**Chương 4**

**Lý thuyết về tiền: Từ cổ đại Đồng tiền Nhật Bản sang tiền ảo Tiền tệ**

Hiện tại, các loại tiền ảo đang là mục tiêu của các hoạt động đầu cơ và chịu nhiều vấn đề khác. Tuy nhiên, nếu một loại tiền ảo lý tưởng có thể trở thành hiện thực, nó được mong đợi rằng nó sẽ bổ sung một khía cạnh hoàn toàn mới cho các hoạt động kinh tế của chúng ta.

Tiền ảo rất giống với tiền gửi tiền ở chỗ dữ liệu được sử dụng như tiền.

Trong khi tiền gửi tiền được kiểm soát tập trung bởi các ngân hàng và các tổ chức tài chính khác

tiền ảo, tiền ảo được duy trì một cách phi tập trung bởi nhiều người. Thông qua phi tập trung, có thể tiết kiệm chi phí đáng kể.

Để đánh giá tiềm năng của các loại tiền ảo, cần hiểu một loại tiền tệ trái ngược với tiền, cái gì phân chia tiền giấy với tiền gửi tiền, và điều gì ngăn cách giữa tiền ảo và tiền gửi. Chương này bao gồm những vấn đề bằng cách đưa ra một lý thuyết mới về tiền

**1 Lịch sử của tiền: Từ tiền hàng hóa đến tiền ảo**

Để hiểu những đổi mới mà tiền ảo đã mang lại và được mong đợi để mang lại cho xã hội của chúng ta, chúng tôi mong muốn nghiên cứu các loại tiền tệ khác nhau đã được sử dụng trong quá khứ và hiện tại và so sánh chúng với các loại tiền ảo.

**1.2.1 Gold Standard (Dùng vàng làm đơn vị tiên tệ để trao đổi)**

Cho đến giữa những năm 1930, ở Hoa Kỳ, chính phủ đã đảm bảo việc chuyển đổi của các hóa đơn đô la cho vàng, được gọi là hệ thống tiền tệ có thể chuyển đổi. Ngay lập tức sau khi độc lập, theo Đạo luật tiền đúc năm 1792, đồng 10 đô la được định nghĩa hợp pháp để chứa 16,04 gam vàng nguyên chất (nói cách khác, 1 troy ounce vàng = 19,319 đô la).

Sau đó, lượng vàng đã giảm xuống còn 15,05 gam dưới Đạo luật tiền đúc năm 1837 (1 troy ounce vàng = 20,67 đô la). Sau đó, vào năm 1900, Đạo luật Tiêu chuẩn Vàng đã được thông qua đặt vàng làm tiêu chuẩn duy nhất để mua lại tiền giấy. Tỷ lệ chuyển đổi này được giữ cho đến năm 1933.

Vào giữa thế kỷ 19, đã có lúc các chính quyền tiểu bang, các thành phố, ngân hàng thương mại và các công ty khác nhau đã phát hành các tờ đô la chuyển đổi đối với vàng và trái phiếu chính phủ. Theo một hệ thống như vậy, khi một ngân hàng gặp khó khăn về tài chính, nhiều người yêu cầu rút tiền gửi cùng một lúc. Ngân hàng sẽ phá sản vì không ngân hàng nào có thể đáp ứng nhu cầu lớn về rút tiền. Điều đó đã kích hoạt nhu cầu rút tiền đối với các ngân hàng khác, điều này đã làm đình trệ hệ thống tiền tệ nói chung. Hiện tượng này được gọi là “chạy ngân hàng”.

Để giải quyết vấn đề này, Hoa Kỳ đã thông qua Đạo luật Dự trữ Liên bang năm 1913. Theo đạo luật này, Ngân hàng Dự trữ Liên bang được chỉ định là ngân hàng phát hành tiền được gọi là Ghi chú Dự trữ Liên bang. Ghi chú Dự trữ Liên bang dần dần thay thế các tiền giấy do chính phủ và các ngân hàng thương mại phát hành. Trong thời gian này liên tục, 1 troy ounce vàng được cố định ở mức 20,67 đô la.

Sự sụp đổ của Sở giao dịch chứng khoán New York vào năm 1929 đã gây ra một số

doanh nghiệp phá sản và 744 ngân hàng thất bại chỉ trong 10 tháng đầu năm. Sau đó,

cuộc khủng hoảng kéo dài, và kinh tế trì trệ tiếp tục cho đến năm 1945, khi Thế giới

Chiến tranh thứ hai kết thúc. Đây là thời kỳ được gọi là thời kỳ Đại suy thoái.

Năm 1932, Ủy ban Pecora, do Ferdinand Pecora lãnh đạo, được thành lập tại Senate để điều tra nguyên nhân của cuộc Đại suy thoái. Thông qua Ủy ban điều tra, đã phát hiện ra rằng trong thời kỳ Đại suy thoái, nhiều vụ chuyển đổi mờ ám đã được tiến hành. Một trong những nguyên nhân chính của cuộc Đại suy thoái là do vận hành 1 cách máy móc như phân bổ lại các khoản lỗ đã được thực hiện giữa các ngân hàng và các công ty con chứng khoán và giữa các công ty chứng khoán với các công ty con ngân hàng của họ.

**1.2.2 Hệ thống tiền Fiat**

Trong nửa đầu những năm 1930, nhiều cải cách thể chế khác nhau của thị trường tài chính

diễn ra để đối phó với cuộc Đại suy thoái. Đặc biệt quan trọng là:

1. Bãi bỏ chế độ Gold Standard

2. Thành lập Tổng công ty Bảo hiểm Tiền gửi Liên bang

3. Tách công ty chứng khoán và ngân hàng thương mại

4. Giới thiệu hệ thống công bố thông tin về thị trường chứng khoán

Những cải cách này nhằm đảm bảo sự ổn định của hệ thống ngân hàng và tăng tính minh bạch của thị trường tài chính nói chung. Ngày nay, tất cả các nước phát triển đã áp dụng cùng một hệ thống tài chính. Sau đó, ba cải cách đầu tiên được giải thích và những điều này liên quan trực tiếp đến hệ thống tiền tệ dựa trên fiat tiền bạc.

**Bãi bỏ Gold Standard** : Sự suy giảm sức khỏe kinh tế của một quốc gia khiến quốc gia này khó duy trì chế độ bản vị vàng. Tại Hoa Kỳ năm 1934, Hầu hết việc sở hữu vàng của tư nhân đã bị cấm bởi Đạo luật Dự trữ Vàng năm 1934; tất cả các cá nhân sở hữu vàng được yêu cầu bán nó cho Bộ Ngân khố. Đạo luật đã phá giá đồng đô la so với vàng, thay đổi 20,67 đô la mỗi ounce troy thành 35 đô la.

**Thành lập Tổng công ty Bảo hiểm Tiền gửi Liên bang** : Khi một cuộc “chạy ngân hàng” xảy ra, như đã thảo luận ở trên, rất khó để ngân hàng nắm giữ đủ tiền mặt để chi trả mọi nhu cầu rút tiền. Nếu các ngân hàng có thể bảo hiểm trước rủi ro như vậy, hệ thống ngân hàng sẽ trở nên ổn định hơn. Với sự cân nhắc như vậy, vào năm 1933, Công ty Cổ phần Bảo hiểm Tiền gửi Liên bang (FDIC) được thành lập. Đối với các ngân hàng là thành viên của FDIC, một khoản tiền gửi nhất định của khách hàng đã được bảo hiểm bằng bảo hiểm trong trường hợp phá sản ngân hàng.

**Tách công ty chứng khoán và ngân hàng thương mại** : Đạo luật Glass – Steagall được thành lập vào năm 1933, tách biệt các hoạt động của chứng khoán các công ty và ngân hàng thương mại. Chứng khoán có thể được coi là chứng chỉ người phát hành hứa hẹn sẽ trả cho các khoản thu nhập trong tương lai. Bán chứng khoán ngụ ý rằng mục đích là đầu tư vào hoạt động kinh doanh của tổ chức phát hành. Công ty chứng khoán là trung gian tạo điều kiện thuận lợi cho việc phát hành và bán lại chứng khoán. Ngân hàng thương mại cung cấp dịch vụ dàn xếp giải quyết để tạo điều kiện thanh toán giữa các chủ tài khoản. Ở dưới Đạo luật Glass – Steagall, các ngân hàng thương mại dành riêng cho việc dàn xếp dàn xếp, và các công ty chứng khoán tập trung vào trung gian đầu tư

***1.3 Tiền tệ Sổ cái***

Ngày nay, các bản ghi trên tài khoản ngân hàng được lưu giữ dưới dạng dữ liệu kỹ thuật số. Như tiền gửi ngân hàng cho thấy, hồ sơ thanh toán trên tài khoản ngân hàng có thể đóng vai trò của một loại tiền tệ, được gọi là tiền gửi. Các loại tiền ảo trên blockchain cũng hồ sơ các giao dịch dưới dạng dữ liệu số. Như điều này cho thấy, dữ liệu giao dịch kỹ thuật số có thể được sử dụng như một đơn vị tiền tệ nếu hồ sơ chính xác và không thể bị giả mạo.

**Sổ cái** là một “cuốn sổ ghi chép vĩnh viễn”. Có thể an toàn khi cho rằng "vĩnh viễn" trong định nghĩa này bao hàm cả “chính xác” và “không thể xác minh”. Vì cả ký gửi và tiền ảo được lưu giữ dưới dạng sổ cái, chúng có thể được gọi là sổ cái tiền tệ.

**1.3.1 Tiền gửi : Tiền tệ dữ liệu tập trung**

Các ví dụ quen thuộc nhất về tiền tệ gửi tiền là tài khoản séc ở Hoa Kỳ. Thay vì viết séc, ngày nay, nhiều người sử dụng chuyển khoản điện tử bằng cách mà tiền có thể được chuyển trực tuyến với chi phí rất thấp. Tiền gửi đã bắt đầu thay đổi cuộc sống hàng ngày của chúng ta vào cuối những năm 1970 đến đầu những năm 1980. Trong giai đoạn này, tiền lương bắt đầu được gửi trực tiếp vào tài khoản của người lao động, trong khi trước đó, mọi người đã được trả bằng séc và tiền mặt.

Về mặt lý thuyết, một ngân hàng có thể cung cấp một loại tiền gửi cho khách hàng của mình bằng cách theo dõi tất cả các giao dịch từ tài khoản này sang tài khoản khác và đảm bảo rằng một khoản thanh toán từ một tài khoản tại một thời điểm cụ thể không vượt quá số dư tại thời điểm đó. Các giao dịch được sắp xếp theo thời gian. Sau khi bản ghi đó được tạo, nó dễ dàng trích xuất các giao dịch có liên quan đến một tài khoản cụ thể.

Tiền mặt là một IOU quy định xã hội nợ người nắm giữ tiền mặt (năng lực mua hàng bằng giá trị của IOU). Một khoản tiền gửi trong tài khoản ngân hàng là IOU của ngân hàng để

chủ tài khoản. Do đó, không có gì ngạc nhiên khi tiền gửi ngân hàng đóng vai trò như một loại tiền tệ ở mức độ mà IOU của ngân hàng được các chủ tài khoản tin cậy.

Hiện tại, tiền gửi hoàn toàn bổ sung thêm cho tiền giấy. Nói cách khác, hệ thống tài khoản tiền gửi ngân hàng có chức năng là tiền vì khách hàng tin tưởng ngân hàng trả lại tiền mặt bất cứ khi nào họ yêu cầu rút tiền.

**1.3.2 Tiền ảo: Tiền tệ có sổ cái phi tập trung**

Tiền ảo là một loại tiền tệ sổ cái mới, trong đó sự tin tưởng được đảm bảo bởi cơ chế hoàn toàn khác với tiền gửi. Tiền gửi, là một loại tiền tệ có sổ cái truyền thống, được quản lý tập trung bởi ngân hàng. Nhiều công nhân nỗ lực duy trì tính toàn vẹn của hồ sơ giao dịch, điều này tạo ra tin tưởng vào những hồ sơ đó. Ngược lại, tiền ảo duy trì tính toàn vẹn của dữ liệu bằng cách một thuật toán máy tính liên quan đến nhiều người theo cách phi tập trung tạo ra hồ sơ giao dịch. Tính toàn vẹn của dữ liệu không được duy trì bởi một cơ quan cũng không phải là một cá nhân đơn lẻ mà là một thuật toán cùng với nhiều người xử lý dữ liệu một cách độc lập thông qua thuật toán.

Cái khó trên Internet là làm thế nào để liên kết tài khoản này với tài khoản khác, làm thế nào để giữ hồ sơ thanh toán / nhận giữa các tài khoản, cách đảm bảo tính chính xác và cách để tạo một sổ cái sẽ không bao giờ bị giả mạo. Công nghệ chuỗi khối, công nghệ mà nhiều loại tiền ảo dựa trên, là công nghệ đầu tiên cho thấy những khó khăn này có thể được khắc phục trên Internet một cách hoàn toàn mở và phi tập trung

**2 Tiền và chức năng của nó**

Tiền có vai trò gì trong nền kinh tế? Điều quan trọng là phải giải quyết câu hỏi này trước khi bàn về vai trò của tiền ảo. Tiền có ba chức năng cơ bản: đo lường giá trị, phương tiện trao đổi và lưu trữ giá trị.

Giao dịch là một hoạt động nhằm thiết lập các điều kiện cho một cuộc trao đổi và sau đó thực hiện trao đổi. Để thực hiện một cuộc trao đổi, cần phải đánh giá xem giá trị của một hàng hóa cụ thể. Để đánh giá như vậy, một thang giá trị là cần thiết để hàng hóa có thể được đo lường. Điều cần thiết là một thang điểm phải cho phép bốn các phép toán cộng, trừ, nhân, chia số học; không có khả năng này, không có hai hàng hóa nào có thể được đo lường với nhau.

Là một vật lưu trữ giá trị, tiền bạc cho phép chủ nhân tiết kiệm sức mua cho đến khi cần

mua hàng hóa và dịch vụ. Đây là một chức năng mà một phương tiện trao đổi phải có để sửa chữa sự lệch lạc của các cơ hội giao dịch. Một vật liệu đó là rất dễ hỏng, chẳng hạn như kem, không bao giờ có thể được coi là phương tiện trao đổi.

Để sử dụng một hàng hóa cụ thể như tiền, nó phải có cả ba chức năng của tiền. Vì kim cương được mọi người muốn có và không bị phân hủy, chúng rất tốt cho một phương tiện trao đổi và một kho lưu trữ giá trị. Tuy nhiên, kim cương không phù hợp với bốn các phép tính toán học. Nếu một viên kim cương được chia thành hai mảnh, giá trị của nó sẽ giảm đáng kể. Các mảnh đã chia không thể ghép lại với nhau. Điều này nghĩa là rằng kim cương không phù hợp với tư cách là một thang đo giá trị. Các chất phóng xạ như uranium có thể tốt cho thang giá trị và lưu trữ giá trị. Tuy nhiên, quá nguy hiểm nếu mang theo từng phần nhỏ, điều này ngụ ý rằng uranium không thể phục vụ như một phương tiện trao đổi. Sắt rất tốt cho một thang giá trị và một phương tiện trao đổi. Tuy nhiên, sắt gỉ quá nhanh để trở thành một lưu trữ giá trị so với đồng, điều này giải thích tại sao, về mặt lịch sử, đồng tiền xu đã phổ biến hơn tiền sắt.

**3 Chi phí giao dịch và tiền**

Lịch sử cho thấy rằng một loại tiền mới đã và ngay bây giờ, được giới thiệu khi có thể tiết kiệm chi phí giao dịch hiện tại bằng cách tăng cường niềm tin vào tiền. Cái này có đã góp phần tạo ra một nền kinh tế có chất lượng kinh tế thị trường cao hơn. Trong phần này, tôi sẽ xem xét quá trình này.

***3.1 Tiền hàng hóa***

Chất liệu nào tốt cho tiền? Câu trả lời đầu tiên xuất hiện trong đầu thật quý giá kim loại như vàng và bạc. Bởi vì mọi người đều muốn những kim loại quý này và có thể mang chúng theo từng phần nhỏ, nó hoàn hảo như một phương tiện trao đổi. Bởi vì những kim loại quý đó không dễ bị mất giá trị, chúng rất tốt cho việc lưu trữ giá trị. Hơn nữa, những kim loại này có thể dễ dàng bị chia thành các mảnh nhỏ và nấu chảy thành một đoạn lớn. Điều này ngụ ý rằng chúng tốt cho bốn phép tính số học.

Một vấn đề của những kim loại quý này là chúng quá quý. Điều này nghĩa là rằng chúng không thích hợp cho các giao dịch nhỏ. Đồng là kim loại phù hợp hơn cho các giao dịch nhỏ. Bởi vì đồng không bị gỉ nhanh như sắt, đồng xu đã được sử dụng rộng rãi trong nhiều thế kỷ. Ngoài ra, đồng đã được sử dụng hàng ngày cho các công cụ và đồ trang trí.

Trước đây, hàng hóa thực tế như lụa, lúa mạch hoặc gạo được sử dụng như một phương tiện trao đổi. Mặc dù chúng mỏng manh hơn nhiều so với kim loại quý, nhưng có thể chúng dễ chấp nhận hơn đối với nhiều nhà giao dịch bình thường như một phương tiện trao đổi trong thế giới mà vàng, bạc và đồng không có sẵn.

***3.2 Tiền tệ và chi phí giao dịch***

Không giống như tiền hàng hóa, có những loại tiền mà giá trị của nó không trực tiếp liên quan đến việc sử dụng hàng hóa. Đó là tiền tệ. Cho dù đó là tiền giấy hay sổ cái tiền tệ, giá trị của nó bắt nguồn từ việc chúng được mọi người chấp nhận như tiền. Nói cách khác, một loại tiền tệ đóng vai trò tiền tệ được hỗ trợ bởi sự tin tưởng của mọi người. Như đã thảo luận ở trên, cách niềm tin vào tiền tệ được tạo ra khác nhau giữa tiền giấy, tiền gửi và tiền ảo. Tiền giấy được đảm bảo bởi một chính sách tiền tệ của chính phủ, tiền tệ tiền gửi được hỗ trợ bởi hoạt động của ngân hàng và tiền ảo được hỗ trợ bởi các thuật toán phi tập trung.

Việc chuyển từ tiền hàng hóa sang tiền tệ có thể được giải thích bằng việc giảm chi phí giao dịch liên quan đến việc sử dụng tiền hàng hóa. