Chương 3

Bitcoin

Mục tiêu bài học

- Hiểu được lịch sử ra đời và tác động của Bitcoin
- Biết các cách lưu trữ và giao dịch Bitcoin
- Hiểu được hạn chế và đề xu hướng cải tiến

Nội dung bài học

- Sự ra đời của Bitcoin
- Khối và mạng Bitcoin
- Lưu trữ cục bộ
- Lưu trữ nóng và lưu trữ lạnh
- Ví trực tuyến và giao dịch
- Cơ chế hoạt động của Bitcoin và đào coin
- Hạn chế và cải tiến

Sự ra đời của Bitcoin

Hoàn cảnh ra đời

- **Khủng hoảng tài chính toàn cầu 2008**:
  - Niềm tin vào các tổ chức tài chính bị suy giảm nghiêm trọng
  - Hệ thống tài chính tập trung bộc lộ nhiều điểm yếu như lạm dụng quyền lực, thiếu minh bạch và dễ bị thao túng
- **Mục tiêu:**
  - Tạo một hệ thống thanh toán phi tập trung (decentralized), minh bạch và không phụ thuộc vào bên thứ ba

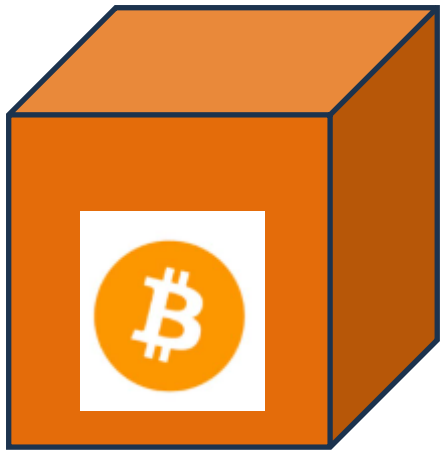
Sự ra đời của Bitcoin

Satoshi Nakamoto: mật danh của người hoặc nhóm người (vẫn còn là một ẩn số) đã công bố whitepaper với tiêu đề "*Bitcoin: A Peer-to-Peer Electronic Cash System*" vào tháng 10 năm 2008.

- **Whitepaper** mô tả chi tiết cách hoạt động của Bitcoin như một loại tiền mã hóa sử dụng công nghệ Blockchain.

  - Ngày 03/01/2009 block đầu tiên của Bitcoin được tạo ra
  - Nội dung của **Genesis Block** có thông điệp: "*The Times 03/Jan/2009 Chancellor on brink of second bailout for banks*" (ám chỉ sự mất niềm tin vào hệ thống ngân hàng truyền thống)

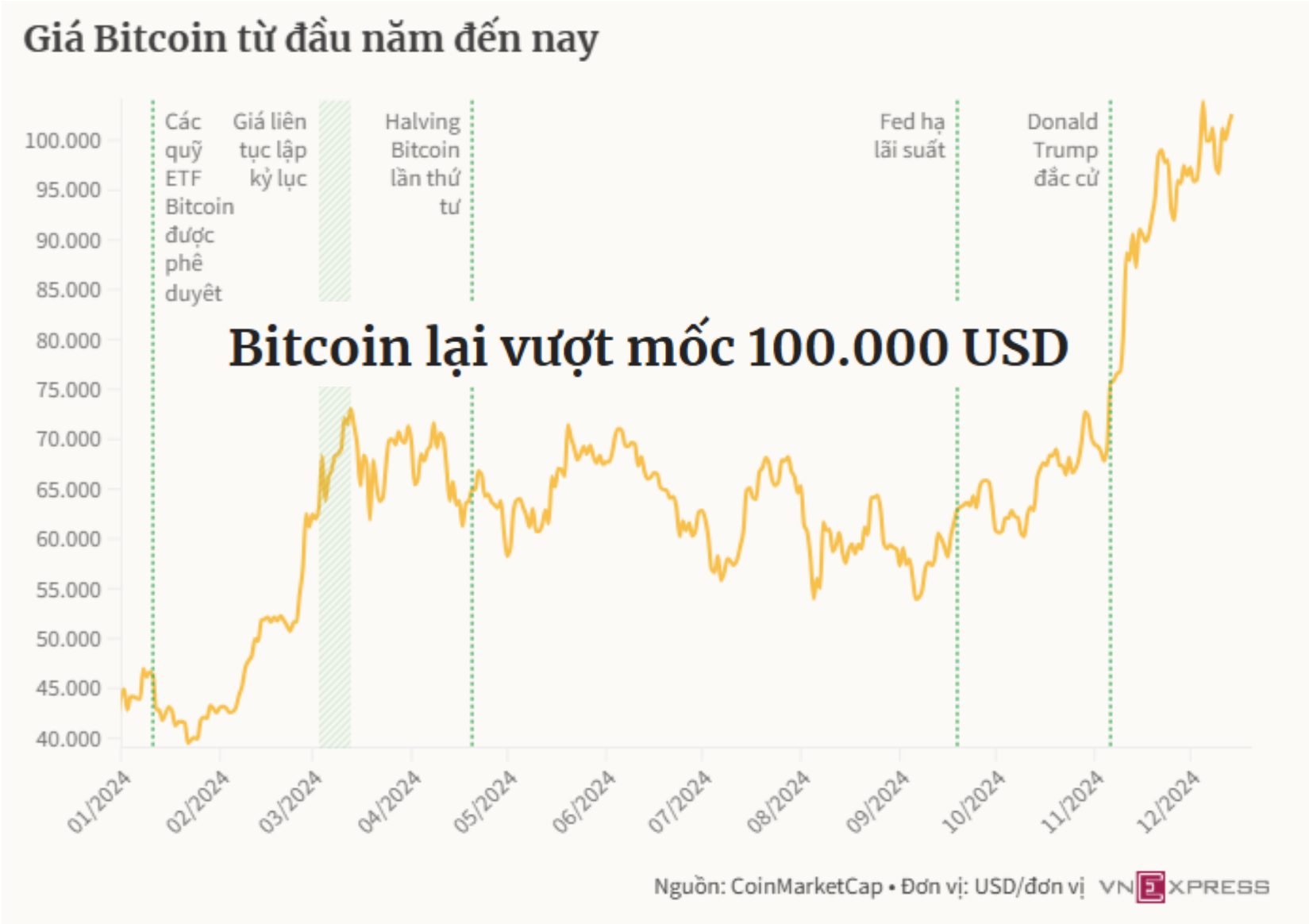
Genesis Block (Block #0)



