**2. Các mô hình và cách thức hoạt động của Blockchain**

Blockchain bao gồm ba khái niệm quan trọng: blocks (khối), nodes (nút) and miners (thợ đào).

**Blocks**

Đơn vị lưu trữ dữ liệu của Blockchain được gọi là block. Mọi chain đều bao gồm nhiều blocks và mỗi block có ba phần tử cơ bản:

* Dữ liệu trong một block.
* Một số nguyên 32 bit được gọi là Nonce (Number only used once). Nonce được sinh ra ngẫu nhiên khi một block được tạo. Sau đó, số nonce được thêm vào hàm hash của block.
* Một hàm băm (hash) có chức năng tóm tắt dữ liệu từ một chuỗi dữ liệu có độ dài bất kỳ thành một giá trị chuỗi ký tự hoặc số duy nhất có độ dài cố định (256 bit).

Ví dụ: với thuật toán hash SHA256, chuỗi “Hello World” sẽ trở thành:

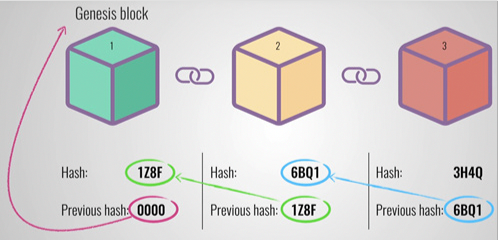
SHA256(“Hello World”) = a591a6d40bf420404a011733cfb7b190d62c65bf0bcda32b57b277d9ad9f146e

Bất cứ sự thay đổi nhỏ nào trong dữ liệu gốc đều dẫn tới sự thay đổi hoàn toàn của giá trị băm:

SHA256 (“Hello Worl”) = 12fec4c65dd4455c48aff8977a7cd8ccb97539ad4cd7c37f13cf71ba8bee9a98

**Miners**

Miners tạo ra các block mới trên một chain thông qua quá trình mining.



Trong blockchain, mỗi block đều có hàm hash và số nonce riêng biệt, nhưng cũng tham chiếu đến hàm hash của block trước đó trong cùng một chain. Vì vậy, việc khai thác (mining) một block không dễ dàng, đặc biệt là trên các chain lớn.

Các thợ đào (miners) sử dụng phần mềm đặc biệt nhằm giải quyết các bài toán phức tạp để tìm ra được số nonce mà tạo ra một hàm hash được chấp nhận. Bởi vì số nonce có chiều dài 32 bits còn kết quả của hash có chiều dài 256 bits nên có khoảng bốn tỷ tổ hợp nonce-hash có thể phải được khai thác (mine) trước khi tìm được kết quả đúng. Khi điều đó xảy ra, những thợ đào (miners) được cho là đã tìm thấy "golden nonce" và block của họ được thêm vào chuỗi.

Khi thực hiện thay đổi đối với block đã có trước đó trong một chain, ta bắt buộc phải khai thác (mine) lại không chỉ block đó mà còn tất cả các block sau nó. Đây là lý do tại sao việc thao túng công nghệ blockchain cực kỳ khó khăn vì việc tìm ra các “golden nonce” đòi hỏi một lượng lớn thời gian và khả năng tính toán.

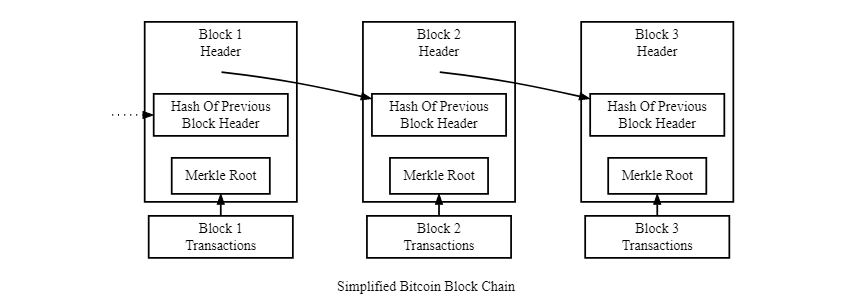
Khi một block được khai thác (mine) thành công, những thay đổi được tất cả các nodes trên mạng chấp nhận và người khai thác (miner) được thưởng crypto currency.

**Nodes**

Node đóng vai trò là cơ sở hạ tầng của Blockchain. Nó là các nút giúp lưu trữ, truyền tải và bảo quản dữ liệu blockchain, vì vậy về mặt lý thuyết, một blockchain tồn tại trên các node.

Cốt lõi của nó dựa trên các nguyên tắc của mạng P2P (Peer to Peer). Trong hầu hết các mạng, không có máy chủ trung tâm, mà là sự đồng thuận giữa những node.

Khi một thợ đào (miner) hay người xác thực (validator) thêm một block giao dịch mới vào blockchain, họ sẽ truyền block tới tất cả (hoặc một phần, tùy vào thuật toán đồng thuận của blockchain sử dụng) các node trên mạng.



Cách hoạt động node như sau:

* Các node kiểm tra xem một block giao dịch có hợp lệ không và chấp nhận hoặc từ chối nó.
* Nếu chấp nhận, các node sẽ lưu trữ các block giao dịch (lưu trữ lịch sử giao dịch blockchain).
* Các node phát và lan truyền lịch sử giao dịch này đến các node khác để đồng bộ hóa với blockchain (cập nhật về lịch sử giao dịch).