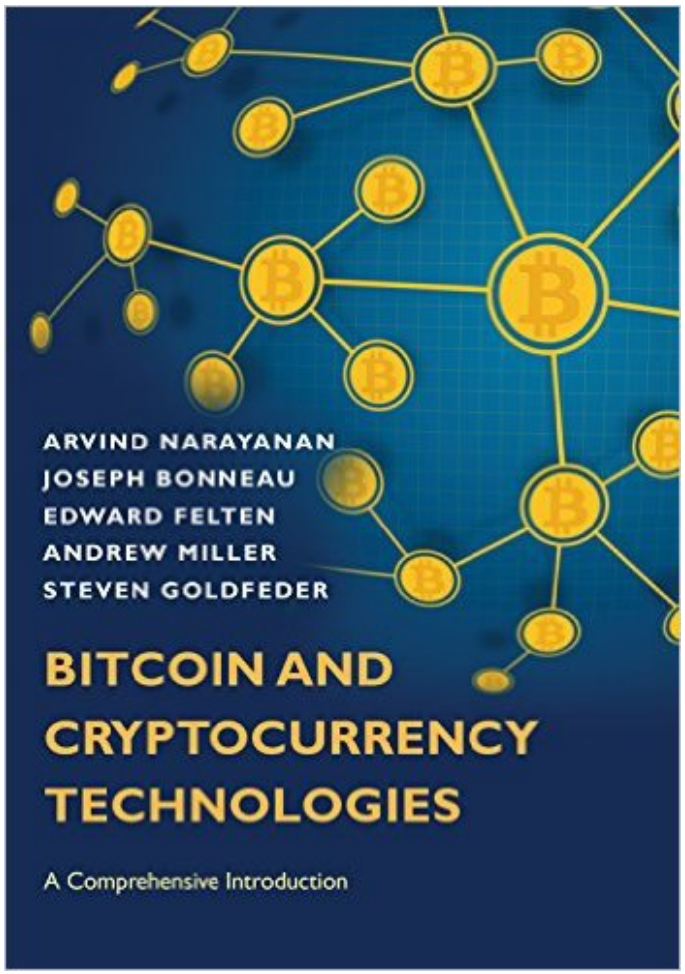
ĐẠI HỌC BÁCH KHOA HÀ NỘI
VIỆN CÔNG NGHỆ THÔNG TIN VÀ TRUYỀN THÔNG

Nhập môn an toàn thông tin

Giới thiệu sơ lược về Bitcoin

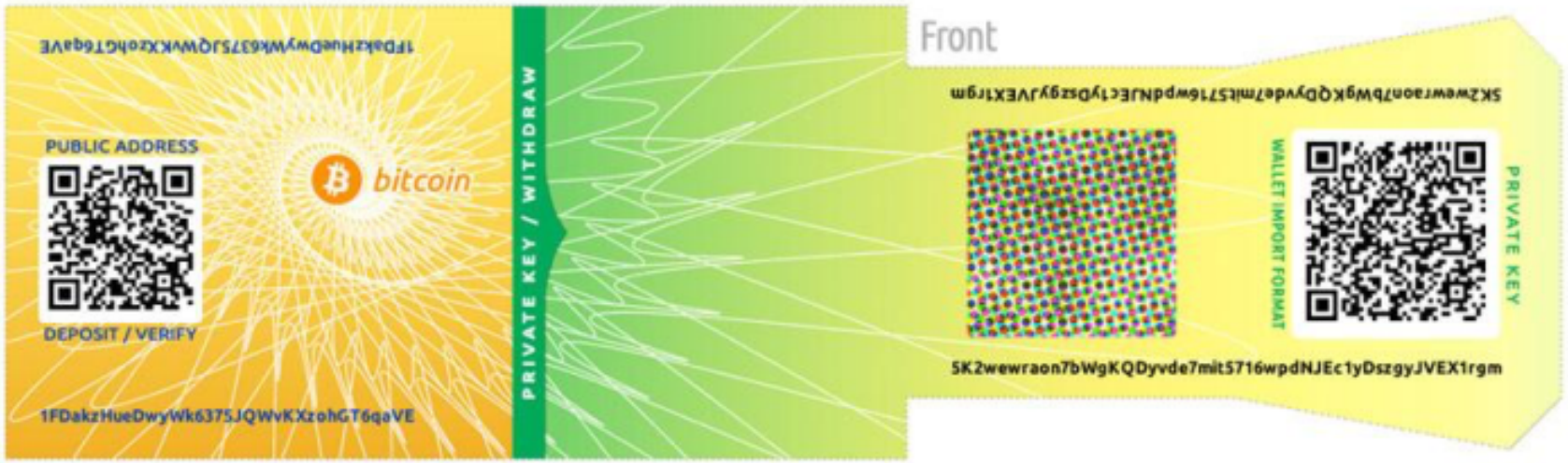
Ngày 3 tháng 6 năm 2021

Tài liệu tham khảo



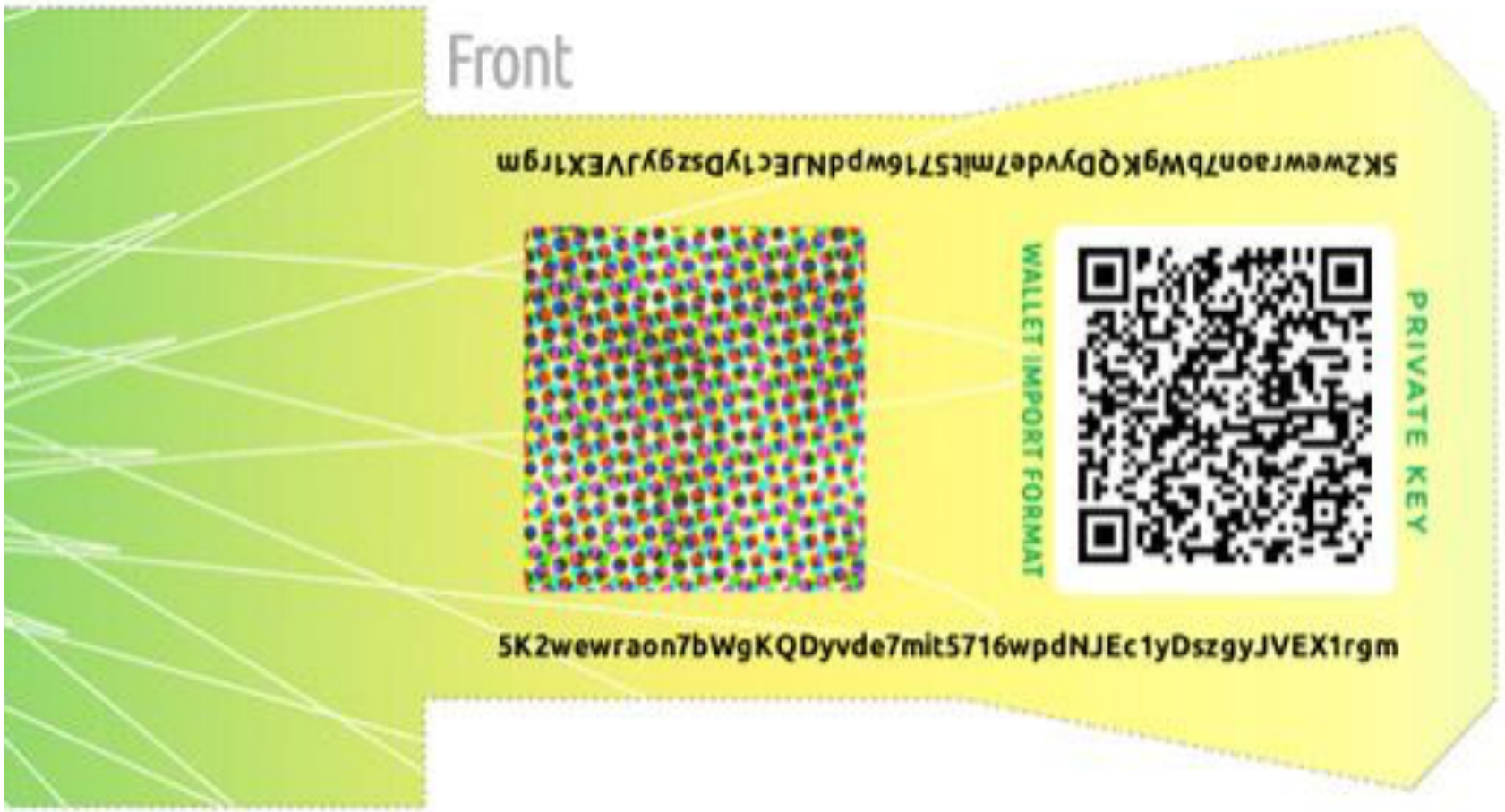
Nội dung

Bitcoin Paper Wallet



Hình: Tạo ra với `https://bitcoinpaperwallet.com/`

