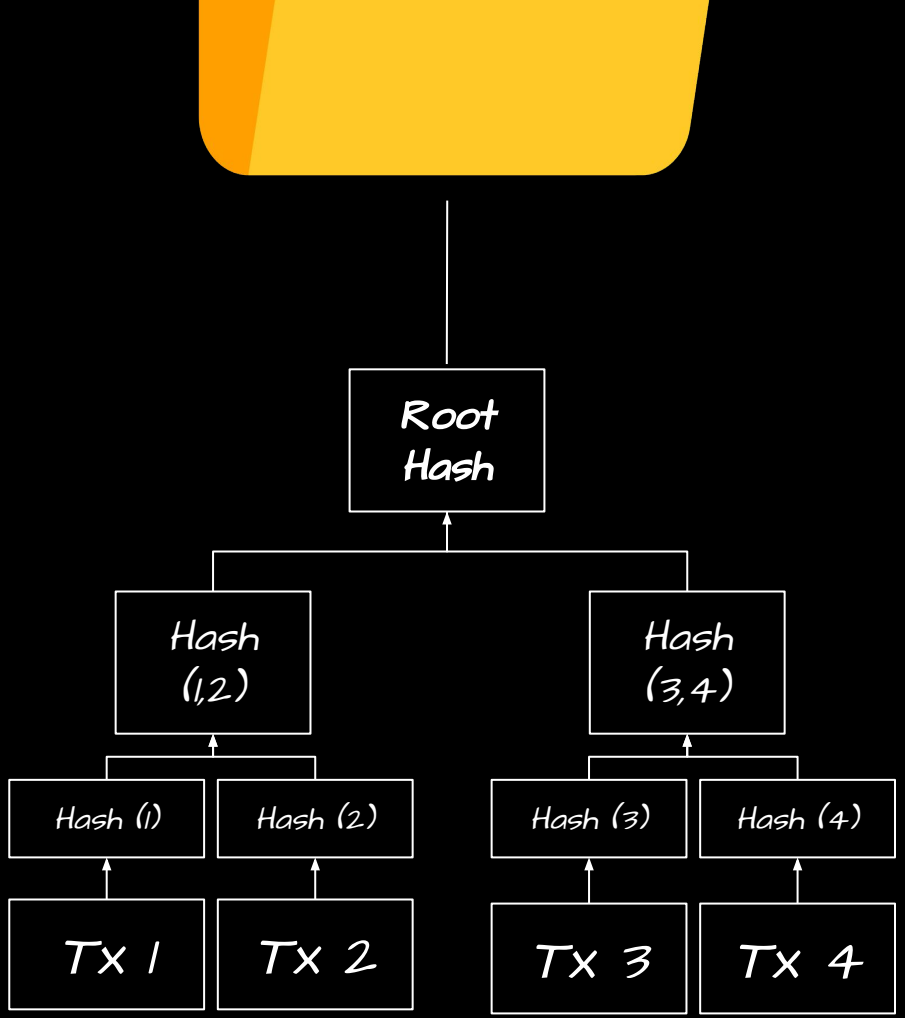
every 10 minutes on avg.



bitcoin's blockchain

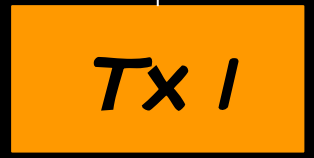
sequentially-linked blocks

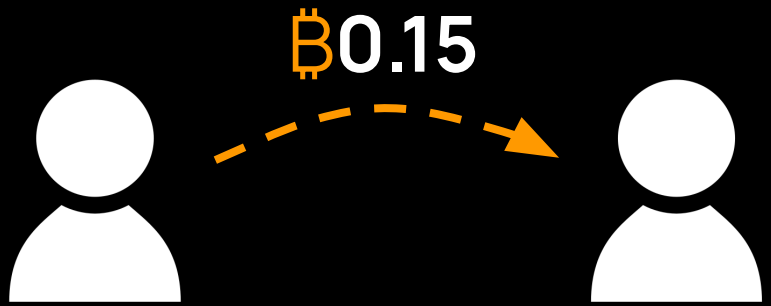
historical record of all confirmed transactions



Merkle tree

data structure that helps reduce storage space and easily prove transaction validity



