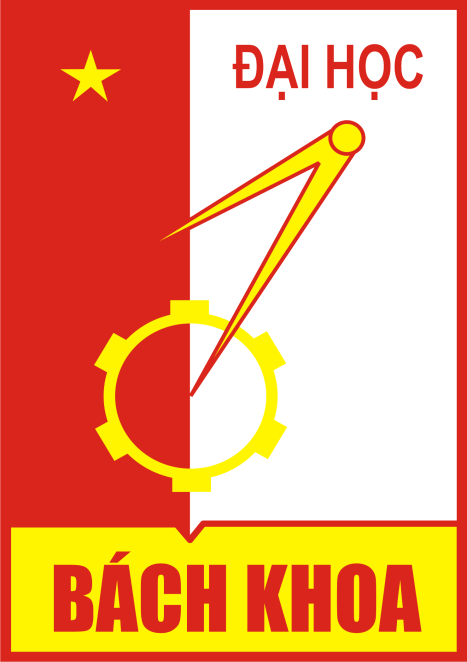
TRƯỜNG ĐẠI HỌC BÁCH KHOA HÀ NỘI

VIỆN CÔNG NGHỆ THÔNG TIN VÀ TRUYỀN THÔNG

-----o0o-----



**BÁO CÁO PROJECT II**

Đề tài: TÌM HIỂU VỀ CÔNG NGHỆ BLOCKCHAIN

Giảng viên hướng dẫn: TS. Phạm Huy Hoàng

Sinh viên thực hiện: Trần Văn Kiên 20152081

Hà Nội, 06/2018

BÁO CÁO PROJECT II

***Đề tài: Tìm hiểu về công nghệ Blockchain***

**Lịch sử của Blockchain**

Blockchain đã được giới thiệu với phát minh bitcoin trong năm 2008 và sau đó là được phát triển thành phiên bản thực tế vào năm 2009. Đối với chương trình này, nó đã giới thiệu ngắn gọn như một chương trình đầy đủ về bitcoin sau này, nhưng nó cũng rất cần thiết để tham khảo bitcoin vì không có nó, lịch sử của blockchain chưa hoàn thành. Khái niệm tiền điện tử không phải là mới, từ những năm 1980, các giao thức tiền điện tử đã tồn tại dựa trên mô hình được đề xuất bởi David Chaum.

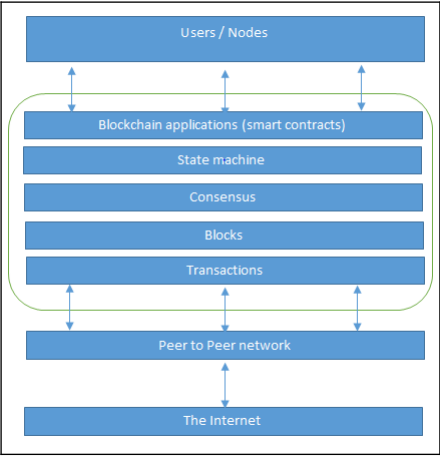
***Chương 1. Giới thiệu các khái niệm cơ bản về tính toán phân tán dựa trên công nghệ blockchain nào. Nó cũng bao gồm lịch sử, định nghĩa, tính năng, loại và lợi ích của blockchains cùng với các cơ chế đồng thuận là cốt lõi của công nghệ blockchain.***

**Giới thiệu về Blockchain**

Có nhiều định nghĩa khác nhau về blockchain; Nó phụ thuộc vào cách bạn nhìn vào nó. Nếu bạn nhìn nó từ góc độ kinh doanh, nó có thể được định nghĩa trong ngữ cảnh đó, nếu bạn nhìn vào nó từ góc độ kĩ thuật, người ta có thể định nghĩa nó theo quan điểm đó.

Blockchain tại lõi của nó là sổ kế toán phân phối ngang hàng, an toàn về mặt mã hóa, chắp vá, không thay đổi (cực kỳ khó thay đổi), và có thể cập nhật thông qua sự đồng thuận hoặc thỏa thuận giữa các đồng nghiệp.

Blockchain có thể được coi là một lớp của một mạng ngang hàng được phân phối chạy trên đầu trang của Internet, như có thể thấy bên dưới trong biểu đồ. Nó tương tự như SMTP, HTTP, hoặc FTP chạy trên đầu trang của TCP / IP. Điều này được thể hiện trong sơ đồ sau:

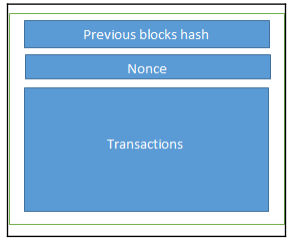


**Chế độ xem mạng của một blockchain**

Từ quan điểm kinh doanh, một blockchain có thể được định nghĩa là một nền tảng trong đó các đồng nghiệp có thể trao đổi các giá trị bằng cách sử dụng các giao dịch mà không cần một trọng tài trung tâm tin cậy. Đây là một khái niệm mạnh mẽ và một khi độc giả hiểu nó, họ sẽ nhận ra tiềm năng sóng thần của công nghệ blockchain. Điều này cho phép blockchain là một cơ chế đồng thuận phi tập trung mà không có cơ quan duy nhất nào chịu trách nhiệm của cơ sở dữ liệu.

Một khối đơn giản là một tập hợp các giao dịch được nhóm lại với nhau để sắp xếp chúng một cách hợp lý. Nó được tạo thành từ các giao dịch và kích thước của nó là biến tùy thuộc vào loại và thiết kế của blockchain được sử dụng. Một tham chiếu đến một khối trước đó cũng được bao gồm trong khối trừ khi nó là một khối genesis. Một khối genesis là khối đầu tiên trong blockchain được mã hóa cứng tại thời điểm blockchain được bắt đầu. Cấu trúc của một khối cũng phụ thuộc vào loại và thiết kế của một blockchain, nhưng nói chung có một vài thuộc tính cần thiết cho chức năng của một khối, chẳng hạn như tiêu đề khối, con trỏ tới các khối trước đó, dấu thời gian, nonce, bộ đếm giao dịch, giao dịch và các thuộc tính khác.

Điều này được thể hiện trong một sơ đồ khối đơn giản như sau. Đây là một mô tả chung của một khối; các cấu trúc khối cụ thể liên quan đến công nghệ blockchain của chúng sẽ được thảo luận sau trong cuốn sách với các chi tiết kỹ thuật chuyên sâu hơn:



Cấu trúc của một khối

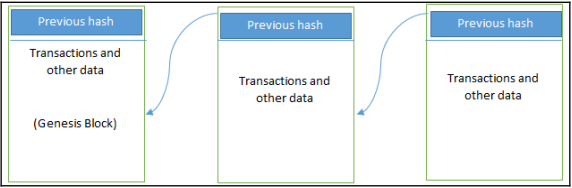
**Các định nghĩa kỹ thuật khác nhau của blockchains**

Blockchain là một cơ chế đồng thuận phi tập trung. Trong một blockchain, tất cả các đồng nghiệp cuối cùng đi đến một thỏa thuận liên quan đến trạng thái của một giao dịch.

Blockchain là một sổ kế toán được chia sẻ được phân phối. Blockchain có thể được coi là sổ kế toán được chia sẻ của các giao dịch. Giao dịch được sắp xếp và được nhóm thành các khối. Hiện tại, mô hình thế giới thực dựa trên cơ sở dữ liệu riêng mà mỗi tổ chức duy trì trong khi sổ kế toán phân phối có thể phục vụ như một nguồn chân lý duy nhất cho tất cả các tổ chức thành viên đang sử dụng blockchain.

Blockchain là một cấu trúc dữ liệu; nó về cơ bản là một danh sách liên kết sử dụng con trỏ băm thay vì con trỏ bình thường. Hash con trỏ được sử dụng để trỏ đến khối trước đó.

Cấu trúc của một blockchain chung có thể được hình dung với sự trợ giúp của sơ đồ sau:



**Các yếu tố chung của một blockchain**

Địa chỉ

Địa chỉ là số nhận dạng duy nhất được sử dụng trong giao dịch trên blockchain để biểu thị người gửi và người nhận. Địa chỉ thường là khóa công khai hoặc được lấy từ khóa công khai. Mặc dù các địa chỉ có thể được tái sử dụng bởi cùng một người dùng nhưng chính địa chỉ là duy nhất. Tuy nhiên, trong thực tế, một người dùng không thể sử dụng lại cùng một địa chỉ và tạo một địa chỉ mới cho mỗi giao dịch. Địa chỉ mới được tạo này sẽ là duy nhất. Bitcoin thực chất là một hệ thống bút danh. Người dùng cuối thường không thể nhận dạng trực tiếp nhưng một số nghiên cứu trong việc ẩn danh người dùng bitcoin đã cho thấy rằng người dùng có thể được xác định thành công. Như một thực hành tốt, người dùng gợi ý rằng người dùng tạo địa chỉ mới cho mỗi giao dịch để tránh liên kết giao dịch với chủ sở hữu chung, do đó tránh nhận dạng.

Giao dịch

Một giao dịch là đơn vị cơ bản của một blockchain. Giao dịch đại diện cho việc chuyển giá trị từ địa chỉ này sang địa chỉ khác.

Khối

Một khối bao gồm nhiều giao dịch và một số thành phần khác như khối trước băm (con trỏ băm), dấu thời gian và nonce.

Mạng ngang hàng

Như tên của nó, đây là một cấu trúc liên kết mạng theo đó tất cả các đồng nghiệp có thể giao tiếp với nhau và gửi và nhận tin nhắn.

Ngôn ngữ lập trình hoặc viết mã

Phần tử này thực hiện các hoạt động khác nhau trên một giao dịch. Các tập lệnh giao dịch là các tập lệnh được xác định trước cho các nút chuyển mã thông báo từ địa chỉ này sang địa chỉ khác và thực hiện các chức năng khác. Turing ngôn ngữ lập trình hoàn chỉnh là một tính năng mong muốn của blockchains; tuy nhiên, sự an toàn của các ngôn ngữ đó là một câu hỏi quan trọng và một lĩnh vực nghiên cứu quan trọng và liên tục.

Máy ảo

Đây là phần mở rộng của tập lệnh giao dịch. Một máy ảo cho phép Turing mã hoàn chỉnh được chạy trên một blockchain (như các hợp đồng thông minh) trong khi một kịch bản giao dịch có thể bị hạn chế trong hoạt động của nó. Các máy ảo không có sẵn trên tất cả các blockchains; tuy nhiên, các blockchains khác nhau sử dụng các máy ảo để chạy các chương trình, ví dụ Ethereum Virtual Machine (EVM) và Chain Virtual Machine (CVM).

Máy trạng thái

Một blockchain có thể được xem như là một cơ chế chuyển đổi trạng thái, theo đó một trạng thái được sửa đổi từ dạng ban đầu sang dạng tiếp theo và cuối cùng thành dạng cuối cùng do kết quả của quá trình thực hiện giao dịch và xác nhận bởi các nút.

Nút

Một nút trong một mạng blockchain thực hiện các chức năng khác nhau tùy thuộc vào vai trò của nó. Một nút có thể đề xuất và xác thực giao dịch và thực hiện khai thác để tạo thuận lợi cho sự đồng thuận và bảo mật blockchain. Điều này được thực hiện bằng cách làm theo một giao thức đồng thuận. Các nút cũng có thể thực hiện các chức năng khác như xác minh thanh toán đơn giản (các nút nhẹ), trình duyệt tính hợp lệ và nhiều chức năng khác tùy thuộc vào loại blockchain được sử dụng và vai trò được gán cho nút.

Hợp đồng thông minh

Các chương trình này chạy trên đầu trang của blockchain và đóng gói logic nghiệp vụ được thực hiện khi các điều kiện nhất định được đáp ứng. Tính năng hợp đồng thông minh không có sẵn trong tất cả các blockchains nhưng bây giờ trở thành một tính năng rất mong muốn do sự linh hoạt và sức mạnh nó cung cấp cho các ứng dụng blockchain.

**Đặc điểm của blockchain**

Một blockchain thực hiện các chức năng khác nhau. Chúng được mô tả chi tiết dưới đây.

Sự đồng thuận phân tán

Sự đồng thuận phân tán là nền tảng chính của một blockchain. Điều này cho phép một blockchain để trình bày một phiên bản duy nhất của sự thật được thỏa thuận bởi tất cả các bên mà không có yêu cầu của một cơ quan trung ương.

Xác minh giao dịch

Bất kỳ giao dịch nào được đăng từ các nút trên blockchain đều được xác minh dựa trên một bộ quy tắc xác định trước và chỉ các giao dịch hợp lệ được chọn để đưa vào một khối.

Nền tảng cho hợp đồng thông minh

Blockchain là một nền tảng nơi các chương trình có thể chạy thực thi logic nghiệp vụ thay mặt cho người dùng. Như đã giải thích trước đó, không phải tất cả các blockchains đều có cơ chế thực thi các hợp đồng thông minh; tuy nhiên, đây là một tính năng rất hấp dẫn.

Chuyển giá trị giữa các đồng nghiệp

Blockchain cho phép chuyển giá trị giữa người dùng thông qua mã thông báo. Tokens có thể được coi là một tàu sân bay có giá trị.

Tạo tiền điện tử

Đây là một tính năng tùy chọn tùy thuộc vào loại blockchain được sử dụng. Một blockchain có thể tạo ra tiền điện tử như một sự khích lệ cho các thợ mỏ của nó, những người xác thực các giao dịch và sử dụng các nguồn lực để bảo đảm blockchain.

Tài sản thông minh

Lần đầu tiên có thể liên kết một tài sản kỹ thuật số hoặc vật lý với blockchain theo cách không hủy ngang, sao cho nó không thể được bất kỳ ai khác yêu cầu; bạn có toàn quyền kiểm soát tài sản của mình và không thể chi trả gấp đôi hoặc sở hữu gấp đôi. So sánh nó với một tập tin âm nhạc kỹ thuật số, ví dụ, mà có thể được sao chép nhiều lần mà không cần bất kỳ kiểm soát; trên một blockchain, tuy nhiên, nếu bạn sở hữu nó không ai khác có thể yêu cầu nó trừ khi bạn quyết định chuyển nó cho ai đó. Tính năng này có ý nghĩa sâu rộng nhất là trong Quản lý quyền kỹ thuật số (DRM) và hệ thống tiền điện tử, trong đó phát hiện chi tiêu kép là yêu cầu quan trọng. Vấn đề chi tiêu gấp đôi lần đầu tiên được giải quyết bằng bitcoin.

