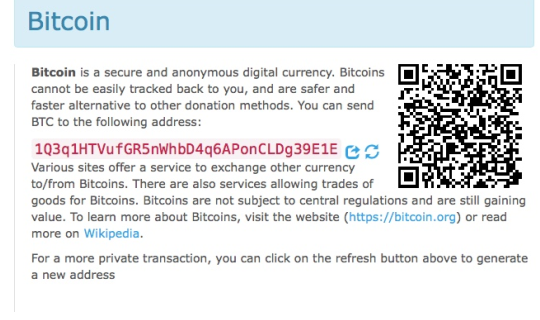
CHAPTER 6

BITCOIN AND ANONYMITY (cont)

1. How to de-anonymize Bitcoin ( cách ẩn danh bitcoin)

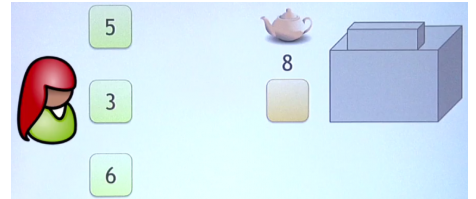
2.1 Ví dụ quyên góp WikiLeaks



Trong trang thanh toán cùa WikiLeaks họ có địa chỉ Bitcoin để gửi thanh toán đến. Khi nút làm mới được nhấn thì địa chỉ để gửi bitcoin sẽ thay đổi. WikiLeaks đảm bảo rằng mỗi lần một người nào đó truy cập trang để thanh toán thì một địa chỉ Bitcoin mới sẽ được tạo cho mục đích đó. Họ muốn nhận mọi giao dịch tại địa chỉ mới. Từ đó đảm bảo tốt nhất về việc ẩn danh cho người nhận Bitcoin. Và chắc chắn rằng các địa chỉ này phải được liên kết với nhau.

* 1. Làm thế nào để liên kết các địa chỉ nhận Bitcoin khác nhau

Hãy tưởng tượng rằng Alice đi đến một cửa hàng và muốn mua một ấm trà có giá 8 BTC. Nhưng Alice không có 8 BTC trong một địa chỉ duy nhất. Có lẽ cô ấy có 3 địa chỉ với 5, 3 và 6 BTC tương ứng. Vì vậy, cô ấy cần kết hợp các đầu vào khác nhau trong một giao dịch duy nhất để thực hiện thanh toán. Người xem giao dịch này có thể nghĩ rằng giao dịch có hai yếu tố đầu vào chỉ có thể xảy ra nếu cả hai địa chỉ đều nằm dưới sự kiểm soát của cùng một người dùng.



Nói cách khác, chi tiêu được chia sẻ là bằng chứng kiểm soát chung của hai địa chỉ khác nhau , và không chỉ. Các địa chỉ có thể được liên kết quá mức . Trong thực tế, nếu Alice sử dụng Bitcoin từ địa chỉ thứ hai và thứ ba, sẽ có một Bitcoin còn lại, có thể được sử dụng sau này trong một giao dịch mới. Tất cả các địa chỉ được sử dụng làm đầu vào của giao dịch mới có thể được liên kết với nhau và với địa chỉ được sử dụng trong giao dịch trước đó. Vì vậy, có thể truy xuất một nhóm địa chỉ đầy đủ thuộc cùng một chủ đề.

* 1. Phân tích ẩn danh trong hệ thống Bitcoin.

Clustering of Addresses ( phân cụm địa chỉ)

Change Addresses ( thay đổi địa chỉ)

* 1. Anonimity cho cá nhân.

Bây giờ, có thể đặt nhãn cũng cho cá nhân không? Điều này có thể xảy ra theo một vài cách:

Bitcoin được sử dụng để thực hiện các giao dịch tương tác trực tiếp với người bán. Vì vậy, nó có thể liên kết một địa chỉ cho cá nhân và bắt đầu từ đó để xác định cụm.

