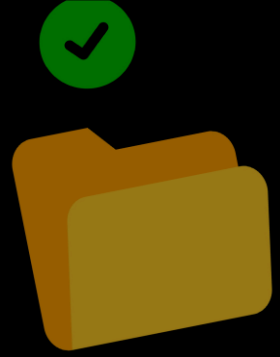
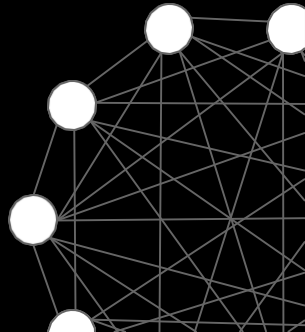
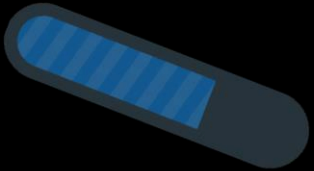


฿3.125



Thuật ngữ **Bitcoin**

@anilsaidso



Nội dung

 **Bitcoin**

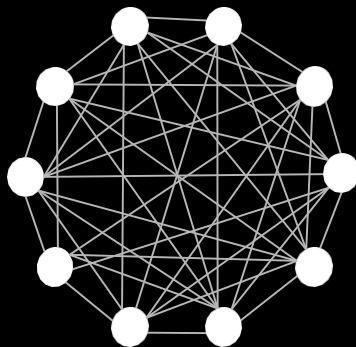
 **Lightning Network**

 **N.O.S.T.R.**

Bitcoin

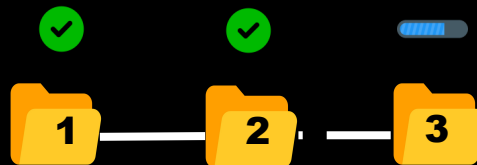
bitcoin

Tiền



mạng lưới

Kết nối các máy chủ



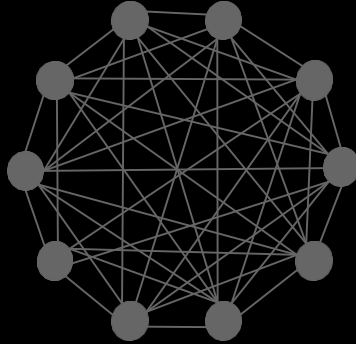
dữ liệu chuỗi

nối các giao dịch đã xác minh

₿3.125

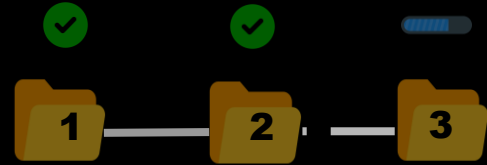
bitcoin

Tiền



mạng lưới

kết nối các máy chủ



dữ liệu chuỗi

nối các giao dịch đã xác minh

trong số
21 Triệu
tổng cung

₿3.125

=12,500,000
satoshis

bitcoin

Đơn vị gốc
của chuỗi dữ liệu Bitcoin



100,000,000
sats

1 BTC

satoshi

Một bitcoin có thể
được chia nhỏ
thành 100 triệu
satoshis (*sats*)

฿0

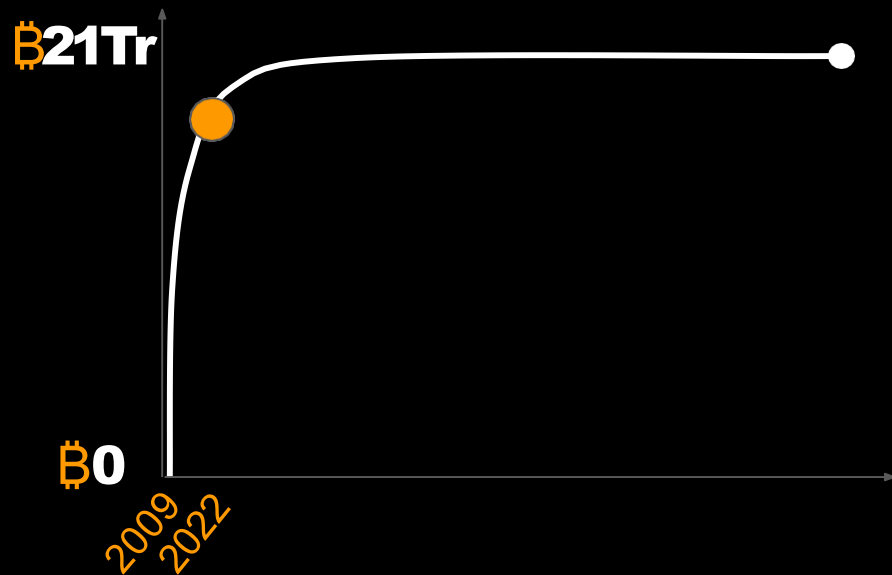


฿21Tr

Nguồn cung phát hành

@anilsaidso

Đây là tổng số
lượng Bitcoin tối đa
sẽ được đào ra và
lưu hành.



lịch cung ứng

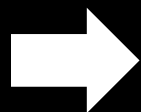
lịch trình
sản xuất bitcoin
được lập trình sẵn.