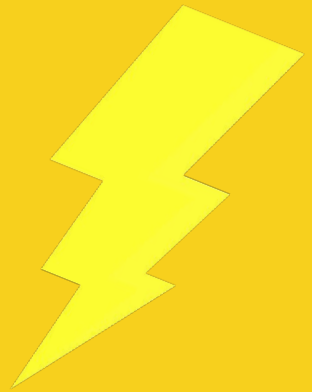


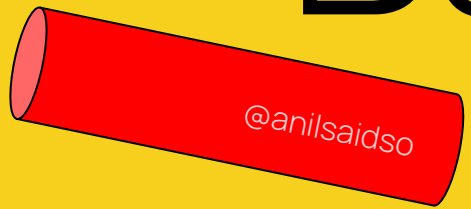
transaction

transfer of ownership of bitcoin between network participants

cryptographically signed by the sender

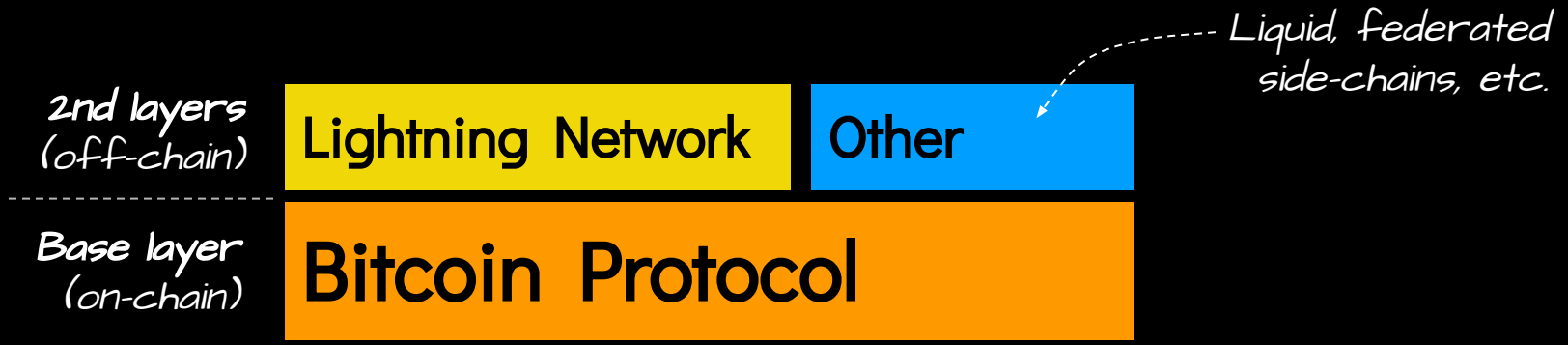
Lightning Network Basics





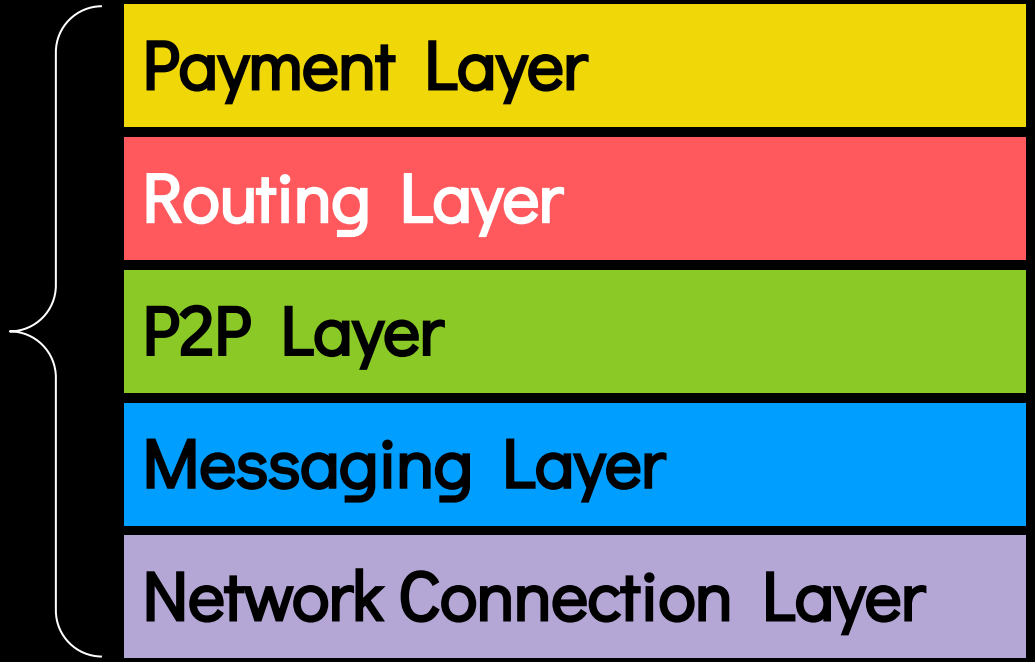
Lightning Network