Khóa bí mật

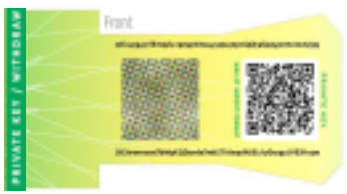

Front
5K2wewraon7bWgKQDyvde7mit5716wpdNJEc1yDszgyJVEX1rgm
WALLET IMPORT FORMAT
PRIVATE KEY
5K2wewraon7bWgKQDyvde7mit5716wpdNJEc1yDszgyJVEX1rgm

Chuyển tiền giữa Alice và Bob

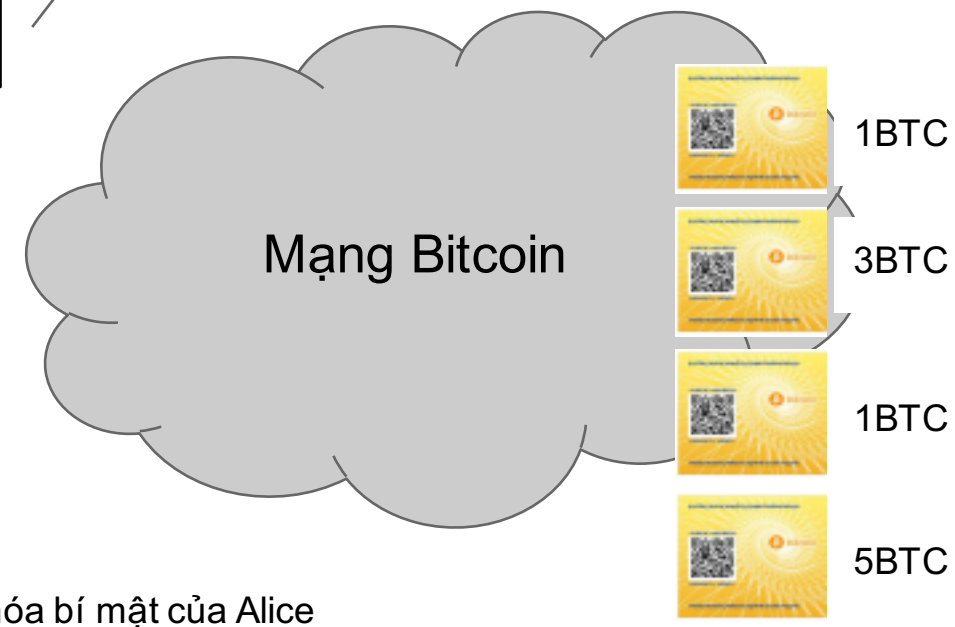
Alice và Bob xác định bởi khóa công khai

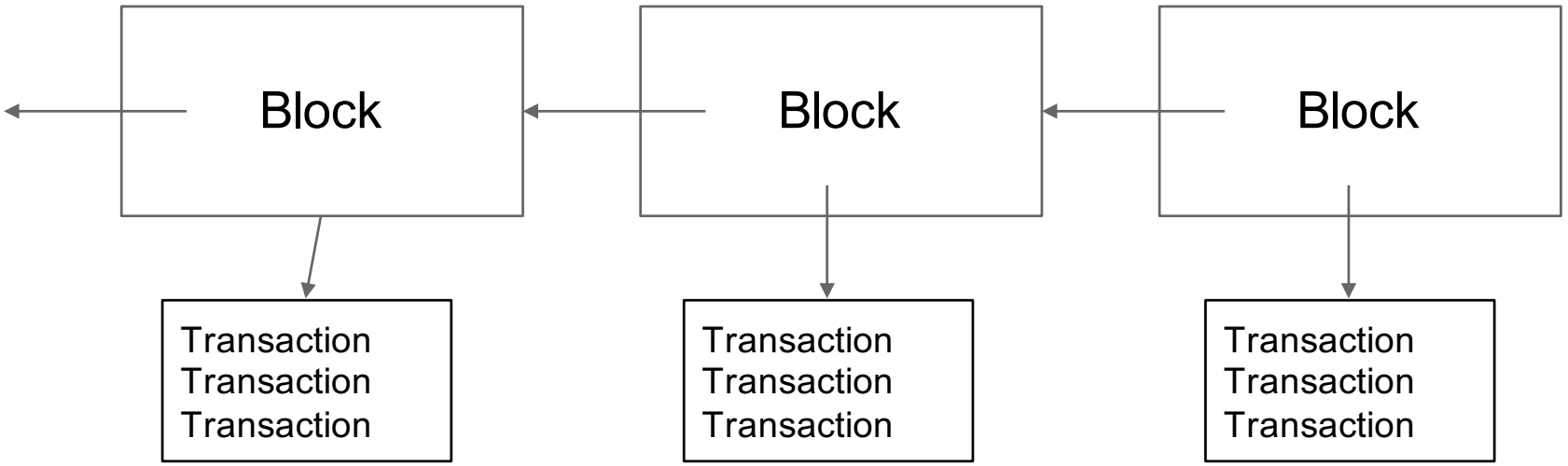
Chuyển 10 Bitcoins của tôi cho Bob.

