



Proof of Stake là gì?



Nội dung



1. Proof of Stake là gì?
2. Cách hoạt động của Proof of Stake?
3. Đặc điểm của Proof of Stake là gì?
4. So sánh Proof of Stake với Proof of Work

1. Proof of Stake là gì?



Proof of Stake (bằng chứng cổ phần) là một thuật toán làm việc của Blockchain. PoS cho phép người dùng kiếm được phần thưởng cho việc xác thực các khối trên blockchain

Có thể hiểu nôm na là người dùng sẽ ký gửi một lượng tài sản nhất định để trở thành Validator (người xác thực) của Blockchain.

Không giống như Proof of Work (được sử dụng bởi Bitcoin), người dùng không cần

phần cứng mining đắt tiền hoặc lượng điện lớn. Thay vào đó, mạng lưới lựa **chọn các cá nhân để validate các block** dựa trên lượng coin mà họ sở hữu.

Lượng coin sở hữu càng cao, người dùng càng có nhiều khả năng được chọn để validate.

1. Proof of Stake là gì?

Các Validator này sẽ xác minh các giao dịch trên mạng lưới, gửi bằng chứng vào khối. Nếu đúng, các Validator sẽ được nhận thưởng là lạm phát của Blockchain, hoặc phí giao dịch thu về. Nếu sai, họ sẽ chịu phạt là mất đi tất cả, hoặc một lượng tài sản đã ký gửi.



2. Cách Proof of Stake hoạt động

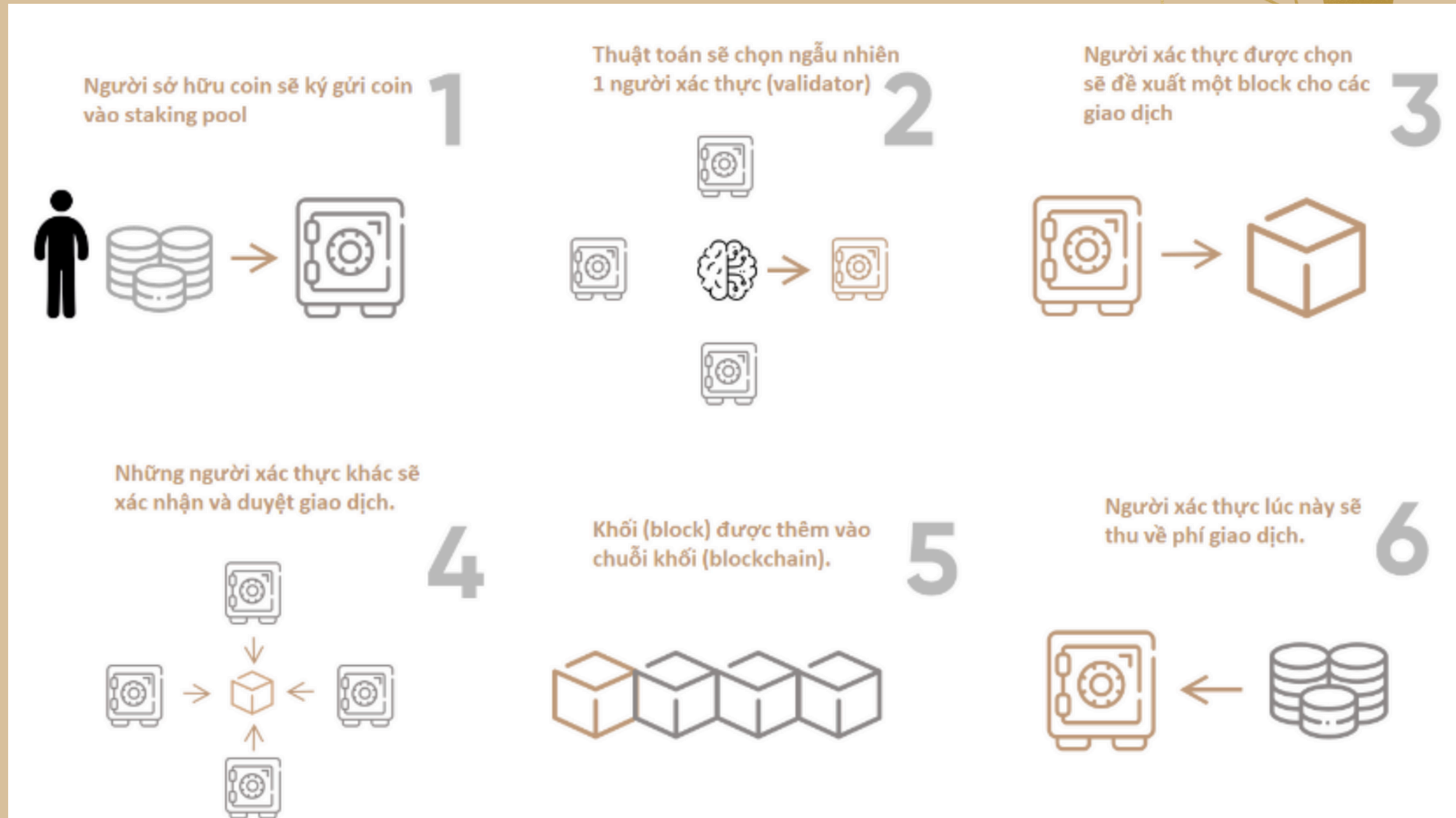


Với PoS, người dùng có thể xác thực các giao dịch để đổi lấy phần thưởng. Số lượng phần thưởng tỷ lệ thuận với số token mà người dùng nắm giữ. Có nhiều cách để thực hiện PoS, nhưng phương pháp phổ biến nhất là "Bằng chứng cổ phần được ủy quyền" (DPoS).

