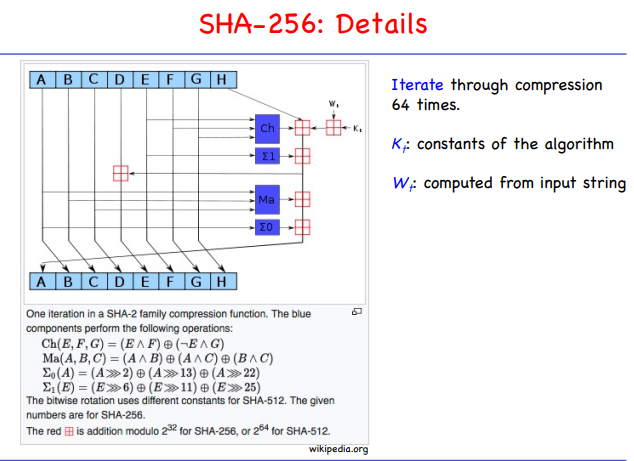
Chapter 5.

BITCOINT MINNING

1. Nhiệm vụ của các Bitcoint Miners. (The Task of Bicoin Miners)
   1. Tham gia vào mạng lưới, lắng nghe các transaction.

* Xác nhận tất cả các giao dịch được đề xuất.
  1. Lắng nghe các block mới, duy trì các chuỗi khối khác.
* Khi xuất hiện 1 block mới thì xác nhận nó.
  1. Lắp ráp 1 khối hợp lệ mới.
  2. Tìm một “nonce” để block đó được hợp lệ.
* Một Nonce: là một số được sử dụng để tìm một hash hợp lệ.
  1. Hi vọng là mọi người accept block mới của mình.
  2. Kiếm lợi nhuận.

1. Phần cứng để đào (Mining Hardware).
   1. SHA-256.

* SHA (Secure Hash Algorithm hay thuật toán băm an toàn) là năm thuật toán được chấp nhận bởi FIPS dùng để chuyển đoạn dữ liệu nhất định thành một đoạn dữ liệu có chiều dài không đổi với xác xuất khác biệt cao.
  + SHA-256 được phát triển bởi NSA (National Security Agency hay Cục an ninh quốc gia Mỹ) vào năm 2001. Trả ra kết quả 256-bit2.2. GPU Mining.
* GPU được thiết kế để hỗ trợ cho đồ họa có hiệu suất cao.
* Đặc trưng nổi bật:
  + Tính song song cao.
  + Thông lượng cao.
* Lần đầu tiên được sử dụng vào năm 2010.
* Được triển khai trong OpenCL. OpenCL là một ngôn ngữ lập trình dựa trên C, cho phép lập trình song song giữa GPU và CPU. OpenCL được đưa ra để làm 1 chuẩn GPGPU duy nhất, cho phép sử dụng sức mạnh của GPU vào những công việc tính toán khác ngoài đồ họa.
* Ưu điểm của GPU Mining:
  + Có sẵn, dễ dàng để lắp đặt.
  + Chạy song song ALUs
  + Có thể điều khiển nhiều GPU chỉ bằng 1 CPU.
  + Có thể ép xung.
* Nhược điểm của GPU mining:
  + Sử dụng phần cứng kém. Dễ gây hư hỏng các thiết bị.
  + Tản nhiệt kém. Do phải ép xung lên cao để giải quyết các thuật toán phức tạp nên nhiệt tỏa ra là rất lớn.
  + Sử dụng nhiều điện năng.
  + Ít main board hỗ trợ sử dụng nhiều GPUs.



* 1. FPGA Mining.
* FPGA: Field Programmable Gate Area.
* FPGA là 1 chip silicon chứa trong nó rất nhiều “khối logic” có thể tái cấu hình CLB (Configurable Logic Blocks) được liên kết với nhau bằng các liên kết khả trình (Programmable Interconnect).
* FPGA được sử dụng đầu tiên vào tháng 6 năm 2011
* Được sử dụng trong Verilog.
* Ưu điểm của FPGA Mining:
  + Hiệu suất cao hơn GPU Mining.
  + Tính toán nhanh các thuật toán Bitwise. Bitwise là các thuật toán thực hiện trên các Bit như dịch Bit, đảo Bit, các phép toán AND, OR, XOR, ….
  + Làm mát tốt hơn.
  + Có thể tùy chỉnh hoặc mở rộng phần cứng.
* Nhược điểm của FPGA Mining:
  + Tốn nhiều điện năng hơn GPU Mining.
  + Tối ưu hóa kém cho địa chỉ 32-bit.
  + Kén người dùng do phải có hiểu biết chuyên môn cao.
  + Linh kiện đắt hơn GPU Mining.
  1. Bitcoin ASICs.
* ASIC: Application Specific Intergrated Circuit, là một mạch tích hợp được thiết kế để phục vụ riêng cho một mục đích nào đó
* Lý do áp dụng ASIC vào đào Bitcoins:
  + Đào Bitcoin mạnh mẽ.
  + Có khả năng nâng cấp để đạt được hiệu quả đào tốt hơn card màn hình.
  + Ít tiêu tốn điện năng.

