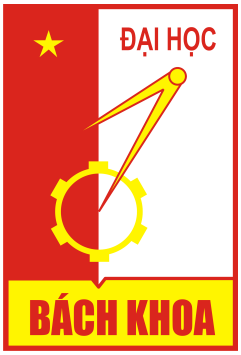
TRƯỜNG ĐẠI HỌC BÁCH KHOA HÀ NỘI
VIỆN CÔNG NGHỆ THÔNG TIN VÀ TRUYỀN THÔNG

———————— * ————————



BÁO CÁO MÔN HỌC

TÍNH TOÁN PHÂN TÁN

Sinh viên thực hiện : **Nguyễn Bình Minh**

MSSV : **20152453**

GV hướng dẫn : **TS. Đào Thành Chung**

HÀ NỘI
Ngày 15 tháng 12 năm 2018

Mục lục

1 Cơ chế đồng thuận

Cơ chế đồng thuận Proof-of-Stake Voting (PoSV) là giao thức Proof-of-Stake (PoS) cơ bản với cơ chế bỏ phiếu công bằng

2 Kiến trúc TomoChain

Kiến trúc chuỗi TomoChain duy trì một tập các masternodes trong sự nhất quán thông qua giao thức đồng thuận TomoChain.

- Coin-holder (người nắm giữ TOMO) phải giữ ít nhất 1 lượng coin tối thiểu được yêu cầu để trở thành masternode.
- Các ứng viên sẽ nhận phiếu bầu từ phía coin-holder.
- Những ứng viên nhận được nhiều phiếu bầu nhất sẽ được lựa chọn trở thành Masternodes.
- Việc tạo block sẽ được xoay vòng và luân chuyển đi kèm với cơ chế đồng thuận hai lớp.
- Masternode sau khi tiến hành việc tạo và xác thực block sẽ được nhận thưởng.

TomoChain với kĩ thuật mới gọi là Double Validation với cơ chế Randomization. Kĩ thuật mới này làm giảm đáng kể xác suất có chuỗi không hợp lệ trong blockchain.

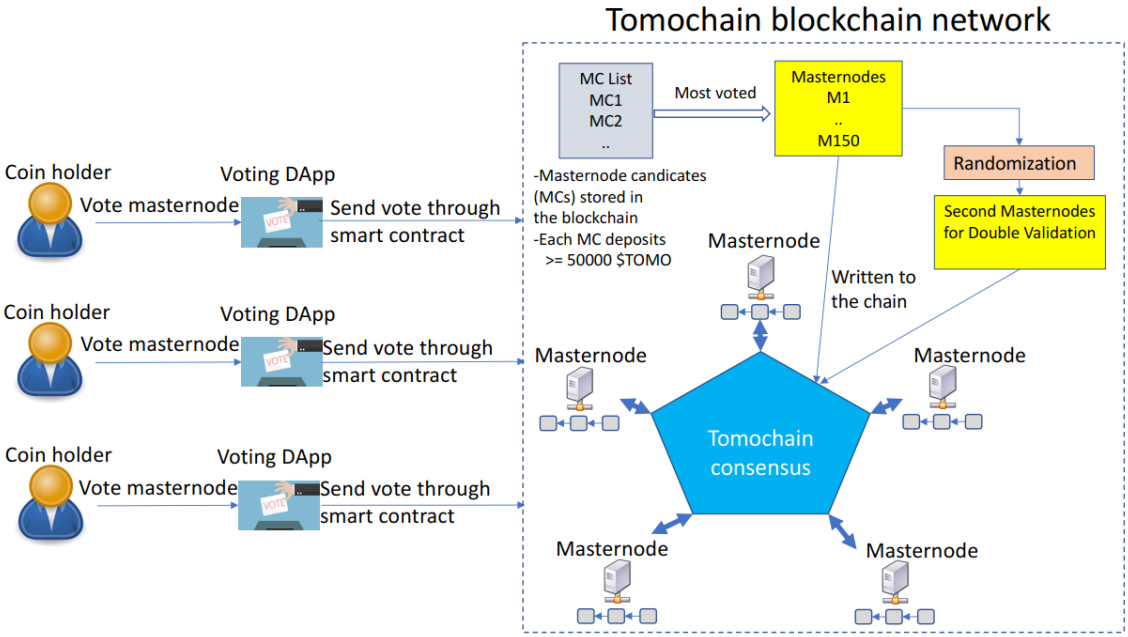
3 Election Leader

3.1 Coin-holders, Masternodes

Coin-holder là những người dùng join vào mạng , mà sở hữu và chuyển giao TOMO.

Masternodes là fullnodes mà duy trì một bản copy của blockchain, tạo những blocks và giữ cho chuỗi nhất quán. Masternodes được chọn thông qua hệ thống bầu cử.

- Yêu cầu đặt cọc để trở thành một ứng viên chạy masternode là 50.000 TOMO
- Những ứng cử viên này sẽ được liệt kê trên Voting DApp, cho coin-holders bầu họ bằng cách gửi TOMO tới smart contract.