Nhà cung cấp bảo mật

Blockchain dựa trên công nghệ mã hóa đã được chứng minh, đảm bảo tính toàn vẹn và tính sẵn có của dữ liệu. Nói chung, tính bảo mật không được cung cấp do các yêu cầu về tính minh bạch. Điều này đã trở thành rào cản chính cho khả năng thích ứng của nó bởi các tổ chức tài chính và các ngành khác cần sự riêng tư và bảo mật của các giao dịch. Như vậy nó đang được nghiên cứu rất tích cực và đã có một số tiến bộ tốt được thực hiện. Có thể lập luận rằng trong nhiều tình huống bảo mật thì không thực sự cần thiết và minh bạch được ưa thích để thay thế. Ví dụ, trong bảo mật bitcoin là không thực sự cần thiết; Tuy nhiên, nó là mong muốn trong một số kịch bản. Nghiên cứu trong lĩnh vực này là rất chín và đã có những tiến bộ lớn đã được thực hiện theo hướng cung cấp bảo mật và riêng tư trên blockchain. Một ví dụ gần đây hơn là Zcash, sẽ được thảo luận chi tiết hơn trong các chương sau. Các dịch vụ bảo mật khác như nonrepudiation và authentication cũng được cung cấp bởi blockchain vì tất cả các hành động được bảo mật bằng cách sử dụng khóa riêng và chữ ký số.

Tính không thay đổi

Đây là một tính năng quan trọng khác của blockchain: các bản ghi đã được thêm vào blockchain là không thay đổi. Có khả năng quay trở lại những thay đổi nhưng điều này được coi là gần như không thể làm vì nó sẽ đòi hỏi một số tài nguyên máy tính không thể kiếm được. Ví dụ, trong trường hợp mong muốn nhiều bitcoin nếu một người dùng độc hại muốn thay đổi các khối trước đó thì nó sẽ yêu cầu tính toán PoW một lần nữa cho tất cả các khối đã được thêm vào blockchain. Khó khăn này làm cho các hồ sơ trên một blockchain thực tế bất biến.

Tính độc đáo

Tính năng này của blockchain đảm bảo rằng mọi giao dịch là duy nhất và chưa được chi tiêu. Điều này đặc biệt có liên quan trong tiền điện tử, nơi phát hiện nhiều và mong muốn chi tiêu gấp đôi là một yêu cầu quan trọng.

Hợp đồng thông minh

Blockchain cung cấp một nền tảng để chạy các hợp đồng thông minh. Đây là những chương trình tự động tự động nằm trên blockchain và đóng gói logic nghiệp vụ và mã để thực hiện một chức năng được yêu cầu khi các điều kiện nhất định được đáp ứng. Đây thực sự là một tính năng mang tính cách mạng của blockchain vì nó cho phép tính linh hoạt, khả năng lập trình và kiểm soát nhiều hành động mong muốn mà người dùng blockchain cần thực hiện theo yêu cầu kinh doanh cụ thể của họ.

**Ứng dụng công nghệ blockchain**

Công nghệ Blockchain có vô số các ứng dụng trong các lĩnh vực khác nhau bao gồm nhưng không giới hạn về tài chính, chính phủ, truyền thông, luật và nghệ thuật. Nơi các trường hợp sử dụng thực tế sẽ được thảo luận chi tiết cho các ngành công nghiệp khác nhau. Nó là đủ để nói cho bây giờ mà hầu như tất cả các ngành công nghiệp đã nhận ra tiềm năng và lời hứa của blockchain và đã bắt tay, hoặc sớm sẽ bắt tay, trên hành trình để được hưởng lợi từ công nghệ blockchain.

**Các loại blockchain**

Dựa trên cách blockchain đã phát triển trong vài năm qua, nó có thể được chia thành nhiều loại với các thuộc tính khác biệt nhưng đôi khi chồng chéo một phần.

Blockchains công cộng

Các blockchains này được mở cho công chúng và bất cứ ai cũng có thể tham gia như một nút trong quá trình ra quyết định. Người dùng có thể hoặc không được khen thưởng vì sự tham gia của họ. Các sổ cái này không thuộc sở hữu của bất kỳ ai và được mở công khai cho bất kỳ ai tham gia. Tất cả người dùng của sổ kế toán không cho phép duy trì bản sao sổ kế toán trên các nút cục bộ của họ và sử dụng cơ chế đồng thuận phân tán để đạt được quyết định về cuối cùng trạng thái sổ cái. Những blockchains này còn được gọi là led-less ledgers.

Blockchains riêng tư

Blockchains riêng tư như tên ngụ ý là tư nhân và chỉ mở cửa cho một tập đoàn hoặc nhóm cá nhân hoặc tổ chức đã quyết định chia sẻ sổ cái trong số họ.

Blockchains bán riêng tư

Ở đây một phần của blockchain là riêng tư và một phần của nó là công khai. Phần tư nhân được kiểm soát bởi một nhóm các cá nhân trong khi phần công khai được mở cho sự tham gia của bất cứ ai.

Sidechains

Đây là một khái niệm mà theo đó tiền xu có thể được chuyển từ một blockchain này sang một blockchain khác và chuyển trở lại. Sử dụng phổ biến bao gồm việc tạo ra các altcoins mới (tiền điện tử thay thế), theo đó tiền xu được đốt cháy như là một bằng chứng về cổ phần thích hợp. Có hai loại sidechain. Ví dụ được cung cấp ở trên cho tiền xu đốt được áp dụng cho một sidechain chốt một chiều. Loại thứ hai được gọi là một sidechain chốt hai chiều, cho phép chuyển động của tiền xu từ chuỗi chính đến sidechain và quay trở lại chuỗi chính khi cần thiết.

Sổ cái được cấp phép

Một sổ kế toán được phép là một blockchain nhờ đó những người tham gia mạng được biết và đáng tin cậy. Sổ cái được phép không cần phải sử dụng một cơ chế đồng thuận phân tán, thay vào đó một giao thức thỏa thuận có thể được sử dụng để duy trì một phiên bản chia sẻ của sự thật về trạng thái của các bản ghi trên blockchain. Cũng không có yêu cầu cho một blockchain được phép để được tư nhân vì nó có thể là một blockchain công cộng nhưng với kiểm soát truy cập quy định.

Sổ cái phân tán

Như tên cho thấy, sổ kế toán này được phân phối giữa những người tham gia của nó và trải rộng trên nhiều trang web hoặc tổ chức. Loại này có thể là riêng tư hoặc công khai. Ý tưởng chính là, không giống như nhiều blockchains khác, các bản ghi được lưu trữ liên tục thay vì được sắp xếp thành các khối. Khái niệm này được sử dụng trong Ripple.

Sổ cái được chia sẻ

Đây là thuật ngữ chung được sử dụng để mô tả bất kỳ ứng dụng hoặc cơ sở dữ liệu nào được chia sẻ bởi công chúng hoặc một tập đoàn.

Blockchains hoàn toàn riêng tư và độc quyền

Những blockchains này có lẽ không có ứng dụng chính thống khi chúng đi chệch khỏi ý tưởng cốt lõi về phân cấp trong công nghệ blockchain. Tuy nhiên trong các cài đặt riêng tư cụ thể trong một tổ chức có thể cần phải chia sẻ dữ liệu và cung cấp một số mức độ bảo đảm về tính xác thực của dữ liệu. Những blockchains này có thể hữu ích trong kịch bản đó. Ví dụ, để cộng tác và chia sẻ dữ liệu giữa các cơ quan chính phủ khác nhau.

Blockchains được mã hóa

Những blockchains này là blockchains tiêu chuẩn mà tạo ra tiền điện tử là kết quả của một quá trình đồng thuận thông qua khai thác hoặc thông qua phân phối ban đầu.

Blockchains không có mã hóa

Đây có thể không phải là blockchains thực vì chúng thiếu đơn vị chuyển giao giá trị cơ bản nhưng vẫn có giá trị trong những tình huống không cần chuyển giá trị giữa các nút và chỉ chia sẻ một số dữ liệu giữa các bên đã tin cậy khác nhau. Trong phần tiếp theo, ý tưởng đồng thuận từ quan điểm blockchain sẽ được thảo luận. Sự đồng thuận là xương sống của một blockchain và cung cấp sự phân quyền kiểm soát như là kết quả thông qua một quá trình tùy chọn được gọi là khai thác mỏ. Sự lựa chọn của thuật toán đồng thuận cũng được điều chỉnh bởi loại blockchain được sử dụng. Không phải tất cả các cơ chế đồng thuận đều phù hợp với tất cả các loại blockchains. Ví dụ, trong các khối lệnh cho phép công khai, sẽ có ý nghĩa khi sử dụng PoW thay vì một số cơ chế thỏa thuận cơ bản mà có lẽ dựa trên bằng chứng về quyền hạn. Do đó, cần chọn một thuật toán đồng thuận phù hợp cho một dự án blockchain.

**Đồng thuận trong blockchain**

Đồng thuận về cơ bản là một khái niệm điện toán phân tán đã được sử dụng trong blockchain để cung cấp một phương tiện đồng ý với một phiên bản duy nhất của sự thật bởi tất cả các đồng nghiệp trên mạng blockchain.

Khoảng hai loại cơ chế đồng thuận sau đây tồn tại:

1. Dựa trên bằng chứng, dựa trên lãnh đạo, hoặc sự đồng thuận Nakamoto, theo đó một nhà lãnh đạo được bầu và đề xuất một giá trị cuối cùng

2. Dựa trên khả năng chịu lỗi của Byzantine, đây là phương pháp truyền thống dựa trên vòng phiếu bầu

*Các thuật toán đồng thuận có sẵn hiện nay hoặc đang được nghiên cứu của blockchain sau đây:*

Bằng chứng công việc

Loại cơ chế đồng thuận này dựa vào bằng chứng rằng đủ tài nguyên tính toán đã được chi tiêu trước khi đề xuất một giá trị cho sự chấp nhận của mạng. Điều này được sử dụng trong bitcoin và các loại tiền điện tử khác. Hiện tại, đây là thuật toán duy nhất đã chứng minh thành công đáng kinh ngạc trước các cuộc tấn công của Sybil.

Bằng chứng về cổ phần

Thuật toán này hoạt động trên ý tưởng rằng một nút hoặc người dùng có đủ số tiền trong hệ thống; ví dụ người dùng đã đầu tư đủ vào hệ thống để bất kỳ nỗ lực độc hại nào sẽ lớn hơn lợi ích của việc thực hiện tấn công trên hệ thống. Ý tưởng này lần đầu tiên được giới thiệu bởi Peercoin và sẽ được sử dụng trong chuỗi Ethereum. Một khái niệm quan trọng khác trong Proof of Stake (PoS) là tuổi đồng xu, có nguồn gốc từ số lượng thời gian và số lượng tiền xu chưa được chi tiêu. Trong mô hình này, cơ hội đề xuất và ký kết sự gia tăng khối tiếp theo với thời đại tiền xu.

Bằng chứng về chứng khoán

Bằng chứng chứng nhận quyền sở hữu (DPOS) là một sự đổi mới so với PoS tiêu chuẩn, theo đó mỗi nút có cổ phần trong hệ thống có thể ủy quyền xác thực giao dịch cho các nút khác bằng cách bỏ phiếu. Điều này được sử dụng trong blockchain bithares.

Bằng chứng về thời gian trôi qua

Được Intel giới thiệu, nó sử dụng Môi trường thực thi tin cậy (TEE) để cung cấp sự ngẫu nhiên và an toàn trong quá trình bầu cử lãnh đạo thông qua thời gian chờ bảo đảm. Nó đòi hỏi bộ vi xử lý Intel SGX (Phần mềm bảo vệ phần mềm mở rộng) để cung cấp bảo đảm an ninh và cho nó được bảo mật.

Đồng thuận dựa trên tiền gửi

Các nút muốn tham gia vào mạng phải đặt vào một khoản tiền đặt cọc trước khi chúng có thể đề xuất một khối.

Bằng chứng về tầm quan trọng

Ý tưởng này rất quan trọng và khác với Proof of Stake. Bằng chứng về tầm quan trọng không chỉ phụ thuộc vào số lượng cổ phần mà người dùng có trong hệ thống mà nó còn giám sát việc sử dụng và di chuyển thẻ của người dùng để thiết lập mức độ tin cậy và tầm quan trọng. Điều này được sử dụng trong Nemcoin.

Liên bang thống nhất hoặc liên bang Byzantine đồng thuận

Được sử dụng trong giao thức đồng thuận sao, các nút trong giao thức này giữ một nhóm các đồng nghiệp được tin cậy công khai và chỉ truyền bá những giao dịch đã được xác thực bởi phần lớn các nút đáng tin cậy.

Cơ chế dựa trên danh tiếng

Như tên cho thấy, một nhà lãnh đạo được bầu trên cơ sở danh tiếng mà nó đã xây dựng theo thời gian trên mạng. Điều này có thể dựa trên việc bỏ phiếu từ các thành viên khác.

Dung sai lỗi Byzantine thực tế

Thực tế Byzantine Fault Tolerance (PBFT) đạt được sự sao chép máy nhà nước, cung cấp khả năng chống lại các nút Byzantine. Các giao thức khác, bao gồm nhưng không giới hạn PBFT, PAXOS, RAFT, và Hiệp định Byzantine Liên bang (FBA), cũng đang được sử dụng hoặc đã được đề xuất sử dụng trong nhiều triển khai khác nhau của hệ thống phân tán và ngăn chặn.

**Định lý CAP và blockchain**

Kỳ lạ thay, có vẻ như định lý CAP bị vi phạm trong blockchain, và đặc biệt là trong việc thực hiện thành công nhất: bitcoin, nhưng đây không phải là trường hợp. Trong blockchains nhất quán được hy sinh trong lợi của sẵn có và dung sai phân vùng. Trong trường hợp này, nhất quán (C) trên blockchain không đạt được đồng thời với dung sai phân vùng (P) và tính khả dụng (A), nhưng nó đạt được theo thời gian. Điều này được gọi là tính nhất quán cuối cùng, trong đó tính nhất quán đạt được là kết quả của quá trình xác nhận từ nhiều nút theo thời gian. Vì mục đích này, khái niệm khai thác được giới thiệu bằng bitcoin; đây là một quá trình tạo điều kiện cho sự thành công của sự đồng thuận bằng cách sử dụng một thuật toán đồng thuận được gọi là PoW. Ở một mức độ cao hơn, khai thác có thể được định nghĩa là một quá trình được sử dụng để thêm nhiều khối vào blockchain.