1. Mining Pool (Bể đào).

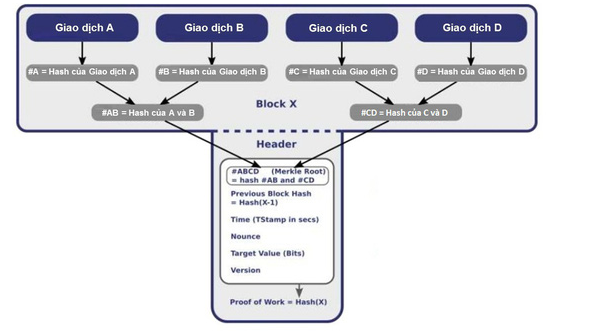
3.1. Khái niệm cơ bản.

* Mining Pool là nơi tập hợp các thợ mỏ, mỗi thợ mỏ đóng góp Hashpower để cùng khai thác các khối Bitcoin để giải quyết 1 block nhanh hơn và chia lợi nhuận theo tỷ lệ đóng góp. Đa số các mining pool đều có thu phí trên lợi nhuận của mỗi thợ mỏ (thu bởi pool manager).

3.2. Thuật toán đào Bitcoin.

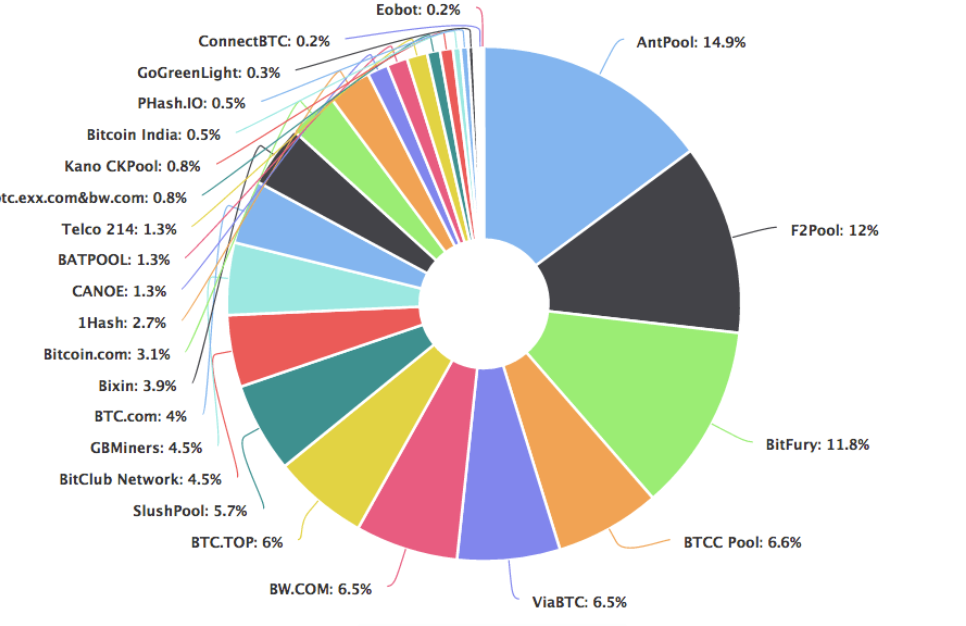
- Trước hết, thông tin về các giao dịch mới phát sinh trong một khoảng thời gian được gói vào trong một khối. Sau đó thông tin này được mã hóa bằng thuật toán SHA-256, mã hóa thành 1 chuỗi 64 ký tự bao gồm chữ và số.

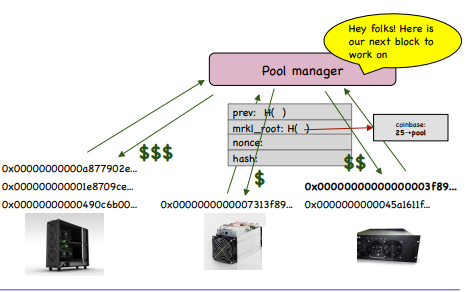
- Sau khi thu được dãy ký tự đã được mã hóa, dãy ký tự này tiếp tục được ghép với **kết quả mã hóa của 1 giao dịch kế tiếp** bằng thuật toán SHA-256 (double hashing) cho tới khi còn 2 kết quả hashing của các giao dịch trong khối này sau khi mã hóa. Quá trình này tạo thành cây Merkle (Merkle tree).