3.2 Bầu chọn (Voting)

Những masternode làm việc chăm chỉ để tạo và xác nhận khối trong hệ thống sẽ được khuyến khích bằng việc tặng TOMO. Hơn nữa, những người nắm giữ token mà bầu chọn cho các masternode này cũng sẽ nhận TOMO theo tỷ lệ lượng TOMO mà họ đã đầu tư cho các masternode qua việc bầu chọn. Các kỹ sư của TomoChain có nhiệm vụ thiết kế ra một cơ chế thưởng công bằng, minh bạch, tự động và dễ tính toán.

Việc bầu chọn được coi như lượng đầu tư của họ cho những masternode họ ủng hộ. Hay một chiến lược bầu chọn giúp tối đa lợi nhuận của họ. Do đó, masternodes luôn phải chạy đua để có vị trí tốt hơn.

Danh sách các ứng viên masternode sẽ được chọn lọc liên tục dựa vào lượng token bầu chọn. Hiệu quả hoạt động của các masternode sẽ được theo dõi và báo cáo ngược lại cho những người nắm giữ token theo 3 thông số sau: CPU, bộ nhớ và số khối được kí thể hiện hiệu suất của họ. Khối được kí cuối cùng cũng chỉ ra hoạt động cuối cùng của một masternode. Có tối đa 150 ứng viên được chọn để trở thành masternode.

3.3 Cơ chế thưởng (Reward Mechanism)

Mỗi epoch bao gồm 900 khối, tương đương với phần thưởng là 250 TOMO trong hai năm đầu tiên. Lượng 250 TOMO này sẽ được chia cho tất cả các masternode theo tỷ lệ số chữ kí mà họ kí trong một epoch. Sau đó, phần thưởng kiếm được bởi mỗi masternode sẽ được chia thành 3 phần:

- Phần thưởng cho cơ sở hạ tầng: 40 %, sẽ được chuyển cho người sở hữu masternode.
- Phần thưởng staking: 50 % sẽ được chuyển cho nhóm những người bầu chọn cho masternode.
- Phần thưởng cho tổ chức sáng lập: 10 % còn lại được kiểm soát bởi tổ chức sáng lập của Masternode (TomoChain)

4 TomoChain Consensus Protocol

4.1 Double Validation Process

Xác thực hai lớp trong TomoChain yêu cầu chữ ký của 2 masternode trong một block để có thể thêm vào blockchain là **block creator** (block producer) và **block verifier** chọn ngẫu nhiên trong các masternode được đã bầu.

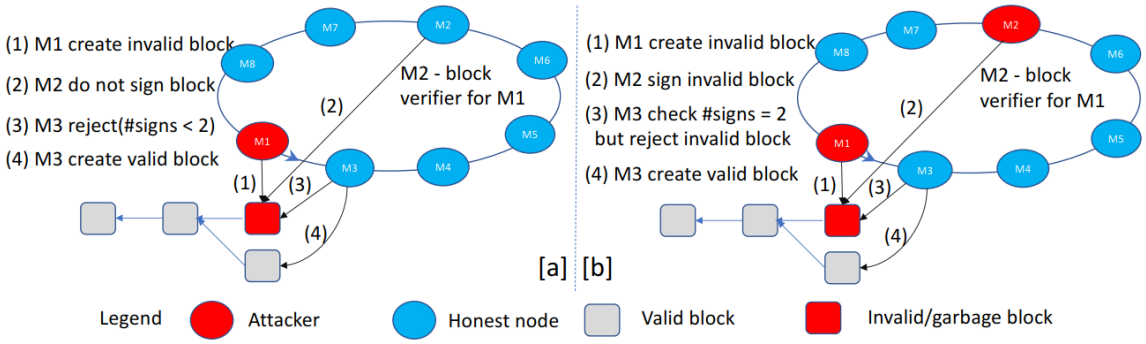


Fig. 3. Double Validation (DV): (a) DV with block creator as an attacker and (b) DV with both block creator and block verifier as attackers

Nếu M2 là kẻ tấn công bắt tay với M1 kí (sign) block100 mặc dù nó là invalid

- Single validation: M2 sau đó tạo block101 là valid, M3 sẽ kí block101 . Khi đó phải 'rebase' để khôi phục tính hợp lệ của blockchain
- Double validation: M3 lúc này sẽ từ chối (reject) block101 do không đủ 2 chữ kí

4.2 Algorithm

Một số kí hiệu và định nghĩa

- Mỗi epoch gồm n (900) block slot,mỗi slot chỉ được tạo 1 block: $e_1 <- \{ sl_1, sl_2, ... , sl_n \}$
- Có tập gồm m (150) masternotes tương tác thông qua giao thức để đạt sự thống nhất: $VC <- \{ V_1, V_2, ... , V_m \}$
- Mỗi masternode V_i có một cặp public/private key (pk_i, sk_i) và giả sử đều biết public key của những node khác.
- Block B_j tạo tại slot sl_i gồm state st_i = Hash(B_{j-1}) , dữ liệu d , chữ ký $Sign_{sk_i}$ (st, d, sl_i)

Algorithm 1: Algorithm illustrated the consensus protocol

Input: m - Number of masternodes, n number of slots in an epoch

Output: The ledger of the blockchain C

begin

Create the empty blockchain (stack) C;
Initiate ICO; coinholders;
Voting for the masternode committee (master nodes) $VC \leftarrow \{V_1; V_2; ..., V_m\}$;
Initiate the first epoch $e_1 \leftarrow \{sl_1, sl_2, ..., sl_n\}$;
Randomly generate the array of second masternodes for the first epoch $SV_1 \leftarrow [v^1_{2.1}, v^1_{2.2}, ..., v^1_{2.n}]$;
Create the genesis block B_0;
Update the blockchain $C \leftarrow C.push(B_0)$;
while true **do**
  while j is less than n **do**
    Create block B_j by the first masternode;
    Update the blockchain $C \leftarrow C.push(B_j)$;
    Validate the block B_j by the second masternode;
    Broadcast and validate the block B_j by VC_i;
    if B_j has more than 3/4 masternode committee members sign **then**
      FINALITY($B_j.ID$) = true;
    if j = n **then**
      $j \leftarrow 1$;
    else
      j++;
  if len(C) mod n = 0 **then**
    doCheckpoint();
    Voting for the masternode committee for the next epoch $VC \leftarrow \{V_1; V_2; ..., V_m\}$;
    Random generate the array of verifier masternodes for the next epoch $(i+1)^{th}$;
    $SV_{i+1} \leftarrow [v^{i+1}_{2.1}, v^{i+1}_{2.2}, ..., v^{i+1}_{2.n}]$;
    $e_{i+1} \leftarrow i * n * 2 + e_1$;
    i++;

4.3 Sharding

Thay vì từng masternode lưu trữ tất cả blockchain, thì từng node chỉ cần lưu trữ một phần của nó. TomoChain sử dụng 150 masternodes để tạo blocks và bảo mật mạng. Mỗi epoch, ngẫu nhiên chia 10-15 masternode mỗi shard. Consensus Smart Contracts:

- Voting Smart Contract
- Block Signer Smart Contract

Có một root chain tương tác với shard chain. Root chain được sử dụng chủ yếu để đảm bảo giao dịch trong từng shard nhưng không lưu trữ chi tiết giao dịch. Block tạo ra được công nhận nếu 3/4 trong tổng số masternode trong shard đó xác minh và kí trên đó.

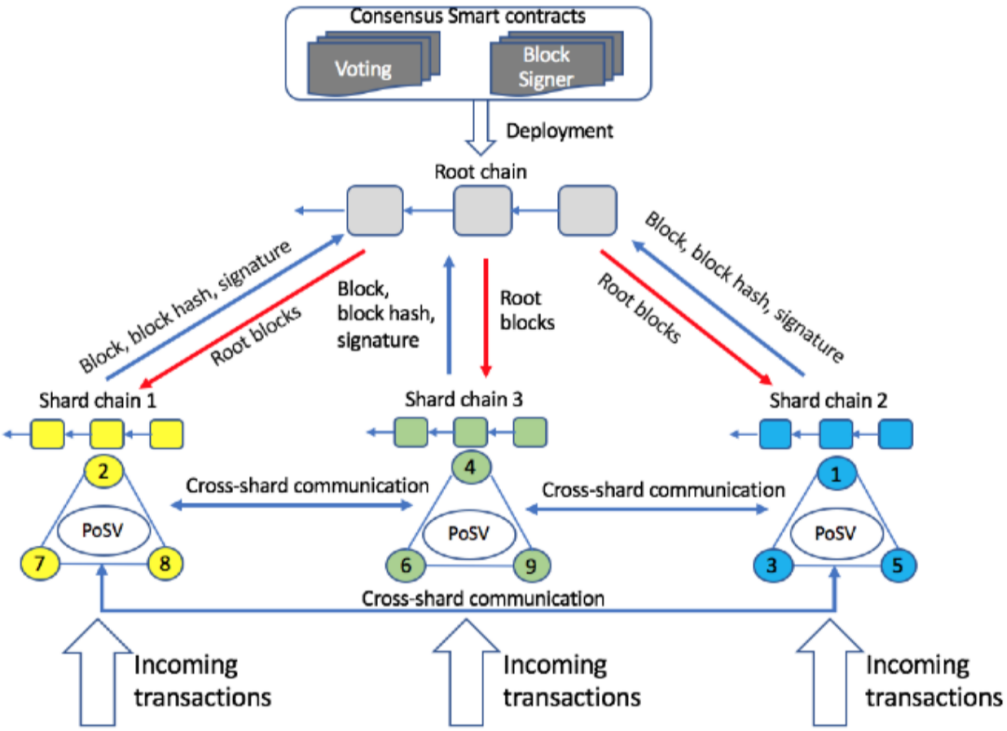


Figure 1: The proposed sharding architecture solution