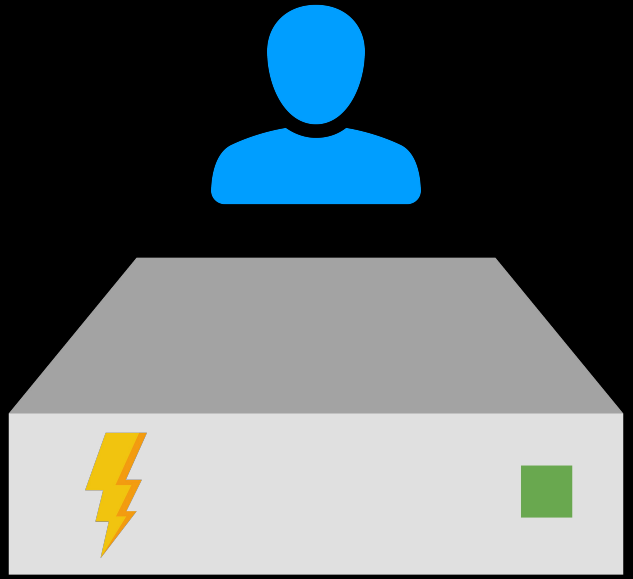
Protocol enabling scalability via instant off-chain payments.



Lightning Network

The LN protocol suite is comprised of **five layers**



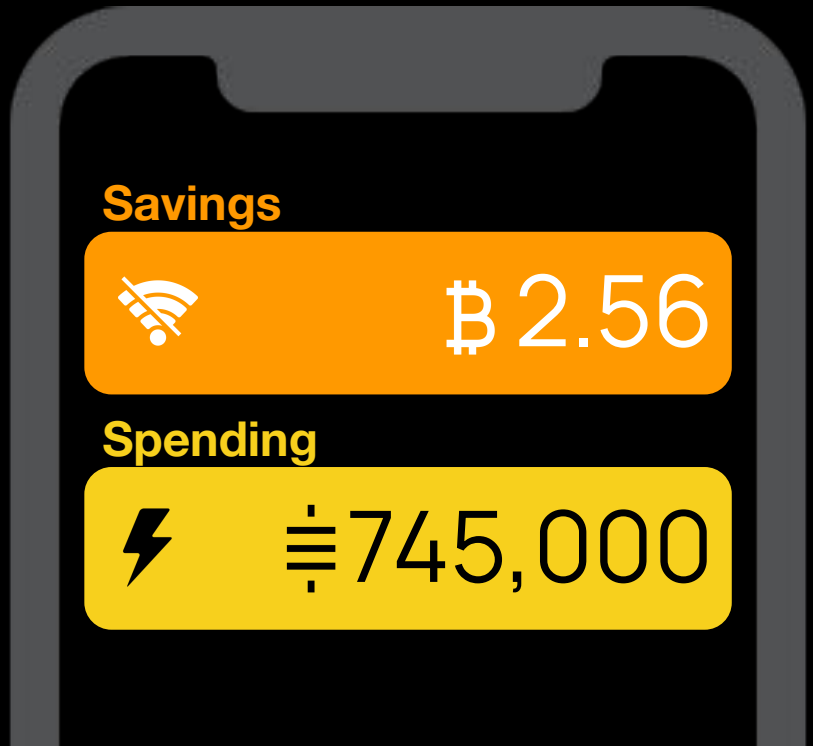


Lightning Node

Hardware that runs specific software to connect to (and interact with) the Lightning Network.