Hầu hết người dùng tương tác với các nhà cung cấp dịch vụ lớn, những người biết danh tính thực sự của họ. Nó là đủ để tìm một giao dịch duy nhất với các nhà cung cấp lớn để có khả năng quay trở lại danh tính thực sự. Tất nhiên, điều này chỉ có thể có đủ sức mạnh autority hoặc với các kỹ thuật hacking.

Thông thường, người dùng xuất bản trực tuyến một số địa chỉ của họ cho mục đích quyên góp hoặc tương tự. Với địa chỉ đơn này, có thể tái tạo lại cụm.

Những kỹ thuật này để lấy danh tính ngày càng trở nên hiệu quả hơn. Vì vậy, đây là một cái gì đó bạn cần phải lo lắng về nếu bạn quan tâm đến sự riêng tư của bạn.

* 1. Các kỹ thuật khác để lấy danh tính.

Cho đến nay, chúng ta vừa thấy các cuộc tấn công có thể chỉ dựa trên dữ liệu công khai và bất biến có sẵn trong blockchain. Ngoài ra, có rất nhiều dữ liệu khác được truyền trên mạng Bitcoin không được chèn vĩnh viễn vào blockchain.

Ví dụ, khi một nút tạo ra một giao dịch, nó kết nối với rất nhiều nút khác để phát sóng nó. Vì vậy, một số nút có thể đặt đầu của chúng lại với nhau và phát hiện ra rằng tất cả chúng đều đã nghe về giao dịch lần đầu tiên. Do đó, họ có thể giả sử rằng nút gửi là nút đã tạo giao dịch. Và họ có thể lấy một số thông tin, chẳng hạn như địa chỉ IP.

Giải pháp: Sử dụng các hệ thống truyền thông riêng như Tor hoặc Mixnet.

Tor : dành cho các hoạt động có độ trễ thấp như duyệt web

Mix nets : được cung cấp ẫn danh tốt hơn, nhưng Tor đang được triển khai và hoạt động.

1. Bitcoin mixing.
   1. Bitcoin mixing

Bitcoin mixing được dùng ở đây nhằm cải thiện, đảm bảo tính ẩn danh thông tin của người gửi cũng như người nhận bitcoin.

Ví dụ: Một số dịch vụ cho phép người dùng đưa vào thông tin , bitcoin sau đó nó sẽ không ghi lại thông tin của người gửi và xử lý toàn bộ bitcoin được lưu trữ sao cho không thể phân biệt bitcoin lẫn nhau. Tiếp theo nó có thể kết hợp chúng thành một giao dịch duy nhất hoặc hợp nhất chúng theo nhiều cách khác nhau. Quan trọng nhất là khi người dùng quay trở lại để rút Bitcoin của họ, thì thông tin công khai trên Blockchain của họ sẽ không được gắn với bitcoin đưa vào. Trên thực tế, họ sẽ nhận được một số tiền đươc gửi qua các tài khoản trung gian khác nhau. Giả sử ai đó đang xem thông tin công khai trong blockchain. Chắc chắn rằng họ sẽ không thể thấy các hoạt động trung gian họ chỉ thấy địa chỉ gửi và các địa chỉ nhận họ sẽ không thể liên kết các địa chỉ gửi với các địa chỉ nhận cùng tương ứng với cùng một người dùng. Vì vậy đảm bảo tính ẩn danh thông tin của người gửi, người nhận.

* 1. Online wallets có thật sự ẩn danh hay không?

Online wallets có cung cấp ẩn danh bởi vì có người đã thử liên kết giữa địa chỉ input với địa chỉ output nhưng nó không thành công.

3.3 So sánh sự khác biệt giữa Online wallets và Mixing service

- Mixing services cung cấp thêm một số chức năng:

+ Không lưu recort của quá trình Mixing. Vì vậy, ngay cả khi họ muốn, họ cũng không thể biết được Bitcoin nào là của bạn đã bỏ vào.

+ Không hỏi thông tin về danh tính và cuộc sống hiện tại của bạn để tương tác với họ.

