# BÀI 9.
# BLOCKCHAIN

Bùi Trọng Tùng,
Viện Công nghệ thông tin và Truyền thông,
Đại học Bách khoa Hà Nội

1

1

## Nội dung

- Giới thiệu về Bitcoin và blockchain
- Ethereum và smart contract
- Tranh luận về blockchain

2

2

# Tiền điện tử

- Khái niệm "tiền điện tử" – "ecash" được giới thiệu lần đầu tiên bởi David Chaum năm 1983 trong bài báo "Blind Signatures For Untraceable Payments"
- Các yêu cầu chính đối với tiền điện tử:
  - Ẩn danh: Che giấu danh tính của người dùng
  - Xác thực: Được chứng thực là có giá trị
  - Chống phát lại: Không thể chi tiêu lần thứ 2
- Vì nhiều lý do khác nhau, phần lớn các đồng tiền điện tử chưa được chính phủ các nước thừa nhận hoặc chưa phổ biến trong thanh toán điện tử
- Các hình thức thanh toán điện tử phổ biến hiện nay:
  - POS – Point of Sale
  - Internet banking
  - Ví điện tử: Paypal, Momo, Zalopay, …

Phải liên kết với một tài khoản ngân hàng → Mô hình tập trung

3

3

# Bitcoin

- Bitcoin là đồng tiền điện tử được sáng lập bởi Nakamoto vào năm 2009 với mục tiêu tạo ra đồng tiền không bị phụ thuộc quản lý, điều hành của bất kỳ tổ chức nào
- Bitcoin tăng giá mạnh từ năm 2011, đạt đỉnh vào năm 2017 (1฿ = 19.666$)
- Kèm theo đó là hàng loạt bê bối:
  - Năm 2010, lỗ hổng bị khai thác dẫn đến 184 tỉ ฿ được sinh ra.
  - Năm 2013, chợ đen SilkRoad sử dụng bitcoin để thanh toán bị triệt phá
  - Năm 2014, sàn giao dịch bitcoin lớn nhất Mt.Gox tuyên bố phá sản
  - Liên tục bị cáo buộc gắn với các hoạt động rửa tiền

4

4

## Bitcoin

- Bitcoin thay thế được hệ thống ngân hàng nếu có thể giải quyết các bài toán cơ bản sau:
  - Thực hiện các giao dịch tiền tệ
  - Quản lý định danh: Đồng tiền thuộc về ai? Ai thực hiện giao dịch?
  - Chống lại hành vi tiêu lại số tiền đã tiêu
- Làm cách nào giải quyết các vấn đề trên bằng công cụ mật mã học?
- Chúng ta cùng thiết kế hệ thống Bitcoin để giải quyết các vấn đề trên

5

5

## Định danh người dùng

- Vấn đề: Cung cấp định danh "mật mã" cho người dùng như thế nào?
  - Không thể làm giả định danh
  - Định danh được chứng thực bởi bên thứ 3 tin cậy
  - Chống từ chối
- Giải quyết:

6

6

# Thực hiện giao dịch

- Nội dung giao dịch: Alice chuyển 10Ƀ cho Bob
- Vấn đề 1: Làm cách nào xác thực được giao dịch do Alice thực hiện?
  - Giải quyết
- Vấn đề 2: Alice có thể tiêu một số tiền nhiều lần (aka. tiêu bao nhiêu tiền là tùy ý)
  - Giải quyết
- Vấn đề 3: Kiểm tra tính tin cậy của giao dịch

7

7

# Bitcoin

- Sử dụng thuật toán Elliptic Curve Digital Signature Algorithm
- Mỗi tài khoản người dùng có 1 cặp khóa
  - Khóa cá nhân($K_R$): 32 byte
  - Khóa công khai($K_U$): 65 byte
- Địa chỉ giao dịch:
  - Bước 1: Băm khóa công khai: RIPEMD-160(SHA-256($K_U$))
  - Bước 2: Thêm checksum
  - Bước 3: Biểu diễn bằng mã Base58

