**Proof of stake là gì?**

Trong các node tham gia, một node sẽ được lựa chọn ngẫu nhiên để trở thành người kiểm định và đóng gói block.

Node tham gia được gọi là các validator (người kiểm định).

Điều kiện để tham gia là các node này cần phải bỏ một khoản tiền vào mạng lưới, mà anh Vitalik Buterin gọi là bet (đặt cược). Ta có thể hiểu nôm na là đặt cọc tiền để chứng minh danh tính bản thân.

Khoản tiền này được gọi bằng từ chuyên môn là Stake.

Khoản tiền này sẽ bị hệ thống thực hiện lock. Và sẽ được unlock sau khi node rút khỏi việc tham gia validator một thời gian (Chú ý việc unlock sẽ không được thực hiện ngay lập tức).

Validator được chọn sẽ thực hiện validate block. Thuật ngữ chuyên môn cho hành động này là forge hoặc mint (phân biệt với mine trong PoW).

Nếu block hợp lệ và ghi được vào chain, validator này sẽ được phần thưởng chính là từ transaction fee.

**Thuật toán lựa chọn validator tiến hành forge**

Thực chất việc lựa chọn này không hoàn toàn ngẫu nhiên mà dựa trên giá trị stake của những validator tham gia.

Giả dụ Alice có stake là 10 USD, Bob có stake là 100 USD. Vậy Bob sẽ có cơ hội cao để được lựa chọn hơn Alice.

Ý tưởng đơn giản là: Ai có giá trị stake cao sẽ có tiếng nói tin cậy.

**Nếu có gian lận thì sao?**

Điều gì xảy ra nếu validator được chọn thực hiện gian lận cố tình validate block giả mạo.

Nếu điều này bị phát hiện (được thông báo lên mạng lưới từ các validator khác), anh ta sẽ bị phạt toàn bộ số tiền trong stake.

Đây cũng là lý do tại sao stake không được hoàn trả ngay sau khi validator từ bỏ quyền tham gia. Tránh trường hợp anh ta validate block giả mạo sau đó từ bỏ quyền luôn để trốn chạy.

Để đảm bảo lợi thu được nhỏ hơn nhiều số tiền bị phạt, stake tối thiểu được quy định của Casper là 1250 ETH.

Nên hiểu là chỉ có 1 block được chấp nhận và thêm vào chain, tất cả các validator đặt stake cho block bị coi là giả mạo (không được thêm vào chain) cũng sẽ mất toàn bộ stake của họ.

Đánh vào các hình phạt kinh tế là điểm then chốt để đảm bảo tính an toàn của PoS, khiến cho việc tấn công và giả mạo trở nên khó khăn hơn.

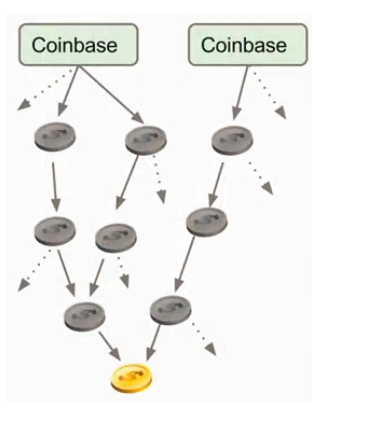
**Chapter 8. Bitcoin as a platform**

1. Bitcoin as an Append – Only Log
   1. Bitcoin as an Append-Only Log.

* Có nghĩa là ta chỉ có thể thêm vào cấu trúc dữ liệu của Bitcoin, và khi ta thêm một cái gì đó, thì điều đó sẽ được lưu giữ mãi mãi. Không có cách nào để update hoặc xóa đi.
  1. Bitcoin for secure timestamping.
* Để đảm bảo được việc bảo mật bằng timestamping (dấu thời gian), ta có thể tính hàm băm của x và submit nó vào blockchain tại thời điểm t.
  1. Secure timestamping applications.
* Proof of knowledge: để chứng minh ta biết được điều gì đó vào thời điểm t. Ví dụ như tôi có 1 ý tưởng tại thời gian t và bây giờ tôi mới thực hiện nó.
* Proof of Receipt: để chứng minh rằng ta thực sự đã nhận được thông tin. Ví dụ như hệ thống bầu cử, server có thể gửi các phiếu bầu về cho client. Trong trường hợp bỏ phiếu kín, bầu cử không được public nhưng server không thể chối bỏ rằng đã nhận lại được phiếu bầu từ client.
* Hash based signature scheme: các lượcđồ chữ ký không yêu cầu tất cả mật mã khóa công khai như các chữ ký số khác.

1. Bitcoin as Smart Property.
   1. Theo dõi chủ sỡ hữu của Bitcoin đó bất cứ lúc nào.

Mỗi Bitcoin đều có lịch sử và ta có thể tra cứu ngược lại tới thời điểm Coinbase tạo ra nó.



Coinbase là một sàn giao dịch tiền điện tử và đồng thời cung cấp dịch vụ ví lưu trữ các đồng coin khác nhau. Hiện nay, Coinbase và Blockchain là hai dịch vụ ví điện tử lưu trữ tiền tốt nhất. Tuy nhiên, thời gian xác nhận giao dịch thành công trên Coinbase sẽ lâu hơn Blockchain. Nhưng vì miễn phí và có nhiều ưu điểm khác giúp cho người dùng thuận tiện trong việc lưu trữ, trao đổi tiền ảo như: Dễ dùng, an toàn, không mất phí nên vẫn có nhiều người sử dụng.

* 1. Smart Property with Fiat Currency.

Ta có thể tạo ra một chữ ký mã hóa trong metadata và gán nó với một số seri của banknote. Và người nào có quyền truy cập và có khóa đăng nhập (sign – in key), sẽ ký kết hợp metadata này với số seri của banknote và sẽ liên kết metadata này với banknote đó. Và có các đặc tính sau:

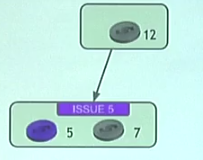
* Currency đó có thể thay thế bất cứ thứ gì.
* Các đặc tính chống giả mạo của tiền tệ được kế thừa cho loại tiền tệ mới này.
* Giá trị cơ bản của tiền tệ cũng được duy trì.
* Nhiều người sẽ không biết metadata mới này và sẽ không phân biệt được tiền giấy này với tiền giấy khác.(tiền có chữ ký của metadata).

VD: một trận đấu bóng đá, thì họ chỉ sử dụng vé để vào cổng. Thì vé vào cổng ở đây được thay thế cho một khoảng tiền bỏ ra để đổi lấy vé vào cổng. Và vé này chỉ phù hợp cho trận đấu đó, và có thể là chỉ định chỗ ngồi cho người cầm vé. Nên trong trường hợp này, vé vào cổng chính là Banknote. Mỗi vé có một số seri riêng biệt để phân biệt với các vé khác. Và số seri đó đã được thông qua, phòng trường hợp giả mạo vé.

* 1. Smart Property with Bicoin: Colored coins.

Colored coins là một loại phương pháp kết hợp tài sản ở thế giới thực với các địa chỉ trên mạng lưới Bitcoin. Ví dụ có thể là một chứng thư cho một ngôi nhà, cổ phiếu, trái phiếu,… Công nghệ này cũng có thể được áp dụng để theo dõi và đăng ký tài sản sỡ hữu trí tuệ.

* Phát triển và trao đổi Colored coin:

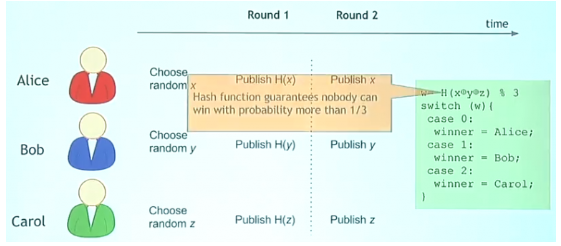
Để tạo một colored coin trong một transaction, ta add một phần nhỏ của metadata mà xác định cho mỗi đầu ra là một màu riêng biệt.

Như ở ví dụ trên, ta thấy 5 bitcoin chuyển thành màu tím, ta nói ta đã ban hành 5 bitcoin màu tím và một output khác là 7 bitcoins không màu.

1. Secure multi – party lotteries in Bitcoin

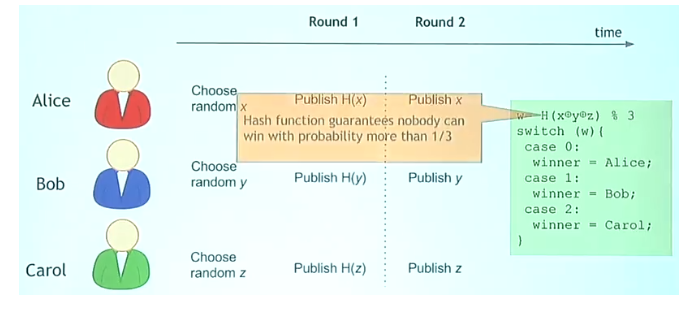
Ví dụ như Alice muốn cá 5$ với Bob về một trận banh tối nay qua mạng Internet. Nhưng độ tin tưởng không có vì Alice không thể đưa 5$ cho Bob qua mạng internet được.

Và giải pháp ở đây là dùng Hash Commitments. Ta sẽ public Hash Commitment có chứa kết quả của trận đấu tối hôm nay sẽ đá của Alice lên mạng bitcoin và sau khi kết thúc trận đấu, ta sẽ dùng input đầu vào để hash ngược trở lại để chứng minh rằng ta đã public điều này trước khi trận đấu diễn ra và nhận được tiền hoặc mất tiền.



Như ví dụ trên, ta có 3 người là Alice, Bob và Carol, và cả 3 người này muốn chơi xổ số với nhau. Trình tự như sau:

* Cả 3 người họ sẽ chọn số ngẫu nhiên, hay còn được gọi là số nonce. Và giữ bí mật số nonce này.
* ở round 1, mọi người sẽ publish những cái commitment có chứa dự đoán của họ, và không tiết lộ số nonce. Và ta phải đảm bảo rằng Round 2 phải được thực hiện ngay sau khi Round 1 kết thúc.
* Ở Round 2, cả 3 người sẽ công khai số nonce này, và mỗi người có thể kiểm tra được rằng 3 số nonce này khớp với chuỗi hash mà họ đã publish từ trước.
* Xác định người chiến thắng: ta có thể dùng một thuật toán đơn giản để xác định được người thắng. Ví dụ, ta sẽ dùng thuật toán để tính hàm hash của 3 số nonce xor với nhau và mod cho 3. Và nếu giả sử ta gán cho 3 người tham gia có số thứ tự từ 0 đến 2, thì nếu số dư nó bằng người nào thì người đó sẽ thắng. Và tính đảm bảo công bằng ở đây thể hiện ở việc ta dùng hàm hash để hash 3 số nonce của 3 người xor lại với nhau nên việc gian lận là không thể xảy ra.

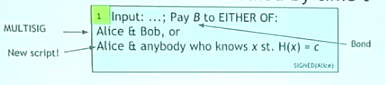


Trong trường hợp 1 trong 3 người không tiết lộ số nonce của họ, ví dụ như Carol thấy Bob và Alice publish số nonce của họ lên và thấy rằng mình đã thua và rút ra khỏi cuộc chơi, không publish số nonce của mình lên, thì ta sẽ dùng một commitment để khắc phục tình trạng này.

Use Timed Hash Commitment for Online Lotteries:

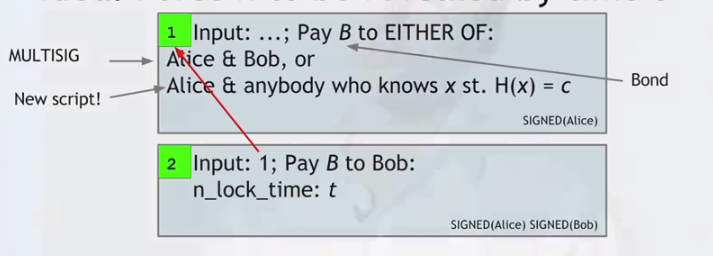
Ý tưởng của việc này là tránh người chơi gian lận bằng cách ép buộc một commitment trong một khoảng thời gian t. Ví dụ, nếu Alice cố gắng tham gia vào một timed hash commitment với Bob, cô ấy sẽ đưa lên một giao ước(bond) và tạo transaction mà sẽ thực hiện giao ước đó bằng 2 trường hợp:

* Cả Alice và Bob đều kí vào giao ước đó (multisignature).
* Alice ký và tiết lộ data bên trong là gì. Trong trường hợp này, có thể kiểm tra được rằng có một giá trị x trong redemption script mà Alice đã commit từ trước.(pay – to – hash – script).



Vậy làm thế nào để Alice và Bob có thể nhận được tiền?

Trong trường hợp 1, cả Bob và Alice đều ký vào transaction rằng Bob sẽ lấy tất cả tiền trong transaction đó, thì ta sẽ dùng n\_lock\_time để chắc chắn rằng Bob không thể lấy giao ước(bond) sớm hơn thời gian t.



ở trong trường hợp 2, Alice có thể publish transaction trước thời gian t để đòi lại bond của cô ấy đã gửi tiền ngược lại cho cô ấy. Nhưng nếu Alice làm thế, cô ấy không chỉ ký tên vào, mà còn phải tiết lộ x. Như vậy nếu Alice không muốn Bob nhận toàn bộ số tiền trong bond thì Alice phải tiết lộ commitement của mình. Và nếu Alice không chịu tiết lộ commitement của cô ấy, cô ấy sẽ mất toàn bộ tiền trong bond mà cô ấy đã gửi lên nên việc Alice có muốn show ra commitment của mình hay không thì tùy thuộc vào bond của cô ấy có chứa giao dịch có nhiều tiền hay không.

Áp dụng Timed commitment vào Lotteries: vẫn là luật chơi như cũ, nhưng thay vì ta dùng một thuật toán đơn giản để tìm ra được người chiến thắng thì ta sẽ dùng Timed Commitment. Nếu trong khoảng thời gian t nào đó mà họ không tiết lộ số nonce của mình, nên nếu Carol thấy rằng mình sẽ thua sau khi thấy được 2 số nonce của Alice và Bob và Carol không muốn tiết lộ số nonce của mình, thì sau khoảng thời gian t, Carol cũng sẽ bị mất toàn bộ tiền trên bond mà Carol đã đặt cược lúc đầu.

1. Bitcoin as Randomness Source.
   1. NIST beacon (đèn tín hiệu NIST)

NIST (National Institute of Standards and Technology)