Alice



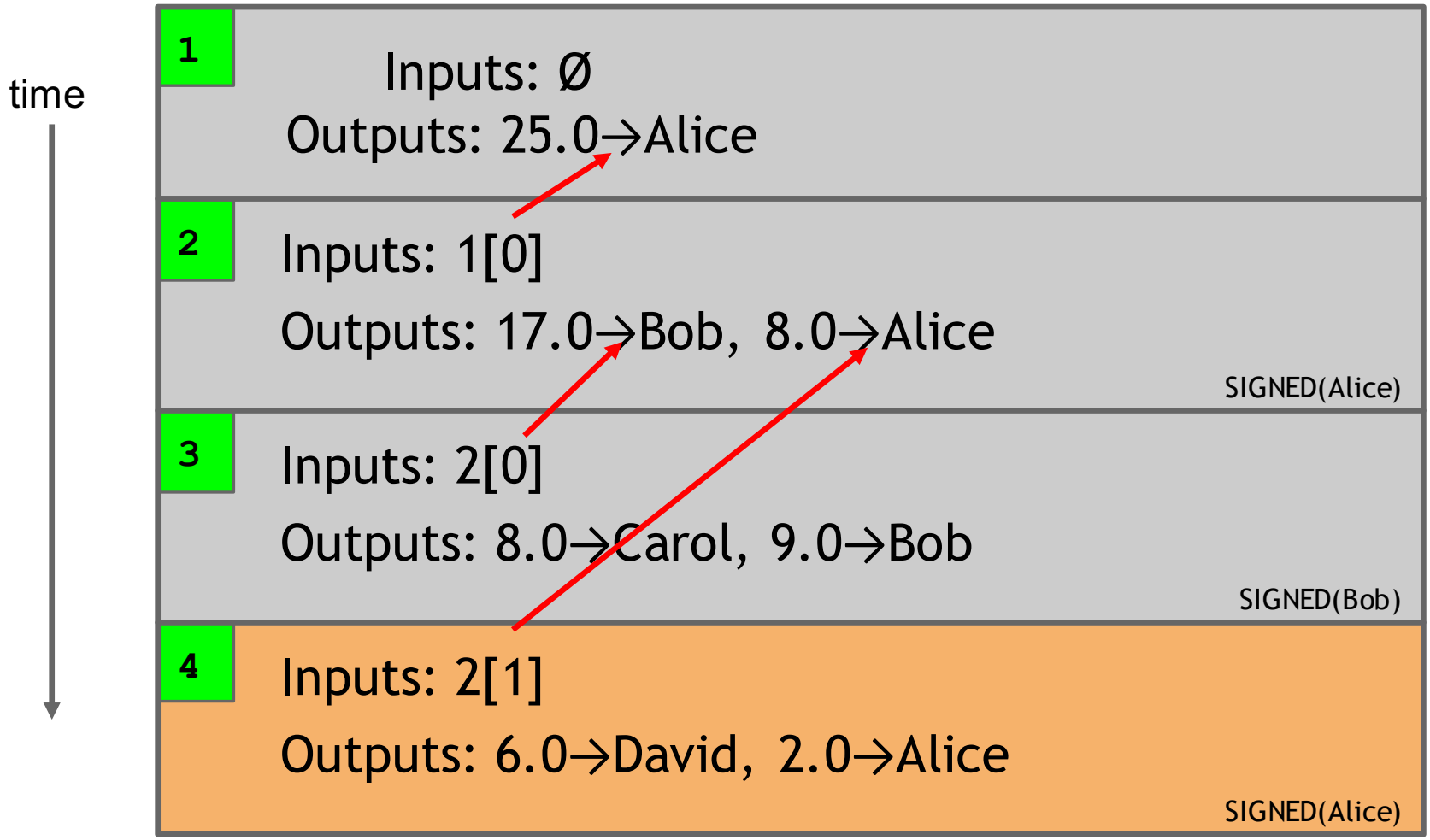
Được ký bởi khóa bí mật của Alice



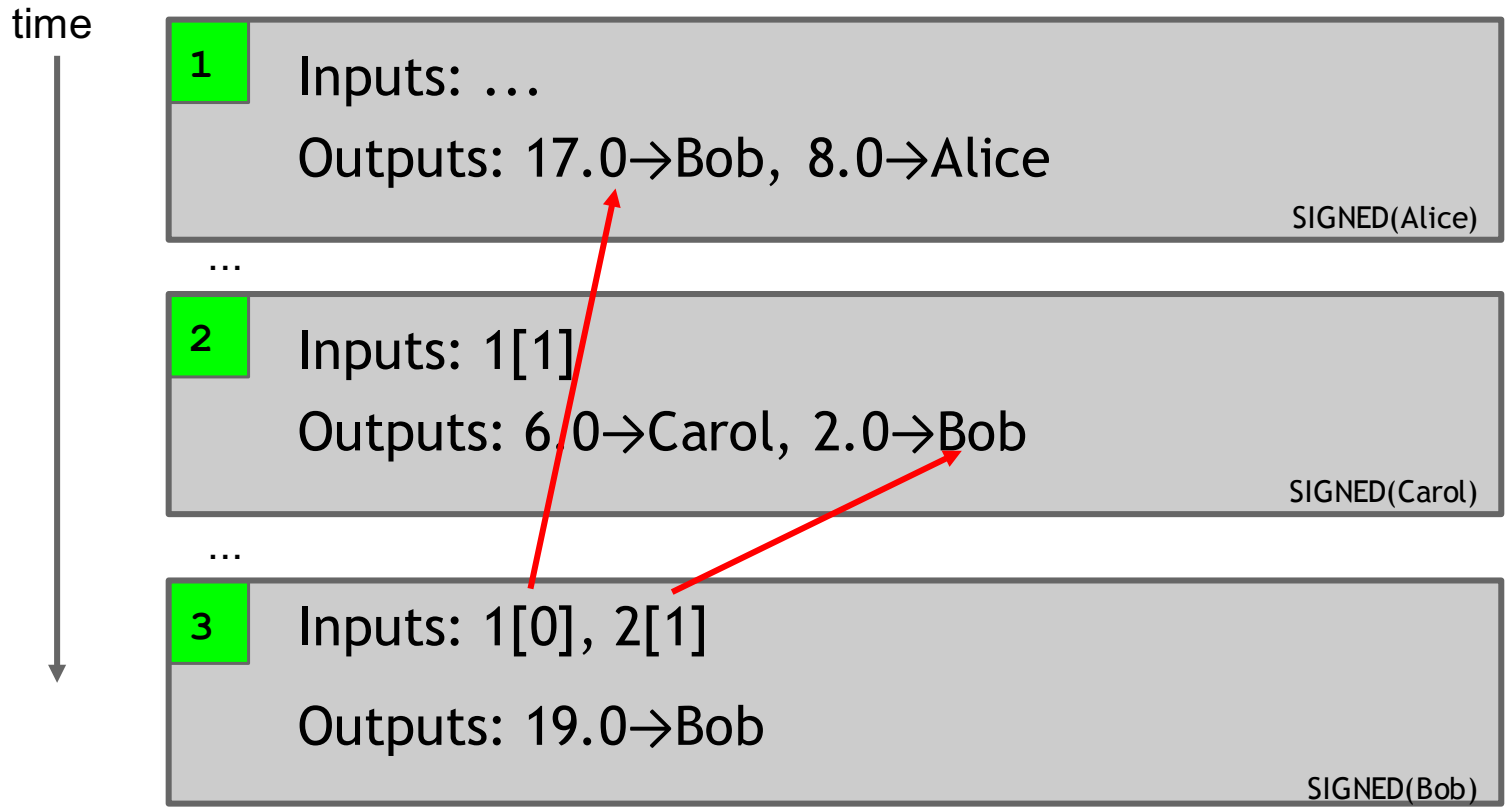


Hình: Mạng Bitcoin tạo thêm một Block sau mỗi 10 phút

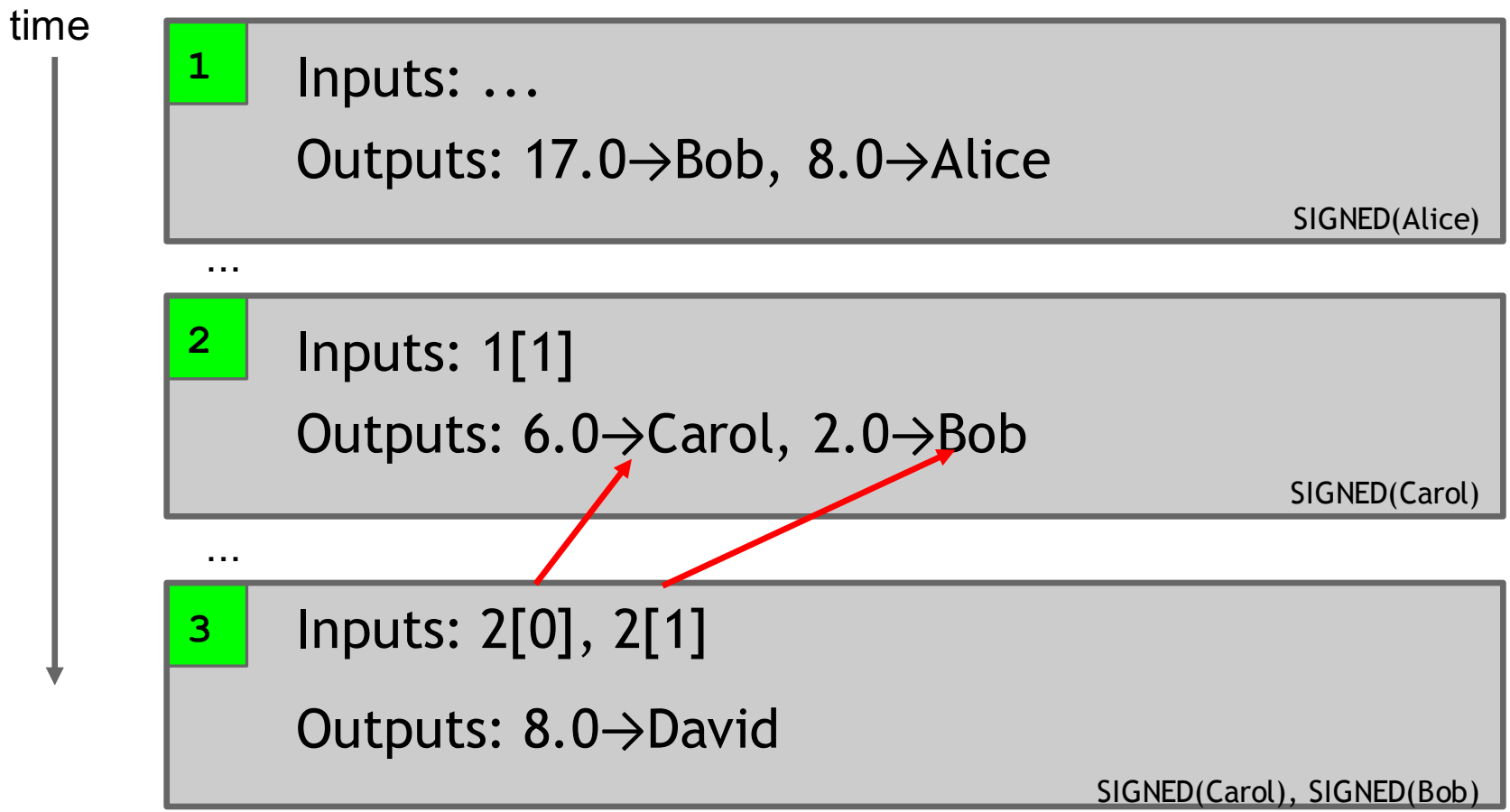
Sổ cái dựa trên giao dịch (Bitcoin)



Gộp nhiều giá trị



Joint Payment



Giao dịch thực tế

metadata

input(s)

output(s)


```
{
    "hash":"5a42590fbe0a90ee8e8747244d6c84f0db1a3a24e8f1b95b10c9e050990b8b6b",
    "ver":1,
    "vin_sz":2,
    "vout_sz":1,
    "lock_time":0,
    "size":404,
    "in":[
     {
       "prev_out":{
        "hash":"3be4ac9728a0823cf5e2deb2e86fc0bd2aa503a91d307b42ba76117d79280260",
        "n":0
       },

         "scriptSig":"30440..."
     },
     {
       "prev_out":{
        "hash":"7508e6ab259b4df0fd5147bab0c949d81473db4518f81afc5c3f52f91ff6b34e",
        "n":0
       },
       "scriptSig":"3f3a4ce81...."
     }
    ],
    "out":[
     {
       "value":"10.12287097",
       "scriptPubKey":"OP_DUP OP_HASH160 69e02e18b5705a05dd6b28ed517716c894b3d42e OP_EQUALVERIFY OP_CHECKSIG"
     }
    ]
}
```

Các thao tác với Bitcoin

- Sinh cặp khóa (hoặc import khóa từ một paper wallet).
- Đưa khóa công khai ("địa chỉ") cho người khác để họ có thể chuyển tiền.
- Tìm khóa công khai của người khác để chuyển tiền.
- Tìm kiếm lịch sử của một địa chỉ.
- Sinh ra một giao dịch Bitcoin để gửi tiền đến một khóa công khai.
- Dùng mã băm của giao dịch như một "biên lai" để tìm kiếm trên mạng.
- Đợi giao dịch được "confirm".