8

8

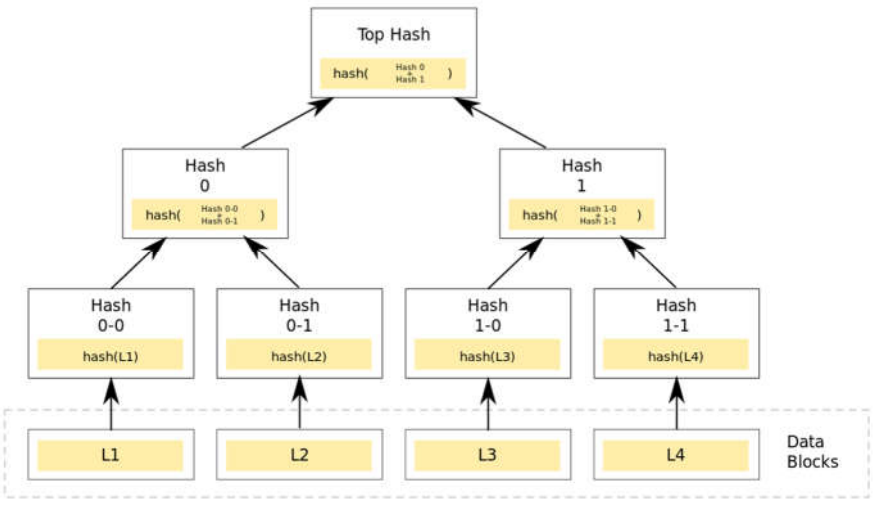
# Blockchain

- Chuỗi các giao dịch sử dụng các giá trị băm để kiểm tra toàn vẹn
- Mỗi giao dịch chữa mã băm của giao dịch trước
- Nhận xét: Khi mã băm trong một giao dịch được xác định là đáng tin cậy thì có thể kiểm tra tính toàn vẹn của mọi giao dịch trước đó.
- Cải thiện hiệu năng: mỗi khối chứa thông tin của nhiều giao dịch.
  - Lưu trữ và kiểm tra mã băm của mỗi giao dịch: cây Merkle

9

9

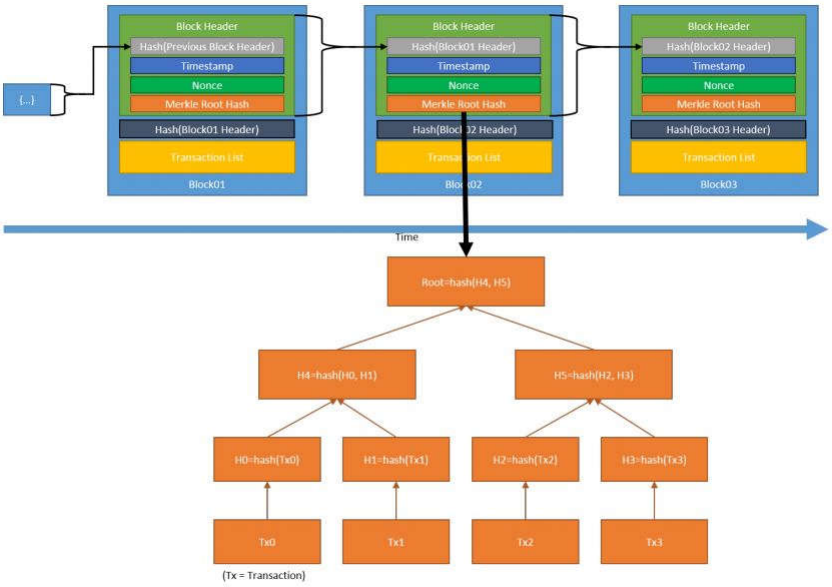
# Cây Merkle




10

10

# Blockchain trong Bitcoin




I1

11

# Xây dựng sổ cái

- Mô hình: P2P
- Mọi nút lưu trữ toàn bộ blockchain
- Một nút muốn tạo giao dịch cần quảng bá giao dịch tới mọi nút khác
- Mỗi nút kiểm tra giao dịch nhận được và tạo khối mới để thêm vào chuỗi
- Vấn đề 1: Có những nút không nhận được giao dịch
- Vấn đề 2: Có những nút gian lận

→ Sử dụng giao thức đồng thuận (consensus protocol)

