REVIEW

1. Zerocoin và zerocash.

Zerocoin được phát triển đầu tiên bởi các nhà mật mã học tại John Hopkins University. Các kỹ thuật này cung cấp một mức độ ẩn danh khác nhau về mặt chất lượng so với giải pháp Mixing. Vấn đề này nằm ở chỗ Zerocoin và Zerocash không tương thích ngược với Bitcoin (backward compatible) mà zerocoin và zerocash chủ yếu tập trung hỗ trợ cho Altcoin.

Zerocoin là một protocol-level mixing. Ta không cần phải tin tưởng 1 mix cụ thể hay một tập hợp mix nào hay một cụm peers nào để đảm bảo tính ẩn danh. Ta chỉ cần dựa vào một số mật mã cơ bản ở dạng rắn (solid), ta không cần dựa vào các thực thi minors để ẩn danh. Đó hoàn toàn là một mật mã đảm bảo.

Basecoin: là một Altcoin. Basecoin có thể convert thành Zerocoin và ngược lại. và khi thực hiện convert này, thì các liên kết giữa basecoin trước khi convert và sau khi convert bị phá hủy.

Vậy Zerocoin là một mật mã chứng minh rằng bạn có sỡ hữu một Basecoin và biến nó trở nên không thể sử dụng được (unspendable). Các miners có thể kiểm tra proof này và nhờ vào việc kiểm tra này, bạn mới có quyền mua lại (redeem) một Basecoin mới để đổi lấy Zerocoin.

Có 2 khó khăn ở đây đó là: làm sao để xây dựng Proof này. Và làm sao để đảm bảo rằng mỗi Proof chỉ được sử dụng 1 lần, được sử dụng 1 lần để mua lại Basecoin vì nếu không có properti này, sẽ xảy ra lỗi Double spending.

Ta sẽ dùng Zero – knowledge Proof. Zero – knowledge Proof là một cách mà một người có thể chứng minh một statement - mà không cần tiết lộ bất cứ thông tin nào khác – để dẫn đến statement đó là đúng.

Tính chất của zero – knowledge proof:

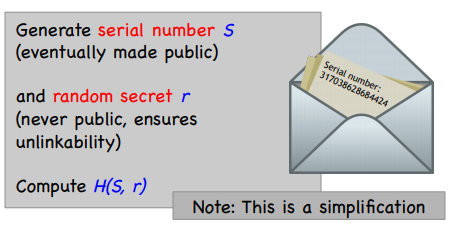
* Tính hoàn thiện: Nếu câu lệnh đúng thì Verifier sẽ chấp nhận sự chứng minh được kiểm chứng bởi Prover.
* Tính bền vững: Nếu Prover không trung thực, Verifier từ chối kiểm chứng của Prover.
* Zero-Knowledge: Nếu tuyên bố là đúng, Verifier sẽ không quan tâm đến câu lệnh của Prover

Zerocoin được tạo ra bằng cách đúc (minting) và bất cứ ai cũng có thể làm được và có mệnh giá tiêu chuẩn (standard denominations). Hãy giả sử rằng Zerocoin đáng giá 1 Basecoin.

Minting Zerocoin không tự động tạo ra giá trị. Nên ta không có tiền từ việc Minting đó. Nó chỉ tạo ra giá trị khi nó được đặt lên trên mạng lưới Blockchain.

Cách tạo ra một Zerocoin: sử dụng mật mã cam kết.

Mật mã cam kết (cryptographic commitment): tưởng tượng việc bạn dùng một số seri **S**, và số seri này ngẫu nhiên mà bạn tạo ra, và đặt nó vào trong một phong bì. Tức là ta sẽ tạo ra thêm một Secret number ngẫu nhiên **r** và số này sẽ không được public và thực hiện hàm Hash để hash số seri ngẫu nhiên **S** và số bí mật **r. H(S,r)**



Ta sẽ tạo tùy ý một serial number cho Zerocoin của mình. Có độ dài ngẫu nhiên và chưa từng được sử dụng trên hệ thống. Đồng thời, ta cũng tạo một secret number và không public nó.

Sau đó, tạo một cam kết (commitment) với số seri này tương ứng với việc bỏ nó vào trong một cái phong bì và niêm phong nó lại. Sau đó đặt nó lên trên mạng lưới blockchain. Đó là lúc Zerocoin được tồn tại. Điều này giống như việc ta đốt một basecoin và làm cho nó trở nên không thể giao dịch được. Và cái cam kết mật mã (cryptographic commitment) này thay thế cho địa chỉ người nhận.

Ta dùng basecoin để đúc Zerocoin. Và cái cam kết, với cái phong bì niêm phong mà ta đã đặt Zerocoin trong đó, là những gì cho phép ta mua lại Zerocoin sau này để đổi lấy basecoin lần nữa.

Để sử dụng Zerocoin này, ta phải tiết lộ Serial number bên trong phong bì. Và các miners có nhiệm vụ xác minh Serial number đó đã được sử dụng trước đây hay chưa. Việc chứa Serial number bên trong phong bì giúp ngăn chặn tình trạng Double Speding.

Tiếp theo, ta tạo một Zero – knowledge Proof, chứng minh được rằng ta có secret number r, sao cho giá trị băm của serial number với secret number ứng với một trong các zerocoin trong chuỗi blockchain. Nhưng nó sẽ không tiết lộ số r. Nhưng bằng một cách nào đó, bạn phải chứng minh được rằng ta đang giữ số r đó bằng cách kết hợp với serial number mà ta đã public từ trước với số r đó, ta sẽ thu được kết quả Zerocoin mà ta đã từng up lên trên mạng blockchain.

Vì vậy, mọi người sẽ dựa vào bằng chứng này để xác minh được rằng ta đã dùng một basecoin trước đây và bây giờ ta có quyền được mua lại một basecoin đó.

Ta có thể chọn một đồng xu bất kỳ trong blockchain và sử dụng nó làm đầu vào cho một transaction mới trong đó có một basecoin và các miners sẽ cho phép ta làm điều đó.

Tóm lại, cho vào một Zerocoin, lấy ra một Zerocoin nhưng hai Zerocoin này khác nhau hoàn toàn. Và ta không thể làm điều này thêm lần nào nữa vì lúc này, serial number sẽ được public. Và một serial number sẽ tương ứng với một zerocoin và ta chỉ biết serial number nào tương ứng với zerocoin của mình và cái nào không phải của mình.

Tính ẩn danh của Zerocoin: Bởi vì ta giữ secret number **r**, thì cho dù bạn có bị lộ serial number, không biết đầu vào ngẫu nhiên khác, **r**, không ai có thể dùng bruce force để tìm và đoán xem thử zerocoin này tương ứng với serial number nào.

1. Zerocash

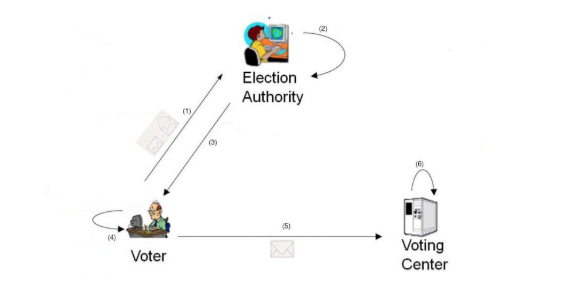
Zerocash sử dụng loại mã hóa phức tạp hơn gọi là Snarks. Và ta có thể vận hành cả hệ thống mà không cần sử dụng Basecoin nào.

Tất cả các transactions trong zerocash là zerocoin, nên Zerocash trở nên không thể sử dụng để trao đổi bởi vì nó không có basecoin. Và vì thế, nên việc chia hoặc gộp các coins hay các transaction trong Zerocash sẽ không sử dụng Basecoin.

Và ta có thể đặt các giá trị giao dịch, số tiền giao dịch bên trong các cam kết. Và những cam kết này sẽ không được hiển thị lên mạng lưới blockchain. Và sổ cái (ledger) chỉ ghi lại sự tồn tại của các giao dịch đó (nghĩa là trong sổ cái chỉ ghi lại những giao dịch đó thành công hay không. Nó sẽ không lưu lại địa chỉ người gửi, người nhận và số tiền giao dịch). Nên chỉ có người gửi và người nhận mới biết chính xác transaction đó có giá trị là bao nhiêu.

Khác nhau cơ bản giữa Zerocoin và Zerocash là ta có thể thực thi Zerocash mà không cần basecoin nào.

1. Blinding Signature.



Thuật toán RSA trong blinding Signature.

* Giả sử C muốn D ký lên thông điệp m nhưng không được biết nội dung của m. Giả sử khóa công khai của D là *(e, n)* và khóa cá nhân là *(d, n).*
* Đầu tiên C “blind hóa” thông điệp **m** thành **m’**, ta tính : **m’ = m.r­e mod n** trong đó **r** là số phát sinh ngẫu nhiên. Sau đó C gửi kết quả của **m’** cho D. Vì **r** là biến ngẫu nhiên nên phép tính **m.re mod n** cũng là ngẫu nhiên. Nên **m’** sẽ không để lộ bất kỳ thông tin gì liên quan đến **m**.
* D ký lên Blind message này bằng phép tính **s’ = (m’)d mod n** và gửi ngược về cho C
* Cuối cùng, C muốn “unblind” message bằng phép tính:

s = s’.r -1 mod n

Phép tính này đúng là vì các khóa RSA thõa mãn phương trình: r ed = r mod n

Nên s = s’. r -1 = (m’)d. r -1 = md.red.r -1 = md.r.r -1 = md mod n

Cho biết số r là gì để chứng minh cái mess đó là của mình