* Trong khi Online wallet thường có độ uy tín và quy định kinh doanh. Vì vậy họ có thể sẽ yêu cầu danh tính của bạn và lưu trữ hồ sơ, giữ liên kết danh tính và địa chỉ Bitcoin.
* Khi bạn bỏ tiền vào Mixing services, thì bạn muốn gửi nó trở lại một địa chỉ khác ngay lập tức. Nói cách khác, ta không hoàn toàn tin tưởng vào Mixing services. Trong khi với Online wallet, ta có thể tin tưởng hơn và thường được dùng để gửi tiền dài hạn.

1. Mixing Services.
   1. Sử dụng một loạt các mixes thay vì một cái.

Việc sử dụng một loại các mixes sẽ làm tăng độ phức tạp và an toàn hơn là sử dụng 1 cái.

* 1. Uniform Transactions (Giao dịch Uniform).

Một điều quan trọng là kết quả của các mixes transactions phải có cùng kết quả và có cùng chunk size.

* 1. Sử dụng phần mềm khách hàng tự động.

Như Wallet Software. Phần mềm này tự động biết cách tương tác với mixes này để đảm bảo sự an toàn của người dùng.

* 1. Mixes Fees.

Phí xác suất: 0.1% mixing fee = mix swallow chunk with 0.1% chance.

1. Decentralized Mixing (Mixing phân cấp).

* Loại bỏ Mixing services.q
* Thay thế chúng bằng giao thức mixing peer-to-peer.
* Lợi ích:
  + Ngăn chặn được boottrapping.
  + Không thể xảy ra trộm cắp.
  + Có thể ẩn danh tốt hơn.
  1. CoinJoin.

Người dùng cùng nhau tạo ra một giao dịch duy nhất kết hợp tất cả inputs.

* 1. Thuật toán CoinJoin.

1. Tìm “đồng nghiệp” muốn mix.
2. Trao đổi địa chỉ input/output.
3. Tạo transaction
4. Gửi cho các peers, lấy signatures. (trước khi ký tên, mỗi peers phải check thử xem là output đã được present hay chưa).
5. Broadcast transaction.
   1. Khó khăn CoinJoin.
6. Làm sao để tìm peer?

* Sử dụng các server không tin cậy (untrusted server). Đó là một loại server nơi người dùng khác nhau có thể tìm thấy nhau. Nhưng người dùng phải tin tưởng vào server đang chạy giao thức.

1. Làm sao để giải quyết việc ẩn danh?

* Ta có thể xây dựng một cơ chế định tuyến ẩn danh (anonymous routing mechanism) đặc biệt để chỉ những người tham gia mới có thể sử dụng giao thức này. Và cách này được gọi là giải mã mixnets (decryption mixnets).

1. Làm sao để giải quyết tấn công DdoS?

* Một cách khác là có thể xây dựng một hệ thống mật mã cho phép xác định một hoặc nhiều peers độc hại đã khởi chạy “denial services” và kích chúng ra khỏi hệ thống.

1. Zerocoin và Zerocash.

6.1. Zerocoin.

Zerocoin là mật mã được pha trộn vào trong giao thức (protocol). Ngoài ra, nó không phụ thuộc vào bên thứ ba để xóa các records. Nó không tương thích ngược với Bitcoin và giao dịch sẽ thấp hơn Bitcoin.

6.2. Basecoin

Sửu dụng Altcoin thay vì Bitcoin.

Altcoin (viết tắt của Bitcoin alternative) là tên gọi chung của những loại cryptocurrency khác với Bitcoin. Phần lớn các Altcoin đều là những phiên bản cải tiến của Bitcoin.

Zerocoin là phần mở rộng của Basecoin.