12

12

# Giao thức đồng thuận

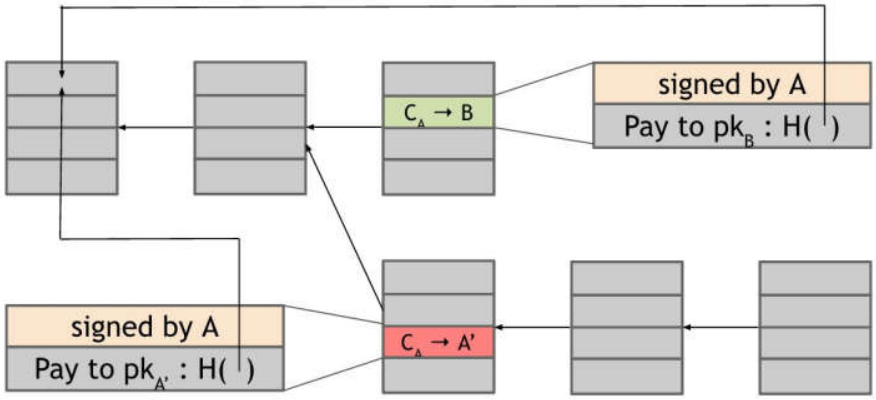
- Các giao dịch mới được phát quảng bá tới mọi nút
- Mỗi nút tập hợp một số giao dịch mới vào trong một block
- Trong mỗi vòng, một nút ***ngẫu nhiên*** phải phát quảng bá block mà nó tạo ra
- Các nút khác chấp nhận block nếu mọi giao dịch trong block này là hợp lệ (chưa được tiêu, chữ ký hợp lệ)
- Các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

13

13

# Chi tiêu 2 lần

- Double-spend attack




14

14

# Giao thức đồng thuận

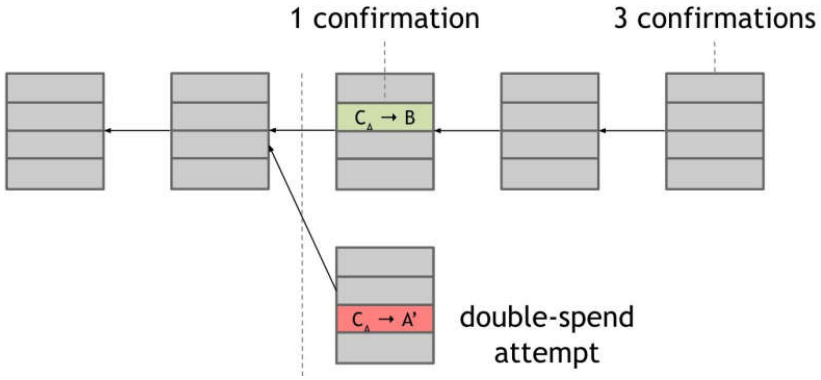
- Gian lận chi tiêu 2 lần (và một số tình huống tương tự) có thể dẫn đến chia nhánh trong blockchain
  - Một nhánh dừng phát triển khi giao dịch gian lận trong nhánh đó bị phát hiện
- Vấn đề: Nhánh nào được chấp thuận?
- Giải quyết:
- Vấn đề: Giao thức đồng thuận sụp đổ nếu ai đó nắm được quyền điều khiển >50% số nút trong mạng (Sybil attack)
- Vấn đề: Làm cách nào để biết rằng nút được chọn hành xử trung thực?
- Giải quyết:

15

15

# Tự bảo vệ trước gian lận chi tiêu 2 lần

- Đợi cho đến khi khối chứa giao dịch được chấp nhận qua n lần(Bitcoin chấp thuận n = 6)




16

16

## PoW - Chọn nút tạo block

- Ý tưởng: Yêu cầu các nút thực hiện một công việc nào đó. Nếu nút nào hoàn thành xong trước, nút đó được quyền tạo block.
  - Thực hiện công việc: tốn nhiều thời gian + tài nguyên
  - Kiểm tra kết quả: dễ dàng
- Bitcoin: tìm một số sao cho giá trị băm của số đó bắt đầu bằng N bit 0
  - N: Độ khó của bài toán
  - Thực hiện công việc: băm $2^N$ giá trị
  - Kiểm tra kết quả: băm 1 lần