₿50

₿25

₿12.5

₿6.25



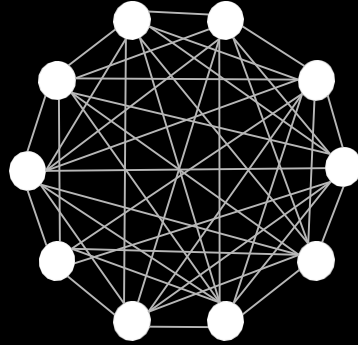
₿3.125

Chia đôi (halving)

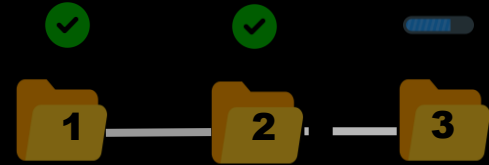
tốc độ sản xuất bitcoin mới cho một khối sẽ bị giảm đi 50%, sau mỗi lần đóng gói 210,000 khối dữ liệu (khoảng 4 năm/lần).

₿3.125

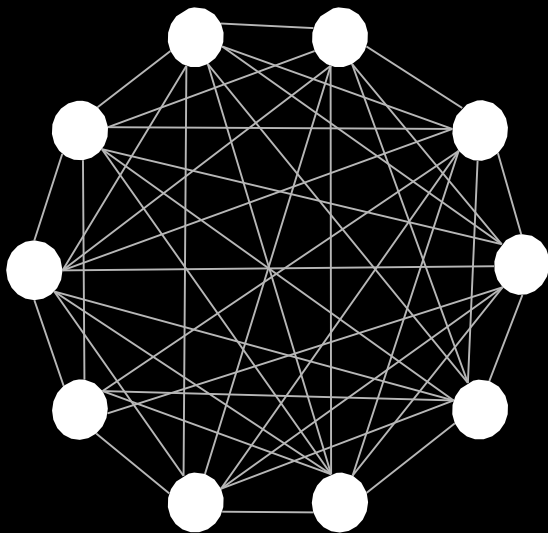
bitcoin
tiền



mạng lưới
Kết nối các máy chủ



dữ liệu chuỗi
nối các giao dịch đã xác minh



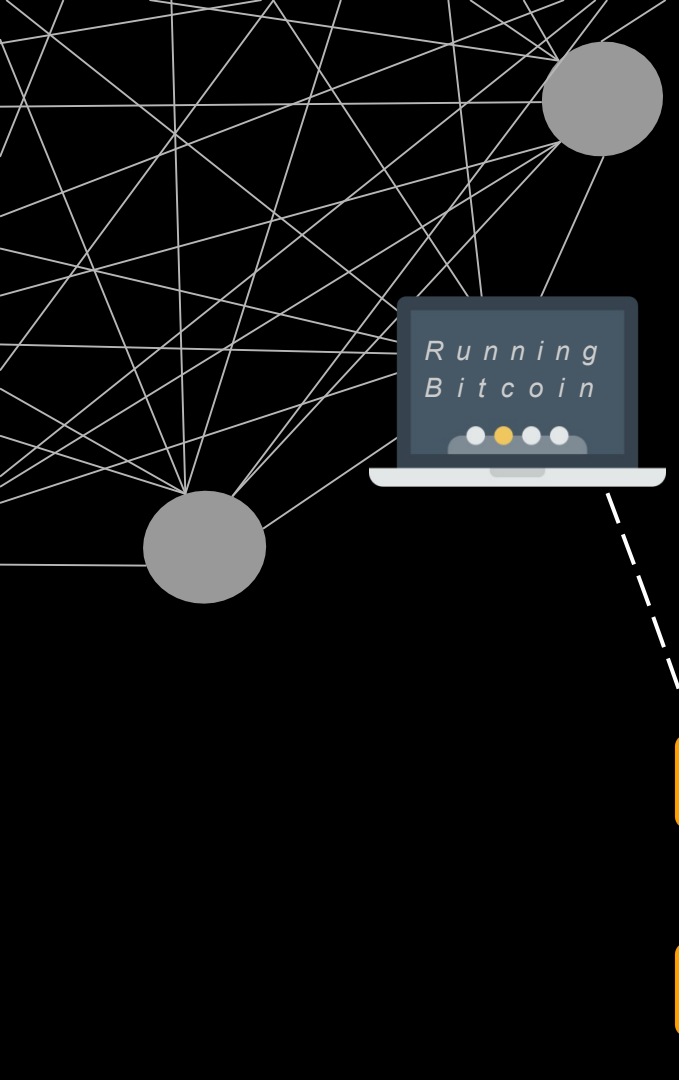
Mạng lưới bitcoin

Tập hợp các máy chủ
được kết nối theo 1
tổ hợp các quy tắc
chung.



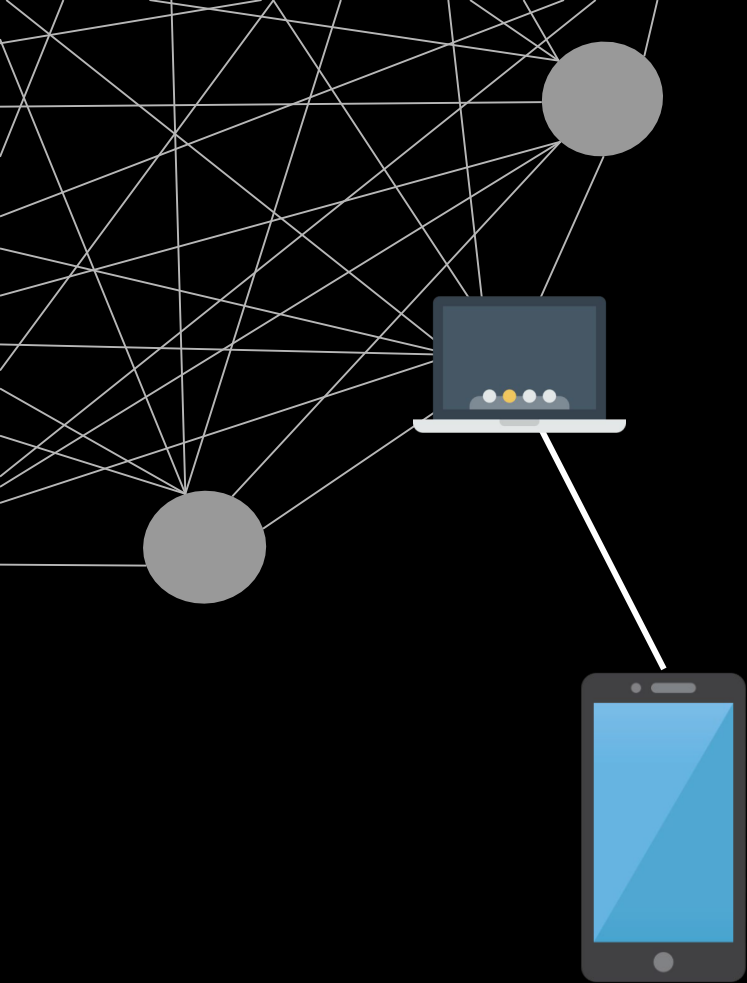
Phần mềm bitcoin

Phần mềm mã
nguồn mở được
viết theo 1 tập hợp
các quy tắc.



Máy chủ

- Chạy phần mềm bitcoin
- Lưu giữ 1 bản sao hoàn chỉnh của chuỗi dữ liệu
- Thực thi các quy tắc của mạng lưới



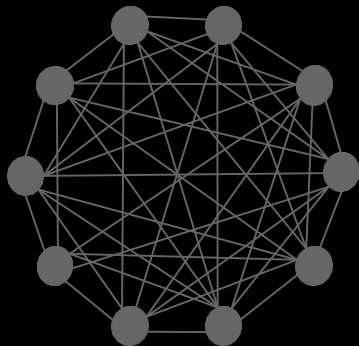
Ứng dụng người dùng

kết nối máy chủ để
tương tác với mạng

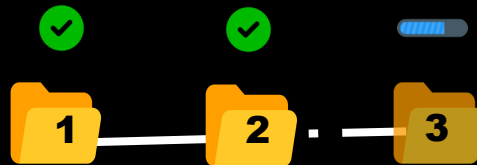
chỉ lưu trữ một phần của
thông tin vào bộ nhớ cứng

Bitcoin

bitcoin
tiền



mạng lưới
kết nối các máy chủ



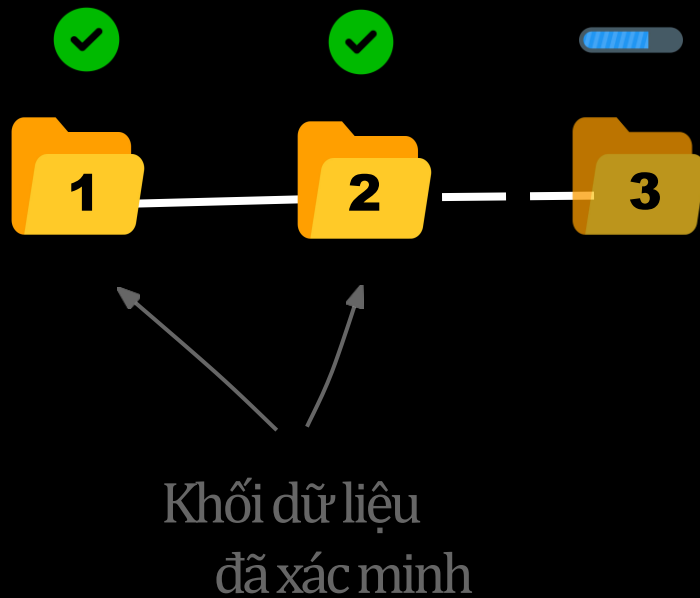
dữ liệu chuỗi
nối các giao dịch đã xác minh



— *Giaodịch 1*
— *Giaodịch 2*
— *Giaodịch 3*

Khối dữ liệu

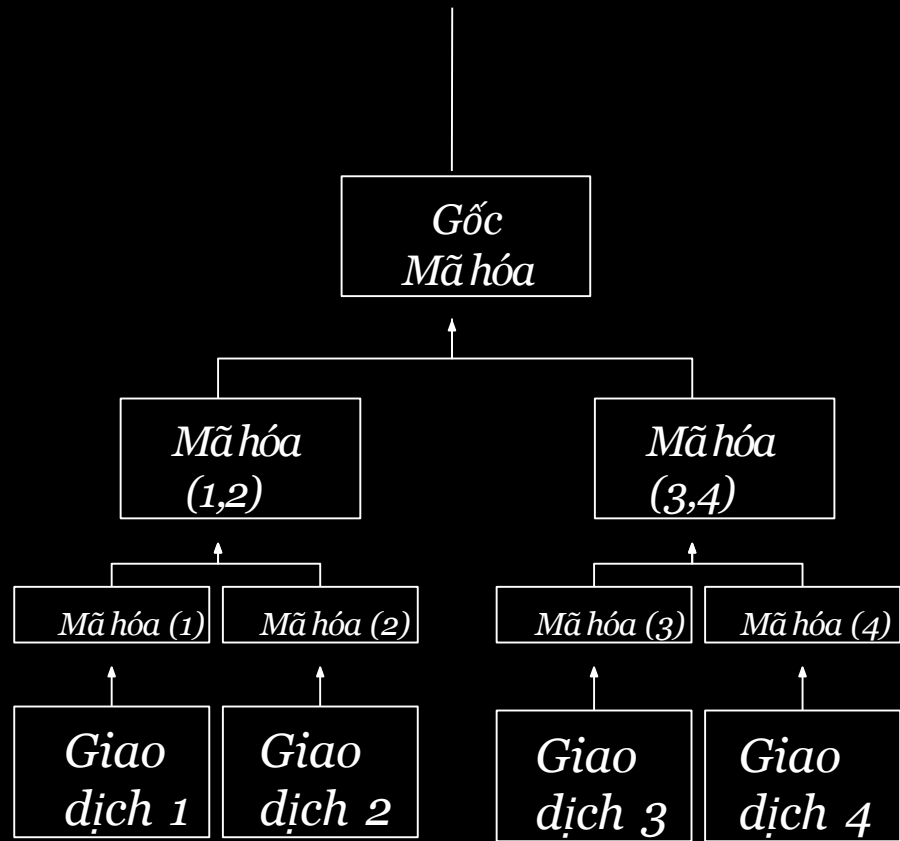
Đóng dấu thời điểm
1 lô giao dịch đã
được xác minh.
trung bình 10 phút/lần.



bitcoin

dữ liệu chuỗi

liên kết các khối dữ liệu
theo trình tự
số cái ghi nhận tất cả các giao
dịch đã được xác nhận trong
lịch sử

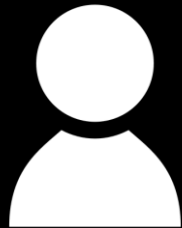


Merkle tree

Cấu trúc dữ liệu tiết kiệm không gian lưu trữ và chứng minh tính hợp lệ của giao dịch dễ dàng.

Mã hóa
(1)

Giao dịch
1



฿0.15

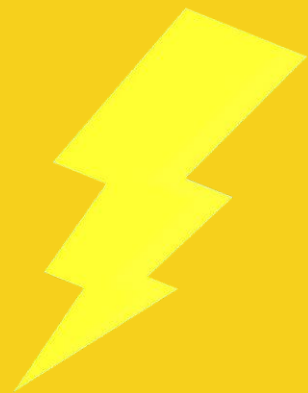


Giao dịch

chuyển đổi chủ sở hữu
bitcoin giữa các thành viên
trong mạng bitcoin
người chuyển sẽ ký mã hóa



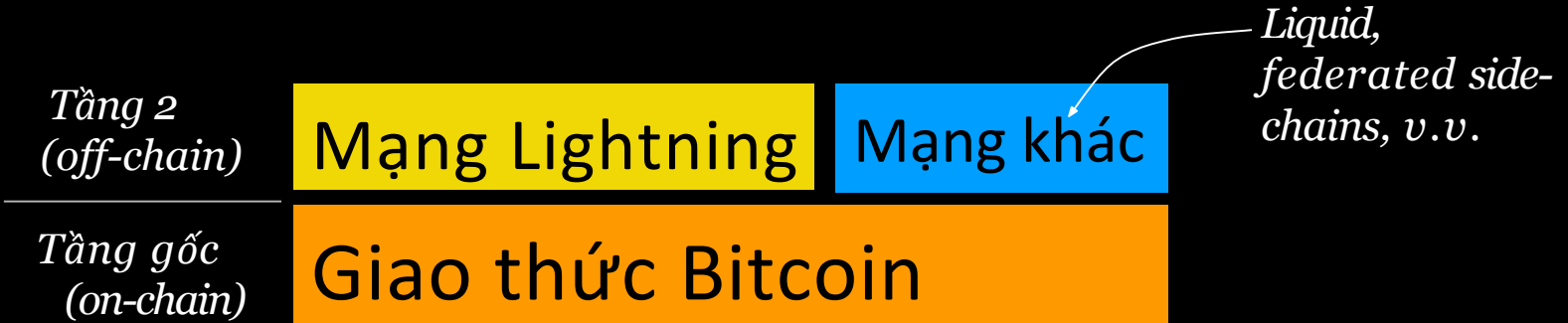
Mạng Lightning Cơ bản



@anilsaidso

Mạng Lightning

Giao thức mở rộng bằng giao dịch ngoại mạng bitcoin.



Mạng

Lightning

Bộ giao thức
lightning bao
gồm **5 tầng**

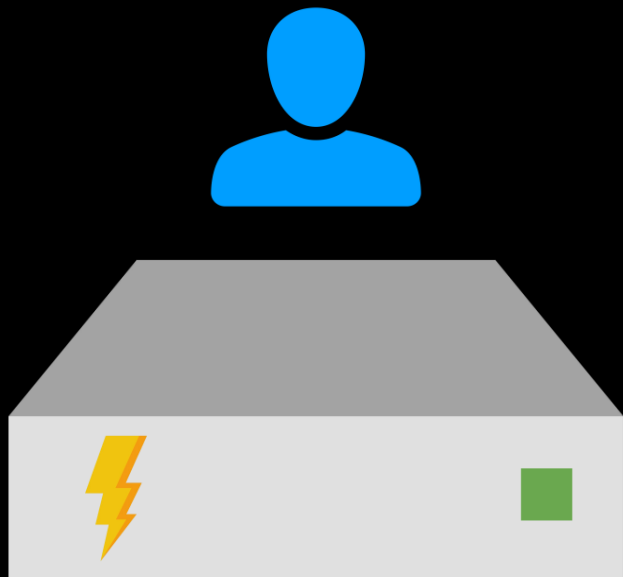
Tầng thanh toán

Tầng định tuyến

Tầng P2P

Tầng tin nhắn

Tầng kết nối mạng



máy chủ *Lightning*

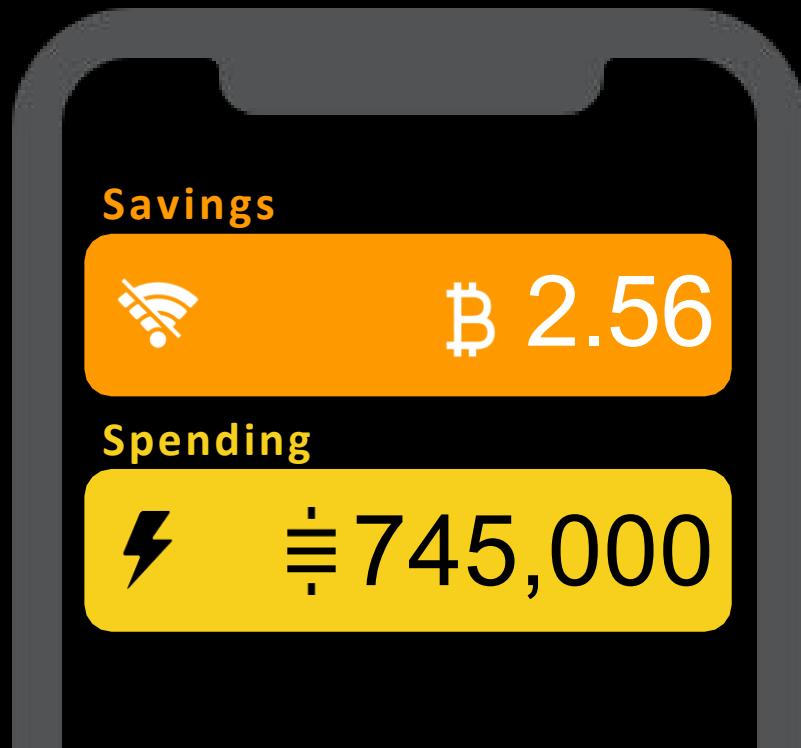
Thiết bị tải và vận hành
phần mềm cụ thể để kết nối
và tương tác với mạng
Lightning.

Ví

Lightning

Ví lightning luôn ở trạng thái kết nối.

* Không nên trữ nhiều bitcoin trong ví này.



Tầng thanh toán

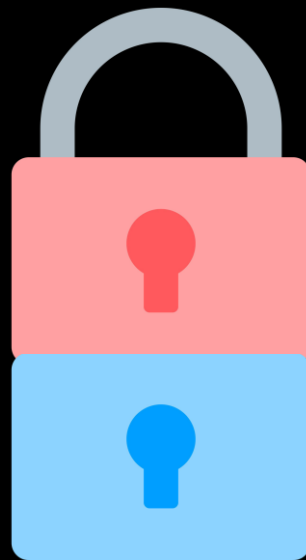
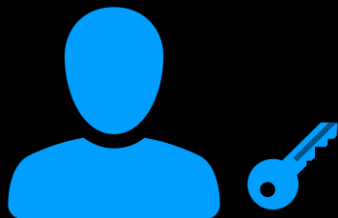
Mỗi liên hệ tài chính
giữa **2** máy chủ



Tổng khả năng thanh toán
của kênh:
150,000 sats

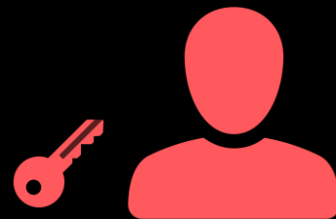
Đa chữ ký

Để mở kênh thanh toán và thực hiện chuyển khoản trên chuỗi dữ liệu Bitcoin cần phải có chữ ký của **2 bên tham gia**.



2 of 2

Số dư:
150,000 sats



Giao dịch ngoại mạng

Một sổ ghi nợ được mở để cập nhật các giao dịch giữa hai bên, sổ dư cuối cùng sẽ được thanh toán trên chuỗi dữ liệu Bitcoin để kết toán và đóng sổ.



Giao dịch 1

Giao dịch 2

Giao dịch 3



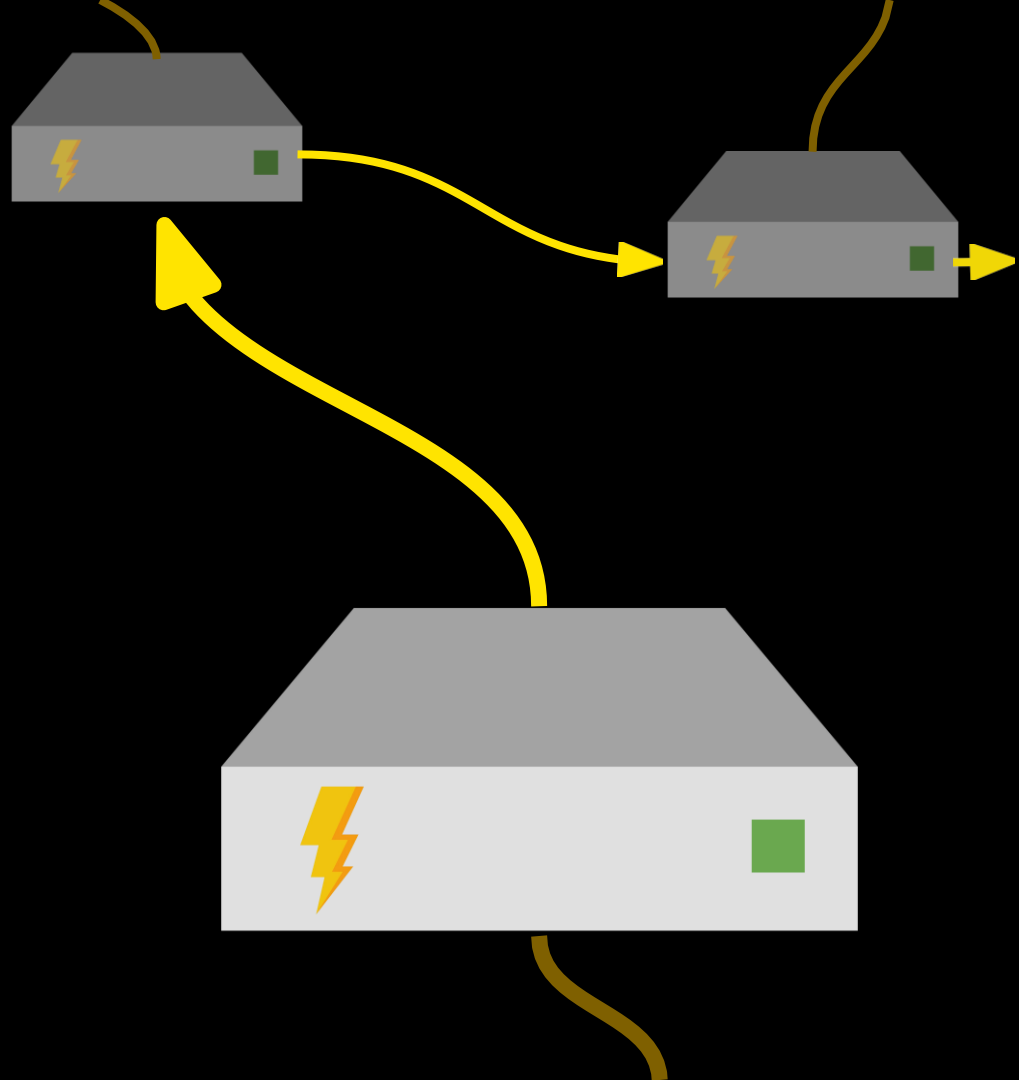
Rút vốn (nội mạng)

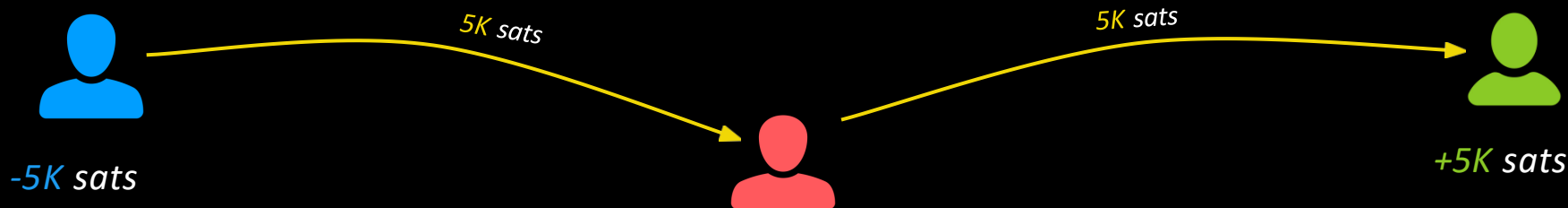
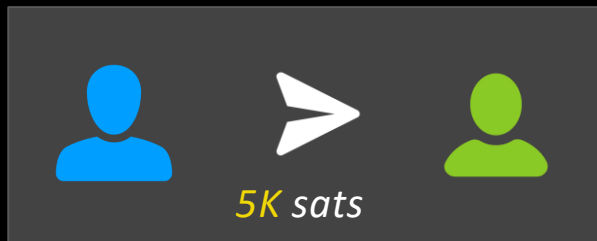
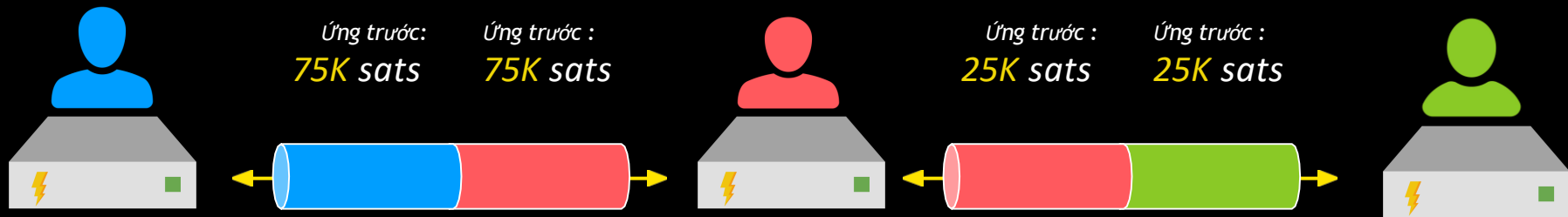
Thực hiện giao dịch

Kết sổ (nội mạng)

Thanh toán định tuyến

Giao dịch chuyển khoản
giữa các bên không cùng
kênh sẽ được chuyển tiếp
qua các kênh trung gian
để đến điểm cuối cùng.







NOSTR

Cơ bản

N.O.S.T.R.

Notes and Other Stuff Transmitted by Relays

Giao thức mở
cho mạng truyền thông tự do
do @fiatjaf sáng lập

THÀNH

PHẦN

NOSTR

Người dùng

Sự kiện

Trạm chuyển tiếp

Ứng dụng cuối



Người dùng

Giống như giao thức bitcoin,
tham gia nostr không cần xin phép.

Để sử dụng giao thức, người
tham gia phải tạo 1 cặp khóa:
khóa chung & **khóa riêng**



Khóa chung

Vai trò giống như tên tài
khoản để mọi người tìm
bạn.

Khóa riêng

Vai trò giống như mật
khẩu, dùng để ký xác
nhận tin nhắn định
danh của bạn.

***BÍ MẬT**

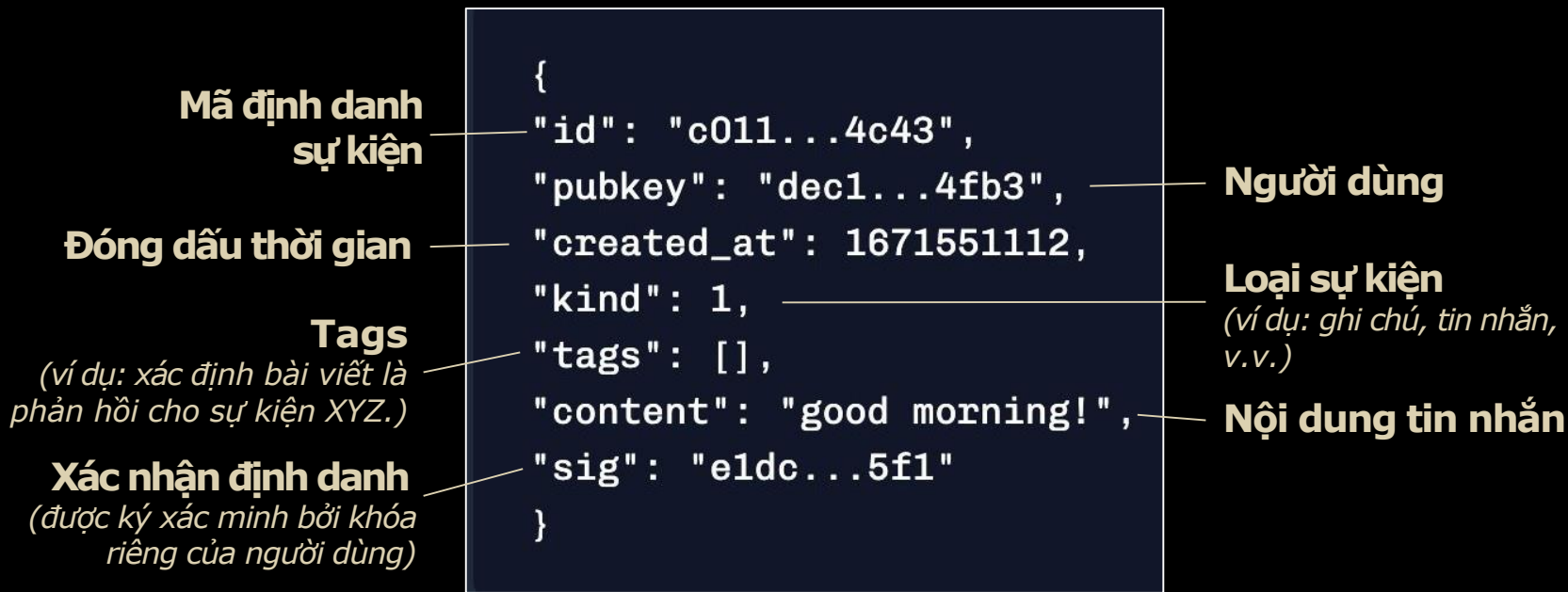
Sự kiện (Events)

Nostr là giao thức để
đóng gói các đối tượng
văn bản đơn giản.

Những đối tượng này gọi là
sự kiện.

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

Thành phần của Sự kiện





Máy chủ trung gian

Nội dung đăng không được gửi trực tiếp đến tất cả người dùng hoặc đến một người nhận cụ thể (P2P).

Nội dung được gửi đến một **máy chủ trung gian**, người dùng có thể đọc được khi kết nối với máy chủ đó.

Máy chủ trung gian có thể là công cộng /tư nhân, miễn phí/thu phí, hoặc cụ thể cho ứng dụng.

(Relays)



Ứng dụng người dùng (Clients)

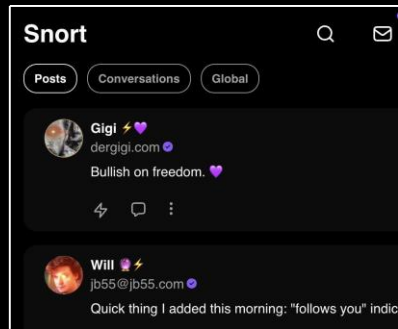
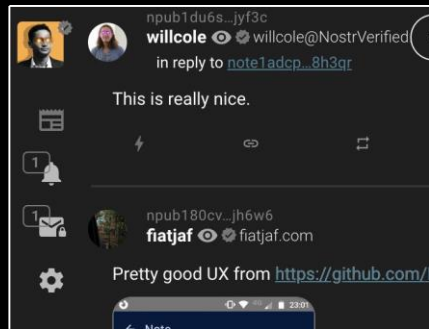
Người dùng tương tác với giao thức nostr thông qua ứng dụng mobile/web.

Có thể sử dụng bất kỳ ứng dụng nào hoặc thậm chí tự tạo ứng dụng riêng của bạn.

Mobile



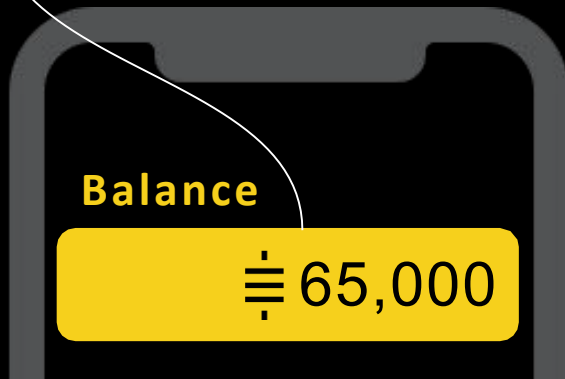
Web (browser)



Ủng hộ (Zaps)

Vì là 1 giao thức mở, Nostr có thể tương tác với ***nhieu*** giao thức mở khác như Lightning.

Khi sử dụng các ứng dụng tương thích, người dùng có thể ủng hộ và thể hiện sự đánh giá của họ đối với nội dung đăng tải bằng cách tặng tiền (zapping) một bài đăng.





Anil

@anilsaidso 

Biên dịch:

@AnhContact 