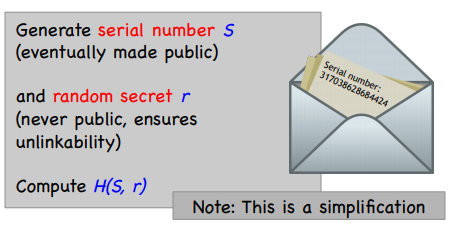
Basecoin có thể được chuyển đổi thành Zerocoin và ngược lại. Và khi thực hiện hoạt động này thì không có liên kết nào giữa Basecoin bản gốc và bản mới.

Như vậy, Zerocoin là một bằng chứng mật mã cho thấy rằng ta là chủ sỡ hữu Basecoin đó và làm cho nó không thể được khai thác từ những người khác. Các miners khi muốn khai thác cần phải được xác minh. Và cung cấp quyền cho phép mua lại Basecoin mới.

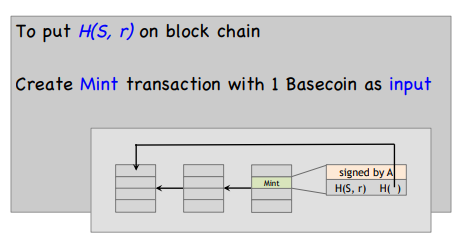
* 1. Zero-knowledge Proof.

Là một phương thức mà một bên ( Peggy prover ) có thể chứng minh cho một bên khác (người xác minh Victor) biết rằng cô ấy biết giá trị x , không truyền đạt bất kỳ thông tin nào ngoài thực tế rằng cô ấy biết giá trị x .

* 1. Minting Zerocoins.



Để Minting Zerocoin: “Committen”(cam kết)

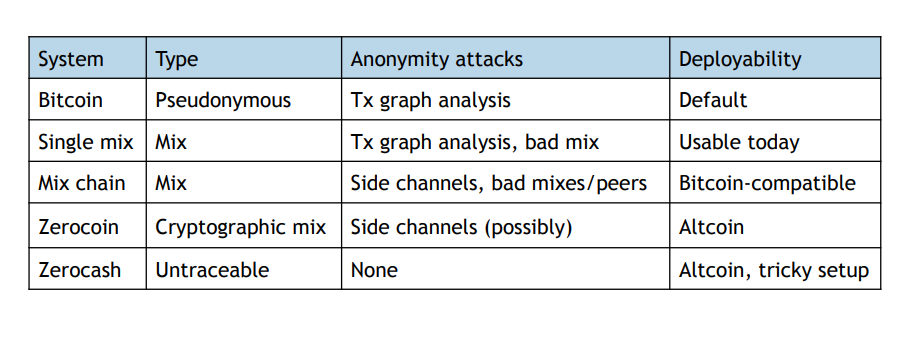
* Tạo serial number **S** (có thể được public) và Random Secret **r**(không được public, bảo đảm tính ẩn danh).
* Thực hiện hàm Hash: H(S,r).
* Để đưa hàm Hash H(S,r) vào chuỗi Blockchain, tạo một Mint transaction với đầu vào là 1 Basecoin.
* Để sử dụng Zerocoin S:
  + Cho biết Serial Number S.(miner sẽ xác nhận rằng S này chưa từng được dùng để giao dịch trước đây).
  + Tạo Zero-knowledge Proof để chứng minh được rằng “tôi biết số **r** mà hàm Hash H(S,r) là một trong những zerocoins trong chuỗi blockchain”.
  + Chọn Zerocoin tùy ý trong blockchain và sử dụng nó làm đầu vào cho giao dịch tiếp theo.
* Tính ẩn danh của Zerocoin: Nếu **r** là bí mật (secret), không ai có thể biết được Zerocoin nào tương ứng với Serial number **S.**
  1. Zerocash.

Zerocash sử dụng một công cụ mã hóa phức tạp hơn gọi là Snarks. Và bạn có thể khởi chạy toàn bộ hệ thống mà không cần sử dụng bất kỳ Basecoin nào.

Zerocash: Untraceable e-cash.

* Tất cả các Transaction đều là Zerocoin.
* Hỗ trợ Spliting và merging.
* Đặt các transaction value vào một “phong bì” (envelope).
* Sổ cái chỉ ghi lại transaction đó có tồn tại hay không.
* Chỉ có người gửi và người nhận biết giá trị của transaction.
* Chứng minh cho các miners biết rằng

**input amount >= output amount.**

* 1. 5 Levels của Anonyity.

1. Tor Browser và Silk Road (con đường tơ lụa).

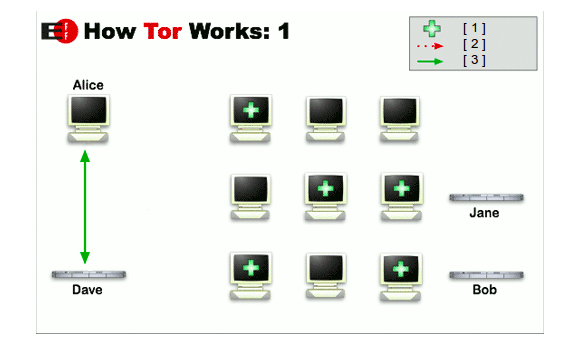
7.1. Tor Browser.

Tor Browser hoạt động trên Tor network, là một Phần mềm mã nguồn mở và miễn phí (FLOSS) và được thiết kế để đem lại khả năng ẩn danh trực tuyến cũng như vượt rào luật cấm.

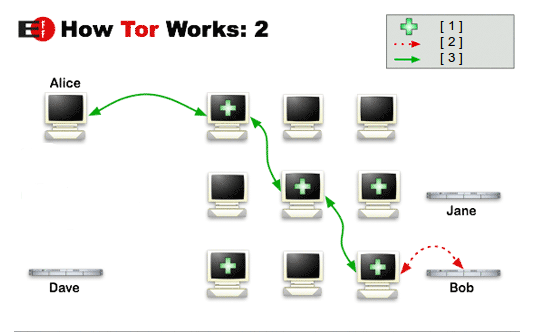
Tor Browser bao gồm hàng nghìn máy trạm được chạy bởi các tình nguyện viên trên toàn thế giới. Mỗi lần Tor Browser thực hiện một kết nối mới, ứng dụng lựa chọn 3 trong số những Tor relays và kết nối vào Internet thông qua chúng. Hệ thống mã hóa mỗi đường đi của dữ liệu khiến cho bản thân giao dịch không biết được đường đi cụ thể trong quá trình gửi và nhận dữ liệu

Ví dụ: Máy tính của Alice sử dụng Tor browser để kết nối đến với máy trạm của Bob:

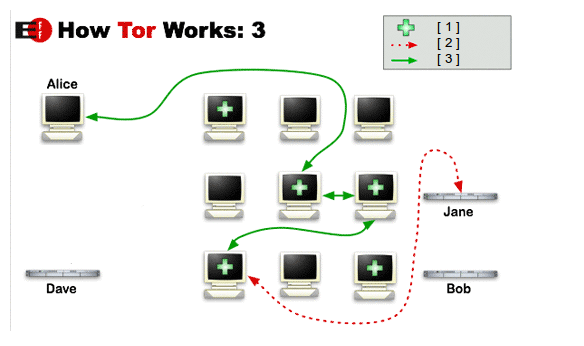
B1: Tor Browser của Alice có chứa các điểm hoặc giao dịch Tor [1] từ thư mục máy trạm của Tor (Dave).



B2: Tor Browser của Alice chọn một đường đi ngẫu nhiên thông qua mạng Tor đến máy trạm cần đến (Bob). Toàn bộ các kết nối bên trong mạng Tor được mã hóa (xanh lá [3]). Trong ví dụ này, kết nối cuối cùng không được mã hóa (đỏ [2]). Kết nối cuối cùng sẽ được mã hóa nếu Alice truy cập vào trang web HTTPS.



B3: Nếu tại một thời điểm sau đó, Alice truy cập vào một máy trạm khác (Jane), Tor Browser của Alice lựa chọn một đường đi ngẫu nhiên khác



7.2. Silk Road.

Được ví như e-Bay của thuốc phiện và các buôn bán phạm pháp khác.

Trình duyệt để truy cập: Tor browser.

Phương thức thanh toán: Bitcoin.

**CHAPTER 7**

**ALTERNATIVE MINING PUZZLES**

1. Essential Mining Puzzles Requirements.(sự cần thiết của yêu cầu khai thác mảnh ghép)

Mining puzzles là cốt lõi của tiền điện tử (cryptocurrency) và thông dụng trong blockchain. Mặt khác, các miners sẽ nhận được tiền từ việc giải quyết các puzzles đó.

Mục tiêu của các miners là nhận được càng nhiều phần thưởng cho các tác vụ họ đang thực hiện, nên họ sẽ:

* Nỗ lực để tìm mọi đường tắt có sẵn để họ có thể giải quyết puzzles đó nhanh hơn và hiệu quả hơn.
* Nếu có bất kỳ phép toán (operations) nào giúp cải thiện mạng tốt hơn nhưng không giúp các miners giải quyết puzzles đó nhanh hơn hoặc thậm chí không mang lại cho họ bất cứ phần thưởng gì, thì họ sẽ không thực hiện điều đó.

Vì thế, Mining Puzzles đóng vai trò quan trọng trong việc chỉ đạo và thúc đẩy sự tham gia của cả mạng lưới. Nên vì thế, nó có một số chức năng như sau:

* Khuyến khích các miners tham gia vào mạng.
* Phải rẻ để xác thực, vì tất cả các node trong mạng phải xác thực kết quả của puzzles đó.
* Puzzles phải có độ khó có thể điều chỉnh được.
* Tiến trình miễn phí (process free): cơ hội giành được câu trả lời của puzzles trong bất kỳ đơn vị thời gian nào đều tỉ lệ thuận với hash power đã đóng góp. Điều này có nghĩa rằng các thợ mỏ lớn với phần cứng rất mạnh chỉ nên có một lợi thế tỷ lệ trong việc khai thác tiếp theo để tìm một giải pháp puzzles khác.

1. ASIC Resistant Mining Puzzles.
   1. Giảm sự khác biệt giữa phần cứng chuyên biệt (specific) và phần cứng thông thường.

Để giảm thiểu sự khác biệt này là tìm một số Mining Puzzles giúp làm giảm thiểu khoảng cách giữa phần cứng custom và phần cứng chuyên biệt cho mining.

* 1. Giảm sự khác biệt giữa phần cứng trong tương lai và ASICs hiện tại.

Để giảm thiểu sự khác biệt này là tìm một số Mining Puzzles giúp làm giảm thiểu khoảng cách giữa các thiết bị trong tương lai với thiết bị ASIC mà chúng ta hiện có.

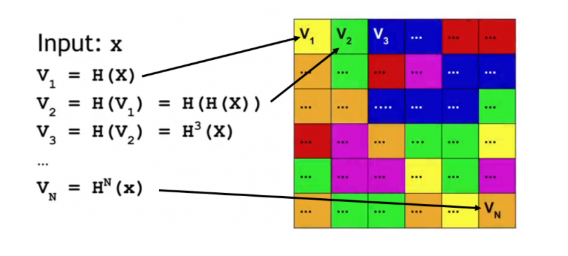
1. Scrypt.
   1. Định nghĩa.

Scrypt là một hàm băm được sử dụng lần đầu tiên bởi đồng tiền điện tử Litecoin, và được xem như là một thay thế cho hàm băm SHA-256 nổi tiếng. Scrypt và SHA-256 được sử dụng như các thuật toán khai thác trong các giao thức Litecoin và Bitcoin tương ứng.

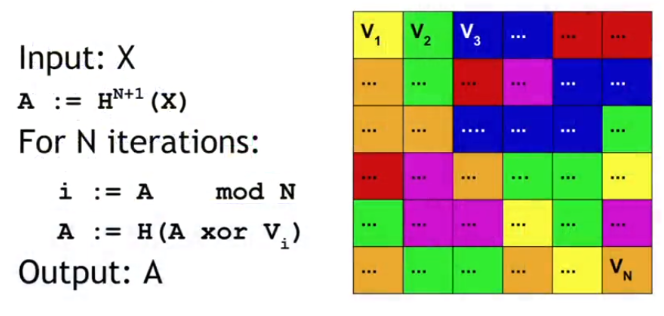
* 1. Tính toán Scrypt.

Hai phép tính hàm băm Scrypt của 1 chuỗi đầu vào x, H(x) gồm 2 phần:

* Điền vào một khối lớn bộ nhớ truy cập ngẫu nhiên với các giá trị ngẫu nhiên. Khối đó có thể được xem như là một ma trận được lắp đầy với N lần lặp lại. Giá trị đầu tiên V­1 là hàm băm của x, giá trị thứ 2 V2 là giá trị băm của V1. Và cứ thế đến Vn.



* Đọc từ khối này theo thứ tự ngẫu nhiên. Sau đó, ta sử dụng bộ tích lũy A để chọn các giá trị từ các ô đó theo cách ngẫu nhiên. Lúc đầu, giá trị đầu tiên là hàm băm được áp dụng cho Vn. Tại mỗi lần lặp, ta tính toán lại giá trị index của mục được chọn khi còn phần còn lại của phép chia A cho N. Sau đó, ta tính toán giá trị A tiếp theo bằng hàm băm A:= H(A xor Vi). Giá trị cuối cùng của A sau N lần lặp lại sẽ là giá trị đầu ra.



* 1. Nhược điểm của Scrypt.
* Cần N bước và N ô nhớ để kiểm tra tính chính xác của Proof. Nên nó rất nặng trên mạng peers để xác nhận các miners khác làm việc.
* Một số ASIC hỗ trợ Scrypt đã ra đời.

1. Blockchain mining: Proof of Useful Work
   1. Primecoin

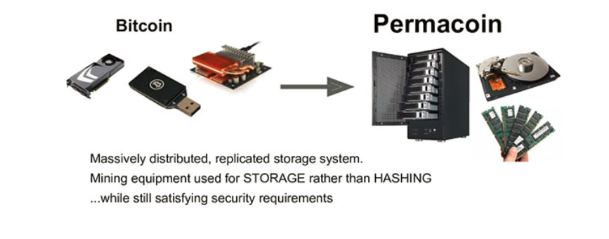
Primecoin là một loại tiền mã hóa, được phát hành trong thị trường đào coin phân tán. Primecoin giới thiệu một hình thức đồng thuận ban đầu dựa vào các con số nền tảng và là loại tiền mã hóa đầu tiên trên thế giới được thiết kế với công nghệ máy tính khoa học.

Việc tìm kiếm một giải pháp trong Primecoin đòi hỏi phải tìm một chuỗi Cunningham (Cunningham Chain).

Chuỗi Cunningham là một dãy số nguyên tố p, trong đó mỗi số có dạng 2ia+1.

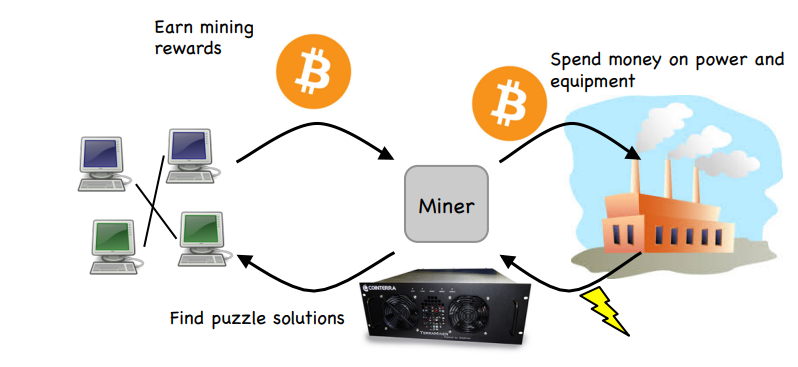
* 1. Permacoin.