Nội dung

Bitcoin: A Peer-to-Peer Electronic Cash System

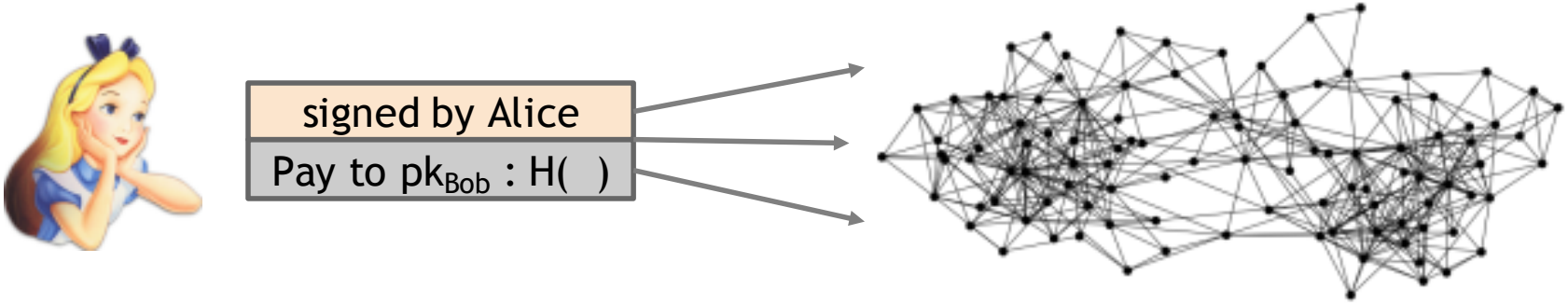
Satoshi Nakamoto
satoshin@gmx.com
www.bitcoin.org

Abstract. A purely peer-to-peer version of electronic cash would allow online payments to be sent directly from one party to another without going through a financial institution. Digital signatures provide part of the solution, but the main benefits are lost if a trusted third party is still required to prevent double-spending. We propose a solution to the double-spending problem using a peer-to-peer network. The network timestamps transactions by hashing them into an ongoing chain of hash-based proof-of-work, forming a record that cannot be changed without redoing the proof-of-work. The longest chain not only serves as proof of the sequence of events witnessed, but proof that it came from the largest pool of CPU power. As long as a majority of CPU power is controlled by nodes that are not cooperating to attack the network, they'll generate the longest chain and outpace attackers. The network itself requires minimal structure. Messages are broadcast on a best effort basis, and nodes can leave and rejoin the network at will, accepting the longest proof-of-work chain as proof of what happened while they were gone.

Cơ chế phi tập trung trong Bitcoin

- Mạng Peer-to-peer: Mở cho mọi người
- Mining (Đào): Mở cho mọi người
- Cập nhật phần mềm: Nhóm phát triển được cộng đồng tin tưởng.

