**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.

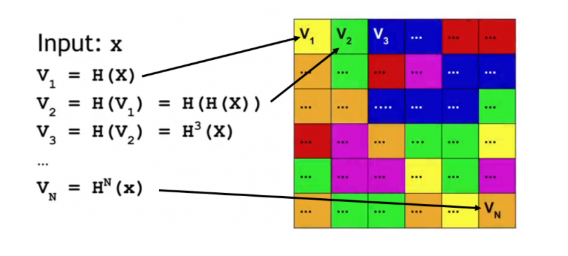
1. Scrypt.
   1. Định nghĩa.

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.

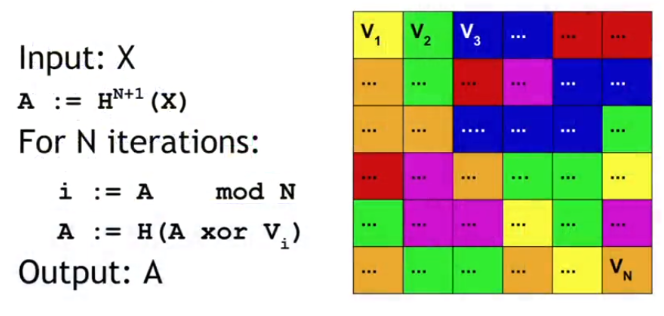
* 1. Tính toán Scrypt.

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.

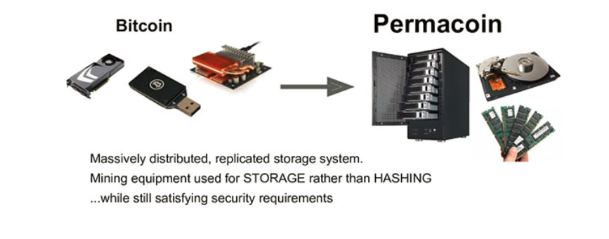
Các điểm mạnh của Primecoin:

Xác nhận nhanh chóng: Với Bitcoin, các giao dịch thường mất trung bình khoảng 10 phút để xác nhận. Tuy nhiên, các cổ phiếu Primecoin chỉ mất khoảng 1 phút. Điều này cho phép các giao dịch an toàn được thực hiện nhanh chóng hơn, cứ 6 xác nhận sẽ mất khoảng 50 phút nếu trong Bitcoin nhưng sẽ chỉ mất khoảng 6 phút trong Primecoin.

Tự điều chỉnh tiền thưởng cổ phần: Bitcoin nổi tiếng về thuật toán cung cấp tiền tệ được giám sát và đảm bảo rằng chỉ 21 triệu bitcoin sẽ được phát hành cũng như định rõ tỷ lệ cho mỗi bitcoin này. Primecoin định hướng theo một cách khác. Số lượng Primecoin (XPM) phát hành mỗi cổ phiếu luôn luôn tương đương khoảng 999 được chia cho bình phương của sự cản trở.

* 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.



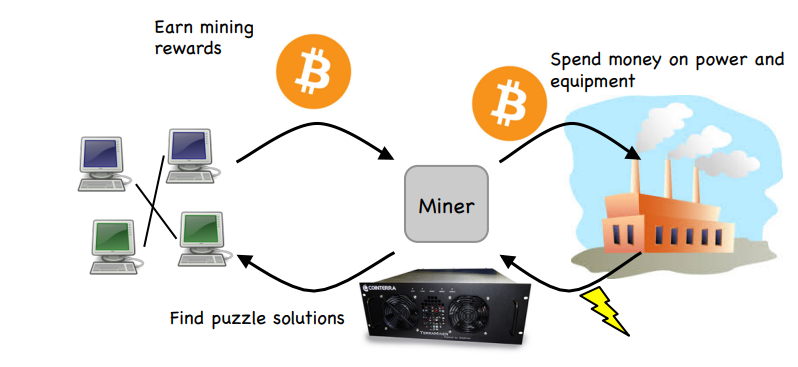
Cách hoạt động của Permacoin:

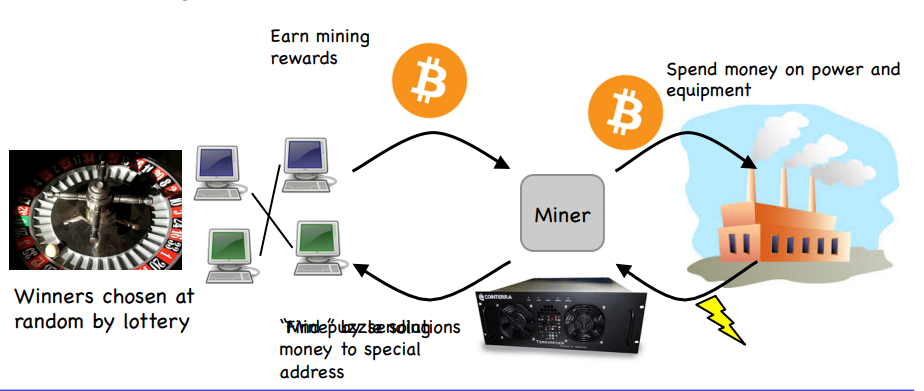
* Nó bắt đầu với một tập tin lớn F và được chia thành nhiều khối. Mạng network có nhiệm vụ lưu trữ nó. Ta có thể tưởng tượng rằng F được chọn ngẫu nhiên bởi trusted dealer từ trước. Và mỗi user lưu trữ tập con của nó.
* Phần đầu tiên liên quan đến việc xây dựng cây Merkle nơi mỗi lá là một phân đoạn 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.

Proof of stake được sử dụng nhiều trong Smart Contract (Casper).

Proof of stake hoạt động như sau: Trong các node tham gia, một node sẽ được chọn ngẫu nhiên để trở thành người kiểm định và đóng gói block. Node này được gọi là các validator. Và điều kiện để tham gia là các node này cần bỏ ra một khoản tiền vào mạng lưới, thường được gọi là **bet** (đặt cược)

* 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.