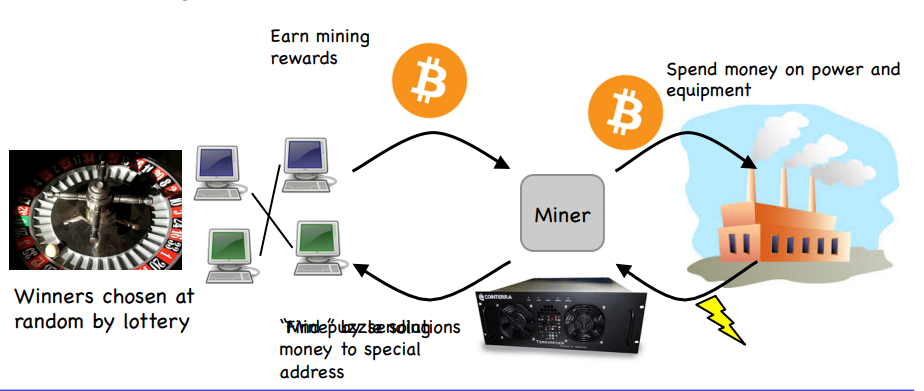
Permacoin được sinh ra để thay thế việc đào Bitcoin bằng ASICs, tính toán hàm băm bằng SHA-2, với các thiết bị lưu trữ như ổ cứng và bộ nhớ. Vì vậy, tác dụng phụ sẽ là phân phối ồ ạt, nhân rộng hệ thống sao lưu.



Cách hoạt động của Permacoin:

* Nó bắt đầu với một tập tin lớn F và được chia thành nhiều khối. Mạng network có nhiệm vụ lưu trữ nó. Ta có thể tưởng tượng rằng F được chọn ngẫu nhiên bởi trusted dealer từ trước. Và mỗi user lưu trữ tập con của nó.
* Phần đầu tiên liên quan đến việc xây dựng cây Merkle nơi mỗi lá là một phân đoạn của tập tin. Mỗi người dùng tạo một cặp khóa để khai thác. Họ sẽ dùng pubic key để giả-ngẫu nhiên (pseudo-ramdomly) chọn tập con để lưu trữ.

1. Proof-of-stake Mining Puzzles.
   1. Proof of work Mining.
   2. Virtual Mining.



* 1. Lợi ích của Vitual Mining.
* Chi phí tổng thể thấp hơn.
* Ít gây tổn hại môi trường.
* Khoản tiết kiệm được phân phối cho tất cả coin holders.
* Không có lợi thế ASIC.

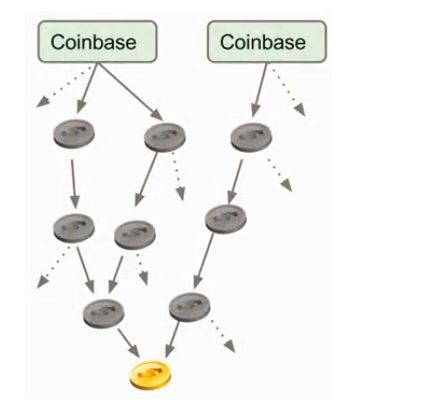
CHAPTER 8

BITCOIN AS PLATFORM

1. Bitcoin as an Append -Only Log and Timestamping.
   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. Trace Bitcoin ownership overtime.

Mỗi bitcoin đều có lịch sử và chúng ta có thể theo dõi nó ngược trở lại cho đến khi nào giao dịch coinbase tạo ra nó.

* 1. Authenticated Metadata for Currency
* Sign desired metadata + banknote serial #: SIGNk(M,#)
* Tiền tệ bây giờ có thể đại diện cho bất cứ điều gì.
* Thừa hưởng thuộc tính chống hàng giả.
* Giá trị nền tảng được duy trì.
* Một số người dùng có thể không hiểu được metadata mới.
  1. Colored Coins.