Với DPoS, người dùng bỏ phiếu cho validator, validator này sau đó sẽ chịu trách nhiệm xác minh các giao dịch và cam kết chúng với blockchain. Validator được thưởng phí giao dịch và họ cũng phải có một lượng token nhất định để đạt điều kiện cho vị trí của mình.

Hệ thống này được thiết kế để ngăn chặn sự tập trung hóa, vì những người xác nhận được cộng đồng lựa chọn thay vì được chỉ định bởi một thực thể duy nhất. Điều đó cũng có nghĩa là người dùng có thể kiếm được phần thưởng ngay cả khi họ không nắm giữ một số lượng lớn token, vì họ có thể chỉ cần ủy thác phiếu bầu của mình cho validator.

2. Cách Proof of Stake hoạt động



3. Đặc điểm của Proof of Stake là gì?



Ưu điểm

- Không đòi hỏi máy cấu hình cao, bất kỳ ai cũng có thể thiết lập các node
- chuyên biệt trên máy tính hoặc serve (máy chủ) của riêng mình.
- Đôi khi có thể Delegate (ủy quyền) cho Validator, nghĩa là người dùng gửi
- coin cho Validator để họ có thêm quyền vote, đổi lại người gửi cũng nhận
- được một phần phần thưởng mà không phải làm gì.
- Tăng khả năng mở rộng và tốc độ giao dịch, cải thiện tính phân quyền vì việc
- validate có thể được thực hiện bởi bất cứ ai stake token trong mạng, tạo ra
- một mạng lưới phi tập trung.
- Proof of Stake tiết kiệm môi trường hơn, không đòi hỏi tiêu thụ nhiều điện
- để hoạt động như Proof of Work (Bitcoin chẳng hạn).

3. Đặc điểm của Proof of Stake là gì?



Nhược điểm

- Khi ủy quyền hoặc làm Validator, thì người dùng sẽ được thêm số lượng
- coin, nhưng sẽ bị giam vốn, hoặc đôi khi bị mất giá coin và số lượng bù vào
- cũng không đủ hòa vốn.
- Sẽ có trường hợp unlock cần phải đợi một khoảng thời gian, có thể là 1 tuần,
- hay 2 tuần... Điều này sẽ làm người dùng trở tay không kịp khi giá coin điều
- chỉnh.
- Việc khóa token này liên quan đến quản trị, do đó, ai khóa càng nhiều token
- thì tiếng nói của người đó sẽ có trọng lượng hơn, đó chính là lý do vì sao
- Validator cũng cần người dùng ủy thác token cho họ. Điều này dẫn đến
- trường hợp Blockchain mang tính tập trung: Một số ít người có quyền hạn
- quá lớn, dự án phải làm theo họ, đôi khi có những ý kiến không mang lợi ích
- gì cho dự án nhưng vẫn phải làm.

4. So sánh Proof of Stake với Proof of Work

	Proof of Work (PoW)	Proof of Stake (PoS)
Khai thác	Sức mạnh tính toán càng cao, xác suất khai thác một khối càng cao.	Càng stake nhiều tiền, bạn càng có nhiều khả năng được xác thực một khối mới
Làm thế nào một khối được khai thác/xác thực?	Các thợ đào cạnh tranh để giải các câu đố toán học phức tạp	Thông thường, thuật toán sẽ xác định người chiến thắng một cách ngẫu nhiên hoặc dựa trên số lượng tiền đã stake.
Thiết bị khai thác	Phần cứng khai thác chuyên nghiệp, chẳng hạn như ASIC, CPU và GPU	Mọi máy tính hoặc thiết bị di động có kết nối internet
Phần thưởng sẽ được phân bổ như thế nào?	Người đầu tiên khai thác khối sẽ nhận được phần thưởng khối	Người xác thực có thể nhận được một phần phí giao dịch thu được từ khối mà họ đã xác thực
Mạng được bảo mật như thế nào	Hàm băm càng lớn, mạng càng an toàn	Cơ chế khóa tiền mã hóa trên blockchain để bảo mật mạng

Staking là hành động giữ và khóa một lượng coin nhất định để nhận được phần thưởng. Lượng coin này có thể được khóa trong ví tiền điện tử hoặc các nút của một dự án Blockchain trong một khoảng thời gian. Phần thưởng sẽ dựa trên công sức người dùng đã bỏ ra bao gồm: lượng coin stake và thời lượng stake.