Tổng 21 triệu Bitcoin

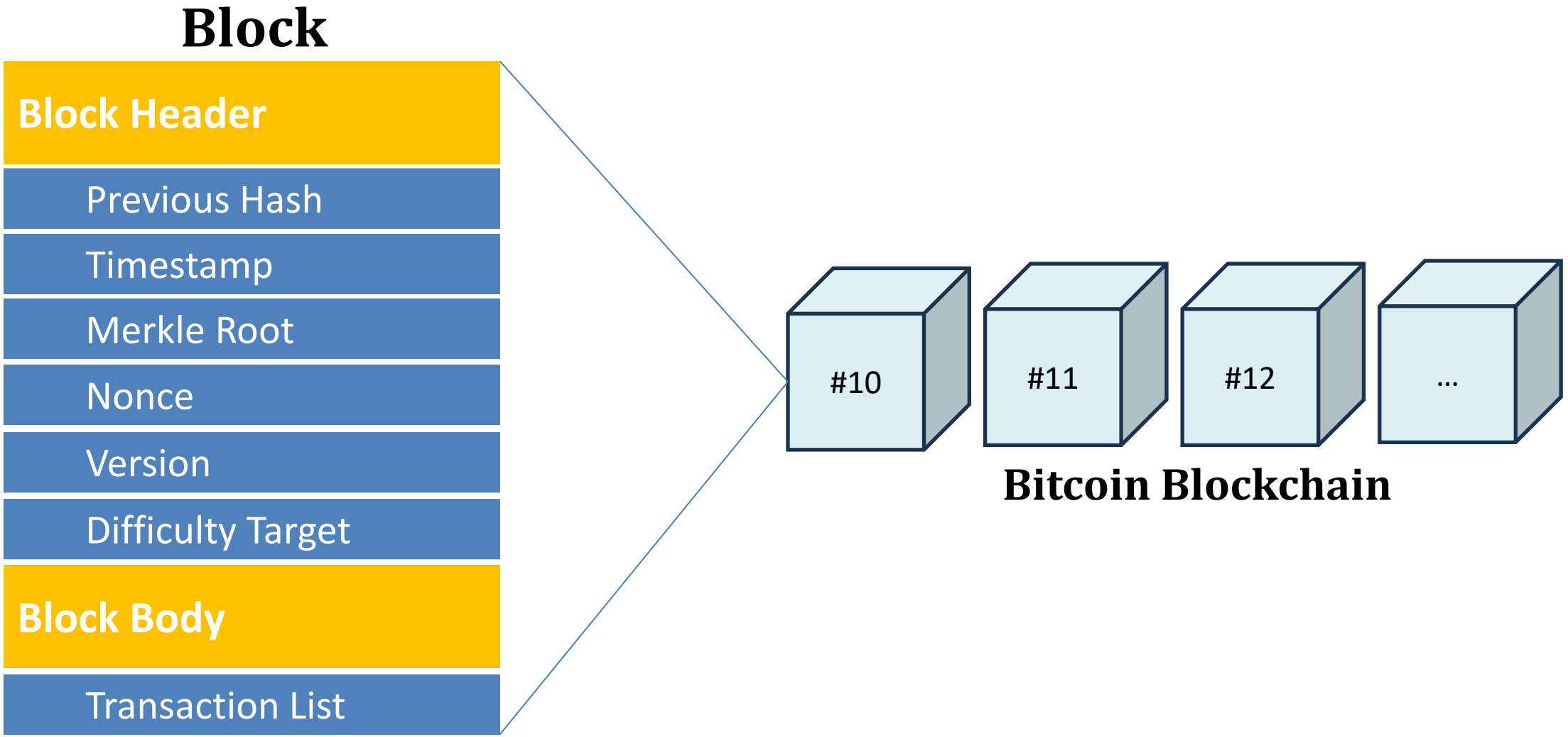
dự kiến sẽ được đào hết vào năm 2140

Tỷ giá Bitcoin



https://vnexpress.net/gia-bitcoin-hom-nay-btc-tro-lai-vuot-moc-100-000-usd-4827755.html

Khối Bitcoin (Bitcoin block)



https://www.blockchain.com/explorer/blocks/btc/876557

Khối Bitcoin (Bitcoin block)

Ví dụ: Một khối Bitcoin chứa thông tin sau