Bitcoin là hệ thống Peer-to-peer



Khi Alice muốn chuyển tiền cho Bob: Alice phát quảng bá giao dịch tới mọi nút trong mạng

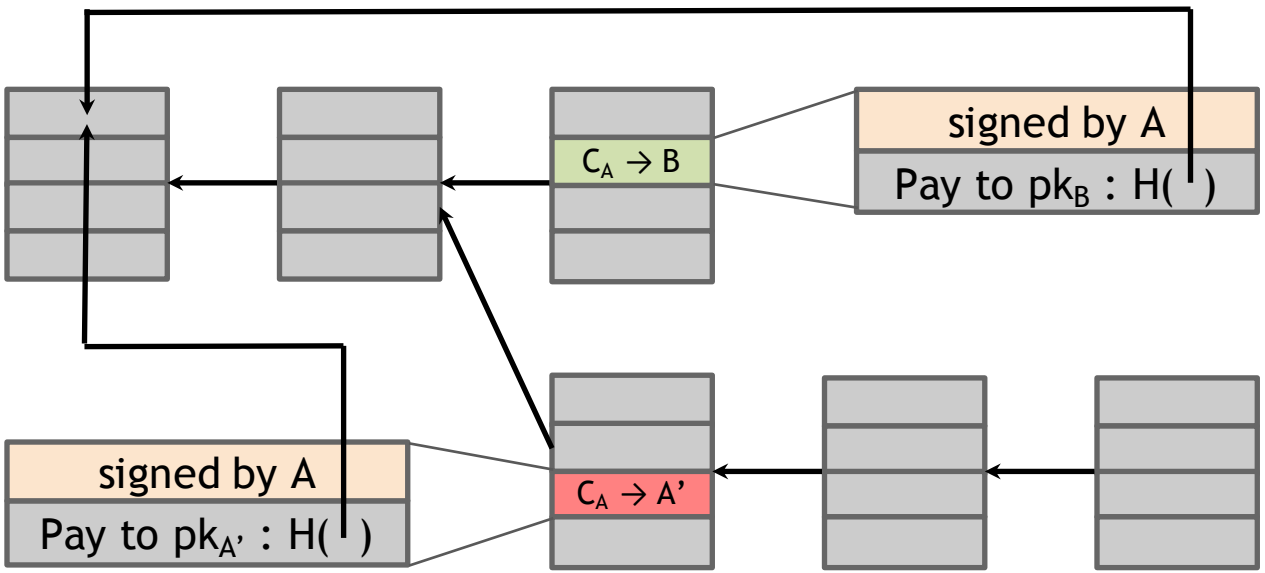
Tại mỗi thời điểm:

- Mọi nút đều có một dãy các Block mà họ đã đồng thuận. Mỗi Block chứa một danh sách các giao dịch.
- Mỗi nút có một tập các giao dịch chưa nằm trong blockchain mà họ lắng nghe được.

Thuật toán đồng thuận của Bitcoin

- Các giao dịch mới được phát quảng bá tới mọi nút
- Mỗi nút tập hợp một số giao dịch mới vào trong một Block
- Trong mỗi vòng, một nút ***ngẫu nhiên*** phải phát quảng bá Block mà nó tạo ra
- Các nút khác chấp nhận Block chỉ nếu mọi giao dịch trong Block này là hợp lệ (chưa được tiêu, chữ ký hợp lệ)
- Các nút thể hiện việc chấp nhận Block này bằng cách thêm mã băm của Block này trong Block tiếp theo mà họ tạo ra.

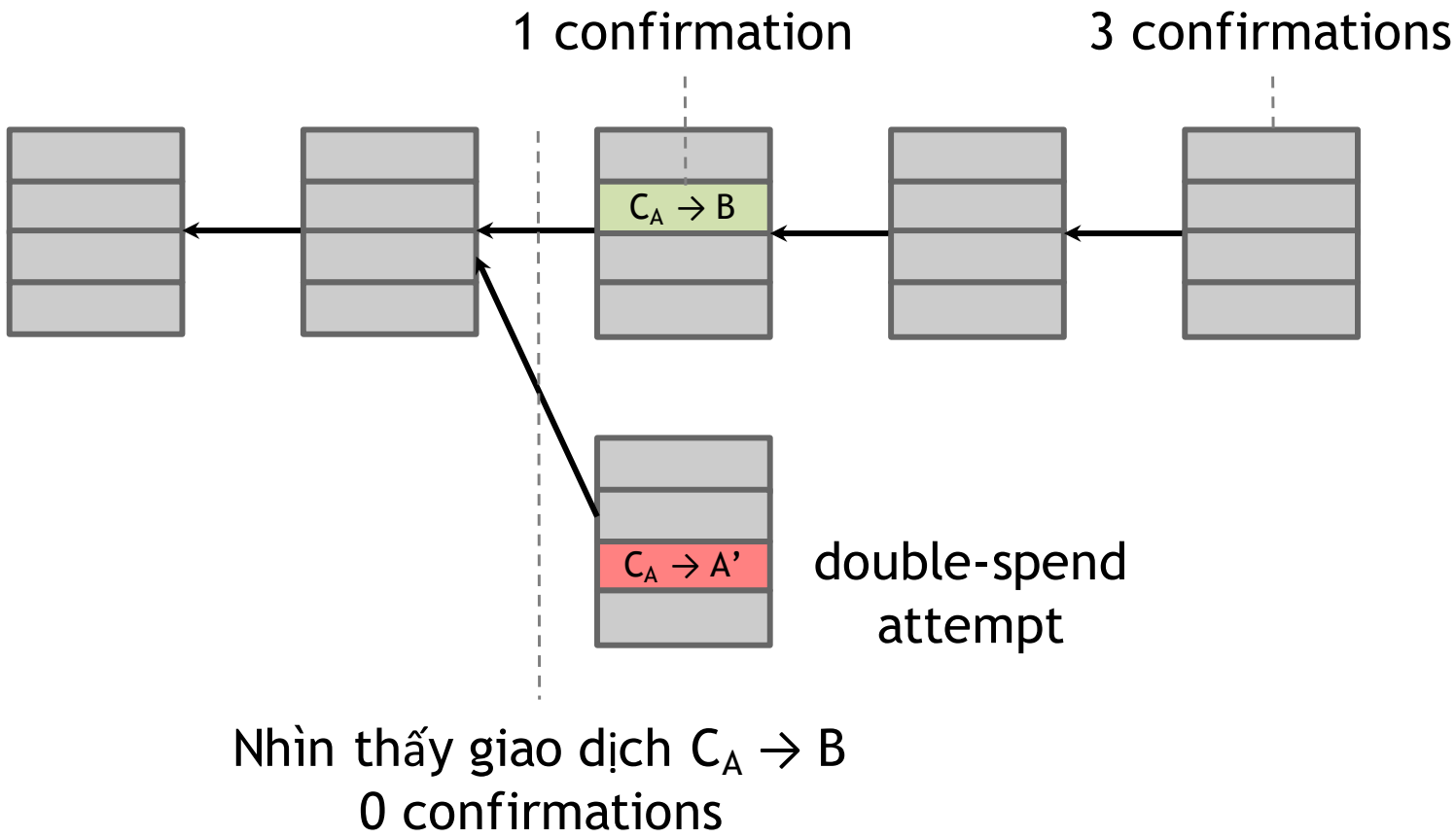
Nút không trung thực trong mạng có thể làm gì?



Double-spending attack

Các nút trung thực trong mạng sẽ mở rộng theo ***nhánh hợp lệ dài nhất***.

Ở góc nhìn của người nhận Bob



- Xác suất bị Double-spending giảm hàm mũ theo số các "confirmation"
- Quy tắc chung: 6 confirmation là đủ đảm bảo chắc chắn.

Tổng kết

- Việc chống giao dịch giả mạo tuy dựa trên Mật mã, nhưng bắt buộc theo cơ chế đồng thuận.
- Việc chống Double-spending thuần túy dựa trên cơ chế đồng thuận.
- Ta không thể chắc chắn 100% một giao dịch nào đó nằm trong nhánh đã được đồng thuận. Chỉ được đảm bảo với một xác suất nào đó.

