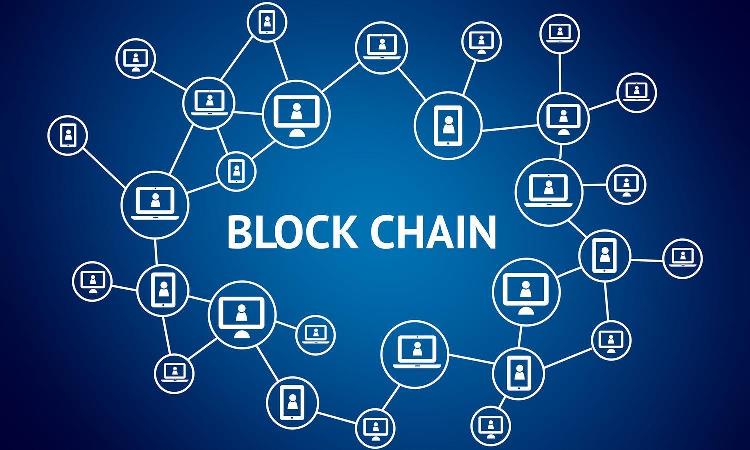
**I. TỔNG QUAN VỀ HỆ THỐNG BLOCKCHAIN**

1. Khái niệm Blockchain

Theo nghĩa đen, Block là khối, Chain là chuỗi. Blockchain là chuỗi các khối liên kết với nhau tạo thành.

Theo chuyên môn kỹ thuật, Blockchain là công nghệ lưu trữ và truyền tải thông tin bằng các khối được liên kết với nhau và mở rộng theo thời gian do đó được gọi là chuỗi khối (Blockchain). Mỗi khối chứa đựng các thông tin về thời gian khởi tạo và được liên kết với các khối trước đó. Blockchain được thiết kế để chống lại sự thay đổi dữ liệu. Thông tin trong Blockchain không thể bị thay đổi và chỉ được bổ sung thêm khi có sự đồng thuận của tất cả các nút trong hệ thống. Ngay cả khi nếu một phần của hệ thống Blockchain sụp đổ, những máy tính và nút khác sẽ tiếp tục hoạt động để bảo vệ thông tin.

Đặc biệt Blockchain có khả năng truyền tải dữ liệu mà không đòi hỏi trung gian để xác nhận thông tin. Hệ thống Blockchain bao gồm nhiều nút độc lập có khả năng xác thực thông tin. Về cơ bản Blockchain là một chuỗi các máy tính mà tất cả phải chấp thuận một giao dịch trước khi nó có thể được xác nhận và ghi lại, giống như việc bạn gửi cái hộp đi mà mọi người đều xác nhận cái hộp đó là của bạn chứ không cần một vị luật sư hay một ngân hàng nào cả. Thông tin thì không thể bị thay đổi và chỉ được bổ sung khi có sự đồng thuận của tất cả các nút trong hệ thống.



Hiểu một cách đơn giản, Blockchain là cuốn sổ cái điện tử, ghi mọi chi tiêu, được sao chép thành hàng ngàn bản, có trên hàng ngàn máy tính rải rác khắp thế giới. Nó không thể bị làm sai lệch, và nó cho phép người dùng sở hữu tài sản và chuyển khoản, được ghi nhận lại mà không cần đến sự xác thực từ một đơn vị nào bên ngoài.

