Một số thuật ngữ:

PoS (Proof of Stake): một thuật toán về việc chứng minh cổ phần, xác định người dùng nào có đủ điều kiện xác nhận khối vào Blockchain, để kiếm được 1 khoản phí khia thác. Những người có nhiều token hơn sẽ được ưu tiên hơn những người ít token

Pow (Proof of Work):một thuật toán về việc chứng minh bằng công, xác định người dùng nào có đủ điều kiện xác nhận khối vào Blockchain, để kiếm được 1 khoản phí khai thác. PoW là công nghệ đào coin đầu tiên trên thế giới mà điển hình là BITCOIN. với PoW, tính đủ điều kiện được xác định qua sức mạnh tính toán chứ không phải số lượng tài sản của thợ mỏ.

Private Key: mã khóa bảo mật riêng tư. Mỗi ví trên blockchain sẽ có 1 private key để truy cập giống mật khẩu. đây là chìa khóa để mwor kho coin, mất khóa này coi như mất coin, nếu bạn lưu coin trên các sàn thì khóa này do các sàn giữ cho bạn.

Tìm Hiểu Về Công Nghệ chuỗi khối Blockchain

1. ***Công nghệ chuỗi khối (Blockchain) là gì?***

Blockchain là công nghệ **mã hóa tất cả dữ liệu thành các khối và kết nối chúng với nhau để tạo thành một chuỗi dài**. Mỗi khi **một thông tin hoặc giao dịch mới xảy ra, thông tin cũ sẽ không bị mất đi mà thay vào đó, thông tin mới sẽ được lưu vào một khối mới và lần lượt được nối vào khối cũ để tạo thành một chuỗi mới.**

Không chỉ có vậy, **thông tin của Blockchain** không chỉ nằm trên một máy chủ duy nhất mà còn **được tự động phân phối và sao lưu trên nhiều máy chủ khác nhau kết nối với hệ thống Blockchain để mọi người đều có thể xem và kiểm tra các giao dịch của mình**. Điều này có thể **ngăn chặn việc sửa đổi hoặc gian lận và đảm bảo tính minh bạch và an toàn thông tin.**

1. ***Công nghệ chuỗi khối(Blockchain) là sự kết hợp giữa 3 loại công nghệ?***

**Mật mã học**: Sử dụng public key và hàm hash function để đảm bảo tính minh bạch, toàn vẹn và riêng tư.

**Mạng ngang hàng**: Mỗi một nút trong mạng được xem như một client và cũng là server để lưu trữ bản sao ứng dụng.

**Lý thuyết trò chơi**: Tất cả các nút tham gia vào hệ thống đều phải tuân thủ luật chơi đồng thuận (PoW, PoS…) và được thúc đẩy bởi động lực kinh tế.

Trên góc độ business có thể gọi là một sổ cái kế toán, hay một cơ sở dữ liệu chứa đựng tài sản, hay một cấu trúc dữ liệu, mà dùng để ghi chép lại lịch sử tài sản giữa các thành viên trong hệ thống mạng ngang hàng.

Trên góc độ kỹ thuật đó là một phương thức bất biến để lưu trữ lịch sử các giao dịch tài sản.

Trên góc độ xã hội đó là một hiện tượng, mà dùng để thiết lập niềm tin bằng quy tắc đồng thuận giữa các thành viên trong một hệ thống phân cấp.

1. ***Đặc điểm chính của Blockchain.***

**Không thể làm giả, không thể phá hủy các chuỗi Blockchain**: theo như lý thuyết thì chỉ có máy tính lượng tử mới có thể giải mã Blockchain và công nghệ Blockchain biến mất khi không còn Internet trên toàn cầu.