Header

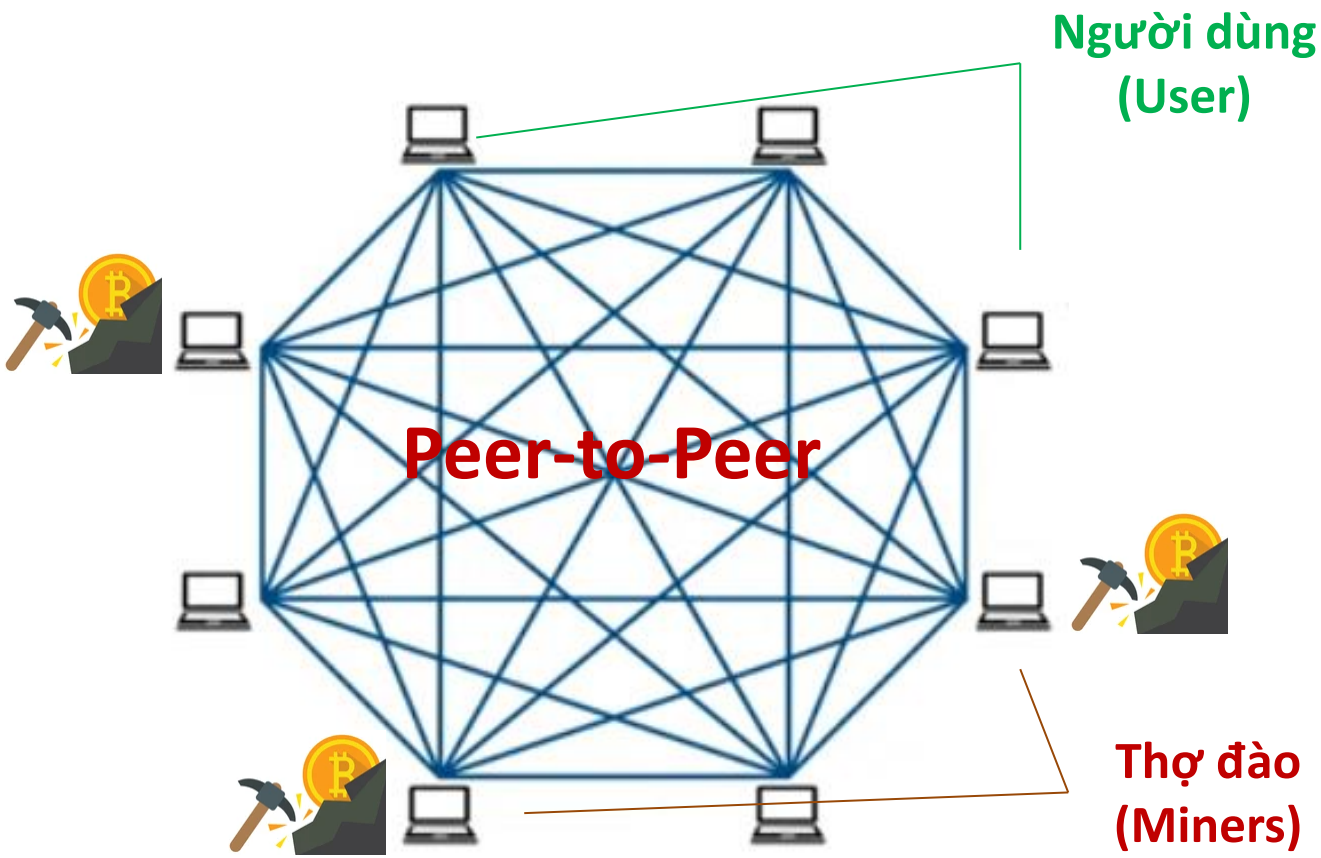
```
Version: 0x20000000
Previous Block Hash: 0000000000000000000abc1234567890defghijklmnopqrstuvwxyz
Merkle Root: 91a3b6c719f19de762184e72543d6165931f24a3a4d537f9f80e9bdf708cfa94
Timestamp: 1673657893 (2023-01-14 15:58:13 UTC)
Difficulty Target: 00000000ffffffffffffffffffffffffffffffffffffffff
Nonce: 3479851
```

Body

```
Transaction 1: Coinbase Transaction
    - Miner receives 6.25 BTC
Transaction 2: Alice sends 2 BTC to Bob
    - Input: Previous Transaction ID: abc123
    - Output: 2 BTC -> Bob
Transaction 3: Bob sends 1 BTC to Charlie
    - Input: Previous Transaction ID: def456
    - Output: 1 BTC -> Charlie
```

Mạng Bitcoin

Mạng Bitcoin là một hệ thống **phi tập trung** (decentralized network) dựa trên công nghệ **Peer-to-Peer (P2P)**



Các nút (Nodes):

- Là các máy tính trong mạng lưu trữ toàn bộ hoặc một phần của Blockchain
- Các nút có nhiệm vụ xác minh giao dịch và duy trì tính toàn vẹn của mạng

Người dùng (Users):

- Sử dụng ví Bitcoin để gửi và nhận Bitcoin
- Tạo giao dịch thông qua phần mềm ví

Thợ đào (Miners):

- Là các nút đặc biệt thực hiện việc **đào coin** bằng cách giải các bài toán mật mã để tạo ra khối mới
- Thợ đào nhận thưởng bằng Bitcoin thông qua **Coinbase Transaction**

Ví (Wallet) là gì?

Ví (Wallet) trong Blockchain, đặc biệt trong mạng Bitcoin là một công cụ phần mềm hoặc phần cứng:

- **Quản lý khóa riêng tư (Private Key):** Để xác thực quyền sở hữu tài sản kỹ thuật số.
- **Quản lý Khóa công khai (Public Key):** Để nhận tài sản từ người khác, dùng để xác minh giao dịch.
- **Tạo và quản lý địa chỉ công khai (Public Address):** Để tương tác trên mạng Blockchain: gửi và nhận tài sản.

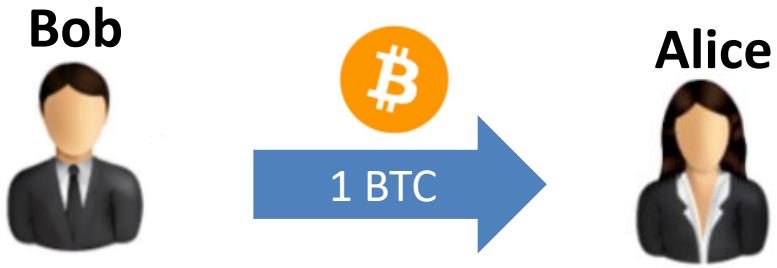
Không lưu trữ trực tiếp tài sản kỹ thuật số (như Bitcoin)

Vai trò của Ví (Wallet)

1. Gửi tài sản kỹ thuật số
2. Nhận tài sản kỹ thuật số
3. Bảo mật tài sản
4. Hiển thị số dư dựa trên các đầu ra (ouput) giao dịch chưa sử dụng (**Unspent Transaction Outputs - UTXOs**) được ghi nhận trên Blockchain

Ví dụ: Ví (Wallet) truy vấn Unspent Transaction Output - UTXO

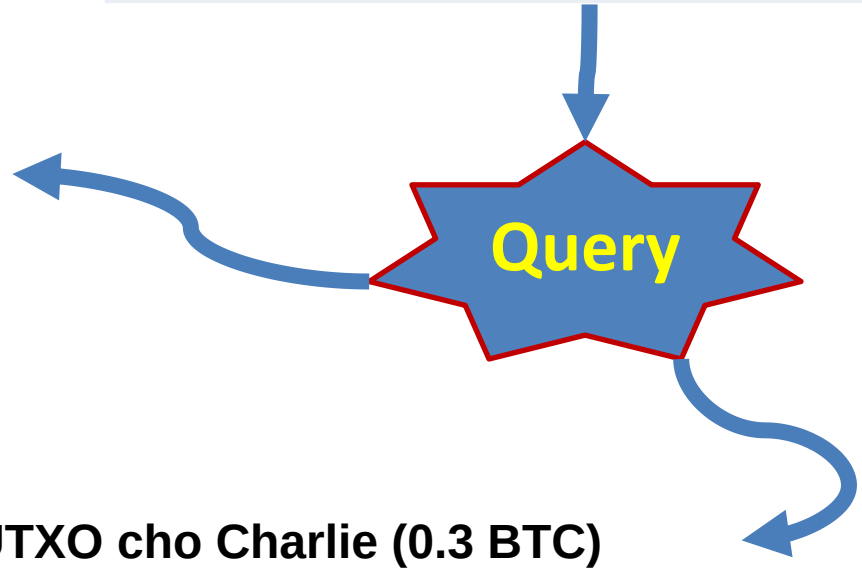
Giao dịch 1



Giao dịch 2

Lịch sử giao dịch Blockchain

Giao dịch
Giao dịch 1: Bob → Alice (1 BTC)
Giao dịch 2: Alice → Charlie (0.3 BTC), Alice (0.7 BTC thối lại)