2. Các phiên bản của công nghệ Blockchain

Công nghệ Blockchain ra đời vào năm 2008 bởi Satoshi Nakamoto. Hiện tại Blockchain được chia làm 3 phiên:

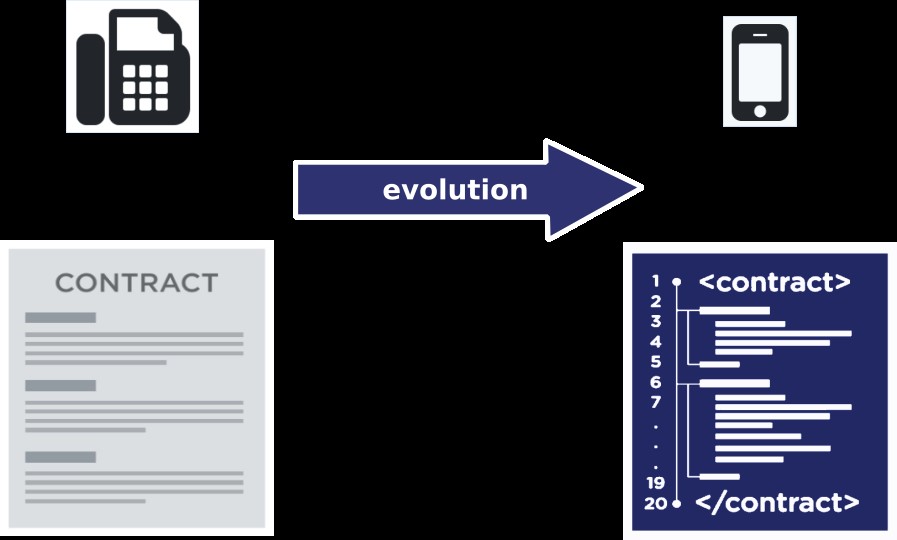
* Blockchain Version 1.0 – Currencies

Ứng dụng vào tiền thuật toán: Bao gồm chuyển đổi tiền tệ, kiều hối và hệ thống thanh toán kỹ thuật số. Đây cũng là lĩnh vực quen thuộc với chúng ta nhất và xem như là lãnh thổ của Bitcoin và những Cryptocurrencies khác.



* Blockchain Version 2.0 – Contracts

Ứng dụng trong xử lý tài chính và ngân hàng: Mở rộng Blockchain, đưa vào các ứng dụng tài chính và thị trường. Các tài sản bao gồm cổ phiếu, chi phiếu, nợ, quyền sở hữu và bất kỳ điều gì có liên quan đến thỏa thuận hay hợp đồng. Hiện nay, nhiều công ty trong ngành dịch vụ tài chính ngân hàng đã chú ý đến tiềm năng của công nghệ Blockchain.



* Blockchain Version 3.0 – Organizing Activity:

Đưa Blockchain vượt khỏi biên giới tài chính, và đi vào các lĩnh vực như giáo dục, chính phủ, y tế và nghệ thuật. Ở những lĩnh vực này sẽ lại có nhiều loại như Physical, Digital hay Human in nature.

Điển hình như Đảng Cộng Hòa tại Utah sử dụng công nghệ Blockchain để giúp các cử tri bỏ phiếu kín, đảm bảo sự công bằng cho mọi cử tri và đại biểu. Hay các bản ghi sức khỏe điện tử (EHR) ở Estonia được lưu trữ và hoạt động dưới công nghệ Blockchain và còn rất nhiều ứng dụng tiềm năng khác đang được triển khai rộng rãi.