17

17

## PoW - Chọn nút tạo block

- PoW khiến cho nút gian lận phải tốn rất nhiều chi phí để giả mạo giao dịch
- Nhưng đồng thời, không nút nào giải bài toán nếu không có lợi ích
- Bitcoin: phần thưởng cho nút tạo được block
  - Cố định: hiện tại là 12.5Ƀ/ 1 block. Giảm một nửa sau mỗi 4 năm.
  - Phí giao dịch: tùy thuộc người thực hiện giao dịch

  → "đào coin"
  - Phần thưởng chỉ được chi trả khi nhánh đó được chấp nhận

18

18

## Một số vấn đề khác

- Lan truyền thông tin trong mạng P2P tiêu tốn rất nhiều băng thông
- Giao dịch rác
- Khi chi phí đào > phần thưởng, Bitcoin sẽ dừng hoạt động
- Bitcoin có thực sự ẩn danh?

19

19

## Tranh cãi liên quan đến bitcoin

- Sử dụng cho các hoạt động tội phạm
- Tiêu tốn năng lượng
- Rủi ro tài chính

20

20

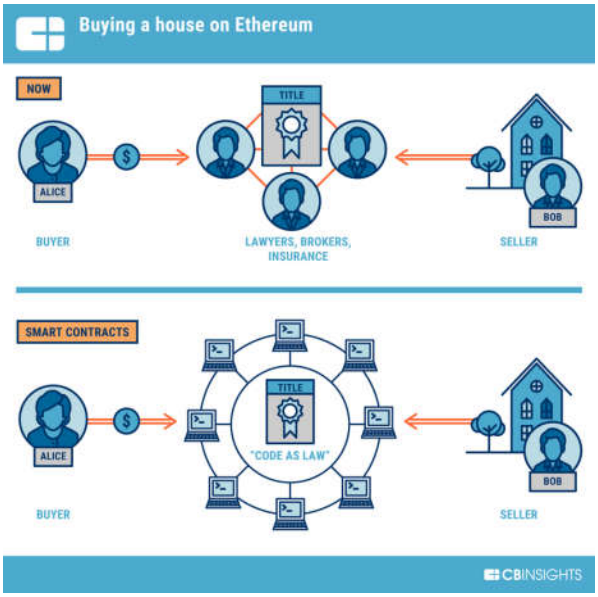
# Etherium và smart contract

- Bitcoin giới hiệu khái niệm về “blockchain” ứng dụng cho giao dịch tiền tệ
  - Sử dụng ngôn ngữ script với tập lệnh và cú pháp hạn chế
- Thực tế blockchain có tiềm năng lớn hơn
  - Nội dung block có thể chứa các đoạn mã thực thi
- Năm 2015, đồng tiền Ethereum ra đời
  - Ứng dụng blockchain xây dựng hợp đồng thông minh (smart contract) → blockchain 2.0
  - Khái niệm “smart contract” được giới thiệu năm 1994: bản thỏa thuận giữa các bên với các điều khoản được thực hiện tự động bởi chương trình máy tính.

21

21

# Một ví dụ về hợp đồng thông minh




22

22

# Ethereum

- Hợp đồng thông minh được xây dựng bằng các ngôn ngữ kịch bản giống Javascript
- Thực thi hợp đồng thông minh trong máy ảo EVM để tạo thành EVM bytecode
- EVM bytecode được gửi lên mạng Ethereum để chờ đưa vào blockchain. Để hợp đồng được xử lý và công nhận, người dùng phải trả phí bằng gas.
- Hệ thống Ethereum từng xuất hiện lỗ hổng dẫn đến 50 triệu $ bị đánh cắp
  - Tấn công tái sinh (reentrancy attack)
  - Sự kiện dẫn đến sự phân tách thành Ethereum và Ethereum Classic

23

23

# Vấn đề của smart contract

- Smart contract được xây dựng bằng ngôn ngữ lập trình → có thể xuất hiện rất nhiều lỗ hổng trong smart contract
- https://consensys.github.io/smart-contract-best-practices/known_attacks/

24

24

# Thảo luận



25