**Bất biến**: dữ liệu trong Blockchain không thể sửa (có thể sửa nhưng sẽ để lại dấu vết) và sẽ lưu trữ mãi mãi.

**Bảo mật**: Các thông tin, dữ liệu trong Blockchain được phân tán và an toàn tuyệt đối.

**Minh bạch**: Ai cũng có thể theo dõi dữ liệu Blockchain đi từ địa chỉ này tới địa chỉ khác và có thể thống kê toàn bộ lịch sử trên địa chỉ đó.

**Hợp đồng Thông minh**: là hợp đồng kỹ thuật số được nhúng vào đoạn code if-this-then-that (IFTTT), cho phép chúng tự thực thi mà không cần bên thứ ba.

1. ***Các loại Blockchain***

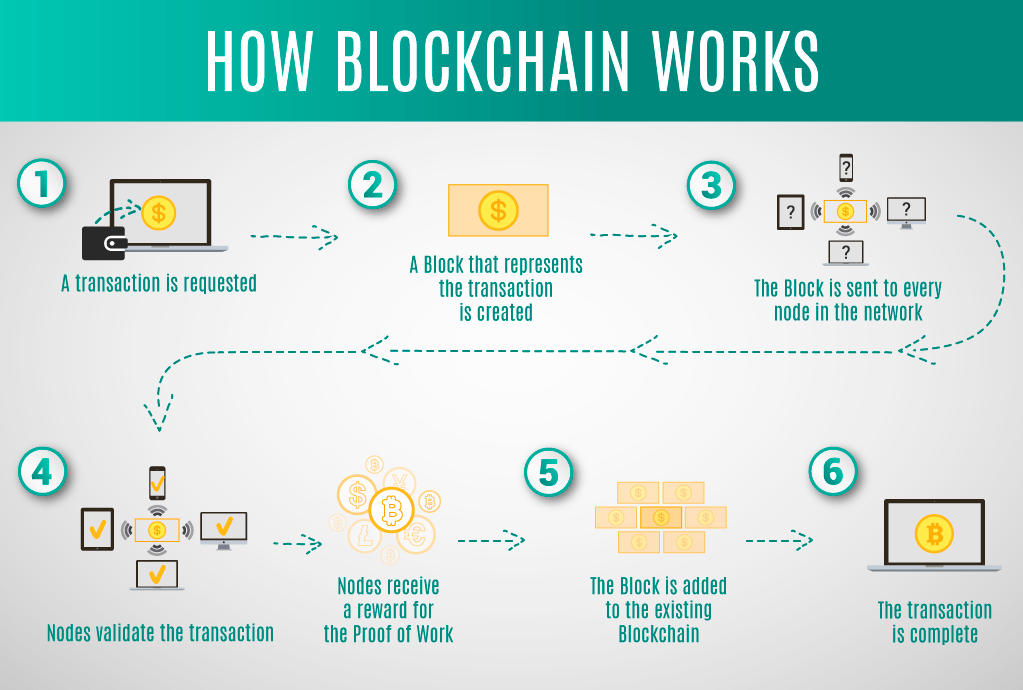
Hệ thống Blockchain chia thành 3 loại chính:

**Public**: Bất kỳ ai cũng có quyền đọc và ghi dữ liệu trên Blockchain. Quá trình xác thực giao dịch trên Blockchain này đòi hỏi phải có hàng nghìn hay hàng vạn nút tham gia. Do đó để tấn công vào hệ thống Blockchain này là điều bất khả thi vì chi phi khá cao. Ví dụ: Bitcoin, Ethereum…

**Private**: Người dùng chỉ được quyền đọc dữ liệu, không có quyền ghi vì điều này thuộc về bên tổ chức thứ ba tuyệt đối tin cậy. Tổ chức này có thể hoặc không cho phép người dùng đọc dữ liệu trong một số trường hợp. Bên thứ ba toàn quyền quyết định mọi thay đổi trên Blockchain. Vì đây là một Private Blockchain, cho nên thời gian xác nhận giao dịch khá nhanh vì chỉ cần một lượng nhỏ thiết bị tham gia xác thực giao dịch. Ví dụ: Ripple là một dạng Private Blockchain, hệ thống này cho phép 20% các nút là gian dối và chỉ cần 80% còn lại hoạt động ổn định là được.