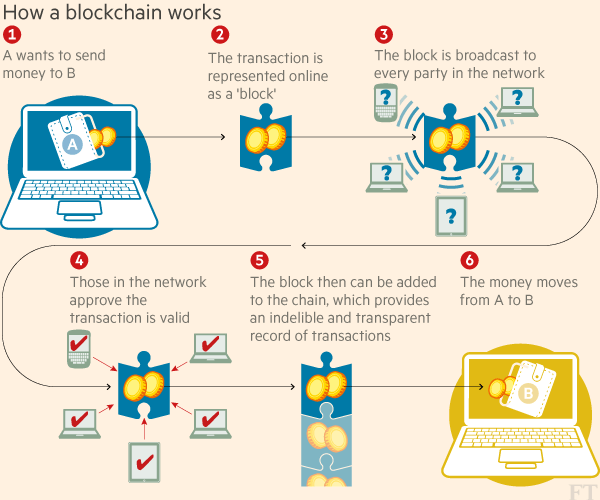


3. Hoạt động của Blockchain

Hệ thống Blockchain sử dụng các thuật toán giúp nó có thể truyền tải dữ liệu mà không thông qua trung gian để xác nhận thông tin. Hệ thống Blockchain tồn tại nhiều nút (Node) độc lập với khả năng xác nhận thông tin. Mọi thông tin trong Blockchain có thể thay đổi hoặc bổ sung thêm khi có sự chấp nhận của tất cả các nút trên hệ thống. Blockchain vẫn hoạt động bình thường khi một phần của hệ thống sụp đổ, những máy tính và các nút vẫn hoạt động để bảo vệ thông tin, giữ cho Blockchain không bị mất dữ liệu.

* Cách hoạt động của công nghệ Blockchain

1. Người dùng yêu cầu một giao dịch (mua, bán, trao đổi).
2. Yêu cầu sẽ được phát tới các mạng ngang hàng P2P (Peer to Peer: bao gồm các máy tính (được gọi là Node) kết nối với nhau).
3. Các máy tính trong hệ thống này sẽ xác thực giao dịch cùng với thông tin người dùng thông qua các thuật toán trong Blockchain.
4. Sau khi giao dịch được xác nhận, chúng sẽ được kết hợp với những giao dịch khác tạo nên một khối (gọi là Block) trong hệ thống Blockchain – Nơi nó sẽ tồn tại và không thể sửa đổi.
5. Hoàn thành giao dịch.



* Ví dụ thực tế về cách hoạt động của một giao dịch trong Blockchain

Ví dụ anh A mua một món đồ từ Công Ty B. Cả hai đều có ví Bitcoin (hoặc các Altcoin khác). Giao dịch sẽ xuất phát từ Ví của anh A thông qua một “lệnh đề xuất” với Blockchain làm cho ví của anh A vơi đi và tăng phần đó vào ví của Công Ty B.

Hệ thống các máy tính (Node) trong mạng Blockchain sẽ thực hiện các bước xác nhận sự thay đổi thông qua các thuật toán. Khi lệnh đề xuất này được đưa ra nó sẽ phải qua một loạt các bước kiểm tra (thông qua các Node) khác nhau, bằng cách kiểm tra “cuốn sổ cái”, để liệu xem anh A còn đủ số Bitcoin mà A muốn dùng để chi trả hay không. Nếu mọi thứ được đảm bảo, các Node đặc biệt gọi là các Miner (thợ mỏ) sẽ “đóng gói” đề xuất của anh A với các giao dịch tương tự đã được xác nhận khác và tạo thành một Block mới rồi chuyển vào “cuốn sổ” Blockchain. Giao dịch thành công!

**II. SƠ LƯỢC VỀ BITCOIN VÀ ETHEREUM**

1. Bitcoin

Bitcoin là một loại tiền mã hóa, được phát minh bởi một người ẩn danh tên Satoshi Nakamoto dưới dạng phần mềm mã nguồn mở từ năm 2009. Bitcoin có thể được trao đổi trực tiếp bằng thiết bị kết nối Internet mà không cần thông qua một tổ chức tài chính trung gian nào.



Bitcoin có cách hoạt động khác hẳn so với các loại tiền tệ điển hình: Không có một ngân hàng trung ương nào quản lý nó và hệ thống hoạt động dựa trên một giao thức mạng ngang hàng trên Internet. Sự cung ứng của Bitcoin tự động và hạn chế được phân chia theo lịch trình định sẵn dựa trên các thuật toán. Bitcoin được cấp tới các máy tính "đào" Bitcoin để trả công cho việc xác minh giao dịch Bitcoin và ghi chúng vào cuốn sổ cái được phân tán trong mạng ngang hàng - được gọi là blockchain. Cuốn sổ cái này sử dụng Bitcoin là đơn vị kế toán. Mỗi bitcoin có thể được chia nhỏ tới 100 triệu đơn vị nhỏ hơn gọi là satoshi.