* Kết quả hashing cuối cùng được ghép cùng với các thông tin khác trong khối, bao gồm kết quả hashing của khối trước đó, nhãn thời gian ghi chép việc khởi tạo khối và tham số **nonce** là biến chạy ngẫu nhiên. Kết quả hashing cuối cùng này sẽ có dạng chuỗi 256-bit chẳng hạn có dạng:

(1) ‘0000641727781545e50c0235823c9ae0785d419499cc5a5dcdff2332a53f0f7f’.

* Thuật toán Bitcoin quy định, một khối mới chỉ có thể được khởi tạo khi thợ mỏ tìm được kết quả hashing cuối cùng này nhỏ hơn giá trị target (Target value) đang duy trì trong hệ thống.
* Ví Dụ , Target value mà hệ thống đang duy trì là: ‘00007bbd6491304360d142bd5f32610214937c263b0bc6c44b3ac04574b62d4c’, thì kết quả hashing (1) ở trên được coi là hợp lệ, bởi vì các ký tự đầu ‘00006’ nhỏ hơn ‘00007’ của Target value.
* Sau đó, kết quả này ngay lập tức được chuyển tới các block khác trong mạng lưới để xác nhận. Sau khi có đa số (trên 50%) số block trong blockchain xác nhận kết quả, block mới chính thức được tạo thành.
* Một số Mining Pool:
  1. Cơ chế hoạt động của Mining Pool.
* Sau khi khối trước đó đã được tìm thấy, Pool manager sẽ tiếp tục đi tìm các transactions và ráp lại thành 1 block và sẽ thông báo cho toàn bộ miners trong pool đó rằng cái block đó sẽ là cái block tiếp theo mình sẽ làm.
* Pool manager sẽ ráp các transaction thành 1 Merkle tree và được thêm vào block đó. Và phải đảm bảo rằng trong block đó chứa root của Merkle tree của transaction.
* Sàn giao dịch Coinbase sẽ tạo coins mới và gán quyền sỡ hữu cho pool đó.
* Block header sẽ được gửi cho toàn bộ miners trong pool đó và bắt đầu làm việc.
* Sau đó, các miners sẽ từ từ tìm các khối hoặc các mảnh, tới khi nào một trong các miners hy vọng tìm được 1 valid block mà sau đó sẽ được published.
* Sau đó, tất cả các miners sẽ gửi tất cả các mảnh (shares) thu được về cho pool manager.
* Pool manager sẽ lấy được doanh thu kiếm được từ block đã được published và phân chia lại cho các miners dựa trên số công việc họ đã làm được



* 1. Mining pool Protocol
* Các API để tìm nạp khối và gửi các mảnh (Shares).
  + **Stratum** : server sẽ cung cấp các Client Template để các client có thể sử dụng để thực hiện các công việc độc lập. Bao gồm block header và thông tin giao dịch trước đó. Khi có sự thay đổi khối, việc chuyển đổi data cũng sẽ thực hiện rất nhanh. Không như các giao thức khác, Stratum không sử dụng phương thức HTTP. Stratum sử dụng ít băng thông nhất trong tất cả các loại phương thức.
  + **Getwork**: đây là kiểu đào bình thường. Server sẽ gửi cho Client các block header không có bất cứ transaction nào hoặc bất kỳ cách nào để sửa đổi ngoại trừ giá trị nonce. Client bị giới hạn để thử tất cả các giá trị nonce có thể có và sau đó sẽ cần thêm các request từ Server. Điều này gây ra việc sử dụng băng thông rất lớn cho mining hardware.
  + **Getblockshare**:
  1. Mining Pool Variations (Các biến thể của mining pool).
* **Pay Per Share**: cung cấp một khoản thanh toán tức thời, đảm bảo mỗi cổ phần được giải quyết bởi một thợ mỏ. Thợ mỏ được thanh toán từ số dư hiện tại của khoản tiền và có thể thu hồi khoản thanh toán ngay lập tức. Mô hình này cho phép các thợ mỏ chuyển giao nhiều rủi ro cho nhà điều hành pool. Do đó, mức phí cho phương pháp này là cao nhất.
* **Proportional** : khi một khối được tìm thấy, phần thưởng được phân phối theo tỷ lệ cho tất cả thợ mỏ dựa trên số cổ phần họ đã từng tìm thấy.
* **“Luke-jr” approach**:

1. Mining Incentives and Strategies (khuyến khích và chiến lược).

* Một số hướng chiến lược:
  + Transaction được thêm vào các block là các transations có transaction fee là thấp nhất.
  + Block đứng đầu phải là khối có chuỗi hợp lệ dài nhất.
  + Cách chọn giữa các khối va chạm (colling Blocks) : khối đầu tiên nghe được.
  + Khi nào thông báo có khối mới : ngay sau khi tìm được chúng.