Phương thức lưu trữ của Bitcoin

Bitcoin sử dụng các loại phương thức lưu trữ khác nhau để bảo quản **private key** (khóa riêng tư) – thành phần quan trọng nhất trong giao dịch Bitcoin.

Lưu trữ cục bộ (Local Storage)

Khóa riêng tư (private key) được lưu trữ trực tiếp trên thiết bị cá nhân như: máy tính, điện thoại hoặc ổ cứng

- Toàn quyền kiểm soát thông tin và khóa riêng tư
- Không phụ thuộc vào dịch vụ bên thứ ba
- Rủi ro thiết bị bị hỏng hoặc mất, nhiễm virus

Phần mềm ví

Electrum wallet

Lưu trữ nóng (Hot Storage)

Là hình thức lưu trữ **private key** trên thiết bị hoặc trên máy chủ (server) của nhà cung cấp dịch vụ ví, có kết nối trực tiếp với internet

- Giao dịch nhanh chóng, dễ dàng thực hiện
- Truy cập mọi lúc, mọi nơi khi có kết nối internet
- Nguy cơ bị tấn công cao

Phần mềm ví trên thiết bị cá nhân

Electrum wallet

Trust wallet

MetaMask wallet

Ví trên máy chủ Blockchain.com

https://www.blockchain.com/wallet

Lưu trữ lạnh (Cold Storage)

- Lưu trữ **private key** ngoại tuyến, không kết nối internet
- Phổ biến dưới các hình thức như ví phần cứng (hardware wallet), ví giấy (paper wallet), hoặc ổ cứng lưu trữ offline.

- Khóa riêng tư không bị lộ qua internet
- Loại bỏ nguy cơ bị tấn công qua mạng
- Phải thao tác thủ công để thực hiện giao dịch
- Mất thiết bị hoặc giấy lưu trữ

Ví phần cứng

Trezor wallet

Ledger wallet

Ví giấy (Paper Wallet): Khóa riêng tư được in hoặc ghi trên giấy

Ổ cứng/USB ngoại tuyến

Ví Trực Tuyến (Online Wallet)

Ví trực tuyến là loại ví lưu trữ **private key** trên máy chủ của một nhà cung cấp dịch vụ hoặc nền tảng trực tuyến.

- Có thể truy cập từ mọi nơi chỉ cần có internet
- Dễ sử dụng
- Phụ thuộc vào nhà cung cấp
- Nếu nhà cung cấp bị hack, người dùng có thể mất Bitcoin.

Nhà cung cấp dịch vụ

Blockchain.com

https://www.blockchain.com/wallet

BINANCE

https://www.binance.com/en

coinbase

https://www.coinbase.com/en-gb/wallet

Cơ chế hoạt động của Bitcoin

Bitcoin hoạt động dựa trên nền tảng công nghệ **Blockchain** và các nguyên tắc mật mã học. Chi tiết về cơ chế hoạt động:

1. **Giao dịch Bitcoin:** Quá trình chuyển đổi giá trị Bitcoin từ một người dùng sang người khác

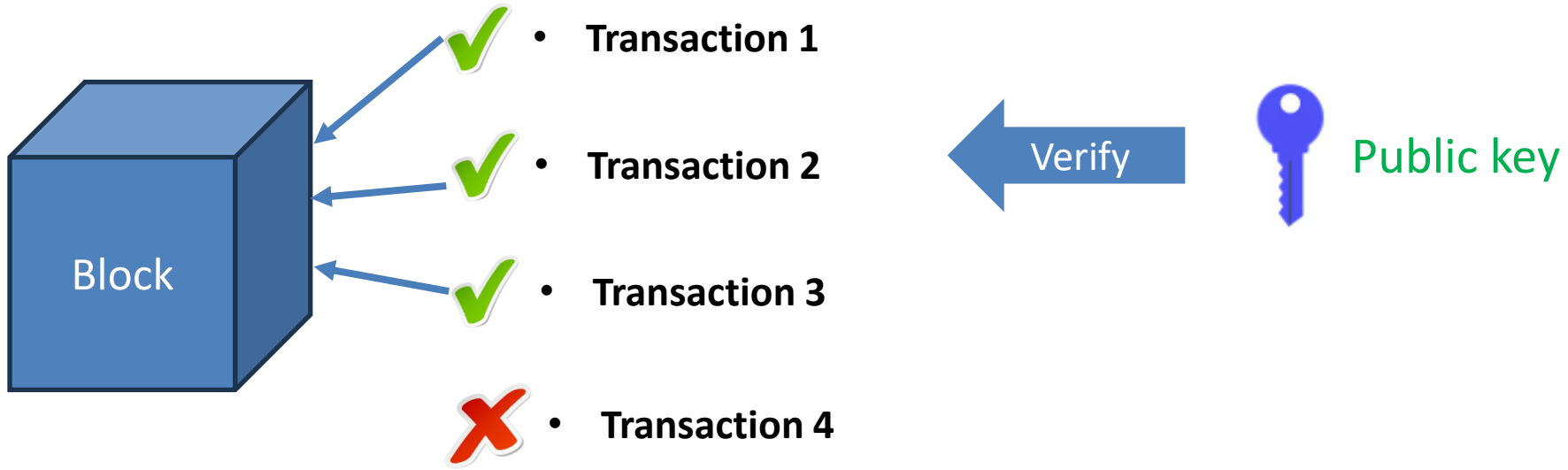
- **Input**: Tham chiếu đến giao dịch trước đó
- **Output**: Số bitcoin được gởi và địa chỉ ví người nhận

- Sử dụng **private key**
- Chứng minh quyền sở hữu giao dịch từ ví người gởi

- Giao dịch được gởi vào mạng Bitcoin Peer-to-Peer (P2P)

2. Xác minh giao dịch:

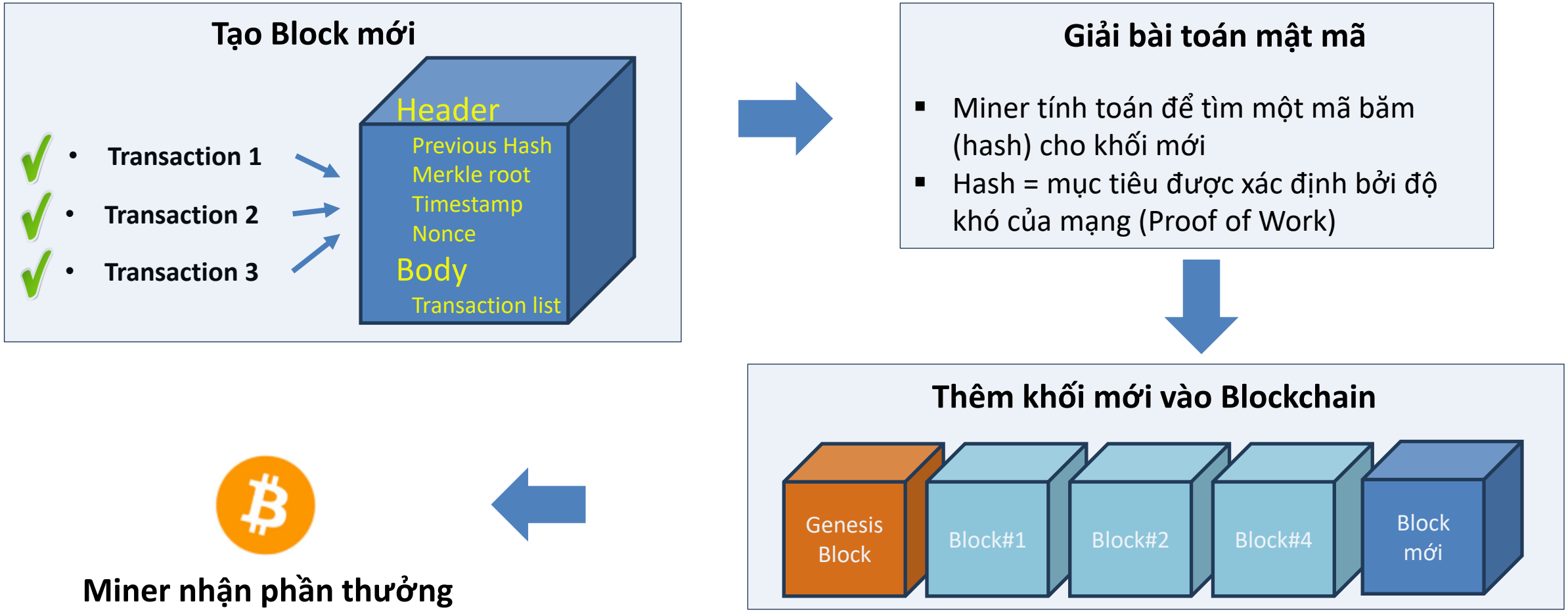
- Các nút trong mạng xác minh tính hợp lệ được ký hợp lệ bằng **khóa riêng tư** của người gửi
- Người gửi có đủ Bitcoin trong ví để thực hiện giao dịch
- Giao dịch không bị trùng lặp (double-spending)



Các thợ đào thu thập các giao dịch hợp lệ và tổ chức chúng thành một **khối (block)**

3. Đào coin và tạo khối (block) mới:

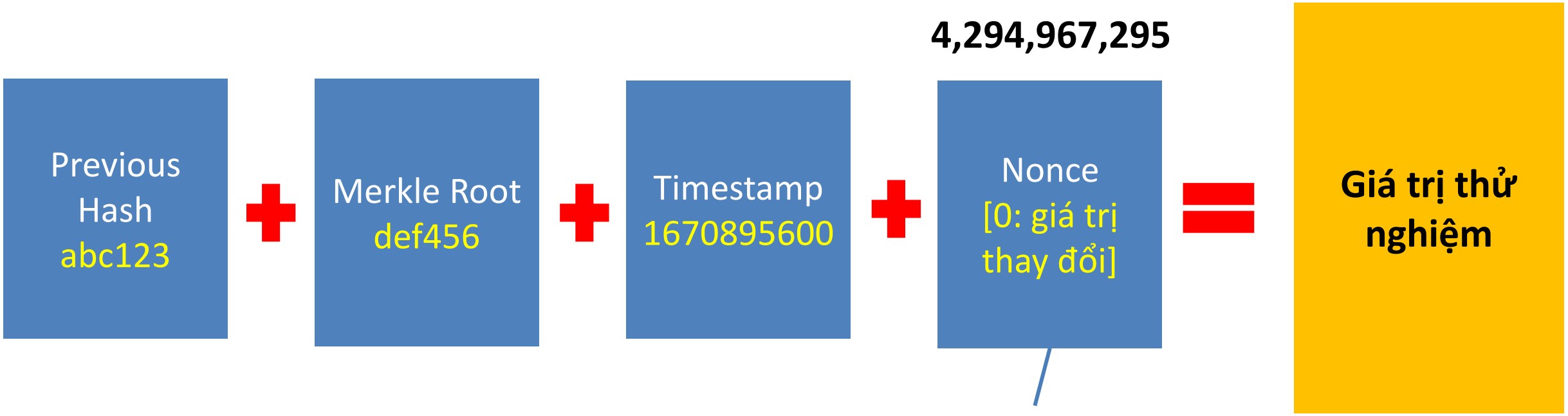
- Các thợ đào giải bài toán mật mã để thêm khối mới vào Blockchain



Thuật toán đào Bitcoin

- Thuật toán đào Bitcoin là quá trình mà các thợ đào (miners) sử dụng sức mạnh tính toán để giải các bài toán mật mã nhằm tạo ra các khối mới và duy trì sự bảo mật cho mạng Bitcoin
- Đây là một phần của cơ chế Proof of Work (PoW), một cơ chế đồng thuận quan trọng trong Blockchain của Bitcoin

Thuật toán đào Bitcoin



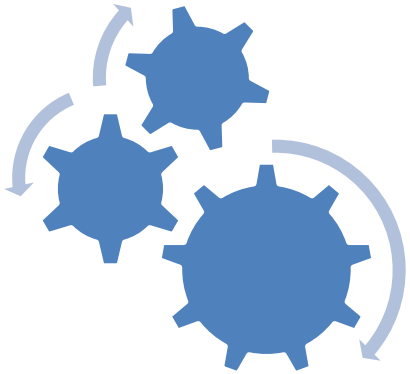
- Số rất đặc biệt (nguyên dương)
- Tìm được None hợp lệ chính tìm ra Bitcoin

Thuật toán đào Bitcoin

Giá trị thử nghiệm

abc123
def456
1670895600
0

Thuật toán băm
(SHA-256)



Mã băm

4aa16c9282a6866902b49461
370b057a6b7276bcd5ffab4c6
9f1056c00cf5fbc

Difficulty Target: 000000006

Thuật toán đào Bitcoin

Độ khó: 8

Nonce: 0

Mục tiêu: 00000000

Mã băm: 4aa16c9282a6866902b49461370b057a6b

7276bcd5ffab4c69f1056c00cf5fbc

Kiểm tra:
Khác nhau hoàn toàn

Tìm một **mã băm bằng giá trị mục tiêu (Target)** đã được xác định bởi độ khó của mạng Bitcoin

Thuật toán đào Bitcoin

Độ khó: 8

Nonce: 19851210

Mục tiêu: 00000000

Mã băm: 0000000082a6866902b49461370b057a6b

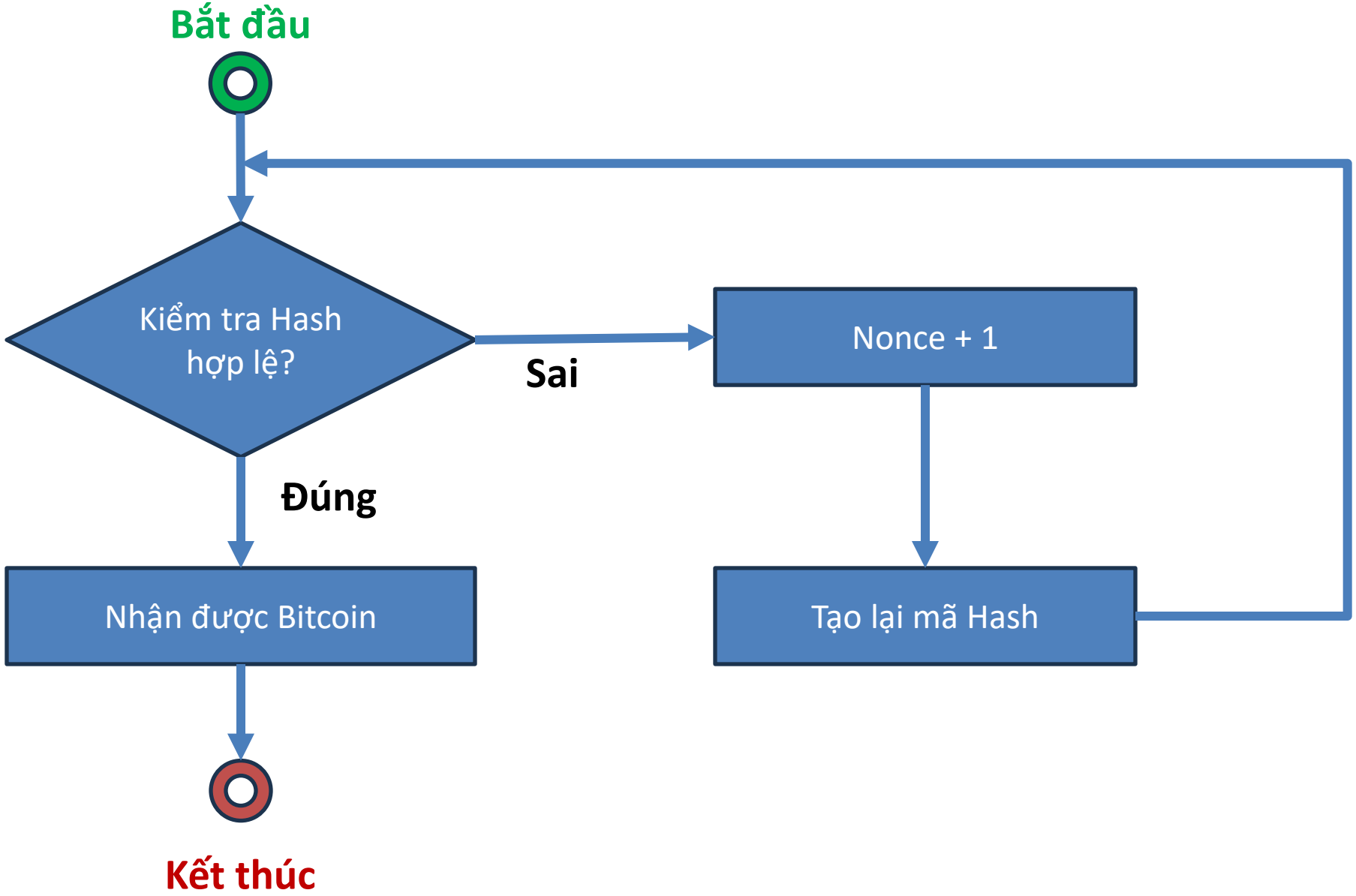
7276bcd5ffab4c69f1056c00cf5fbc

Kiểm tra:
Hoàn toàn hợp lệ

Ví dụ : Quy trình giải mã băm thành công

- Thợ đào thử các giá trị **Nonce** từ 0, 1, 2, … và tính toán mã băm:
  1. **Nonce** = **0** → **Hash** = 7b8f9ds3zyx... (không hợp lệ)
  2. **Nonce** = **1** → **Hash** = 6a3b126bfe... (không hợp lệ)
  3. …
  4. **Nonce** = **346723** → **Hash** = 000000009abcdef... (hợp lệ)
- Thợ đào tìm được mã băm hợp lệ với **Nonce** = **346723** và phát tán khối

Sơ đồ luồng đào Bitcoin



Hạn chế và cải tiến đào Bitcoin

Hạn chế

- Tiêu tốn năng lượng
- Tốc độ giao dịch chậm
- Tính tập trung hóa
- Cạnh tranh gay gắt và chi phí cao
- Khả năng tấn công (51%)

Cải tiến

- Chuyển từ Proof of Work (PoW) sang Proof of Stake (PoS)
- Các cơ chế đồng thuận khác: Proof of Authority (PoA), Delegated Proof of Stake (DPoS)

Thực hành

Source code: *#Thuật toán đào Bitcoin cơ bản*

Course: 010100087602 - Công nghệ chuỗi khối (HK2 năm 2024 - 2025)


Thank you