What is Blockchain?

Dang Quang Vu

December 26, 2022

Contents

1 State

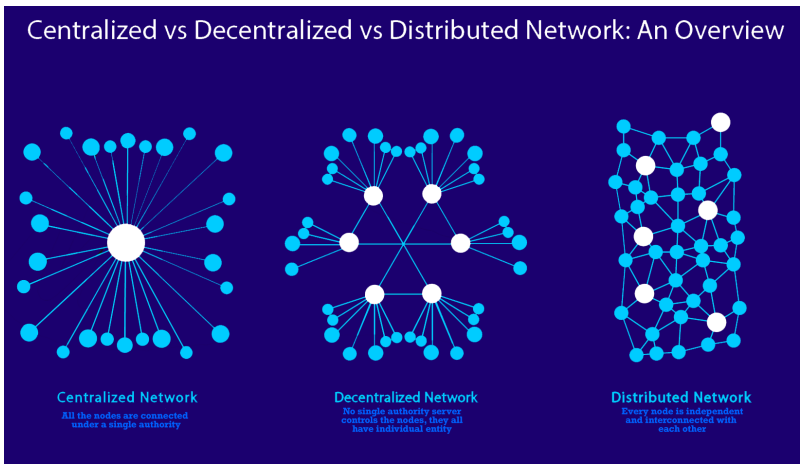
- State (trạng thái) - Là 1 cách để máy tính lưu trữ dữ liệu và thay đổi dữ liệu đó.

  X=0 -> X=1

- program state
- Examples: Version Control
  - Các Version là 1 state
  - Các step Version chuyển đổi thì được gọi là transaction

2 Decentralized Environment

- Là hệ thống phi tập trung!
- Vậy câu hỏi đặt ra ở đây:
  - Ai sẽ là người quyết định sự thay đổi của 1 state?
  - Những người ra vào hệ thống sẽ làm gì?
  - Khi có 2 người cùng đưa ra quyết định cùng 1 lúc thì làm gì?



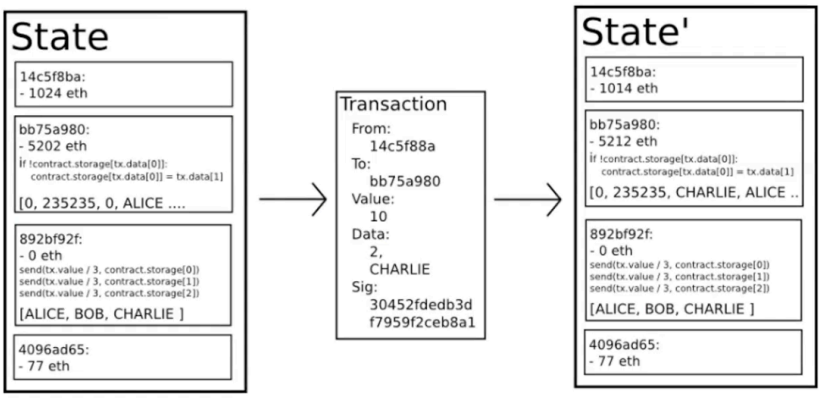
3 Decentralized Features

- Level of Decentralization
  - Các nhiệm vụ khác nhau của các `Participants`
- Bảo Mật
  - Single failure tolerance
  - Availability
  - => Problem Security
- Hiệu xuất
  - Sự đồng ý của toàn bộ các participants để đồng thuận.
  - Vấn đề về truyền tải dữ liệu, thông điệp hoặc giao tiếp của các participants

4 Blockchain Concepts

- A hệ thống chia sẽ dữ liệu trong một môi trường phi tập trung `decentralized`
- Blockchain require
  - `Immutability` - Tính Bất Biến
  - `Transparency` - Tính Minh Bạch

5 State Machine



6 What is Blockchain?

- Danh sách liên kết của các block - một block sẽ chứa 1 lượng thông tin nhất định
- Các thành viên trong hệ thông blockchain sẽ cùng nhau chia sẻ 1 lượng dữ liệu cùng nhau để tạo ra 1 loại dữ liệu duy nhất.
- `các dữ liệu sẽ được công khai, và có tính chất append-only`