Bitcoin hoạt động dựa vào các thuật toán chữ kí số dựa trên đường cong Elliptic và được xác nhận bởi chuỗi các quá trình xử lý các hàm băm SHA256.

2. Ethereum

Ethereum là một nền tảng phần mềm mở dựa trên công nghệ Blockchain cho phép các nhà phát triển xây dựng và triển khai các ứng dụng dựa trên hệ sinh thái phân tán (Decentralized applications).



Ethereum được xem là một loại tiền mã hóa (Cryptocurrency), với đơn vị là Ether hay ETH, tương tự như Bitcoin nhưng không chỉ giới hạn ở khái niệm tiền tệ, Ethereum có thể ứng dụng vào nhiều thứ khác thông qua Smart contract dựa trên công nghệ Blockchain.

3. So sánh Bitcoin và Ethereum

Ethereum có thể làm được tất cả những gì mà Bitcoin làm được, cộng thêm những cải tiến mới mẻ đã giúp cho Ethereum thành công trong thời điểm hiện tại và báo hiệu một tương lai phát triển rất tiềm năng.

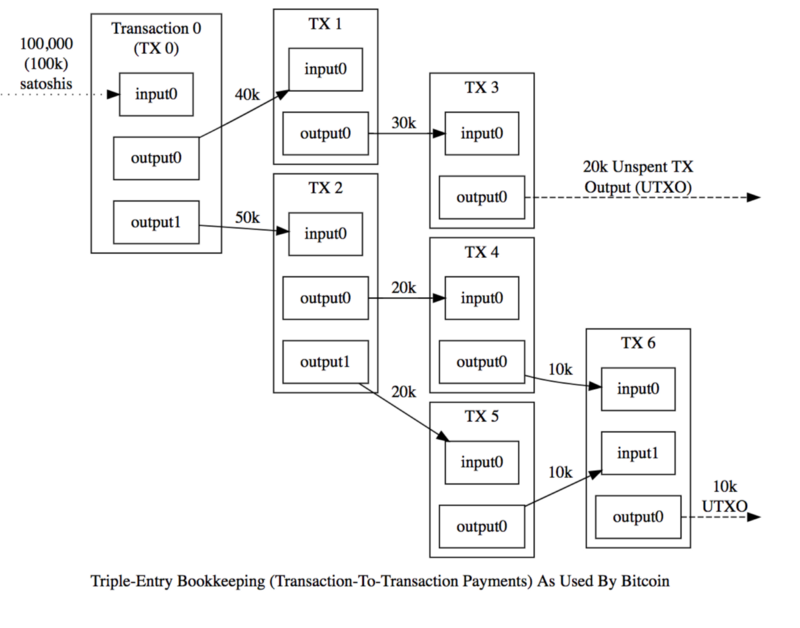
* Thời gian tạo khối Ethereum cực nhanh, chỉ mất khoảng 14 giây trong khi Bitcoin phải mất tới 10 phút để khởi tạo. Ethereum sử dụng giao thức Ghost khiến việc giao dịch trở nên nhanh chóng và vượt trội hơn Bitcoin
* Bitcoin giới hạn số lượng ở con số 21 triệu nhưng Ethereum thì ngược lại, số lượng Ether không giới hạn đã giúp Ethereum chiếm ưu thế hơn so với Bitcoin
* Phí giao dịch của Ethereum được trả bằng Gas (quy đổi được ra ether), được tính dựa trên độ phức tạp của thuật toán, mức độ sử dụng băng thông và nhu cầu lưu trữ. Còn phí giao dịch Bitcoin bị cạnh tranh bình đẳng với nhau để vào được khối của Bitcoin.
* Ethereum cho phép chạy mã Turing-complete, cho phép mọi tính toán được thực thi nếu có đủ khả năng tính toán và thời gian. Tuy nhiên điều này cũng mang lại nhiều rủi ro bị tấn công hơn cho Ethereum so với cấu trúc đơn giản của Bitcoin.
* Có 13% số ether được bán cho lượng người đã tài trợ dự án ban đầu. Còn những người đầu tiên đào Bitcoin nắm giữ số lượng lớn lượng Bitcoin đang phát hành.
* Ethereum chống lại việc sử dụng ASIC như Bitcoin. Người đào Ethereum phải sử dụng card đồ họa vì hàm băm của Ethereum yêu cầu sử dụng bộ nhớ.
* Ethereum chống lại việc đào mỏ tập trung bằng cách sử dụng giao thức Ghost.

**III. UTXO VÀ MÔ HÌNH TÀI KHOẢN/SỐ DƯ**

Hai loại mô hình lưu giữ hồ sơ là phổ biến trong các mạng blockchain ngày nay. Phương thức đầu tiên được gọi là Mô hình UTXO (Unspent Transaction Output) và mô hình thứ hai là Mô hình Tài khoản / Số dư. Mô hình UTXO được Bitcoin sử dụng và Ethereum sử dụng Mô hình tài khoản / số dư.

1. UTXO

Trong Bitcoin, mỗi giao dịch sử dụng đầu ra từ các giao dịch trước đó và tạo ra các kết quả đầu ra mới có thể được sử dụng bởi các giao dịch trong tương lai. Tất cả các giao dịch chưa sử dụng được lưu giữ trong mỗi nút được đồng bộ hóa hoàn toàn và mô hình này được đặt tên là “UTXO”. Ví của người dùng theo dõi danh sách các giao dịch chưa thanh toán được liên kết với tất cả các địa chỉ do người dùng sở hữu và số dư của ví được tính như tổng của các giao dịch chưa thanh toán đó.



Có thể hiểu các giao dịch trong Bitcoin giống với những tấm séc theo một số cách. Khi chúng ta muốn chi tiêu một "đầu ra" của một giao dịch, chúng ta phải chi tiêu toàn bộ tấm séc. Nó tương tự như cách chúng ta không thể bước vào ngân hàng và nói "Tôi muốn lấy một nửa số tiền này". Vì vậy, để gửi tiền bất cứ nơi nào chúng ta phải "tiền mặt" một tờ séc được viết cho mình, và "đầu ra" từ quá trình rút tiền đó là một tấm séc đến đích dự định của chúng ta, và một tấm séc trả lại cho chính mình.

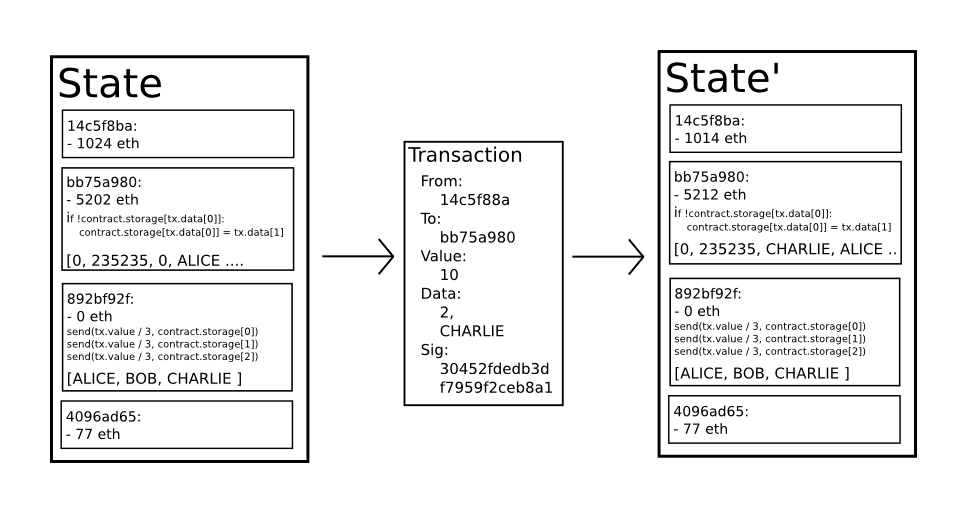
Mỗi tài khoản theo dõi số tiền của nó bằng cách cộng số lượng séc (UTXO) trong ví (liên kết với địa chỉ / ví này). Khi chúng ta muốn chi tiền, chúng ta sử dụng một hoặc nhiều séc (các UTXO hiện có), đủ để trang trải chi phí và có thể nhận được một số thay đổi ngược lại (new UTXO). Mỗi séc chỉ có thể được chi tiêu một lần kể từ đó, sau khi chi tiêu, UTXO sẽ bị xóa khỏi danh sách.

Lợi ích của mô hình UTXO:

* Khả năng mở rộng - Vì có thể xử lý nhiều UTXO cùng một lúc, nó cho phép các giao dịch song song và khuyến khích sự đổi mới khả năng mở rộng.
* Quyền riêng tư - Ngay cả Bitcoin không phải là một hệ thống hoàn toàn ẩn danh, nhưng UTXO cung cấp mức độ riêng tư cao hơn, miễn là người dùng sử dụng địa chỉ mới cho mỗi giao dịch. Nếu có nhu cầu tăng cường quyền riêng tư, các đề án phức tạp hơn, chẳng hạn như chữ ký vòng, có thể được xem xét.

2. Mô hình Tài khoản/Số dư

Khác với trong Bitcoin, Ethereum cũng giống như trong một ngân hàng. Tương tự như việc sử dụng thẻ ATM / thẻ ghi nợ. Ngân hàng theo dõi số tiền mỗi thẻ ghi nợ có và khi chúng ta cần chi tiền, ngân hàng sẽ kiểm tra hồ sơ của mình để đảm bảo chúng ta có đủ số dư trước khi phê duyệt giao dịch.

Điểm nổi bật quan trọng nhất của Ethereum là “Hợp đồng thông minh” và rất khó để xây dựng hợp đồng hoàn chỉnh thông minh dựa trên UTXO. Mô hình tài khoản hướng đối tượng một cách tự nhiên. Mỗi giao dịch sẽ được ghi vào tài khoản tương ứng. Để tạo thuận lợi cho việc quản lý tài khoản, trạng thái thế giới được giới thiệu trong thiết kế. Mỗi giao dịch sẽ thay đổi trạng thái của thế giới. Đây là một phép chiếu của thế giới thực khi mọi thay đổi nhỏ bé sẽ thay đổi thế giới.