**Lợi ích và hạn chế của blockchain**

Nhiều lợi ích của công nghệ blockchain đang được thảo luận trong ngành công nghiệp và được đề xuất bởi các nhà lãnh đạo tư tưởng trên khắp thế giới trong không gian blockchain. 10 lợi ích hàng đầu được liệt kê và thảo luận như sau:

Phân cấp

Đây là một khái niệm cốt lõi và lợi ích của blockchain. Không cần bên thứ ba hoặc trung gian đáng tin cậy xác thực giao dịch; thay vào đó, một cơ chế đồng thuận được sử dụng để đồng ý về tính hợp lệ của các giao dịch.

Minh bạch và tin tưởng

Khi các blockchains được chia sẻ và mọi người có thể thấy những gì có trong blockchain, điều này cho phép hệ thống được minh bạch và kết quả là sự tin tưởng được thiết lập. Điều này có liên quan nhiều hơn trong các tình huống như giải ngân tiền hoặc lợi ích mà theo ý riêng của bạn nên bị hạn chế.

Tính không thay đổi

Một khi dữ liệu đã được ghi vào blockchain, rất khó để thay đổi nó trở lại. Nó không thực sự bất biến nhưng, do thực tế là việc thay đổi dữ liệu là vô cùng khó khăn và hầu như không thể, đây được coi là một lợi ích để duy trì một sổ cái bất biến của các giao dịch.

Tính khả dụng cao

Khi hệ thống dựa trên hàng nghìn nút trong mạng ngang hàng, và dữ liệu được sao chép và cập nhật trên mỗi và mọi nút, hệ thống trở nên có sẵn cao. Ngay cả khi các nút rời khỏi mạng hoặc không thể truy cập được, toàn bộ mạng vẫn tiếp tục hoạt động, do đó làm cho mạng trở nên khả dụng cao.

Độ an toàn cao

Tất cả các giao dịch trên một blockchain được bảo mật bằng mã hóa và cung cấp tính toàn vẹn

Đơn giản hóa các mô hình hiện tại

Mô hình hiện tại trong nhiều ngành như tài chính hoặc y tế là khá thiếu tổ chức, trong đó nhiều thực thể duy trì cơ sở dữ liệu của riêng họ và chia sẻ dữ liệu có thể trở nên rất khó khăn do tính chất khác nhau của các hệ thống. Nhưng như một blockchain có thể phục vụ như một sổ kế toán được chia sẻ giữa các bên quan tâm, điều này có thể dẫn đến việc đơn giản hóa mô hình này bằng cách giảm sự phức tạp của việc quản lý các hệ thống riêng biệt được duy trì bởi mỗi thực thể.

Giao dịch nhanh hơn

Trong ngành tài chính, đặc biệt là trong các chức năng thanh toán sau thương mại, blockchain có thể đóng vai trò quan trọng bằng cách cho phép giải quyết nhanh hơn các giao dịch vì nó không đòi hỏi quá trình xác minh, hòa giải và giải phóng mặt bằng. đã có sẵn trên sổ kế toán được chia sẻ giữa các tổ chức tài chính.

Tiết kiệm chi phí

Vì không có bên thứ ba hoặc nhà thanh toán bù trừ được yêu cầu trong mô hình blockchain, điều này có thể loại bỏ một cách ồ ạt chi phí trên không theo hình thức phí được thanh toán để thanh toán bù trừ nhà ở hoặc bên thứ ba đáng tin cậy.

Những thách thức và hạn chế của công nghệ blockchain

Như với bất kỳ công nghệ nào có những thách thức cần được giải quyết để làm cho một hệ thống mạnh mẽ hơn, hữu ích và dễ tiếp cận hơn. Công nghệ Blockchain cũng không ngoại lệ; trong thực tế rất nhiều nỗ lực đang được thực hiện trong Academia và Công nghiệp để vượt qua những thách thức đặt ra bởi công nghệ blockchain. Một lựa chọn những thách thức nhạy cảm nhất được trình bày như sau:

- Khả năng mở rộng

- Khả năng thích ứng

- Quy định

- Công nghệ tương đối chưa trưởng thành

- Riêng tư

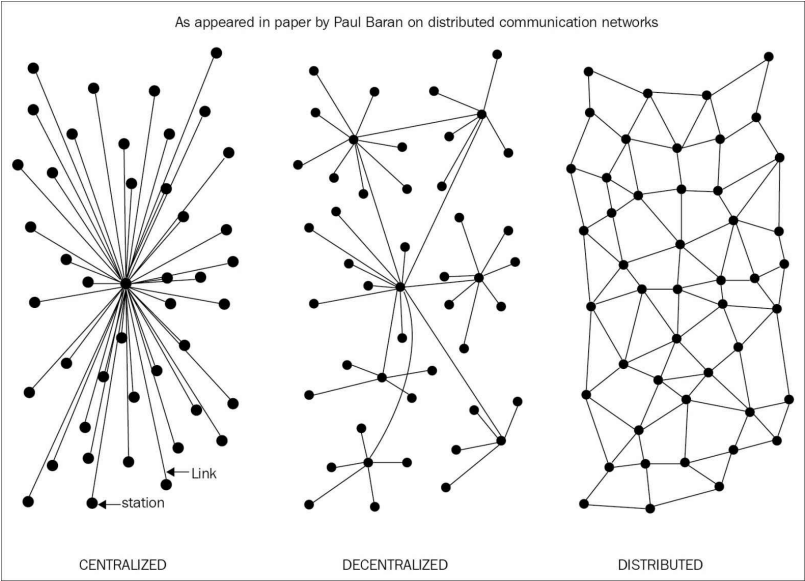
***Chương 2. Phân cấp, bao gồm các khái niệm phân cấp và mối quan hệ của nó với công nghệ blockchain. Các phương pháp và nền tảng khác nhau có thể được sử dụng để phân cấp một quy trình hoặc hệ thống.***

**Phân cấp bằng cách sử dụng blockchain**

Phân cấp là một lợi ích cốt lõi và dịch vụ được cung cấp bởi công nghệ blockchain. Blockchain theo thiết kế là một phương tiện hoàn hảo để cung cấp một nền tảng không cần bất kỳ trung gian và có thể hoạt động với nhiều nhà lãnh đạo khác nhau được lựa chọn thông qua các cơ chế đồng thuận. Mô hình này cho phép bất cứ ai cạnh tranh để trở thành cơ quan ra quyết định.

Công nghệ thông tin và truyền thông (ICT) thường được dựa trên một tập trung

mô hình theo đó các cơ sở dữ liệu hoặc các máy chủ ứng dụng nằm dưới sự kiểm soát của một cơ quan trung ương, chẳng hạn như người quản trị hệ thống. Với bitcoin và sự ra đời của công nghệ blockchain, mô hình này có thay đổi và bây giờ là công nghệ cho phép bất kỳ ai bắt đầu một hệ thống phân quyền (và vận hành nó không có điểm duy nhất của sự thất bại hoặc cơ quan đáng tin cậy duy nhất) có sẵn. Nó có thể được chạy tự chủ hoặc bằng cách yêu cầu một số can thiệp của con người tùy thuộc vào loại và mô hình quản trị được sử dụng trong ứng dụng phi tập trung chạy trên blockchain.



Các loại mạng / hệ thống khác nhau

Sự khác biệt chính giữa hệ thống phân tán và hệ thống phân tán là trong hệ thống phân tán, vẫn tồn tại một cơ quan trung ương điều chỉnh toàn bộ hệ thống, trong khi trong hệ thống phi tập trung, không có quyền nào tồn tại. Một hệ thống phân cấp là một loại mạng, theo đó các nút không phụ thuộc vào một nút chính duy nhất; thay vào đó, kiểm soát được phân phối giữa nhiều nút. Ví dụ, điều này tương tự như một mô hình trong đó mỗi bộ phận trong một tổ chức có máy chủ cơ sở dữ liệu riêng của họ, do đó lấy đi sức mạnh từ máy chủ trung tâm và phân phối nó tới các phòng ban quản lý cơ sở dữ liệu của riêng họ. Một sự đổi mới thực sự trong mô hình phân cấp đã bắt đầu kỷ nguyên mới của các ứng dụng phi tập trung hóa là sự đồng thuận phi tập trung, được giới thiệu với bitcoin. Điều này cho phép người dùng đồng ý về điều gì đó thông qua thuật toán đồng thuận mà không cần một bên thứ ba, trung gian hoặc nhà cung cấp dịch vụ tin cậy trung tâm.

**Phương pháp phân cấp**

Có hai phương pháp có thể được sử dụng để đạt được phân cấp. Những phương pháp đó là:

Không qua trung gian

Điều này có thể được giải thích với sự giúp đỡ của một ví dụ. Hãy tưởng tượng bạn muốn gửi tiền cho bạn bè của bạn ở một quốc gia khác. Bạn đến một ngân hàng sẽ chuyển tiền của bạn đến ngân hàng ở quốc gia bạn chọn với một khoản phí. Trong trường hợp này, ngân hàng giữ một cơ sở dữ liệu trung tâm được cập nhật, xác nhận rằng bạn đã gửi tiền. Với công nghệ blockchain, bạn có thể gửi tiền trực tiếp cho bạn bè mà không cần ngân hàng. Tất cả những gì bạn cần là địa chỉ của bạn bè của bạn trên blockchain. Bằng cách này, người trung gian không còn cần thiết và phân cấp được thực hiện bằng cách giải thể. Tuy nhiên, có thể tranh luận cách phân cấp thực tế trong lĩnh vực tài chính bằng cách giải thể do các yêu cầu về tuân thủ và quy định nặng nề. Tuy nhiên, mô hình này có thể được sử dụng không chỉ trong tài chính mà còn trong nhiều ngành công nghiệp khác nhau.

Thông qua cạnh tranh

Trong phương pháp này, một nhóm các nhà cung cấp dịch vụ cạnh tranh với nhau để được lựa chọn cho việc cung cấp các dịch vụ của hệ thống. Mô hình này không đạt được sự phân quyền hoàn toàn, nhưng ở một mức độ nhất định đảm bảo rằng một nhà cung cấp trung gian hoặc dịch vụ không độc quyền dịch vụ. Trong bối cảnh công nghệ blockchain, một hệ thống có thể được hình dung trong đó các hợp đồng thông minh có thể chọn một nhà cung cấp dữ liệu bên ngoài từ một số lượng lớn các nhà cung cấp dựa trên danh tiếng, điểm số, đánh giá và chất lượng dịch vụ trước đó. Điều này sẽ không dẫn đến việc phân quyền hoàn toàn, nhưng nó cho phép các hợp đồng thông minh tạo ra sự lựa chọn miễn phí dựa trên các tiêu chí được đề cập trước đó. Bằng cách này, một môi trường cạnh tranh được canh tác giữa các nhà cung cấp dịch vụ, theo đó họ cạnh tranh với nhau để trở thành nhà cung cấp dữ liệu được lựa chọn. Trong sơ đồ sau, các mức phân cấp khác nhau được hiển thị. Ở phía bên trái, có một cách tiếp cận thông thường, nơi một hệ thống trung tâm nằm trong tầm kiểm soát; ở phía bên tay phải, hoàn thành việc giải thể; và ở giữa, trung gian cạnh tranh hoặc các nhà cung cấp dịch vụ được hiển thị. Ở giữa, trung gian hoặc nhà cung cấp dịch vụ được lựa chọn dựa trên danh tiếng hoặc bỏ phiếu, do đó đạt được phân cấp một phần.

**Các tuyến để phân cấp**

Mặc dù có các hệ thống tồn tại trước bitcoin hoặc blockchain có thể được phân loại như phân cấp ở một mức độ nhất định, chẳng hạn như chia sẻ tệp BitTorrent hoặc Gnutella, với sự ra đời của công nghệ blockchain nhiều sáng kiến đang được thực hiện để tận dụng công nghệ mới này để phân cấp . Thông thường, blockchain bitcoin là sự lựa chọn đầu tiên cho nhiều người vì nó đã được chứng minh là blockchain bền vững và an toàn nhất với vốn hóa thị trường gần 12 tỷ đô la. Phương án thay thế

cách tiếp cận là sử dụng các blockchains khác, chẳng hạn như Ethereum, hiện là công cụ được nhiều nhà phát triển lựa chọn để xây dựng các ứng dụng phi tập trung.

**Cách phân cấp**

Một khuôn khổ đã được đề xuất bởi Arvind Narayanan và các khuôn khổ khác có thể được sử dụng để đánh giá các yêu cầu phân cấp của nhiều thứ trong bối cảnh công nghệ blockchain. Khuôn khổ cơ bản đề xuất bốn câu hỏi mà, một khi được trả lời, cung cấp một ý tưởng rõ ràng về cách một hệ thống có thể được phân cấp. Những câu hỏi này được liệt kê như sau:

1. Điều gì đang được phân cấp?

2. Cấp độ phân cấp là cần thiết?

3. Blockchain nào được sử dụng?

4. Cơ chế bảo mật nào được sử dụng?

Câu hỏi đầu tiên đơn giản là hỏi hệ thống nào đang được phân cấp. Đây có thể là bất kỳ hệ thống nào, ví dụ như hệ thống nhận dạng hoặc giao dịch. Câu hỏi tiếp theo có thể được trả lời bằng cách xác định mức phân cấp cần thiết bằng cách xem xét quy mô phân cấp đã thảo luận trước đó. Nó có thể được disintermediation đầy đủ hoặc một phần disintermediation. Câu hỏi thứ ba là khá đơn giản, nơi mà các nhà phát triển có thể đưa ra lựa chọn là blockchain nào phù hợp với một ứng dụng cụ thể. Nó có thể

được blockchain bitcoin, blockchain Ethereum, hoặc bất kỳ blockchain khác được coi là phù hợp cho một ứng dụng cụ thể. Cuối cùng, một câu hỏi quan trọng cần phải được trả lời về cơ chế bảo mật về cách bảo đảm an ninh của một hệ thống phân cấp có thể được đảm bảo. Nó có thể là Atomicity, ví dụ, theo đó giao dịch thực hiện đầy đủ hoặc không thực thi gì cả. Nói cách khác, đó là tất cả hoặc không có gì. Điều này đảm bảo tính toàn vẹn của hệ thống. Các cơ chế khác có thể bao gồm danh tiếng, cho phép mức độ tin cậy khác nhau trong một hệ thống.