**Permissioned**: Hay còn gọi là Consortium, một dạng của Private nhưng bổ sung thêm một số tính năng nhất định, kết hợp giữa “niềm tin” khi tham gia vào Public và “niềm tin tuyệt đối” khi tham gia vào Private. Ví dụ: Các ngân hàng hay tổ chức tài chính liên doanh sẽ sử dụng Blockchain cho riêng mình.

1. ***Nguyên lý hoạt động***

******

* ***Nguyên lý mã hóa***

Trên thực tế, cuốn sổ cái luôn được duy trì bởi các máy tính trong mạng ngang hàng được kết nối với nhau. Vì thế, nó sẽ có một số điểm khác biệt:

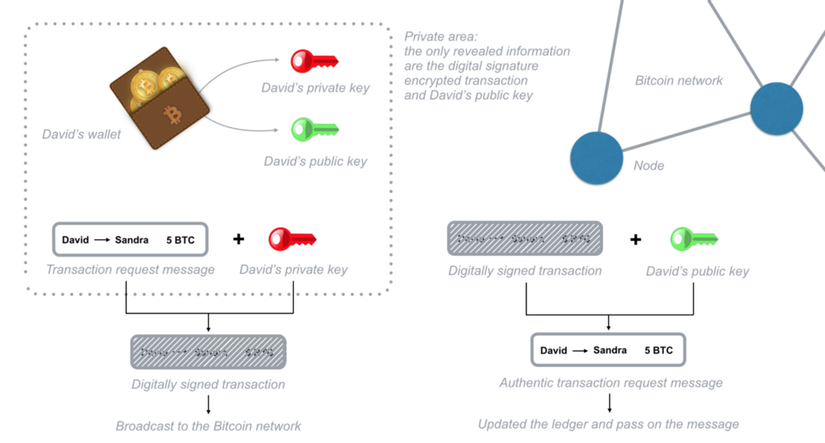
​

Trong hệ thống ngân hàng, chúng ta chỉ biết các giao dịch và số dư tài khoản của riêng mình thì trên blockchain của bitcoin bạn có thể xem các giao dịch của tất cả mọi người.**​**Mạng lưới Bitcoin là mạng lưới phân tán không cần bên thứ ba đóng vai trò trung gian xử lý giao dịch**.​Hệ thống blockchain được thiết kế theo cách không yêu cầu sự tin cậy và bảo đảm bởi độ tin cậy có được thông qua các hàm mã hóa toán học đặc biệt.​Để có thể thực hiện các giao dịch trên blockchain, bạn cần một phần mềm sẽ cho phép bạn lưu trữ và trao đổi các đồng Bitcoin của bạn gọi là ví tiền điện tử. Ví tiền điện tử này sẽ được bảo vệ bằng một phương pháp mã hóa đặc biệt đó là sử dụng một cặp khóa bảo mật duy nhất: khóa riêng tư (private key) và khóa công khai (public key).**

**Nếu một thông điệp được mã hóa bằng một khóa công khai cụ thể thì chỉ chủ sở hữu của khóa riêng tư là một cặp với khóa công khai này mới có thể giải mã và đọc nội dung thông điệp.**

**Khi mã hóa một yêu cầu giao dịch bằng khóa riêng tư, có nghĩa là bạn đang tạo ra một chữ ký điện tử được các máy tính trong mạng lưới blockchain sử dụng để kiểm tra chủ thể gửi và tính xác thực của giao dịch. Chữ ký này là một chuỗi văn bản và là sự kết hợp của yêu cầu giao dịch và khóa riêng tư của bạn.**

**Nếu một ký tự đơn trong thông điệp yêu cầu giao dịch này bị thay đổi thì chữ ký điện tử sẽ thay đổi theo. Vì thế, hacker khó có thể thay đổi yêu cầu giao dịch của bạn hoặc thay đổi số lượng Bitcoin mà bạn đang gửi.**