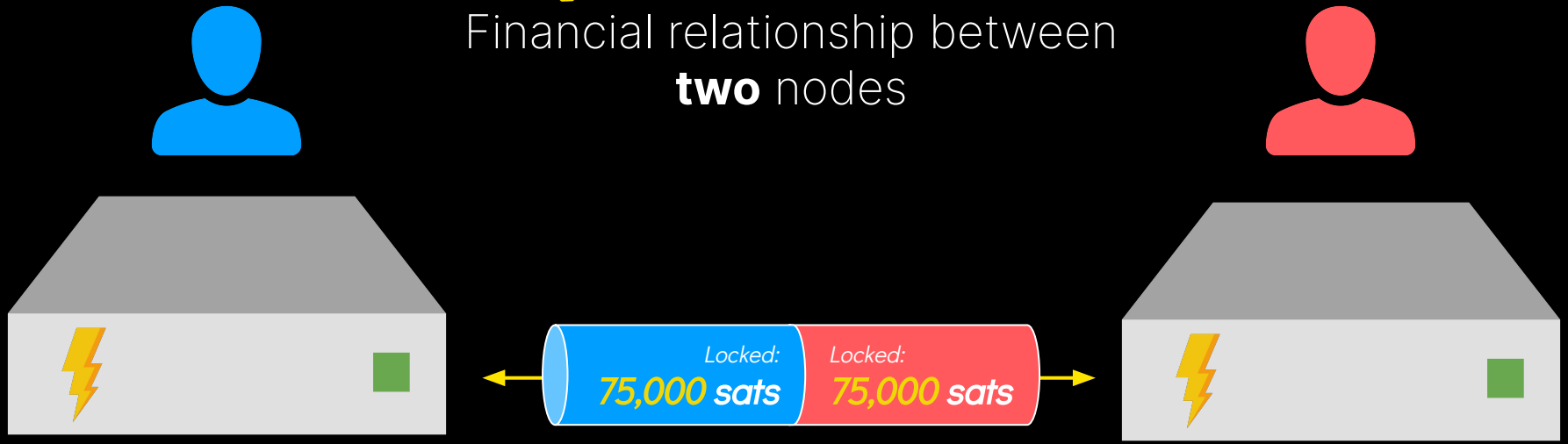
Lightning Wallet

A lightning wallet is **always online**. It should not be used to store large amounts.



Payment Channel

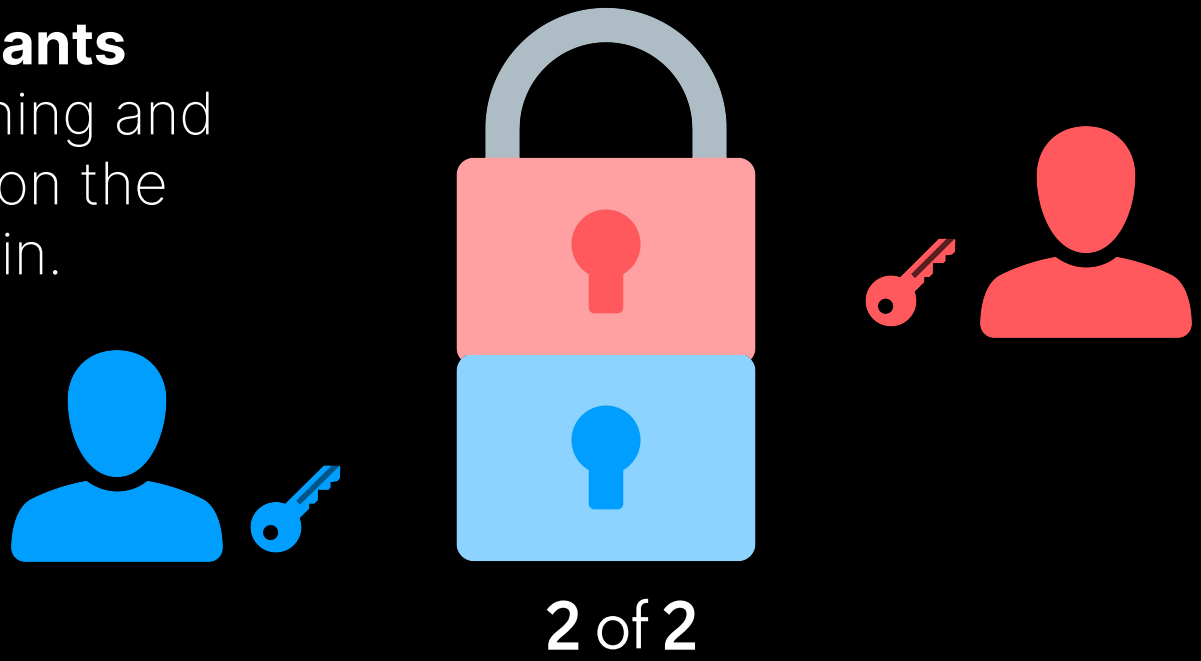
Financial relationship between
two nodes



Total Channel Capacity:
150,000 sats

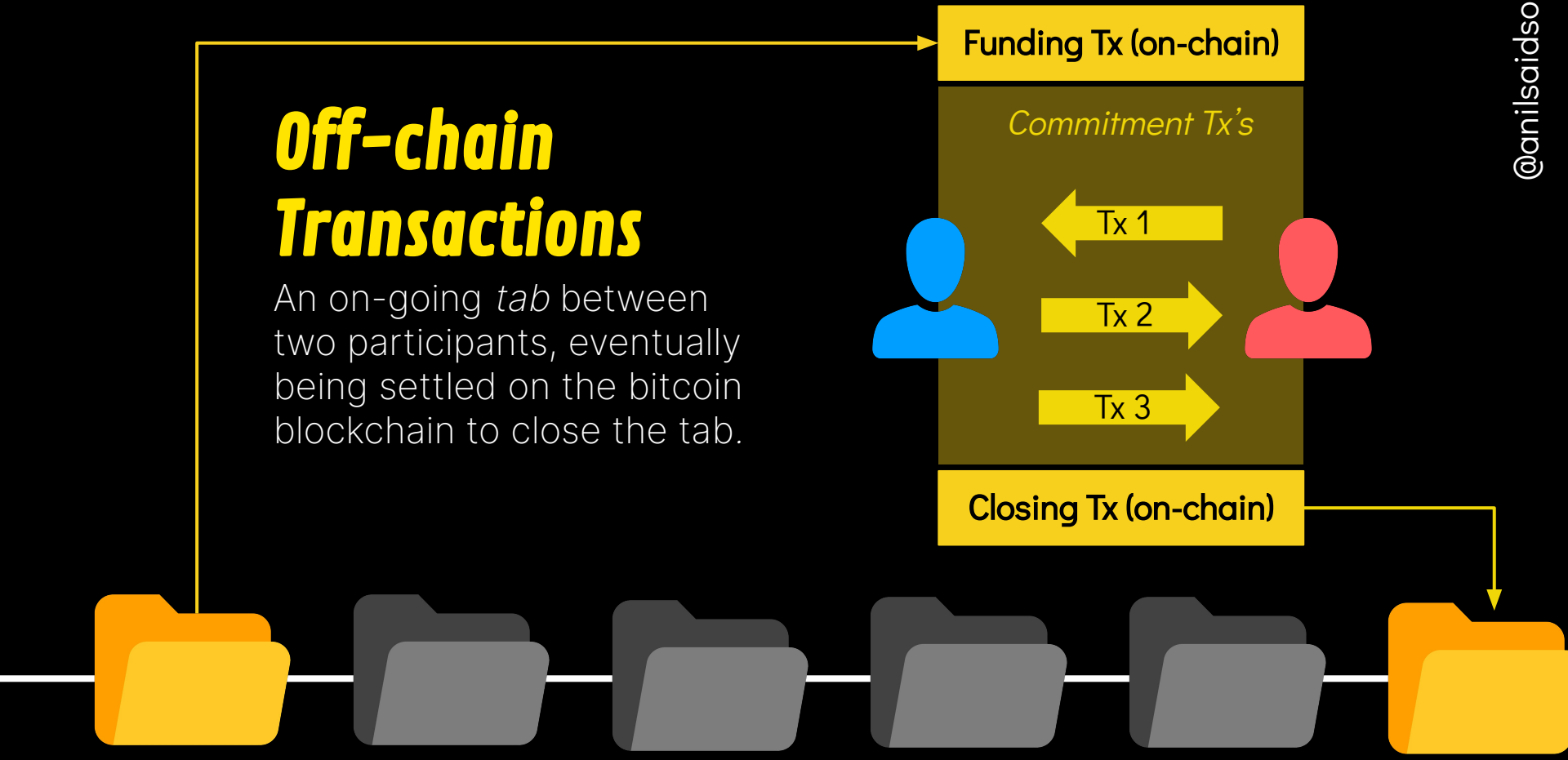
Multisignature

A payment channel requires the **signatures of both participants** (2-of-2) for opening and final settlement on the bitcoin blockchain.



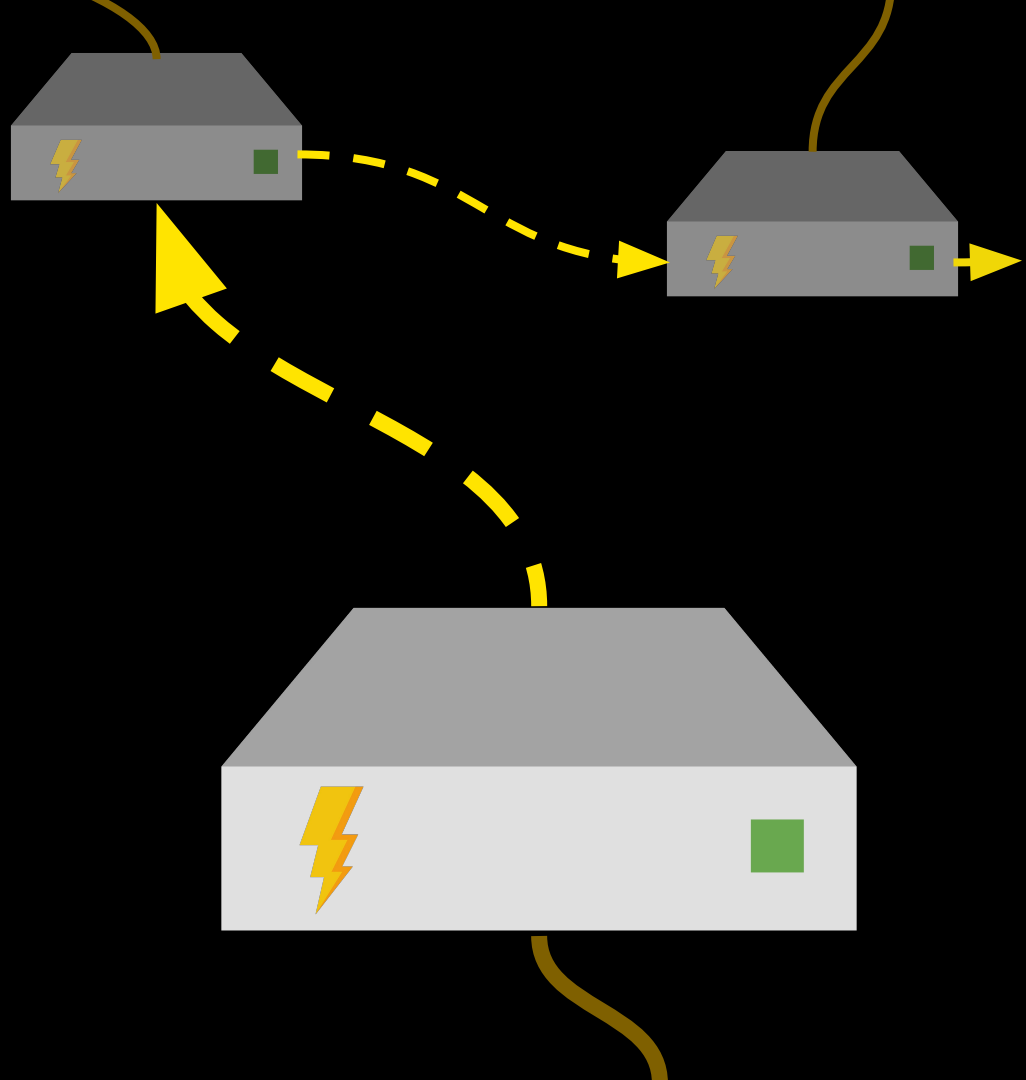
Off-chain Transactions

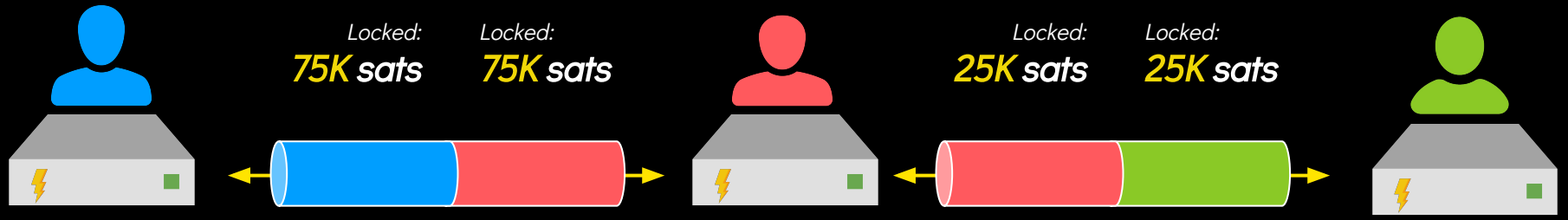
An on-going *tab* between two participants, eventually being settled on the bitcoin blockchain to close the tab.



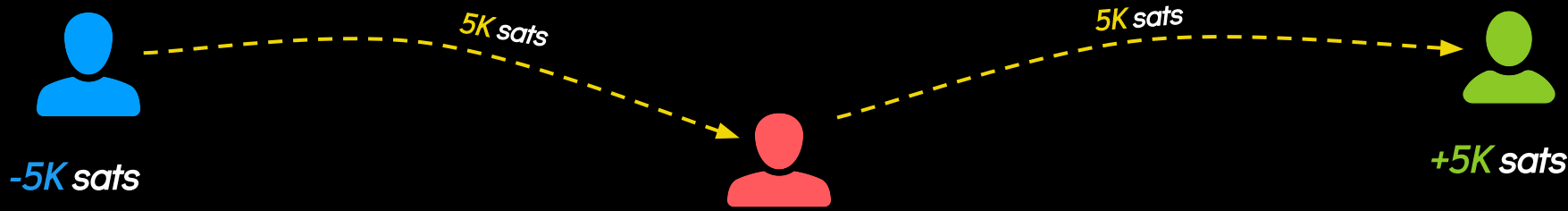
Payment Routing

Lightning payments between non-channel partners must be forwarded (*routed*) to their final destination.