**Blockchain và phân cấp hệ sinh thái đầy đủ**

Để đạt được sự phân cấp hoàn chỉnh, nó là cần thiết rằng môi trường xung quanh blockchain cũng được phân cấp. Blockchain chính nó là một sổ kế toán phân phối chạy trên đầu trang của các hệ thống thông thường. Các yếu tố này bao gồm lưu trữ, giao tiếp và tính toán. Có những yếu tố khác, chẳng hạn như danh tính và sự giàu có, theo truyền thống dựa trên các mô hình tập trung và có nhu cầu phân cấp các khía cạnh này để đạt được một hệ sinh thái phân cấp hoàn toàn.

Lưu trữ

Dữ liệu có thể được lưu trữ trực tiếp trong một blockchain, và với điều này, nó đạt được sự phân cấp, nhưng một bất lợi lớn của phương pháp này là blockchain không thích hợp để lưu trữ một lượng lớn dữ liệu theo thiết kế. Nó có thể lưu trữ các giao dịch đơn giản và một số dữ liệu tùy ý nhưng chắc chắn không thích hợp để lưu trữ hình ảnh hoặc các khối dữ liệu lớn, như trường hợp trong các hệ thống cơ sở dữ liệu truyền thống. Một lựa chọn tốt hơn là sử dụng các bảng băm được phân phối (DHT).

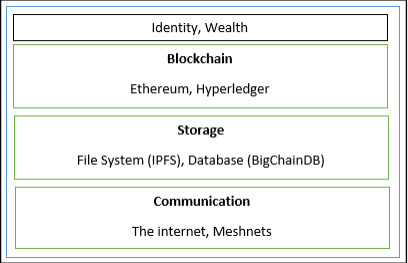
Giao tiếp

Nó thường được coi là Internet (lớp giao tiếp trong blockchain) được phân cấp. Điều này đúng ở một mức độ nào đó vì tầm nhìn ban đầu của Internet là phát triển một hệ thống phi tập trung. Các dịch vụ như e-mail và lưu trữ trực tuyến đều dựa trên mô hình nơi nhà cung cấp dịch vụ kiểm soát và người dùng tin tưởng họ để cung cấp cho họ quyền truy cập vào dịch vụ khi được yêu cầu. Mô hình này dựa trên sự tin cậy của cơ quan trung ương (nhà cung cấp dịch vụ) và người dùng không kiểm soát được dữ liệu của họ; thậm chí mật khẩu được lưu trữ trên các hệ thống của bên thứ ba đáng tin cậy. Có nhu cầu cung cấp quyền kiểm soát cho từng người dùng theo cách truy cập dữ liệu của họ được bảo đảm và không phụ thuộc vào một bên thứ ba. Truy cập Internet (lớp giao tiếp) dựa trên các nhà cung cấp dịch vụ Internet (ISP) hoạt động như một trung tâm trung tâm cho người dùng Internet. Nếu ISP bị đóng cửa vì lý do chính trị hoặc bất kỳ lý do nào khác, thì không thể kết nối với mô hình này. Một cách khác là sử dụng các mạng lưới. Mặc dù chúng bị hạn chế về chức năng so với Internet, chúng vẫn cung cấp một sự thay thế phi tập trung nơi các nút có thể nói chuyện trực tiếp với nhau mà không cần một trung tâm trung tâm như một ISP.

Tính toán

Phân cấp máy tính hoặc xử lý đạt được bằng công nghệ blockchain như Ethereum, nơi các hợp đồng thông minh với logic nghiệp vụ nhúng có thể chạy trên mạng. Các công nghệ blockchain khác cũng cung cấp các nền tảng lớp xử lý tương tự, nơi logic nghiệp vụ có thể chạy qua mạng theo cách phi tập trung.

Sơ đồ dưới đây cho thấy tổng quan hệ sinh thái phân cấp, ở tầng dưới cùng, Internet hoặc Meshnets cung cấp một lớp giao tiếp phi tập trung, sau đó một tầng lưu trữ sử dụng các công nghệ như IPFS và BigChainDB để cho phép phân cấp, và cuối cùng, bạn sẽ thấy blockchain lớp xử lý phân cấp. Blockchain có thể, trong một cách hạn chế, cung cấp một lớp lưu trữ quá, nhưng nghiêm túc cản trở tốc độ và năng lực của hệ thống; do đó, các giải pháp khác như IPFS và BigChainDB phù hợp hơn để lưu trữ lượng lớn dữ liệu theo cách phân cấp. Ở trên cùng, các lớp Identity và Wealth được hiển thị. Nhận dạng trên Internet là một chủ đề rất lớn và các hệ thống như bitAuth và OpenID đã cung cấp dịch vụ xác thực và nhận dạng với các mức độ phân cấp và giả định bảo mật khác nhau. Blockchain có khả năng cung cấp các giải pháp cho các vấn đề khác nhau. Một khái niệm liên quan đến Identity gọi là Tam giác của Zooko đòi hỏi một hệ thống đặt tên trong một giao thức mạng được an toàn, phân cấp và có ý nghĩa đối với con người. Người ta phỏng đoán rằng một hệ thống chỉ có thể có hai trong số các thuộc tính này cùng một lúc, nhưng với sự ra đời của blockchain, ở dạng Namecoin, vấn đề này đã được giải quyết. Tuy nhiên, điều này không phải là thuốc chữa bách bệnh và đi kèm với những thách thức riêng của nó, chẳng hạn như sự phụ thuộc vào người dùng để lưu trữ và duy trì khóa cá nhân một cách an toàn. Điều này mở ra các câu hỏi chung khác về sự phù hợp của phân cấp. Có lẽ việc phân cấp không phù hợp trong mọi tình huống. Các hệ thống tập trung tốt sẽ có xu hướng hoạt động tốt hơn trong nhiều trường hợp.



Hợp đồng thông minh

Một hợp đồng thông minh có thể được coi là một chương trình phân cấp nhỏ. Hợp đồng thông minh không nhất thiết cần một blockchain để chạy; tuy nhiên, do những lợi ích bảo mật mà công nghệ blockchain cung cấp, nó bây giờ trở thành một tiêu chuẩn để sử dụng blockchain như một nền tảng thực thi phi tập trung cho các hợp đồng thông minh. Một hợp đồng thông minh thường chứa một số logic nghiệp vụ và một lượng dữ liệu hạn chế. Các diễn viên hoặc người tham gia trong blockchain sử dụng các hợp đồng thông minh này hoặc họ tự chủ thay mặt cho những người tham gia mạng. Các chương trình nhỏ này nằm trên blockchain và thực hiện logic nghiệp vụ nếu một số tiêu chí cụ thể được đáp ứng. Thông tin thêm về hợp đồng thông minh sẽ được cung cấp trong Chương 6, Hợp đồng thông minh, được dành riêng cho một cuộc thảo luận chi tiết về các hợp đồng thông minh.

Tổ chức phi tập trung (Decentralized organizations)

Tổ chức phi tập trung (DOs) là các chương trình phần mềm chạy trên một blockchain và dựa trên ý tưởng của các tổ chức con người thực sự với con người và các giao thức. Khi DO, theo hình thức của một hợp đồng thông minh hoặc một tập hợp các hợp đồng thông minh, được thêm vào blockchain, nó trở thành phi tập trung và các bên tương tác với nhau dựa trên mã được xác định trong phần mềm DO.

Tổ chức tự trị phân cấp (Decentralized autonomous organizations)

Cũng giống như DOs, một tổ chức tự quản phân cấp (DAO) cũng là một chương trình máy tính hơn là chạy trên một blockchain và được nhúng bên trong nó là các quy tắc quản trị và logic nghiệp vụ. DAO và DO về cơ bản giống nhau, nhưng sự khác biệt chính là DAO là tự trị, có nghĩa là chúng hoàn toàn tự động và chứa logic thông minh giả tạo, trong khi DO thiếu tính năng này và dựa vào đầu vào của con người để thực hiện logic nghiệp vụ. Ethereum blockchain dẫn đầu với sự ra đời của DAOs lần đầu tiên. Trong DAO, mã được coi là thực thể quản lý chứ không phải là con người hoặc hợp đồng giấy. Một Curator, tuy nhiên, là một thực thể con người tham gia như một người duy trì mã này và hoạt động như một người đánh giá đề xuất cho cộng đồng. DAO có khả năng thuê các nhà thầu bên ngoài nếu đủ đầu vào được nhận từ các chủ thẻ (người tham gia).

Nền tảng cho phân cấp

Có rất nhiều nền tảng có sẵn để phân cấp ngay bây giờ. Nhiều công ty trên khắp thế giới đã giới thiệu các nền tảng hứa hẹn sẽ giúp phát triển ứng dụng phân tán dễ dàng, dễ truy cập và bảo mật cho người dùng. Một số tên nổi bật được thảo luận ở đây.

***Chương 3, Mật mã và Cơ sở kỹ thuật, giới thiệu mật mã cơ sở lý thuyết, cần thiết để hiểu đầy đủ về công nghệ blockchain. Các khái niệm như mật mã khóa công khai và riêng tư, với các ví dụ thực tế.***

**Giới thiệu**

Mật mã học là khoa học làm cho thông tin an toàn trong sự hiện diện của các đối thủ. Nó cung cấp một phương tiện giao tiếp an toàn trong sự hiện diện của các đối thủ với các nguồn tài nguyên vô hạn. Mật mã được sử dụng để mã hóa dữ liệu để nếu bị chặn bởi kẻ thù, dữ liệu là vô nghĩa đối với chúng mà không cần giải mã, yêu cầu khóa bí mật. Mật mã thường được sử dụng để cung cấp một dịch vụ bảo mật. Ngày của riêng nó, nó không thể được coi là một giải pháp hoàn chỉnh nhưng phục vụ như là một khối xây dựng quan trọng trong một hệ thống an ninh lớn hơn để giải quyết một vấn đề an ninh. Mật mã học cung cấp các dịch vụ bảo mật khác nhau, chẳng hạn như Bảo mật, Liêm chính, Xác thực, (Xác thực đối tượng và Xác thực nguồn gốc dữ liệu) và không từ chối. Ngoài ra, trách nhiệm giải trình cũng được yêu cầu trong các hệ thống bảo mật khác nhau.

**Toán học**

Là đối tượng của mật mã dựa trên toán học, phần này sẽ giới thiệu một số khái niệm cơ bản sẽ giúp bạn hiểu các khái niệm sau này trong chương.

Bộ

Tập hợp là một tập hợp các đối tượng riêng biệt, ví dụ: X = {1, 2, 3, 4, 5}.

Nhóm

Một nhóm là một nhóm giao hoán với một thao tác kết hợp hai phần tử của tập hợp. Hoạt động nhóm được đóng và liên kết với phần tử nhận dạng được xác định. Ngoài ra, mỗi phần tử trong tập hợp có một nghịch đảo. Đóng (đóng) có nghĩa là nếu, ví dụ, các phần tử A và B nằm trong tập hợp, thì phần tử kết quả sau khi thực hiện thao tác trên các phần tử cũng nằm trong tập hợp. Kết hợp nghĩa là việc nhóm các phần tử không ảnh hưởng đến kết quả của phép toán.

Trường

Trường là tập hợp chứa cả nhóm cộng và nhóm nhân. Chính xác hơn, tất cả các phần tử trong tập hợp tạo thành một nhóm cộng và nhân. Nó đáp ứng các tiên đề cụ thể để bổ sung và nhân lên. Đối với tất cả các hoạt động của nhóm, luật phân phối cũng được áp dụng. Luật quy định rằng cùng một khoản tiền hoặc sản phẩm sẽ được sản xuất ngay cả khi bất kỳ điều khoản hoặc yếu tố nào được sắp xếp lại.

Một trường hữu hạn

Một trường hữu hạn là một trường có tập các phần tử hữu hạn. Còn được gọi là trường Galois, các cấu trúc này có tầm quan trọng đặc biệt trong mật mã học vì chúng có thể được sử dụng để tạo ra kết quả chính xác và không có lỗi của phép tính số học. Ví dụ, các trường hữu hạn chính được sử dụng trong mã hóa đường cong elip để xây dựng vấn đề logarit rời rạc.

Thứ tự

Đây là số phần tử trong một trường.

Các trường chính

Đây là một trường hữu hạn với số nguyên tố chính. Nó có các quy tắc cụ thể cho phép cộng và phép nhân, và mỗi phần tử nonzero trong trường có nghịch đảo. Phép cộng và phép nhân được thực hiện modulo p.

Vòng

Nếu có thể xác định nhiều thao tác trên một nhóm abelian, nhóm đó sẽ trở thành một vòng. Ngoài ra còn có một số đặc tính cần được thỏa mãn. Một vòng phải có các đặc tính đóng và liên kết và phân phối.

Một nhóm tuần hoàn

Một nhóm tuần hoàn là một kiểu nhóm có thể được tạo ra bởi một phần tử đơn lẻ được gọi là bộ tạo nhóm. Nói cách khác, nếu thao tác nhóm được áp dụng nhiều lần cho một phần tử cụ thể trong nhóm, thì tất cả các phần tử trong nhóm có thể được tạo ra.

Một nhóm abelian

Một nhóm abelian được hình thành khi hoạt động trên các phần tử của một tập hợp là giao hoán. Luật giao hoán về cơ bản có nghĩa là thay đổi thứ tự của các yếu tố không ảnh hưởng đến kết quả của hoạt động, ví dụ, A X B = B X A.

Số học mô-đun

Còn được gọi là số học đồng hồ, số trong mô-đun số học quấn quanh khi chúng đạt đến một số cố định nhất định. Số cố định này là số dương được gọi là mô đun và tất cả các hoạt động được thực hiện liên quan đến số cố định này. Trong một tương tự với một đồng hồ, có số từ 1 đến 12. Khi nó đạt đến 12, số 1 bắt đầu một lần nữa. Nói cách khác, số học này đề cập đến các phần dư sau khi hoạt động phân chia. Ví dụ, 50 mod 11 là 6 vì 50/11 để lại phần còn lại của 6. Điều này hoàn thành một giới thiệu cơ bản về một số khái niệm toán học; trong phần tiếp theo, bạn sẽ được giới thiệu về mật mã.

**Mật mã học**

Mật mã cung cấp các dịch vụ bảo mật khác nhau và các dịch vụ bảo mật.

**Bảo mật**

Bảo mật là sự đảm bảo rằng thông tin chỉ có sẵn cho các thực thể được ủy quyền.

**Tính toàn vẹn**

Tính toàn vẹn là sự đảm bảo rằng thông tin chỉ có thể được sửa đổi bởi các thực thể được ủy quyền.

**Xác thực**

Xác thực cung cấp sự đảm bảo về danh tính của một thực thể hoặc tính hợp lệ của một thông báo. Có hai loại xác thực, được thảo luận ở đây.

**Không bác bỏ**

Không bác bỏ là đảm bảo rằng một thực thể không thể từ chối một cam kết hoặc hành động trước đó bằng cách cung cấp bằng chứng không thể tha thứ. Đây là một dịch vụ bảo mật cung cấp bằng chứng không thể tha thứ cho thấy một hành động cụ thể đã xảy ra. Thuộc tính này là rất cần thiết trong các tình huống có thể tranh chấp, theo đó một thực thể đã từ chối các hành động được thực hiện, ví dụ, đặt hàng trên một hệ thống thương mại điện tử. Dịch vụ này tạo ra bằng chứng mật mã trong các giao dịch điện tử để trong trường hợp có tranh chấp, nó có thể được sử dụng như một xác nhận của một hành động. Không từ chối đã là một khu vực nghiên cứu tích cực trong nhiều năm. Tranh chấp trong giao dịch điện tử là một vấn đề phổ biến và cần phải giải quyết chúng để tăng mức độ tin cậy của người tiêu dùng trong dịch vụ.

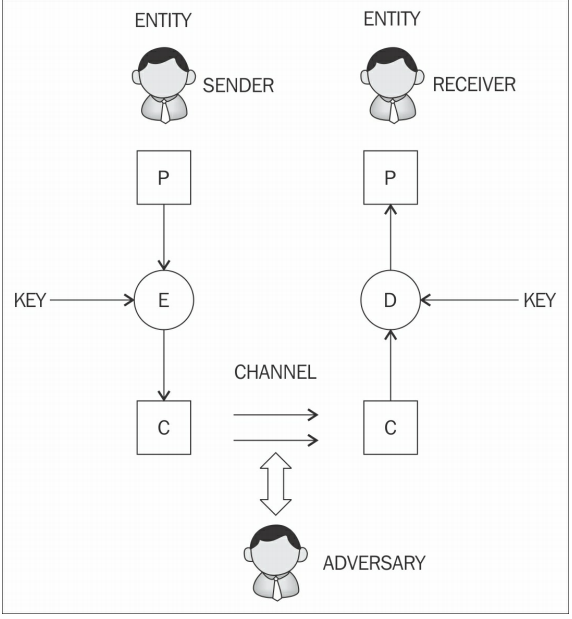
**Trách nhiệm giải trình**

Trách nhiệm giải trình là sự đảm bảo rằng các hành động ảnh hưởng đến an ninh có thể được truy nguồn từ bên chịu trách nhiệm. Điều này thường được cung cấp bằng cách đăng nhập và kiểm tra các cơ chế trong các hệ thống cần kiểm toán chi tiết do tính chất của doanh nghiệp, ví dụ, trong các hệ thống giao dịch điện tử. Các bản ghi chi tiết rất quan trọng để theo dõi các hành động của một thực thể, ví dụ, khi một giao dịch được đặt trong một bản ghi kiểm tra có ngày và thời gian, danh tính của thực thể được tạo và lưu trong tệp nhật ký. Tệp nhật ký này có thể

tùy chọn được mã hóa và có thể là một phần của cơ sở dữ liệu hoặc tệp nhật ký văn bản ASCII độc lập trên một hệ thống.

**Các mã hóa nguyên thủy**

Các mã hóa nguyên thủy là các khối xây dựng cơ bản của một giao thức hoặc hệ thống bảo mật. Trong phần sau, bạn được giới thiệu các thuật toán mã hóa cần thiết cho việc xây dựng các giao thức và hệ thống an toàn. Giao thức bảo mật là một tập hợp các bước được thực hiện để đạt được mục tiêu bảo mật cần thiết bằng cách sử dụng các cơ chế bảo mật thích hợp. Các loại giao thức bảo mật khác nhau đang được sử dụng, chẳng hạn như các giao thức xác thực, các giao thức không loại bỏ và các giao thức quản lý khóa. Một mô hình mật mã chung được thể hiện trong sơ đồ sau:



Entity: Đây là người hoặc hệ thống gửi, nhận hoặc thực hiện các thao tác trên dữ liệu

Sender: Người gửi là một thực thể truyền dữ liệu

Receiver: Người nhận là một thực thể nhận dữ liệu

Adversary: Đây là một thực thể cố gắng phá vỡ dịch vụ bảo mật

Key: Khóa là một số dữ liệu được sử dụng để mã hóa hoặc giải mã dữ liệu

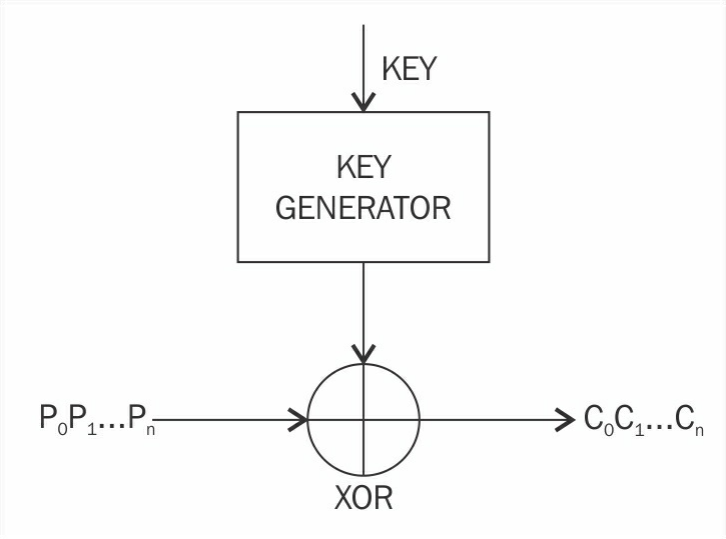
Channel: Kênh cung cấp phương tiện giao tiếp giữa các thực thể

**Mật mã đối xứng**

Mật mã đối xứng đề cập đến một loại mật mã theo đó khóa được sử dụng để mã hóa dữ liệu giống nhau để giải mã dữ liệu, và do đó nó còn được gọi là mật mã khóa chia sẻ. Chìa khóa phải được thiết lập hoặc đồng ý trước khi trao đổi dữ liệu giữa các bên giao tiếp. Đây là lý do nó còn được gọi là mật mã khóa bí mật. Có hai loại mật mã đối xứng, mật mã dòng và mật mã khối. Chuẩn mã hóa dữ liệu (DES) và Chuẩn mã hóa tiên tiến (AES) là các ví dụ phổ biến về mật mã khối, trong khi RC4 và A5 thường được sử dụng mật mã dòng.

Mã hóa luồng

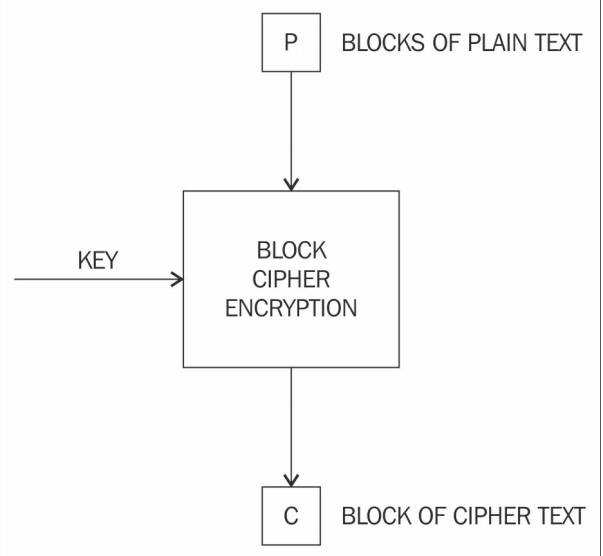
Các thuật toán mã hóa này là các thuật toán mã hóa áp dụng các thuật toán mã hóa trên cơ sở từng bit một cho văn bản thuần túy bằng cách sử dụng luồng chính. Có hai loại mật mã dòng: đồng bộ và không đồng bộ. Mật mã dòng đồng bộ là những nơi mà luồng khóa chỉ phụ thuộc vào khóa, trong khi mật mã dòng không đồng bộ có luồng khóa cũng phụ thuộc vào dữ liệu được mã hóa. Trong mật mã dòng, mã hóa và giải mã về cơ bản là cùng một chức năng vì chúng là các phép bổ sung modulo 2 đơn giản hoặc hoạt động XOR. Yêu cầu quan trọng trong thuật toán mã hóa luồng là tính bảo mật và tính ngẫu nhiên của các luồng chính.



Hoạt động của một mật mã dòng

Chặn mật mã

Đây là những thuật toán mã hóa chia nhỏ văn bản được mã hóa (văn bản thuần) thành các khối có độ dài cố định và áp dụng khối mã hóa theo khối. Mật mã khối thường được xây dựng bằng cách sử dụng chiến lược thiết kế được gọi là mật mã Fiestel.

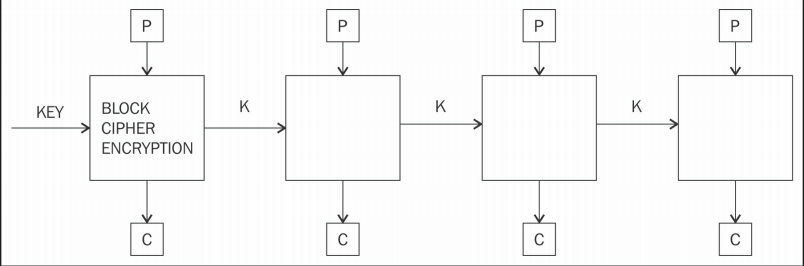


Hoạt động đơn giản của mật mã khối

*Các chế độ hoạt động khác nhau cho mật mã khối là Sách mã điện tử (ECB), chuỗi khối mật mã (CBC), Chế độ phản hồi đầu ra (OFB) hoặc chế độ truy cập (CTR). Các chế độ này được sử dụng để xác định cách thức mà một chức năng mã hóa sẽ được áp dụng cho văn bản thuần túy.*

Sách mã điện tử (ECB)

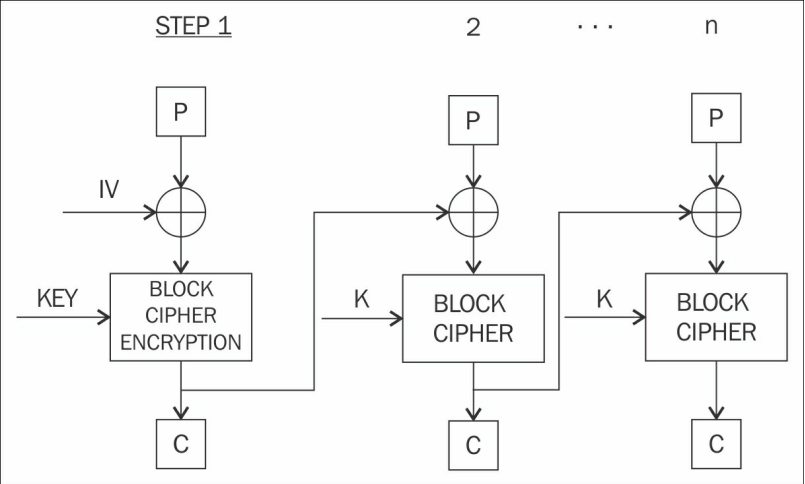
Đây là một chế độ hoạt động cơ bản trong đó dữ liệu được mã hóa được tạo ra như là kết quả của việc áp dụng thuật toán mã hóa từng người một cho từng khối văn bản thuần túy. Đây là chế độ đơn giản nhất nhưng không được sử dụng trong thực tế vì nó không an toàn và có thể tiết lộ thông tin:



Chế độ sách mã điện tử cho mật mã khối

Chuỗi khối mật mã

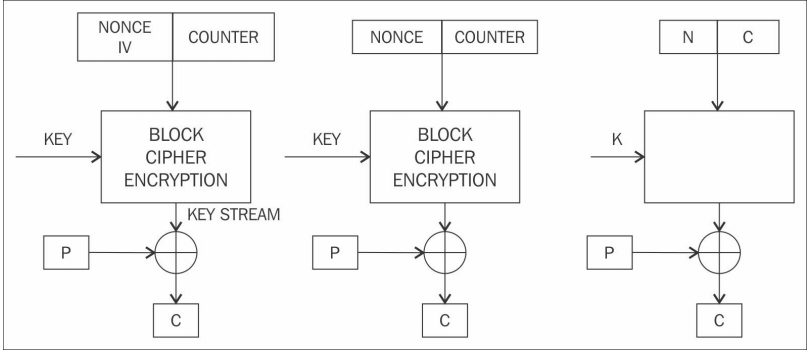
Trong chế độ này, mỗi khối văn bản thuần là XORed với khối được mã hóa trước đó. Chế độ CBC sử dụng vector khởi tạo IV để mã hóa khối đầu tiên. Đó là khuyến cáo rằng IV được chọn ngẫu nhiên:



Chế độ chuỗi khối mã hóa

Chế độ truy cập

Chế độ CTR có hiệu quả sử dụng mật mã khối làm mật mã dòng. Trong trường hợp này, một nonce duy nhất được cung cấp được nối với giá trị bộ đếm để tạo ra một luồng khóa:

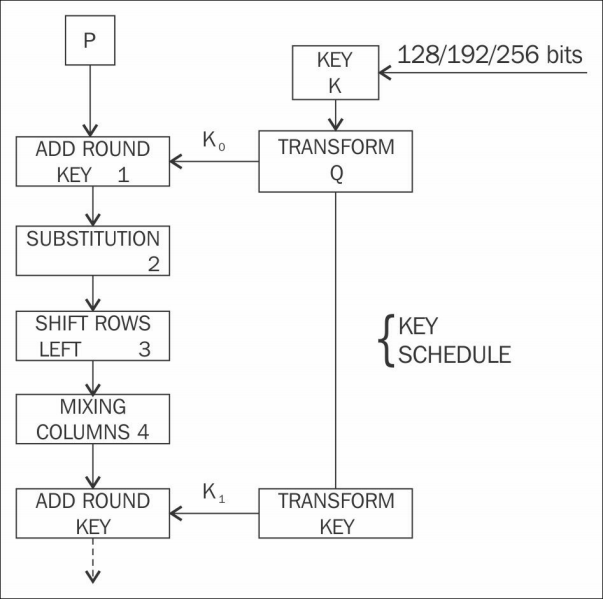


**Tiêu chuẩn mã hóa dữ liệu (DES)**

DES đã được Viện Tiêu chuẩn và Công nghệ Quốc gia Hoa Kỳ (NIST) giới thiệu như là một thuật toán chuẩn để mã hóa và được sử dụng chính trong những năm 1980 và 1990, nhưng nó đã không được chứng minh là có khả năng chống lại các cuộc tấn công bạo lực, do những tiến bộ trong công nghệ và nghiên cứu mã hóa.

**Tiêu chuẩn mã hóa nâng cao (AES)**

Năm 2001, sau một cuộc thi mở, một thuật toán mã hóa tên là Rijndael được phát minh bởi các nhà mật mã Joan Daemen và Vincent Rijmen được chuẩn hóa là AES với những sửa đổi nhỏ của NIST vào năm 2001. Cho đến nay, không có cuộc tấn công nào chống lại AES tốt hơn phương pháp bạo lực. Rijndael gốc cho phép các kích cỡ khóa và khóa khác nhau là 128 bit, 192 bit và 256 bit, nhưng trong tiêu chuẩn AES, chỉ cho phép kích thước khối 128 bit. Tuy nhiên, kích thước khóa 128 bit, 192 bit và 256 bit được cho phép.



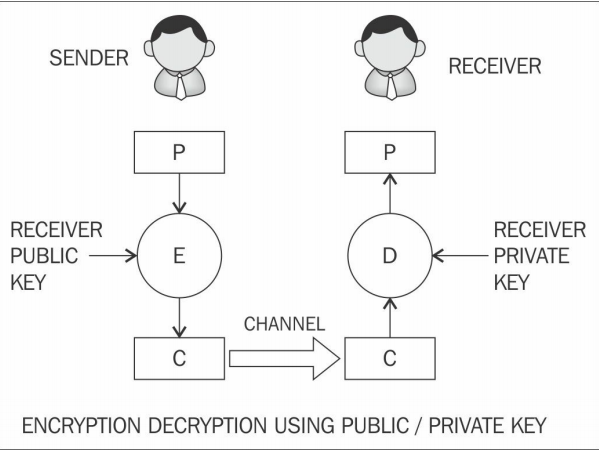
Biểu đồ khối AES, hiển thị vòng 1, trong bước trộn cuối cùng không được thực hiện

Các ví tiền điện tử khác nhau sử dụng mã hóa AES để mã hóa dữ liệu được lưu trữ cục bộ. Đặc biệt trong ví bitcoin, AES 256 ở chế độ CBC được sử dụng.

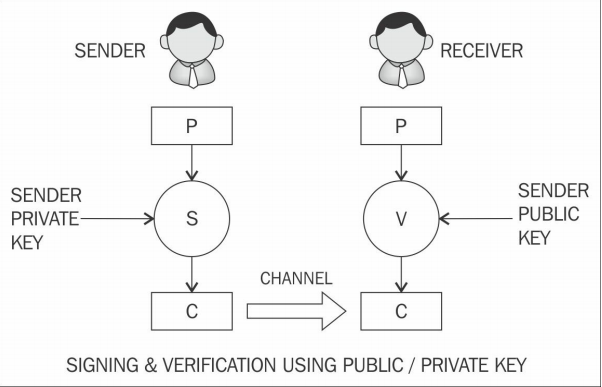
**Mật mã bất đối xứng**

Mật mã không đối xứng đề cập đến một loại mật mã theo đó khóa được sử dụng để mã hóa dữ liệu khác với khóa được sử dụng để giải mã dữ liệu. Còn được gọi là mật mã khóa công khai, nó sử dụng khóa công khai và riêng tư để mã hóa và giải mã dữ liệu tương ứng.

Tổng quan về mật mã khoá công khai được hiển thị trong sơ đồ sau:



Một biểu đồ khác cho thấy cách mã hóa khóa công khai có thể được sử dụng để xác minh tính toàn vẹn của thông điệp nhận được bởi người nhận. Trong mô hình này, người gửi ký các dữ liệu bằng cách sử dụng khóa riêng của họ và truyền thông điệp trên cho người nhận. Sau khi nhận được tin nhắn ở phía người nhận, nó có thể được xác minh tính toàn vẹn của nó bằng khóa công khai của người gửi. Lưu ý rằng không có mã hóa nào được thực hiện trong mô hình này. Mô hình này chỉ được sử dụng cho mục đích xác thực và xác thực thư:



Tích phân số nguyên

Các lược đồ này dựa trên thực tế là các số nguyên lớn rất khó để có yếu tố. RSA là ví dụ chính của loại thuật toán này.

Logarit rời rạc

Điều này được dựa trên một vấn đề trong số học mô-đun mà nó rất dễ dàng để tính toán kết quả của chức năng modulo nhưng nó là tính toán không khả thi để tìm số mũ của máy phát điện. Nói cách khác, rất khó để tìm đầu vào từ kết quả. Đây là chức năng một chiều.

Ví dụ, xem xét phương trình sau:

*32 mod 10 =9*

Bây giờ cho 9 phát hiện 2, số mũ của cơ số 3 là rất khó. Vấn đề khó khăn này thường là

được sử dụng trong các trao đổi khóa và thuật toán chữ ký số của Diffie-Hellman.

Đường cong elip

Điều này được dựa trên các vấn đề logarit rời rạc được thảo luận trước đó, nhưng trong bối cảnh đường cong elliptic.Elliptic là một đường cong khối đại số trên một lĩnh vực, có thể được xác định bởi một phương trình được hiển thị ở đây. Đường cong không phải là số ít, có nghĩa là nó không có điểm dừng hoặc ngã tư. Nó có hai biến a, b, cùng với một điểm vô cùng.

y2 = x3 + ax + b

Ở đây, a, b là các số nguyên có thể có các giá trị khác nhau và là các phần tử của trường mà đường cong elip được xác định. Đường cong elliptic có thể được xác định trên thực tế, số hữu tỉ, số phức hoặc trường hữu hạn. Đối với các mục đích mã hóa, đường cong elip trên các trường hữu hạn được sử dụng thay cho các số thực. Ngoài ra, số nguyên tố phải lớn hơn 3. Các đường cong khác nhau có thể được tạo ra bằng cách thay đổi giá trị a, b. Hầu hết các hệ thống mã hóa được sử dụng nổi bật dựa trên các đường cong elliptic là thuật toán chữ ký số Elliptic Curve (ECDSA) và trao đổi khóa Elliptic Curve Diffie-Hellman (ECDH)

**Khóa công khai và riêng tư**

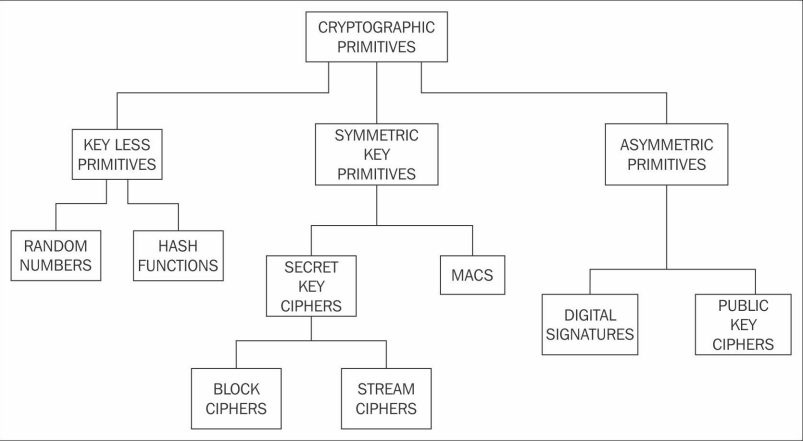
Một khóa riêng, như các tên cho thấy, về cơ bản là một số được tạo ngẫu nhiên được giữ bí mật và được giữ riêng bởi người dùng. Khóa cá nhân cần được bảo vệ và không được cấp quyền truy cập trái phép vào khóa đó; nếu không, toàn bộ lược đồ mã hóa khóa công khai sẽ bị nguy hiểm vì đây là khóa được sử dụng để giải mã thông điệp. Khóa riêng có thể có độ dài khác nhau tùy thuộc vào loại và loại thuật toán được sử dụng. Ví dụ, trong RSA, thông thường, một khóa 1024-bit hoặc 2048 bit được sử dụng. Kích thước khóa 1024 bit không còn được coi là an toàn và ít nhất 2048 bit được khuyến nghị sử dụng trong thực tế.

Khóa công khai là phần công khai của cặp khóa riêng-công khai. Một khóa công khai có sẵn công khai và được xuất bản bởi chủ sở hữu khóa riêng. Bất kỳ ai sau đó muốn gửi cho nhà xuất bản khóa công khai một thông báo được mã hóa có thể làm như vậy bằng cách mã hóa thông báo bằng cách sử dụng khóa công khai đã được xuất bản và gửi nó tới người giữ khóa riêng. Không ai khác có thể giải mã thông điệp vì khóa cá nhân tương ứng được giữ an toàn bởi người nhận dự định. Khi nhận được tin nhắn được mã hóa khóa công khai, người nhận có thể giải mã tin nhắn bằng khóa riêng.

Có một số lo ngại về khóa công khai, chẳng hạn như tính xác thực và nhận dạng nhà xuất bản khóa công cộng.

**Mật mã học nguyên thủy**

Phân loại này của nguyên thủy mật mã có thể được hình dung như được hiển thị ở đây:



**Hàm băm**

Các hàm băm thường được sử dụng để cung cấp các dịch vụ toàn vẹn dữ liệu. Chúng có thể được sử dụng như các hàm một chiều và để xây dựng các nguyên thủy mã hóa khác, như MAC và chữ ký số. Một số ứng dụng sử dụng hàm băm như một phương tiện tạo ra các số ngẫu nhiên giả (PRNGs). Hàm băm không yêu cầu khóa. Có hai thuộc tính bảo mật thực tế và ba hàm băm phải được đáp ứng tùy thuộc vào mức độ yêu cầu của tính toàn vẹn.

Nén các thông điệp tùy ý vào thông báo độ dài cố định

Thuộc tính này có liên quan với thực tế là hàm băm phải có khả năng lấy một văn bản đầu vào dài của bất kỳ độ dài nào và xuất ra một thông điệp nén cố định chiều dài. Hàm băm tạo ra đầu ra được nén theo các kích cỡ bit khác nhau, thường là giữa 128 bit và 512 bit.

Dễ dàng tính toán

Hàm băm là các hàm một chiều hiệu quả và nhanh chóng. Yêu cầu là chúng rất nhanh để tính toán bất kể kích thước thư. Hiệu quả có thể giảm nếu thông điệp quá lớn nhưng chức năng vẫn đủ nhanh để sử dụng thực tế.

Kháng ảnh trước

Xem xét một phương trình:

h (x) = y

Ở đây, h là hàm băm, x là đầu vào, và y là băm. Thuộc tính bảo mật đầu tiên yêu cầu y không thể đảo ngược được tính thành x. x được xem là hình ảnh trước của y, do đó tên gọi là kháng ảnh trước. Điều này cũng được gọi là tài sản một chiều.

Kháng cự hình ảnh thứ hai

Thuộc tính này yêu cầu x và h (x), hầu như không thể tìm thấy bất kỳ thông báo nào khác m, trong đó m! = X và băm của m = băm của x. h (m) = h (x). Thuộc tính này còn được gọi là kháng va chạm yếu.

Va chạm kháng

Thuộc tính này yêu cầu hai thông báo đầu vào khác nhau không được băm vào cùng một đầu ra. Nói cách khác, h (x)! = H (z). Thuộc tính này còn được gọi là kháng va chạm mạnh. Hàm băm, do bản chất của chúng, sẽ luôn có một số va chạm, và đó là nơi mà hai thông điệp khác nhau băm vào cùng một đầu ra, nhưng chúng sẽ không khả thi về tính toán để tìm. Một khái niệm được gọi là hiệu ứng avalanche là mong muốn trong tất cả các hàm băm. Hiệu ứng Avalanche chỉ định rằng một thay đổi nhỏ, thậm chí một thay đổi ký tự đơn lẻ trong văn bản đầu vào, sẽ dẫn đến một kết quả băm hoàn toàn khác.

Message Digest (MD)

Chức năng Message Digest rất phổ biến vào đầu những năm 1990. MD4 và MD5 là thành viên của thể loại này. Cả hai chức năng MD được tìm thấy là không an toàn và không được khuyến khích sử dụng nữa. MD5 là một hàm băm 128 bit thường được sử dụng để kiểm tra tính toàn vẹn của tệp.

Message Digest (MD) (phân loại thông điệp)

Chức năng Message Digest rất phổ biến vào đầu những năm 1990. MD4 và MD5 là thành viên của thể loại này. Cả hai chức năng MD được tìm thấy là không an toàn và không được khuyến khích sử dụng nữa. MD5 là một hàm băm 128 bit thường được sử dụng để kiểm tra tính toàn vẹn của tệp.

Thuật toán băm bảo mật (SHA)

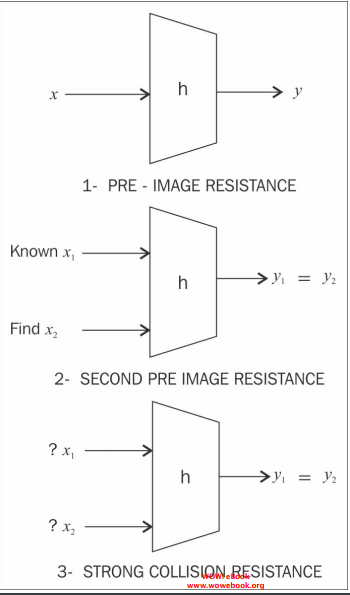
SHA-0: Đây là chức năng 160 bit được NIST giới thiệu vào năm 1993.