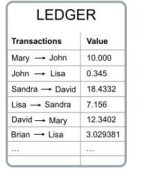
Để gửi Bitcoin (BTC), bạn cần chứng minh rằng bạn sở hữu khóa riêng tư của một chiếc ví điện tử cụ thể bởi bạn cần sử dụng nó để mã hóa thông điệp yêu cầu giao dịch. Sau khi tin nhắn của bạn đã được gửi đi và được mã hóa thì bạn không cần phải tiết lộ khóa riêng tư của bạn nữa

.

* **Quy tắc của sổ cái**

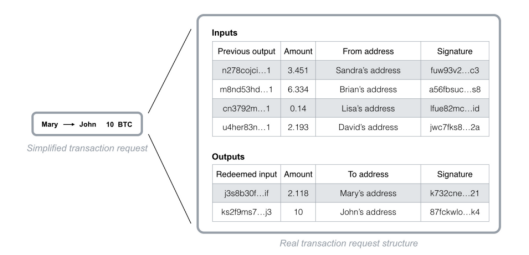
Mỗi nút trong blockchain đều đang lưu giữ một bản sao của sổ kế toán. Do vậy, mỗi nút đều biết số dư tài khoản của bạn là bao nhiêu. Hệ thống blockchain chỉ ghi lại mỗi giao dịch được yêu cầu chứ không hề theo dõi số dư tài khoản của bạn.

Để biết số dư trên ví điện tử của mình thì bạn cần xác thực và xác nhận tất cả các giao dịch đã diễn ra trên mạng lưới mà có liên quan tới ví điện tử của bạn.



Việc xác minh “số dư” này được thực hiện nhờ các tính toán dựa vào liên kết đến các giao dịch trước đó. Nhìn vào hình trên, để gửi 10btc cho John, Mary cần tạo yêu cầu giao dịch bao gồm các liên kết đến các giao dịch đã diễn ra trước đó với tổng số dư bằng hoặc vượt quá 10 btc.

Các liên kết này được xem như là giá trị đầu vào, các nút trong mạng lưới sẽ xác minh xem tổng số tiền của các giao dịch này bằng hoặc vượt quá 10 btc không. Tất cả điều này được thực hiện tự động trong ví điện tử của Mary và được kiểm tra bởi các nút trên mạng lưới Bitcoin, Mary chỉ gửi một giao dịch 10 bitcoin tới ví của John bằng khóa công khai của John.



Vậy, làm thế nào hệ thống có thể tin tưởng các giao dịch đầu vào này và xác thực tính hợp lệ của chúng?

Thực tế là các nút sẽ kiểm tra tất cả các giao dịch có liên quan đến ví tiền điện tử bạn sử dụng trước đó để gửi Bitcoin (BTC) thông qua việc tham chiếu các lịch sử giao dịch. Có một bản ghi sẽ lưu trữ số BTC chưa được dùng và được các nút mạng lưu giữ giúp đơn giản hóa và tăng tốc quá trình xác minh. Vì thế, các ví tiền điện tử tránh được tình trạng chi tiêu đúp giao dịch.

=> “Như vậy sở hữu Bitcoin có nghĩa là có các giao dịch được lưu trong sổ kế toán liên hệ đến địa chỉ ví của bạn mà chưa được sử dụng làm giao dịch đầu vào.”

Mã nguồn trên mạng lưới Bitcoin là nguồn mở, có nghĩa là bất kỳ ai có máy tính kết nối được internet đều có thể tham gia vào mạng lưới và thực hiện giao dịch.

Tuy nhiên, nếu có bất kỳ một lỗi nào trong mã nguồn được sử dụng để phát thông báo yêu cầu giao dịch thì các Bitcoin liên quan sẽ bị mất vĩnh viễn.