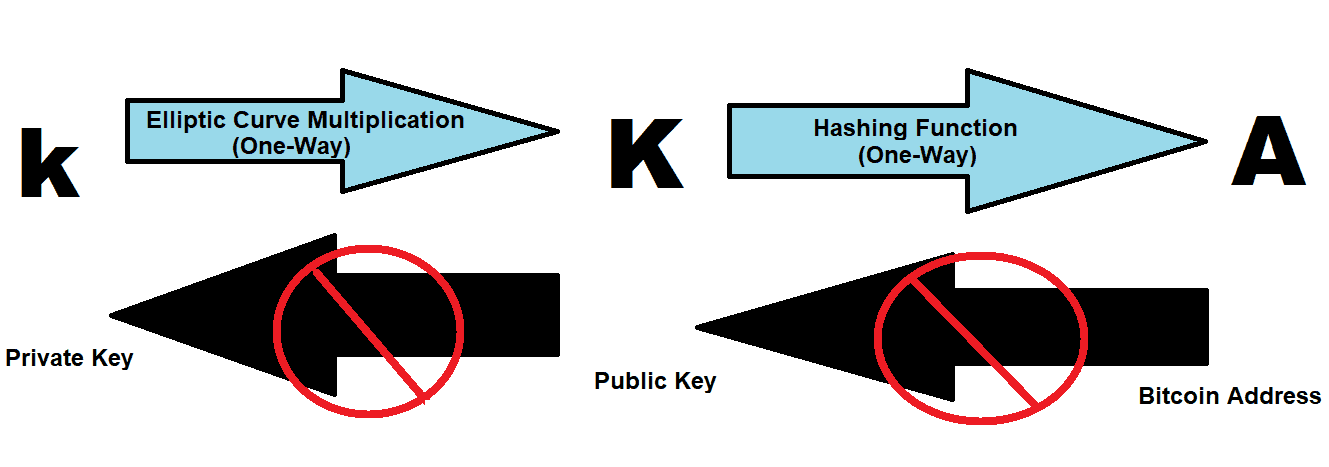
Mô hình tài khoản của Ethereum giúp dễ dàng thực hiện hợp đồng thông minh. Tuy nhiên, hiệu suất luôn là một trở ngại không thể vượt qua. Xét về hiệu suất, UTXO có thể chạy song song trong khi trạng thái thế giới Ethereum khó có thể mở rộng. Các nhà sáng lập nhận thức được điều này, nhưng thật khó để thay đổi.

Lợi ích của mô hình Tài khoản/số dư là:

* Tính đơn giản - Ethereum đã chọn một mô hình trực quan hơn vì lợi ích của các nhà phát triển các hợp đồng thông minh phức tạp, đặc biệt là các hợp đồng yêu cầu thông tin nhà nước hoặc liên quan đến nhiều bên. Một ví dụ là một hợp đồng thông minh để theo dõi các tiểu bang thực hiện các nhiệm vụ khác nhau dựa trên chúng. Mô hình không quốc tịch của UTXO sẽ buộc các giao dịch bao gồm thông tin trạng thái và điều này không cần thiết làm phức tạp thiết kế của các hợp đồng.
* Hiệu quả - Ngoài sự đơn giản, Mô hình tài khoản / số dư hiệu quả hơn, vì mỗi giao dịch chỉ cần xác thực rằng tài khoản gửi có đủ số dư để thanh toán cho giao dịch.

**IV. MÔ HÌNH SINH ĐỊA CHỈ**

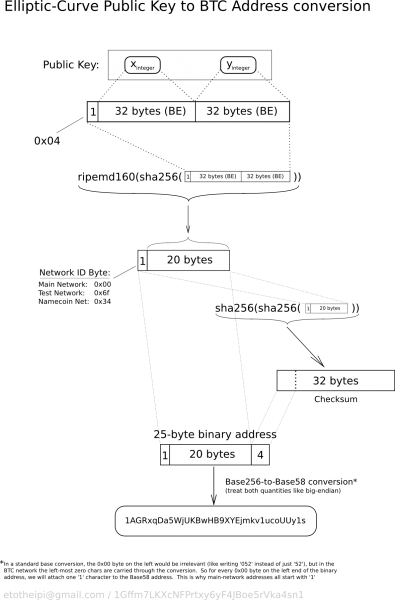
Về cơ bản nguyên lý sinh địa chỉ cả Bitcoin và Ethereum đều giống nhau



Từ một Private Key 32bytes ban đầu sẽ sinh ra Public Key 65bytes (dạng không nén). Việc giao dịch có thể trực tiếp thông qua Public Key. Chúng ta có thể tạo các giao dịch có đích đến là publickey nào đó. Tuy nhiên việc sử dụng publickey quá cồng kệnh và phát sinh nhiều bất tiện. Vì vậy địa chỉ được sử dụng.

Địa chỉ được sinh ra sau quá trình băm publickey. Thuật toán băm trong Bitcoin và Ethereum sự khác biệt.

1. Thuật toán tạo địa chỉ của Bitcoin



2. Thuật toán tạo địa chỉ của Ethereum