SHA-1: SHA-1 được NIST giới thiệu sau đó thay cho SHA-0. Đây cũng là một hàm băm 160 bit. SHA-1 được sử dụng phổ biến trong triển khai SSL và TLS. Cần lưu ý rằng SHA-1 hiện được coi là không an toàn và không được cơ quan cấp chứng nhận cho phép. Cách sử dụng của nó bây giờ không được khuyến khích trong bất kỳ triển khai mới nào. SHA-2: Danh mục này bao gồm bốn hàm được xác định bởi số bit của hàm băm: SHA-224, SHA-256, SHA-384 và SHA-512.

SHA-3: Đây là họ mới nhất của hàm SHA. SHA3-224, SHA3-256, SHA3-384 và SHA3- 512 là thành viên của gia đình này. SHA3 là phiên bản Keccak được tiêu chuẩn hóa của NIST. Keccak sử dụng một phương pháp mới gọi là xây dựng miếng bọt biển thay vì biến đổi Merkle-Damgard thường được sử dụng.

RIPEMD: RIPEMD là từ viết tắt của RACE Integrity Primitives Evaluation Message Digest. Nó dựa trên các ý tưởng thiết kế được sử dụng để xây dựng MD4. Có nhiều phiên bản của RIPEMD, bao gồm 128 bit, 160 bit, 256 bit và 320 bit.

Whirlpool: Điều này dựa trên phiên bản biến đổi của mật mã Rijndael được gọi là W. Nó sử dụng chức năng nén Miyaguchi-Preneel, là một loại hàm một chiều được sử dụng để nén hai đầu vào chiều dài cố định thành một đầu ra chiều dài cố định. Nó là một chức năng nén chiều dài khối duy nhất:



Thiết kế các thuật toán băm bảo mật (SHA)

Trong phần sau, bạn sẽ được giới thiệu về thiết kế SHA-256 và SHA-3. Cả hai đều được sử dụng trong bitcoin và Ethereum, tương ứng. Ethereum không sử dụng NIST Standard SHA-3 nhưng Keccak, là thuật toán gốc được trình bày cho NIST. NIST, sau một số sửa đổi như tăng số vòng và đệm thông điệp đơn giản hơn, chuẩn hóa Keccak thành SHA-3.

SHA-256

SHA-256 có kích thước tin nhắn đầu vào <2 ^ 64 bit. Kích thước khối là 512 bit và có kích thước từ 32 bit. Đầu ra là tiêu hóa 256 bit.

Hàm nén xử lý khối thông điệp 512 bit và giá trị băm trung gian 256 bit.

Có hai thành phần chính của chức năng này: chức năng nén và lịch biểu tin nhắn.

Các thuật toán hoạt động như sau:

Sơ chế:

1. Đệm thông điệp, được sử dụng để làm cho chiều dài của khối thành 512 bit nếu nó nhỏ hơn kích thước khối yêu cầu là 512 bit.

2. Phân tích cú pháp tin nhắn thành các khối tin nhắn để đảm bảo rằng thông điệp và phần đệm của nó được chia thành các khối bằng 512 bit.

3. Thiết lập giá trị băm ban đầu, đó là tám từ 32 bit thu được bằng cách lấy 32 bit đầu tiên của các phần phân đoạn của căn bậc hai của tám số nguyên tố đầu tiên. Các giá trị ban đầu này được lựa chọn ngẫu nhiên để khởi tạo quá trình và đưa ra một mức độ tin cậy rằng không có backdoor tồn tại trong thuật toán. Tính toán băm:

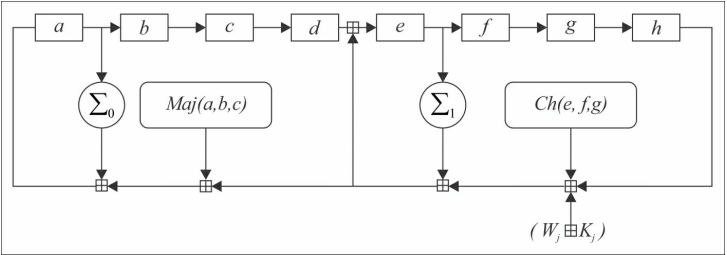
1. Mỗi khối tin nhắn được xử lý theo trình tự và yêu cầu 64 vòng để tính toán đầu ra băm đầy đủ. Mỗi vòng sử dụng các hằng số hơi khác nhau để đảm bảo không có hai vòng nào giống nhau.

2. Đầu tiên, lịch trình tin nhắn được chuẩn bị.

3. Sau đó, tám biến làm việc được khởi tạo.

4. Sau đó, giá trị băm trung gian được tính toán.

5. Cuối cùng, thông báo được xử lý và băm đầu ra được tạo ra:

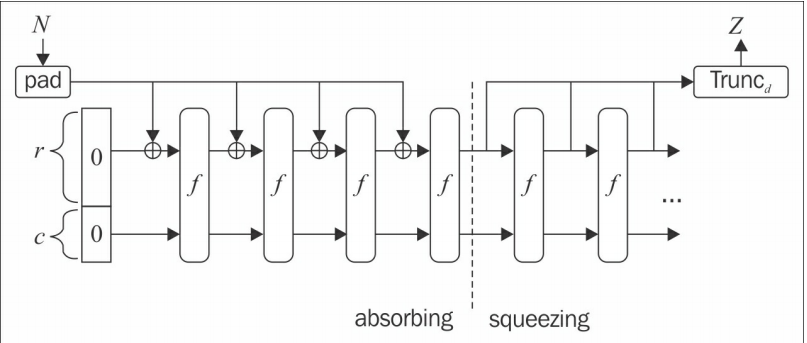


Một vòng hàm nén SHA 256

Thiết kế SHA3 (Keccak)

Cấu trúc của SHA-3 rất khác so với SHA-1 và SHA-2 thông thường. Ý tưởng chính đằng sau SHA-3 được dựa trên hoán vị không có khóa so với các cấu trúc hàm băm thông thường khác sử dụng các hoán vị có khóa. Keccak cũng không sử dụng phép biến đổi Merkle-Damgard thường được sử dụng để xử lý các thông điệp đầu vào có độ dài tùy ý trong hàm băm. Một phương pháp mới hơn được gọi là xây dựng miếng bọt biển và bóp được sử dụng trong Keccak, cơ bản là một hoán vị ngẫu nhiên mô hình. Các biến thể khác nhau của SHA3 đã được chuẩn hóa, chẳng hạn như SHA3-224, SHA3-256, SHA3-384, SHA3-512, SHAKE128 và SHAKE256. SHAKE128 và SHAKE256 là các hàm đầu ra có thể mở rộng cũng được chuẩn hóa bởi các hàm NIST.XOF cho phép đầu ra được mở rộng đến bất kỳ độ dài mong muốn nào.

Sơ đồ sau đây cho thấy mô hình bọt biển và bóp là cơ sở của SHA3 hoặc Keccak. Tương tự như bọt biển, đầu tiên, dữ liệu được hấp thụ vào miếng bọt biển sau khi áp dụng padding, sau đó nó được thay đổi thành một tập con của trạng thái hoán vị bằng cách sử dụng XOR và sau đó đầu ra được vắt ra khỏi hàm sponge đại diện cho trạng thái chuyển đổi. Tỷ lệ là kích thước khối đầu vào của hàm sponge,trong khi năng lực xác định mức độ bảo mật chung:



Mã xác thực thư (MAC)

MAC đôi khi được gọi là các hàm băm có khóa và có thể được sử dụng để cung cấp tính toàn vẹn và xác thực thông báo. Nói cách khác, chúng được sử dụng để cung cấp xác thực nguồn gốc dữ liệu. Đây là các nguyên thủy mã hóa đối xứng sử dụng khóa chia sẻ giữa người gửi và người nhận. MAC có thể được xây dựng bằng cách sử dụng mật mã khối hoặc hàm băm.

MAC sử dụng mật mã khối

Trong phương pháp này, mật mã khối được sử dụng trong chế độ chuỗi khối mã hóa (chế độ CBC) để tạo ra một MAC. Bất kỳ mật mã khối, ví dụ, AES trong chế độ CBC-có thể được sử dụng. MAC của thông điệp trên thực tế là đầu ra của vòng cuối cùng của hoạt động CBC. Độ dài của đầu ra MAC giống với độ dài khối của mật mã khối được sử dụng để tạo MAC. MAC được xác minh đơn giản bằng cách tính MAC của tin nhắn và so sánh nó với MAC nhận được. Nếu chúng giống nhau, thì tính toàn vẹn của thông báo được xác nhận; nếu không, tin nhắn được coi là thay đổi. Cũng cần lưu ý rằng MAC hoạt động giống như chữ ký số, nhưng chúng không thể cung cấp dịch vụ không phân biệt do tính chất đối xứng của chúng.

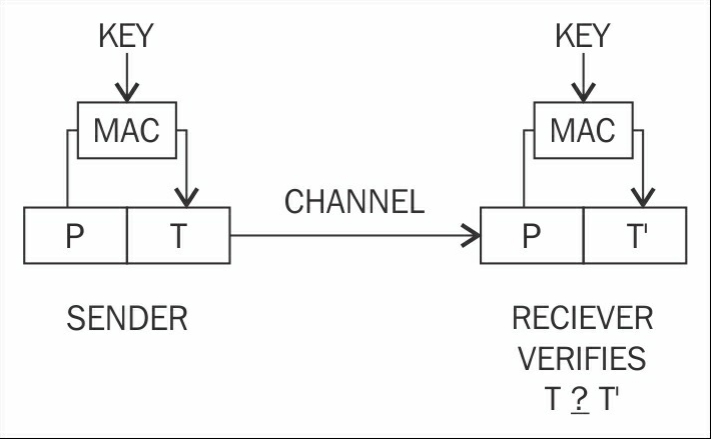
HMAC (MAC dựa trên băm)

Tương tự như hàm băm, chúng tạo ra một đầu ra có độ dài cố định và lấy một thông điệp dài tùy ý làm đầu vào. Trong sơ đồ này, người gửi ký một thông báo bằng cách sử dụng MAC và người nhận xác minh nó bằng cách sử dụng khóa chia sẻ. Khóa được băm bằng thông điệp bằng một trong hai phương thức được gọi là tiền tố bí mật hoặc phương thức hậu tố bí mật. Trong phương thức đầu tiên, khóa được nối với thông báo, có nghĩa là, khóa đến trước và thông báo xuất hiện sau, trong khi ở phương thức thứ hai, khóa xuất hiện sau thông báo:

Tiền tố bí mật: M = MACk (x) = h (k || x)

Hậu tố bí mật: M = MACk (x) = h (x || k)

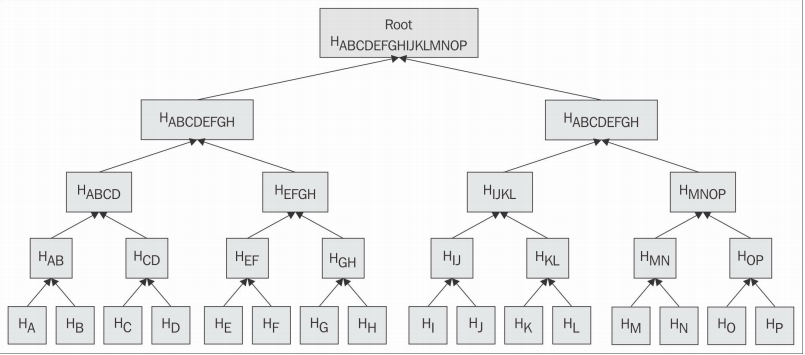
Có ưu và nhược điểm của cả hai phương pháp. Một số cuộc tấn công vào cả hai đề án đã được phát hiện. Có các chương trình xây dựng HMAC sử dụng các kỹ thuật khác nhau, chẳng hạn như ipad và opad (đệm bên trong và đệm ngoài) do các nhà nghiên cứu đề xuất được coi là an toàn với một số giả định:



Cây Merkle

Khái niệm về cây Merkle được giới thiệu bởi Ralph Merkle. Một hình ảnh của cây Merkle được hiển thị ở đây, giúp dễ hiểu. Cây Merkle cho phép xác minh an toàn và hiệu quả các tập dữ liệu lớn.

Nó là một cây nhị phân, trong đó đầu tiên được đặt ở các lá (nút không có con), và sau đó các giá trị của các cặp nút con được băm cùng nhau để tạo ra một giá trị cho nút cha (nút bên trong) cho đến khi giá trị băm đơn được gọi là gốc Merkle đạt được:



Cây Patricia

Để hiểu được cây Patricia, trước tiên, bạn sẽ được giới thiệu khái niệm về một cây trie. Trie hoặc cây kỹ thuật số là cấu trúc dữ liệu cây được sắp xếp được sử dụng để lưu trữ tập dữ liệu.

Thuật toán thực tế để lấy thông tin được mã hóa bằng chữ và số (Patricia), còn được gọi là cây Radix, là một biểu diễn nhỏ gọn của một trie trong đó một nút là con duy nhất của cha / mẹ được hợp nhất với cha mẹ của nó.

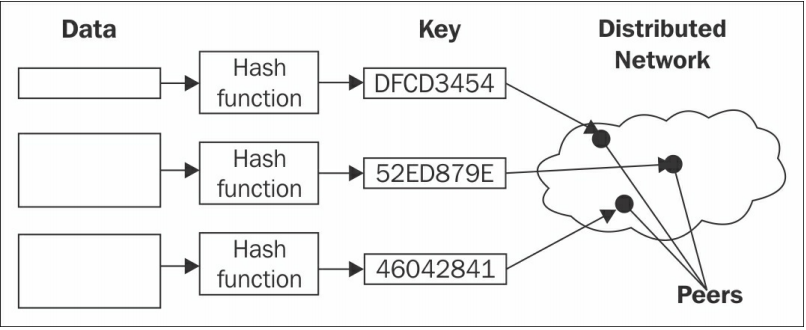
Cây Merkle-Patricia, dựa trên các định nghĩa của Patricia và Merkle, là một cây có nút gốc chứa giá trị băm của toàn bộ cấu trúc dữ liệu.