Nội dung

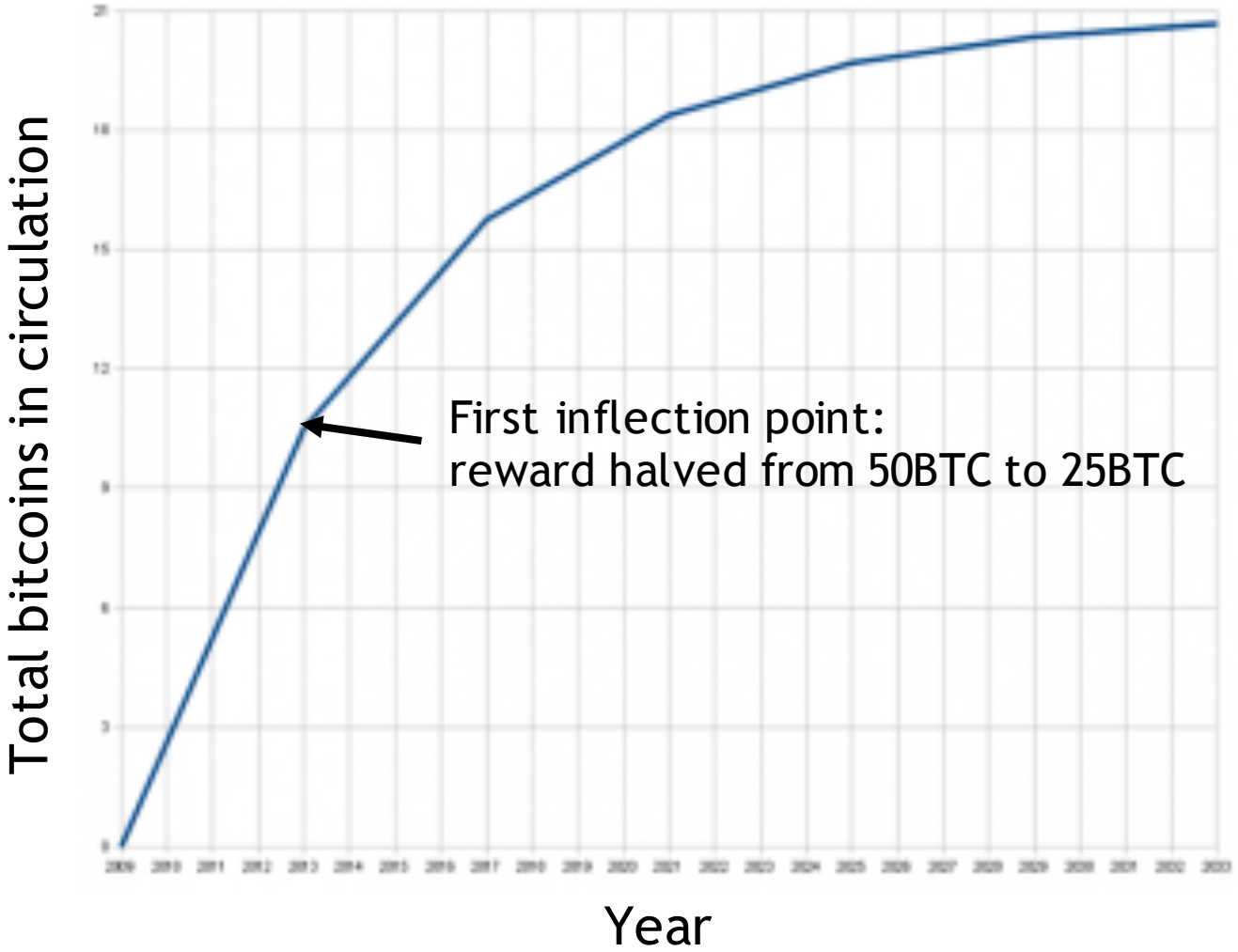
Thưởng 1: cho việc tạo ra Block mới

Người tạo ra Block mới được

- thêm một *giao dịch tạo coin* vào trong Block
- chọn địa chỉ người nhận cho giao dịch này.

Giao dịch này có giá trị cố định: Hiện tại là 12.5 BTC, giảm một nửa sau mỗi 4 năm.

Người tạo Block lấy được phần thưởng này chỉ nếu Block nằm trong nhánh đồng thuận lâu dài.



- Thưởng cho Block mới là cách tạo ra các bitcoin.
- Sẽ hết vào năm 2040. Sẽ không có thêm bitcoin mới trừ khi thay đổi luật.

Thưởng 2: Cho phí giao dịch

- Người tạo ra các giao dịch có thể chọn để giá trị output nhỏ hơn giá trị input.
- Phần dư là phí giao dịch và dành cho người tạo ra Block.
- Đây là việc tình nguyện, giống như tiền tip.
- Tuy nhiên người tạo ra Block có thể chọn giao dịch trả phí cao để thêm vào Block và để lại giao dịch có phí thấp.

Một số vấn đề

- Làm thế nào để chọn ***nút ngẫu nhiên***?
- Làm thế nào để tránh bài toán free-for-all?
- Làm thế nào để tránh Sibil attack?

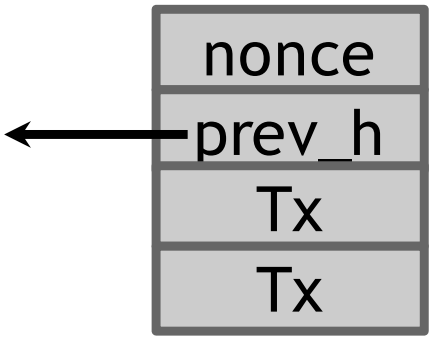
Bằng chứng công việc (Proof-of-work)

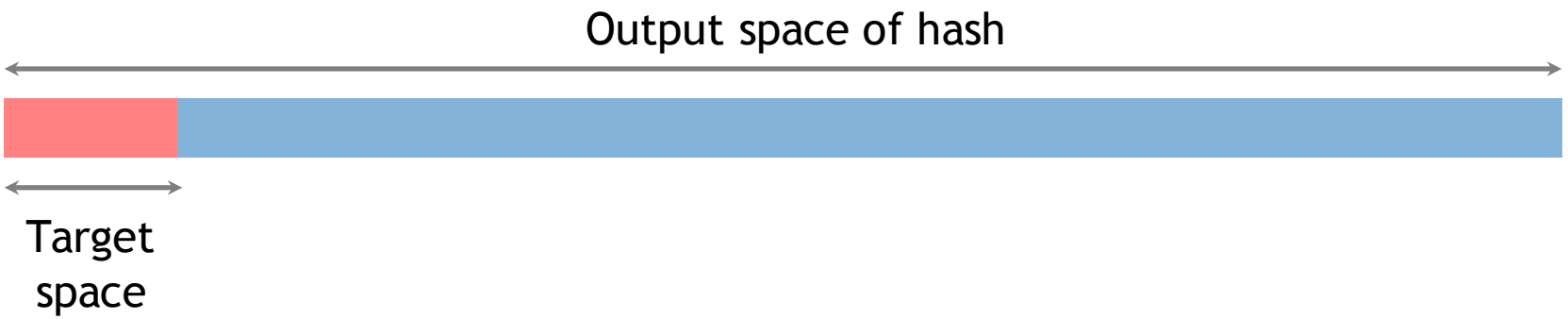
- Để lựa chọn một nút ngẫu nhiên: Ta chọn nút một cách ngẫu nhiên theo tỉ lệ tài nguyên của mỗi nút.
  Ta hy vọng rằng không ai có thể giữ độc quyền tài nguyên này.
- Chọn theo khả năng tính toán: Proof-of-work
- Chọn theo quyền sở hữu: Proof-of-stake

Hash puzzles

Để tạo ra một Block, ta phải tìm giá trị `nonce` thỏa mãn

$$\texttt{H}(\texttt{nonce}|\texttt{prev\_hash}|\texttt{tx}|\cdots|\texttt{tx}) < \texttt{target}.$$





Nếu hàm băm an toàn thì ta chỉ có cách thử các giá trị `nonce` cho đến khi gặp may.

Tính chất PoW 1: Rất khó tính toán

- Như tháng 8/2014, khoảng 10^{20} hash/block.
- Chỉ một số nút quan tâm đến việc tính toán này. Đây là các máy đào (Miner).