Locked:
75K sats
Locked:
75K sats
Locked:
25K sats
Locked:
25K sats


5K sats


5K sats
5K sats
-5K sats
+5K sats

@anilsaidso

NOSTR

Basics

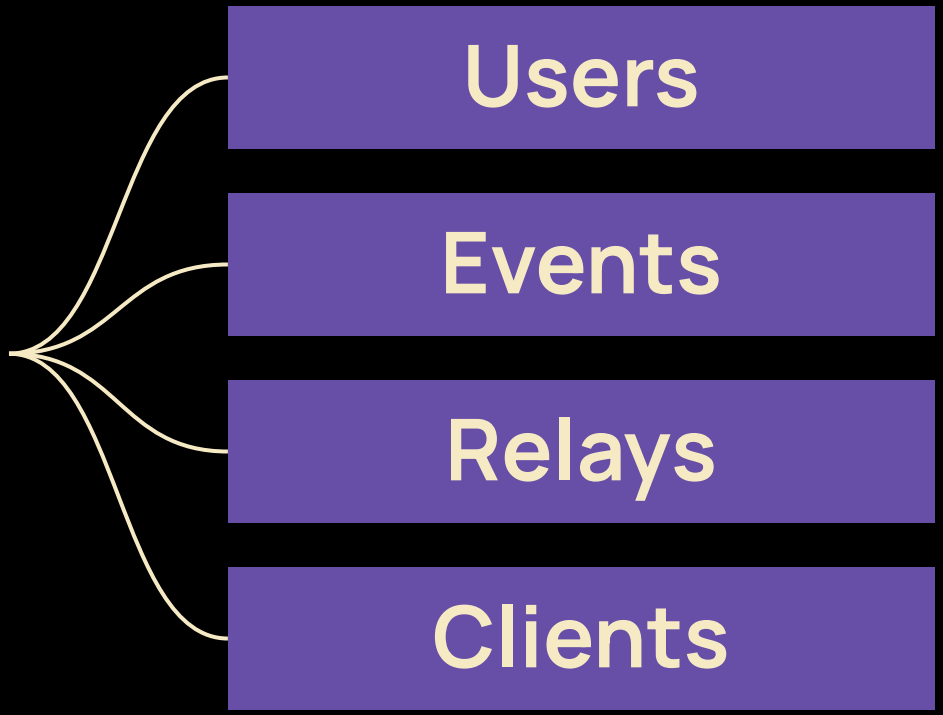
@anilsaidso

N.O.S.T.R.

Notes and Other Stuff Transmitted by Relays

An **open protocol** for censorship-resistant communication networks created by @fiatjaf

WHAT MAKES UP NOSTR



Users

Similar to the bitcoin protocol, nostr is **permissionless**.

To use the protocol a user generates a key pair:
public key & **private key**

Public Key
Like a username, it's how others can find you.

Private Key
Like a password, it's used for signing messages to prove authenticity.
***DO NOT SHARE**