Bảng băm được phân phối (DHT)

Bảng băm là một cấu trúc dữ liệu được sử dụng để ánh xạ các khóa tới các giá trị. Bên trong, hàm băm được sử dụng để tính toán chỉ mục thành một nhóm các nhóm, từ đó có thể tìm thấy giá trị yêu cầu. Các thùng chứa các bản ghi được lưu trữ trong chúng bằng cách sử dụng khóa băm và được sắp xếp theo thứ tự cụ thể.

Với định nghĩa được cung cấp trước đó trong tâm trí, người ta có thể nghĩ về bảng băm được phân phối như một cấu trúc dữ liệu nơi dữ liệu được trải rộng trên các nút và nút khác nhau tương đương với các nhóm trong một peer-topeer vào mạng.

Sơ đồ dưới đây cho thấy DHT hoạt động như thế nào. Ví dụ cho thấy dữ liệu được truyền qua hàm băm, kết quả là tạo ra một khóa nhỏ gọn. Khóa này sau đó được liên kết với dữ liệu (giá trị) trên mạng ngang hàng. Khi người dùng trên mạng yêu cầu dữ liệu (thông qua tên tệp), tên tệp có thể được băm một lần nữa để tạo ra cùng một khóa và bất kỳ nút nào trên mạng sau đó có thể được yêu cầu để tìm dữ liệu tương ứng. DHT cung cấp sự phân cấp, khả năng chịu lỗi và khả năng mở rộng:



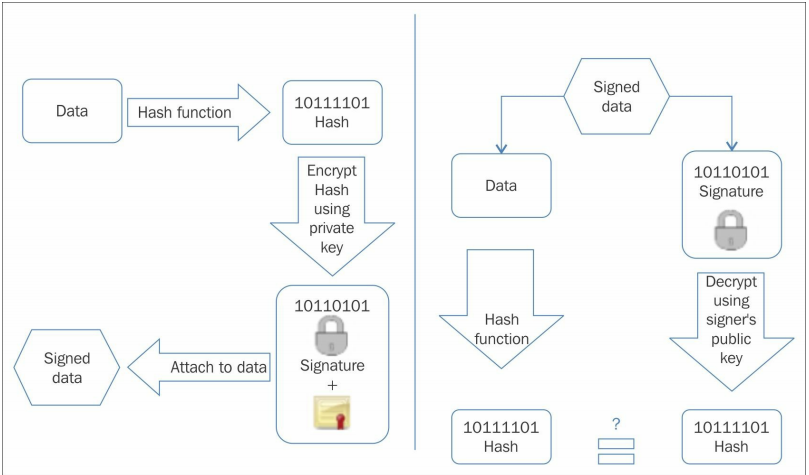
Chữ ký số

Chữ ký số cung cấp một phương tiện kết hợp một thông điệp với một thực thể mà từ đó thông điệp đã được bắt nguồn. Chữ ký số được sử dụng để cung cấp xác thực nguồn gốc dữ liệu và không có sự sai lệch. Chúng được tính theo hai bước. Các bước cấp cao của lược đồ chữ ký số RSA được đưa ra như sau:

1. Tính toán giá trị băm của gói dữ liệu. Điều này sẽ cung cấp sự đảm bảo tính toàn vẹn dữ liệu vì băm có thể được tính toán ở đầu của người nhận một lần nữa và được kết hợp với băm ban đầu để kiểm tra xem dữ liệu đã được sửa đổi trong quá trình chuyển. Về mặt kỹ thuật, việc ký thông báo có thể hoạt động mà không cần băm dữ liệu trước, nhưng không được coi là an toàn.

2. Bước thứ hai ký hiệu giá trị băm với khóa riêng của người ký. Vì chỉ có ca sĩ có khóa riêng, tính xác thực của chữ ký và dữ liệu đã ký được đảm bảo. Chữ ký số có một số thuộc tính quan trọng, chẳng hạn như tính xác thực, không xác định và không thể sử dụng. Tính xác thực có nghĩa là chữ ký số được xác minh bởi một bên nhận. Thuộc tính unforgeability đảm bảo rằng chỉ người gửi tin nhắn mới có thể sử dụng chức năng ký bằng cách sử dụng khóa riêng. Nói cách khác, không ai khác có thể sản xuất tin nhắn đã ký đã được người gửi hợp pháp tạo ra. Không sử dụng lại có nghĩa là chữ ký số không thể tách rời khỏi một tin nhắn và được sử dụng cho một thông điệp khác một lần nữa.

Hoạt động của chức năng chữ ký số chung được hiển thị trong sơ đồ sau:



Nếu người gửi muốn gửi thư đã được xác thực tới người nhận, có hai phương pháp có thể được sử dụng. Hai phương pháp tiếp cận này sử dụng chữ ký số với mã hóa được giới thiệu ở đây.

Đăng nhập rồi mã hóa

Trong phương pháp này, người gửi ký điện tử dữ liệu bằng cách sử dụng khóa riêng, nối chữ ký vào dữ liệu, sau đó mã hóa dữ liệu và chữ ký số bằng khóa công khai của người nhận. Đây được coi là một lược đồ an toàn hơn so với lược đồ mã hóa sau đó được mô tả tiếp theo.

Mã hóa ký hiệu sau đó

Trong phương pháp này, người gửi mã hóa dữ liệu bằng khóa công khai của người nhận và sau đó ký số hóa dữ liệu đã mã hóa.

**Thuật toán chữ ký số Elliptic Curve (ECDSA)**

Để ký và xác minh bằng cách sử dụng lược đồ ECDSA, cặp khóa đầu tiên cần được tạo:

1. Đầu tiên, xác định đường cong elip E:

1. Với modulus P.

2. Hệ số a và b.

3. Điểm phát A tạo thành một nhóm cyclic của bậc tự q.

2. Một số nguyên d được chọn ngẫu nhiên sao cho 0 <d <q.

3. Tính khóa công khai B sao cho B = d A.

Khóa công khai là sextuple của biểu mẫu được hiển thị ở đây:

Kpb = (p, a, b, q, A, B)

Khóa cá nhân được chọn ngẫu nhiên d trong Bước 2:

Kpr = d

Bây giờ chữ ký có thể được tạo ra bằng cách sử dụng khóa riêng và khóa công khai.

1. Đầu tiên, chọn một phím tạm thời Ke, trong đó 0 <Ke <q. Cần đảm bảo rằng Ke thật sự

ngẫu nhiên, và không có hai chữ ký nào có cùng khóa; nếu không, khóa riêng có thể được tính toán.

2. Một giá trị R khác được tính bằng cách sử dụng R = Kế A, nghĩa là nhân số A (điểm phát) và

chìa khóa tạm thời ngẫu nhiên.

3. Khởi tạo một biến r với giá trị tọa độ x của điểm R. r = xR.

4. Chữ ký có thể được tính như sau:

S = (h(m) + dr) mod q

Ở đây, m là thông điệp mà chữ ký được tính và h (m) là băm của thông báo

m.

Việc xác minh chữ ký được thực hiện bằng cách làm theo quy trình này.

1. Giá trị phụ trợ w được tính bằng w = s-1 mod q.

2. Giá trị phụ trợ u1 = w. h (m) mod q.

3. Giá trị phụ trợ u2 = w. r mod q.

4. Tính điểm P, P = u1A + u2B.

5. Việc xác minh được thực hiện như sau.

6. r, s được chấp nhận như là một chữ ký hợp lệ nếu x-phối hợp của điểm P tính trong Bước 4 có

cùng giá trị với tham số chữ ký r mod q.

đó là:

Xp = r mod q là chữ ký hợp lệ

Xp! = R mod q có nghĩa là chữ ký không hợp lệ

Các ví dụ thực tế khác nhau được hiển thị ở đây, trong đó cho thấy cách chữ ký số RSA có thể là được tạo, sử dụng và xác minh bằng OpenSSL.

**Thị trường và giao dịch tài chính**

Thị trường tài chính tồn tại để tạo thuận lợi cho việc chuyển tiền tiết kiệm từ người tiết kiệm cho nhà đầu tư. Trong một hệ thống kinh tế, có hai lĩnh vực, cụ thể là hộ gia đình và doanh nghiệp. Thị trường tài chính, cốt lõi của họ, hoạt động như một trung gian giữa những người tiết kiệm và các nhà đầu tư. Về cơ bản, có ba loại thị trường, cụ thể là thị trường tiền tệ, thị trường tín dụng và thị trường vốn. Thị trường tiền tệ là các thị trường ngắn hạn, nơi tiền được cho các công ty hoặc ngân hàng cho vay liên ngân hàng. Ngoại hối hoặc FX là một loại thị trường tiền tệ khác, nơi tiền tệ được giao dịch. Thị trường tín dụng bao gồm chủ yếu là các ngân hàng bán lẻ, nơi họ vay tiền từ các ngân hàng trung ương và cho vay các công ty hoặc hộ gia đình dưới hình thức thế chấp hoặc cho vay.

Thị trường vốn tạo thuận lợi cho việc mua và bán các công cụ tài chính, chủ yếu là cổ phiếu và trái phiếu. Thị trường vốn có thể được chia thành hai loại, thị trường sơ cấp và thứ cấp. Cổ phiếu do các công ty phát hành trực tiếp cho các nhà đầu tư trên thị trường sơ cấp, trong khi ở thị trường thứ cấp, các nhà đầu tư bán lại chứng khoán cho các nhà đầu tư thông qua sàn giao dịch chứng khoán. Các hệ thống giao dịch điện tử khác nhau được sử dụng bởi các sàn giao dịch để tạo thuận lợi cho việc giao dịch các công cụ tài chính.

**Thương mại**

Một thị trường là một nơi mà các thương nhân đến để giao dịch. Nó có thể cho các lớp tài sản. Giao dịch có thể được định nghĩa là hoạt động trong đó các nhà giao dịch mua hoặc bán các công cụ tài chính khác nhau để tạo ra lợi nhuận và rủi ro phòng hộ. Các nhà đầu tư, người vay, người thuê nhà, trao đổi tài sản, và con bạc là một vài loại thương nhân. Thương nhân có một vị trí ngắn khi họ nợ một cái gì đó, ví dụ, nếu họ đã bán một hợp đồng và có một vị trí lâu dài khi họ mua một hợp đồng. Có nhiều cách khác nhau để giao dịch, chẳng hạn như thông qua các nhà môi giới hoặc trực tiếp trên sàn giao dịch hoặc trên quầy. Môi giới là đại lý thu xếp giao dịch cho khách hàng của họ. Người môi giới hành động thay mặt khách hàng để đối phó với một mức giá nhất định hoặc với mức giá tốt nhất có thể.

**Trao đổi**

Trao đổi thường được coi là một nơi rất an toàn, quy định và đáng tin cậy cho giao dịch. Gần đây, giao dịch điện tử đã trở nên phổ biến hơn so với giao dịch sàn truyền thống. Bây giờ các nhà giao dịch gửi đơn đặt hàng đến một danh sách đặt hàng điện tử trung tâm, từ đó các đơn đặt hàng, giá và các thuộc tính liên quan được xuất bản cho tất cả các hệ thống liên quan bằng cách sử dụng các mạng truyền thông, về bản chất, tạo ra một thị trường ảo. Các giao dịch trao đổi chỉ có thể được thực hiện bởi các thành viên của sàn giao dịch. Để giao dịch mà không có những hạn chế này, các bên truy cập có thể tham gia giao dịch OTC (Over the Counter) trực tiếp.

**Vòng đời thương mại**

Một vòng đời thương mại tổng quát bao gồm các giai đoạn khác nhau từ vị trí đặt hàng đến thực hiện và sau đó giải quyết. Vòng đời này được mô tả từng bước như sau:

- Thực hiện trước: Lệnh được đặt ở giai đoạn này.

- Thực hiện và đặt phòng: Khi lệnh khớp và được thực hiện, lệnh chuyển đổi thành giao dịch. Ở giai đoạn này, hợp đồng giữa các bên đối tác đã đáo hạn.

- Xác nhận: Đây là nơi cả hai bên đối tác đồng ý với các chi tiết cụ thể của giao dịch.

- Đặt chỗ sau: Giai đoạn này liên quan đến các quy trình kiểm tra và xác minh khác nhau để xác định tính chính xác của giao dịch.

- Giải quyết: Đây là phần quan trọng nhất trong quá trình thương mại và ở giai đoạn này, giao dịch là cuối cùng.

- Qua đêm (xử lý cuối ngày): Các quy trình kết thúc ngày bao gồm tạo báo cáo, tính toán lợi nhuận và thua lỗ và các tính toán rủi ro khác nhau.

Trong tất cả các quy trình được đề cập, nhiều người và chức năng kinh doanh có liên quan. Thông thường, các chức năng này được chia thành các chức năng như văn phòng phía trước, văn phòng trung gian và văn phòng.

**Đặt hàng dự đoán**

Các nhà dự đoán đặt hàng cố gắng kiếm lời trước khi các nhà giao dịch khác có thể thực hiện giao dịch. Điều này được dựa trên dự đoán, nơi một nhà kinh doanh biết cách hoạt động giao dịch của các giao dịch khác sẽ ảnh hưởng đến giá.

Những người đi trước, các nhà giao dịch kỹ thuật theo định hướng tình cảm, và các nhíp là một số ví dụ về những người dự đoán thứ tự.

**Thao túng thị trường**

Thao tác thị trường là bất hợp pháp ở Anh và các nước khác. Các nhà giao dịch gian lận có thể lây lan thông tin sai lệch trên thị trường, điều này có thể dẫn đến biến động giá khiến lợi nhuận bất hợp pháp. Thông thường, hành vi thao túng thị trường dựa trên thương mại và nó bao gồm các thao tác tổng quát và thời gian cụ thể. Các hành động có thể tạo ra sự thiếu hụt nhân tạo về chứng khoán, ấn tượng về hoạt động sai và thao túng giá để có được lợi ích tội phạm được bao gồm trong danh mục này. Cả hai điều khoản được thảo luận trước đó đều liên quan đến tội phạm tài chính. và có khả năng phát triển các hệ thống dựa trên blockchain có thể cản trở sự lạm dụng thị trường.