Tính chất PoW 2: Tham số hóa chi phí tính toán

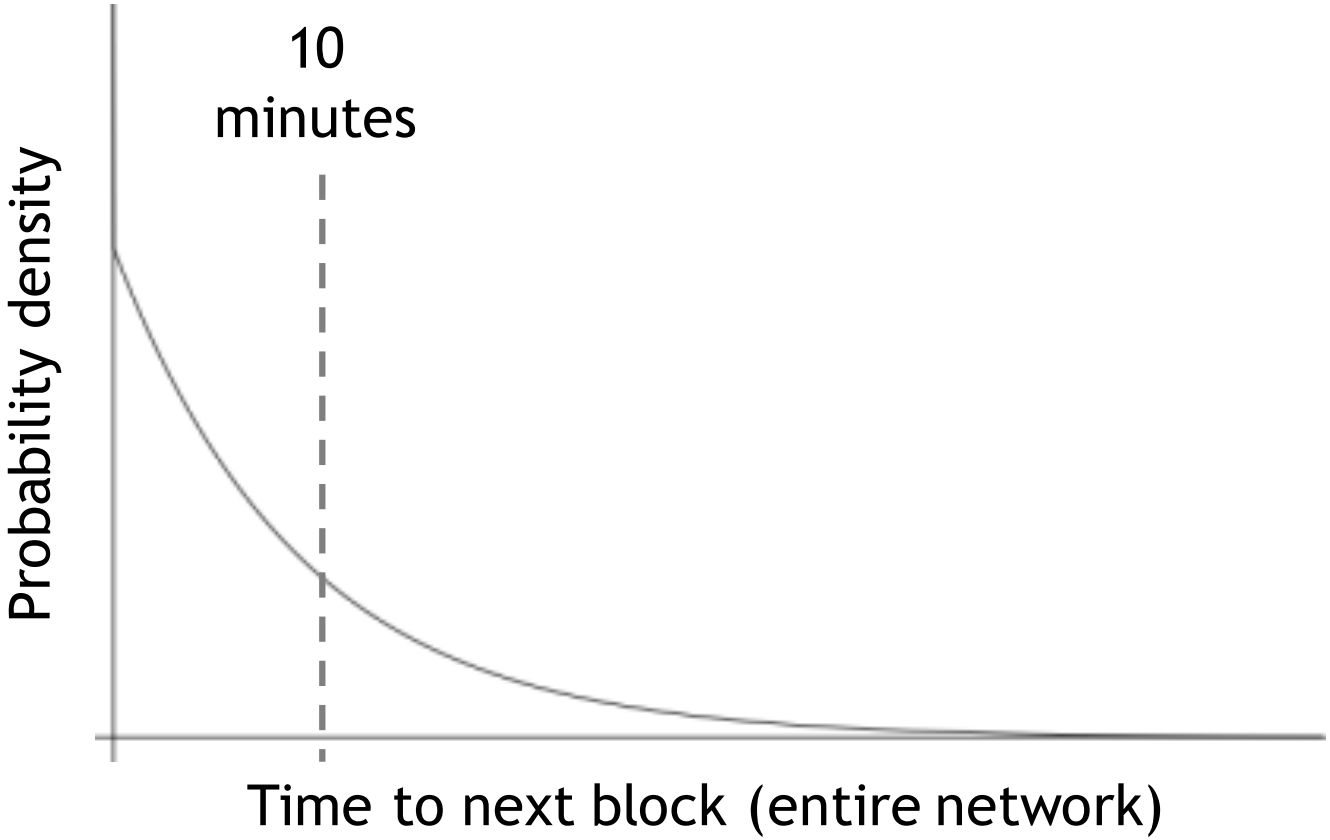
- Các nút tự động tính toán lại `target` sau 2 tuần.
- Mục đích: Thời gian trung bình để tạo ra block mới là 10 phút.

  Prob(Alice tạo ra Block tiếp theo) = tỉ lệ với khả năng hash mà cô ấy có.

Giả sử về tính an toàn

Không có cách nào tấn công hệ thống nếu phần lớn các Miner (tính trọng số theo khả năng Hash) tuân theo giao thức.

Giải hash puzzles theo xác suất



Với mỗi miner, thời gian trung bình để tạo được block là

$$\frac{10 \text{ phút}}{\text{tỉ lệ hash mà anh ta có}}$$

Tính chất PoW 3: Dễ kiểm tra

- `nonce` được công khai như một phần của block
- Các miners khác chỉ cần kiểm tra

$$\texttt{H}(\texttt{nonce} \mid \texttt{prev\_hash} \mid \texttt{tx} \mid \cdots \mid \texttt{tx}) < \texttt{target}.$$

Khi nào thì việc mining có lợi?

Giá trị thưởng cho việc tạo ra Block mới + phí giao dịch > chi phí cho phần cứng + chi phí điện

Tuy nhiên việc này rất khó đánh giá vì

- gồm chi phí cố định và chi phí thay đổi
- phần thưởng phụ thuộc vào tốc độ băm tổng thể.