* ***Nguyên Lý tạo khối***

**Các giao dịch sau khi được gửi lên trên mạng lưới blockchain sẽ được nhóm vào các khối. Các giao dịch trong cùng một khối được coi là đã xảy ra cùng một lúc và các giao dịch chưa được thực hiện trong một khối được coi là chưa được xác nhận. Mỗi nút có thể nhóm các giao dịch với nhau thành một khối và gửi nó vào mạng lưới như một hàm ý cho các khối tiếp theo được gắn vào sau đó.**

Vì bất kỳ nút nào cũng có thể tạo một khối mới nên có một câu hỏi đặt ra là cả hệ thống sẽ đồng thuận với khối nào sẽ là khối tiếp theo?

Để được thêm vào blockchain, mỗi khối phải chứa một đoạn mã đóng vai trò như một đáp án cho một vấn đề toán học phức tạp được tạo ra bằng hàm mã hóa băm không thể đảo ngược.

Cách duy nhất để giải quyết vấn đề toán học như vậy là đoán các số ngẫu nhiên, những số khi mà kết hợp với nội dung khối trước tạo ra một kết quả đã được hệ thống định nghĩa. Do trong mạng lưới luôn có một số lượng lớn các máy tính đều tập trung vào việc đoán ra dãy số này nên mạng lưới quy định mỗi khối được tạo ra sau một quãng thời gian là 10 phút một lần. Nút nào giải quyết được vấn đề toán học như vậy sẽ được quyền gắn khối tiếp theo lên trên chuỗi và gửi nó tới toàn bộ mạng lưới.

* ***Thuật toán bảo mật Blockchain***

Nếu có bất kỳ sự bất đồng về khối đại diện sau cùng của chuỗi thì điều này sẽ dẫn đến khả năng gian lận. Nếu một giao dịch xảy ra trong 1 khối thuộc về đuôi ngắn hơn khi khối tiếp theo được giải quyết, giao dịch đó sẽ trở lại thành giao dịch chưa được xác nhận vì tất cả các giao dịch khác được nhóm vào trong khối kia.

Mỗi block chứa một tham chiếu đến khối trước đó, và tham chiếu đó là một phần của vấn đề toán học cần được giải quyết để truyền khối sau tới mạng lưới. Vì vậy, rất khó để tính toán trước một loạt các block bởi nó cần tính ra một số lượng lớn các số ngẫu nhiên cần thiết để giải quyết một khối và đặt nó trên blockchain.

Các giao dịch trong mạng lưới blockchain của bitcoin được bảo vệ bởi một cuộc chạy đua tính toán toán học: với bất kỳ kẻ tấn công nào muốn cạnh tranh với toàn bộ mạng lưới.

Do đó, giao dịch ngày càng an toàn hơn theo thời gian. Và những khối đã được thêm vào chuỗi trong quá khứ bao giờ cũng an toàn hơn so với những khối mới được thêm vào. Bởi một block được thêm vào chuỗi trung bình cứ 10p một lần cho nên trong khoảng 1h kể từ khi giao dịch được nhóm vào trong khối đầu tiên của nó sẽ tạo ra một xác suất khá cao rằng giao dịch đã được xử lý và không thể đảo ngược.

1. ***Các phiên bản của Blockchain***

**Blockchain 1.0 – Tiền tệ và Thanh toán**: Ứng dụng chính của phiên bản này là tiền mã hoá: bao gồm việc chuyển đổi tiền tệ, kiều hối và tạo lập hệ thống thanh toán kỹ thuật số. Đây cũng là lĩnh vực quen thuộc với chúng ta nhất mà đôi khi khá nhiều người lầm tưởng Bitcoin và Blockchain là một.

**Blockchain 2.0 – Tài chính và Thị trường:** Ứng dụng xử lý tài chính và ngân hàng: mở rộng quy mô của 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.

**Blockchain 3.0 – Thiết kế và Giám sát hoạt động:** 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 là lại có nhiều loại như physical, digital hay human in nature.