7 Blockchain Types

- Permissionless Blockchain
  - Any one can access freely
  - Any one can read

  - Examples: Bitcoin - Ethereum

- Permissoned blockchain
  - Participants need permisson for accessing
  - Readers need permission
  - Examples: HyperLedger Fabric, Corda

- Consortium Blockchaim
  - Participants needs permission for accessing
  - Any one can read
  - Examples: Ripple

8 Thành phần của 1 Blockchain

- Consensus - Proof of Work / 1994 - Thresholded PoS
- Network model
- Data model
- Cryptographic schemes
- Decentralized Model

9 Consensus - Cơ chế đồng thuận

- Nhiệm Vụ Chính
  - Sắp xếp các transactions
  - Đồng thuận cho 1 sự thay đổi mới.
  - Xác thực các transactions.
  - Làm thế nào để tránh được sự sai lệch, hiểu lầm giữa các thành viên trong hệ thống.

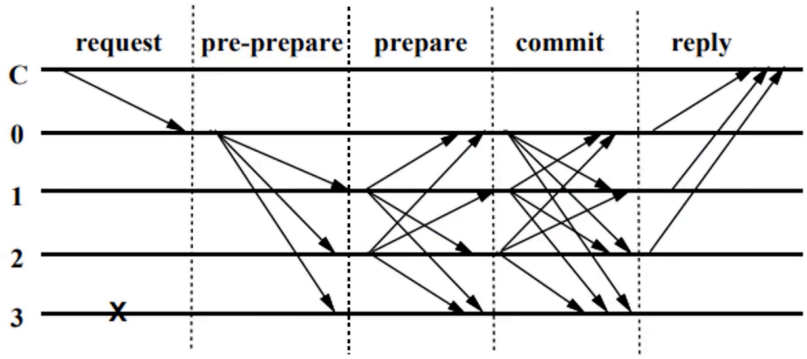
- `2 đề xuất đầu tiên` xuất bản `1999`
  - "Practical Byzantine Fault Tolerance" solution for "Byzantine Generals' Problem" aka arbitrary failure
  - "Proof of Work" - Mục đích tránh spam trong việc gửi Email.

- Types
  - `Permissionless` - Public Blockchain
  - `Permissioned` - Private Blockchain
- Properties
  - Safety - Tránh được sự sung đột khi 2 hoặc nhiều block được xác thực tại cùng 1 thời điểm.
  - Liveness - Tránh được việc sung đột giữa nhiều các participants không đồng thuận tại cùng 1 thời điểm.
- Consensus Types
  - Proof-of-X
    - Permissionless blockchain
    - Requires a proof to participant
    - Example: Proof-of-Work, Stake, Authority, Space Time
  - Practical Byzantine Fault Tolerance - `Schedule Solution`
  - Federated Consensus (2014) - Stellar - Ripper

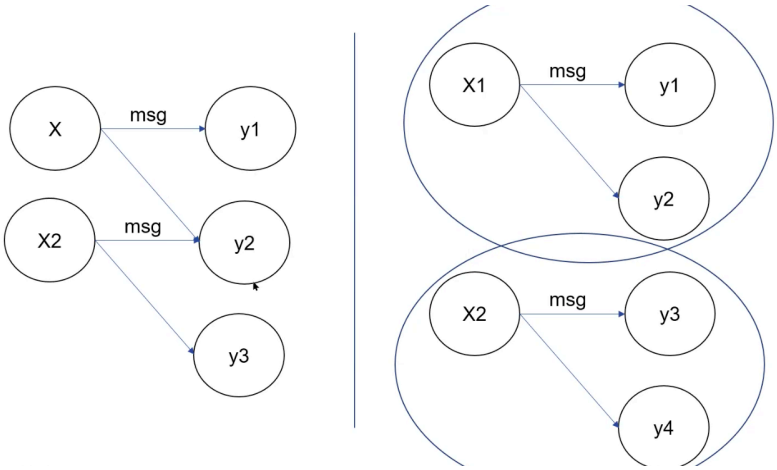
10 Blockchain Consensus Procedure

- Leader finding - Làm sao để tìm ra người đề xuất cái block và đồng ý với cái block đó.
- Propagation of block candidate (Broadcast) - Làm sao để đưa được cái block này đến với các thành viên khác.
- Verification - Block Validation
- Branch - Làm sao để lựa chọn các branch (Fork)
  - Concepts
    - `Longest`
    - `Most focus`
- Incentive - Khuyến khích trả thưởng.

11 Practical Byzantine Fault Tolerance



12 Federated Consensus



13 Network Model

- Synchronous
- Asynchronous
- Partial Synchronous

Synchronous, Asynchronous and Partial Synchronous

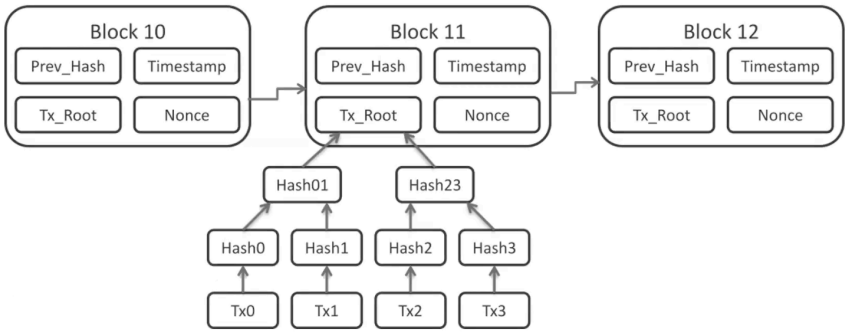
14 State Model | Delta Model

- Blockchain Scan
- Upspent transaction output (UTXO) and extension to eUTXO
  - 1 Transaction sẽ có nhiều inputs và nhiều outputs
  - Phù hợp với các ứng dụng không có nhiều sự tính toán phức tạp.
- Account
  - Lưu trữ dữ liệu vào tài khoản
  - Phù hợp với ứng dụng có nhiều sự đa dạng trong tính toán.
- Key-value

15 Cryptography Schemes

- Hashing - Bảo vệ sự toàn diện của dữ liệu
- Asymmetric key - Mã hoá signature
- Merkle tree
- Zero-knowledge proof
  - zk-STARKs
  - zk-SNARKs
  - zk-EVM

16 Block, transaction's structure

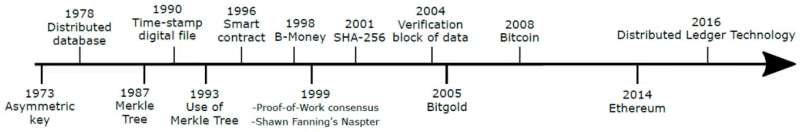


Bitcoin: blockchain structure

```
echo "My Name i's Dang Quang Vu " | sha256sum
```

17 Cryptocurrency

17.1 TimeLine



Timeline of the technologies contributing to blockchain

18 Blockchain Use Cases

19 Layer

Layer-2: Application & Scalable Solution
Layer-1: Virtual Machine - Contract execution
Layer-0: Accounting - Settlement
HardWare

20 Transportation

- Mobility-as-a-Service
- Decision-making ability in Autonomous Driving

21 Health

- Monitoring Patients
- Electronic Health Record
- Drug traceability

22 E-government

- E-Voting
- Centralized bank digital currency
- Identity

23 Security

- Domain name system
- Public key infrastructure
- Log Event Storage

24 Mobile Network - 5G, 6G

- Spectrum sharing
- Edge Computing

25 Web3

- KeyWords
  - Decentralized Web

  - Blockchain Technology
  - Token usage
  - Expection
    * Security
    * Scalability
    * Privacy

26 Web3 Is

- Decentralization / Federated Platform - Tính phi tập trung
- Interoperatbility - Tính tương tác
- Verifiable computing via blockchains

27 NFTs

- non-Fungible Tokens (NFT) - A Financial security
- Metaverse

28 Some Features Technology

- Social Recovery Wallet