4.1.Forking Attack.

- Ý tưởng là thực hiện việc double sending.

- Giả sử như có một số tiền đang được gửi cho Bob và đó là transaction nằm trong chuỗi dài nhất. Thì miners có thể thử để chèn thêm vào một transaction khác hướng tới miners đó kết nối với cái block trước đó mà cái block đó đang chứa 1 transaction khác. Tại thời điểm chèn giao dịch không phải là một phần của chuỗi dài nhất. Nhưng nếu các miners có hơn 50% hash power, anh ta có thể làm cho chuỗi mới trở thành chuỗi dài nhất và có thể rewrite lại lịch sử. Vậy nên transaction hợp lệ giờ đây sẽ hướng tới miners nó chứ không phải hướng về Bob nữa.

4.2. Checkpoint Lockin

* 1. Temporary Block-withholding Attacks
* Giả sử ta có 1 đào được 1 block, thay vì công bố cho toàn mạng và nhận lại phần thưởng, ta giữ lại khối này và tiếp tục khai thác một mình trên blockchain với khối mới này.
* “Khối bí mật” hay “secret block” là khối được bạn đào nhưng giữ lại không công bố cho toàn mạng. Khi bạn tìm được một khối khác, bạn có thể tiến hành công bố cả hai khối này cho mạng. Khi đó:
  + Nhận gấp đôi phần thường mà bạn có thể thu được.
  + Trở thành người kiểm soát hai khối thay vì một và do đó tăng gấp đôi số tiền có thể kiếm được thông qua phí giao dịch
  1. Punitive Forking.
* Là một trong 2 phân nhánh của dạng tấn công Blacklist.
* Giả sử, muốn chặn tất cả các giao dịch từ địa chỉ X, mình sẽ đưa ra thông báo rằng sẽ từ chối toàn bộ các transaction tới mình từ địa chỉ X đó.
* Nhưng để có thể cho địa chỉ X vào blacklist, đòi hỏi ta phải nắm nhiều hơn 51% hash power của mạng đó. Để khi xuất hiện 1 block từ địa chỉ X xuất hiện trong blockchain, ta sẽ bắt đầu tạo 1 phân nhánh và tiếp tục trên nhánh mới mà không chứa nhánh có block được gửi từ địa chỉ X.

CHAPTER 6.

BITCOIN AND ANONYMITY

1. Anonymity Basic.

Anonymity = pseudonymity + unlinkability

* Pseudonymity trong Bitcoin có nghĩa là thay vì dùng tên thật, người dùng sẽ dùng các Public key để giao dịch.
* Unlinkability có nghĩa là các tương tác khác nhau của cùng một người dùng với hệ thống không nên được liên kết với nhau.
  1. Tại sao lại quan tâm đến Unlinkability?
* Có nhiều Services của Bitcoin yêu cầu danh tính thực.
* Các profiles được liên kết có thể bị khử ẩn danh (de-anonymized) bởi nhiều kênh phụ.
  1. Định nghĩa Unlinkability trong Bitcoin
* Unlinkability trong Bitcoin gồm 3 ý chính sau:
  + Khó để liên kết các địa chỉ khác nhau của cùng 1 user.
  + Khó để liên kết các transaction khác nhau của cùng 1 user.
  + Khó để liên kết người gửi giao dịch với người nhận giao dịch đó.
  1. Quantifying Anonymity.
* Việc Unlinkability tất cả các địa chỉ và các transactions là điều khó có thể làm được. Nên thay vào đó, ta sẽ tối đa hóa kích thước của bộ ẩn danh của mình. Bộ ẩn danh là kích thước của một tập các địa chỉ hoặc các transactions mà ta muốn ẩn. Vì vậy, người khác nhìn vào sẽ thấy rằng có hàng ngàn giao dịch trông giống giao dịch của mình, nên sẽ không biết được transaction nào là của mình.
* Để tính toán được bộ ẩn danh này, cần phải xác định cụ thể mô hình của đối thủ. Xác định rõ đối thủ biết gì, chưa biết gì và không biết gì.
  1. Vai trò của Anonymity.
* Currency trên blockchain là hoàn toàn công khai và được theo dõi vĩnh viễn. Nếu như không có ẩn danh, tính riêng tư của currency sẽ không được đảm bảo so với currency ở các ngân hàng truyền thống.