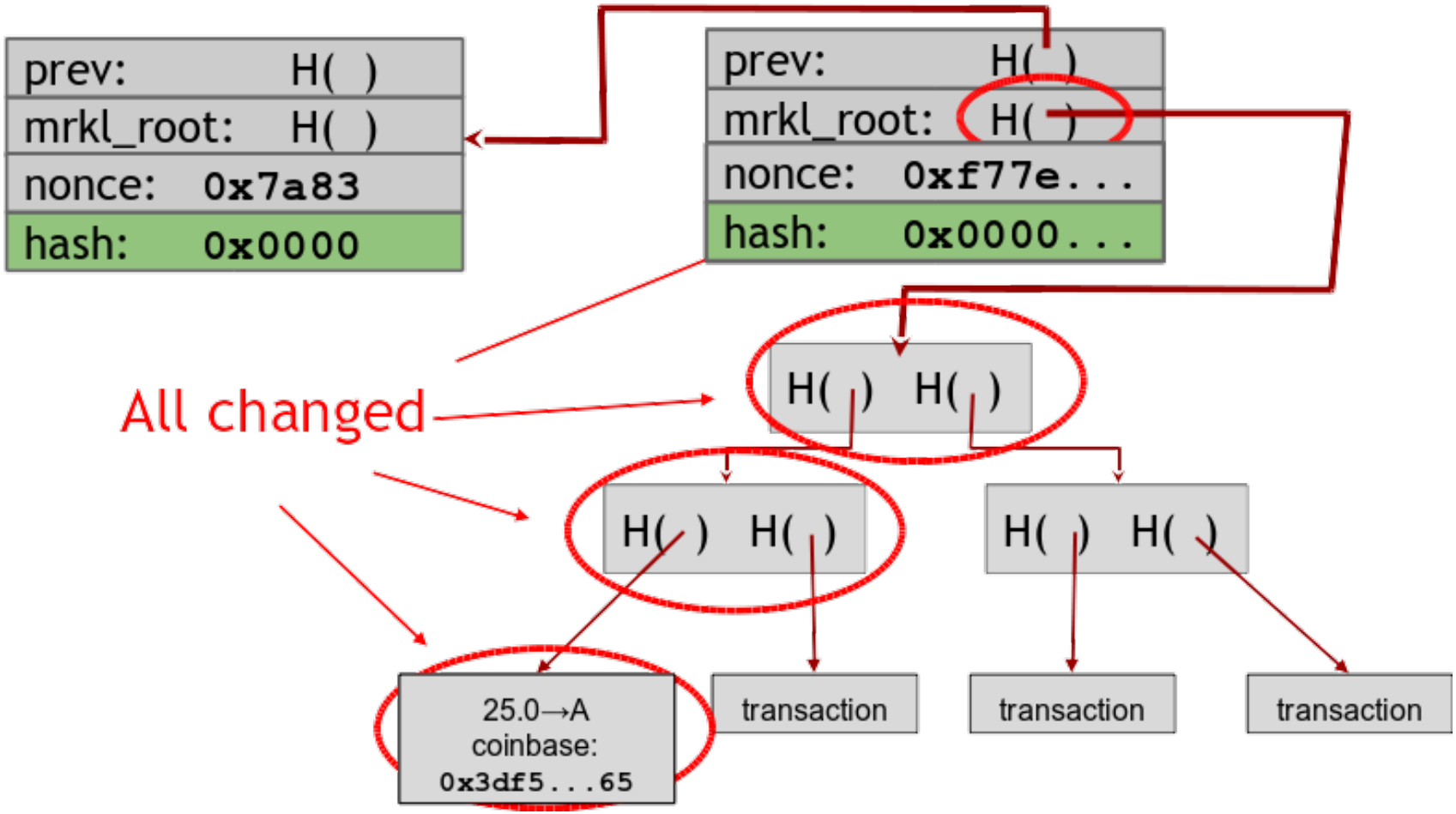
Nội dung

6 bước để đào Bitcoin

1. Lắng nghe các giao dịch trên mạng và kiểm tra tính hợp lệ của các giao dịch.
2. Duy trì blockchain và lắng nghe các Block mới. Kiểm tra tính hợp lệ của Block mới được đề xuất.
3. Nhóm các giao dịch để đưa vào Block. Phải đảm bảo các giao dịch trong Block là hợp lệ.
4. Tìm kiếm giá trị `nonce` để làm Block của mình hợp lệ.
5. Hy vọng rằng các miner khác chấp nhận Block của mình.
6. Profit!

Tìm Block hợp lệ

Tính cây Merkle và tìm nonce



80-byte block header

- 4 bytes: version
- 32 bytes: previous block hash
- 32 bytes: merkle tree of transactions
- 4 bytes: timestamp
- 4 bytes: difficulty target
- 4 bytes: nonce

Ví dụ

```
02000000 ........................... Block version: 2

b6ff0b1b1680a2862a30ca44d346d9e8
910d334beb48ca0c0000000000000000 ... Hash of previous block's header
9d10aa52ee949386ca9385695f04ede2
70dda20810decd12bc9b048aaab31471 ... Merkle root

24d95a54 ........................... Unix time: 1415239972
30c31b18 ........................... Target: 0x1bc330 * 256**(0x18-3)
fe9f0864 ........................... Nonce
```

Mức độ khó

- Miner phải tìm `nonce` thỏa mãn

$$\texttt{H}(\texttt{nonce} \mid \texttt{prev\_hash} \mid \texttt{tx} \mid \cdots \mid \texttt{tx}) < \texttt{target}.$$

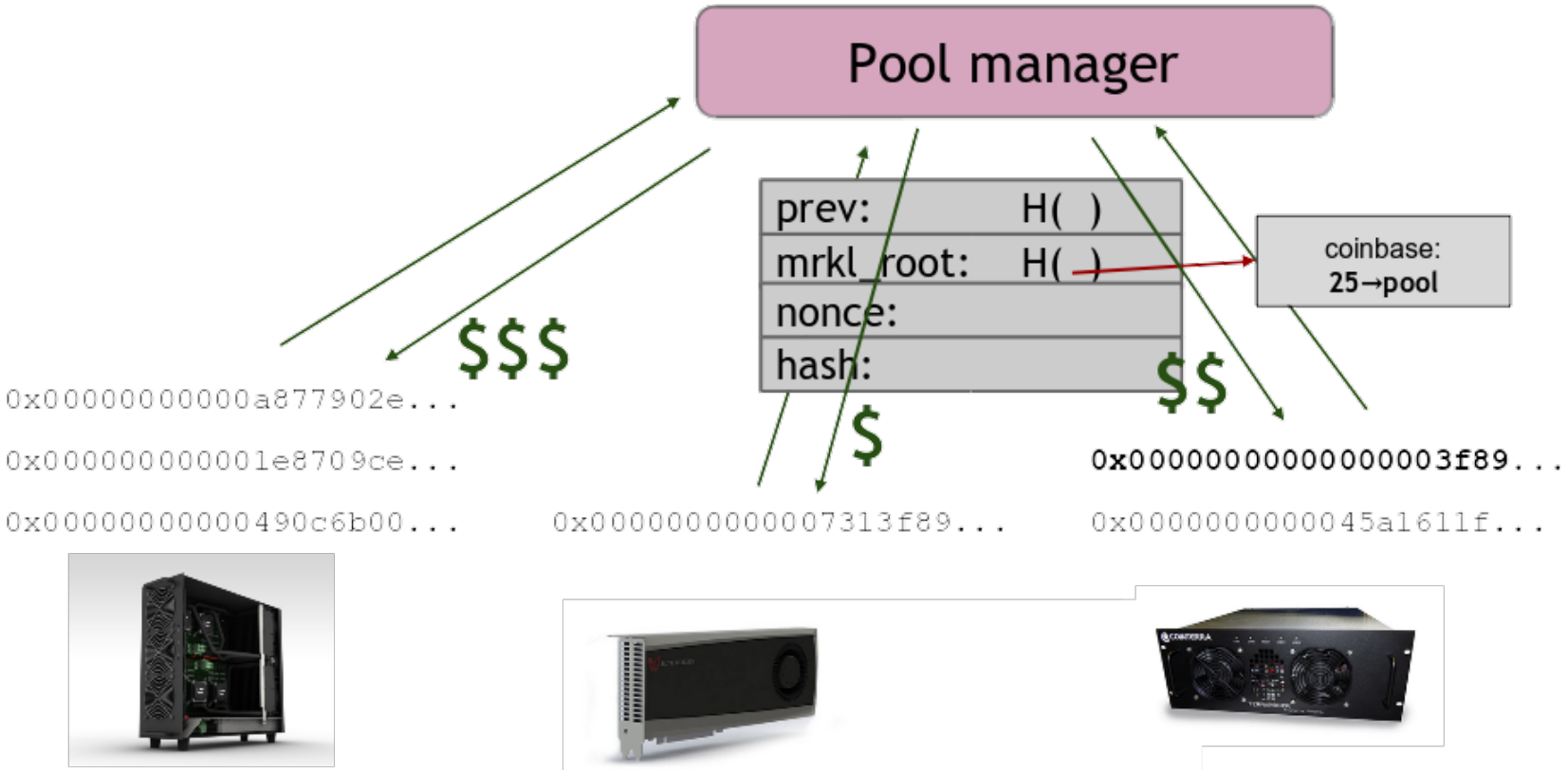
- Mức độ khó của `target` (theo hexa) tháng 8 năm 2015 là
  `0000000000000000172EC0000000000000000000000000000000000000000000`
  Tức là ta phải thử khoảng 2^{67} lần thì mới tìm được `nonce` hợp lệ.
- Mức độ khó được thay đổi sau mỗi 2016 Block theo công thức:

$$\text{next\_difficulty} = \frac{\text{previous\_difficulty} \times \overbrace{2016 \times 10 \text{ phút}}^{2 \text{ tuần}}}{\text{thời gian vừa đào } 2016 \text{ Block}}$$

CPU Mining

```
while (1){
  HDR[kNoncePos]++;
  if (SHA256(SHA256(HDR)) < target)
    return;
 }
```

Mining Pool



Hình: Nhiều người tham gia đào trên cùng một Block và được trả tiền theo số lượng Hash.

Một số địa chỉ có ích

- Khóa học Bitcoin and Cryptocurrency Technologies
  `https://www.coursera.org/learn/cryptocurrency`
- Live Blockchain
  `http://blockchain.mit.edu/blockchain/`
- Bitcoin Developer Guide
  `https://bitcoin.org/en/developer-guide`