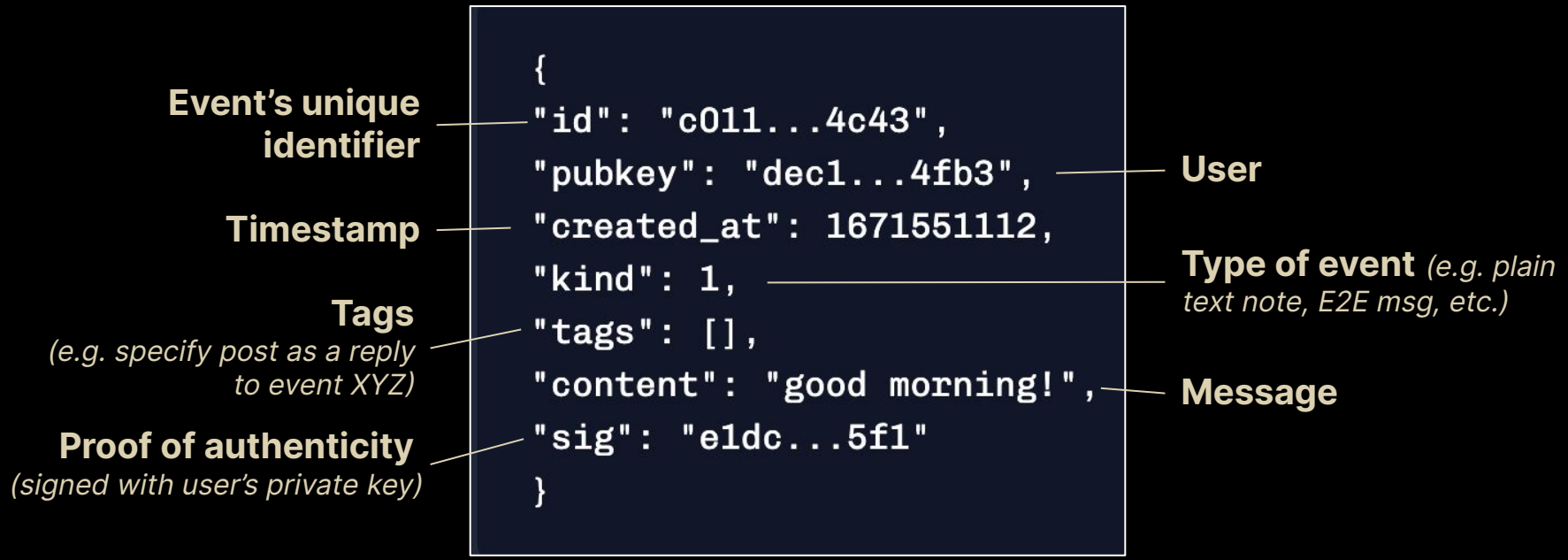
Events

Nostr is a protocol for **packaging** simple text-based objects.

These are called *events*.


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

Anatomy of an Event



💻 Relays

Posting content is not broadcast to all users, nor sent directly to a particular recipient (P2P).

Instead, it is sent to a **relay server**, readable by users also connected to that common relay.

Relays can be public/private, free/paid, or application-specific.

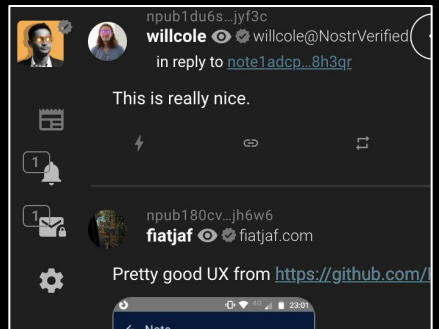
Clients

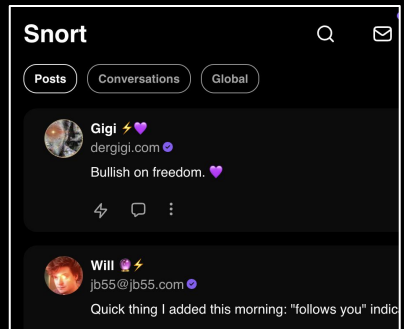
Users interact with the nostr protocol through a *client*.

You can use any client you wish or even build your own.

Mobile

Web *(browser)*

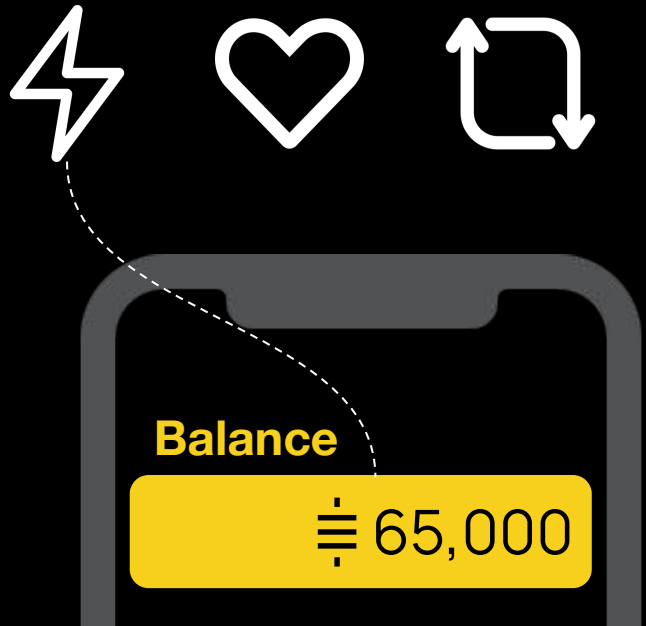




Zaps

As an open protocol, Nostr is interoperable with *other* open protocols such as Lightning.

When using compatible clients, users can show their appreciation for content by *zapping* a post (tipping in bitcoin).



Anil

@anilsaidso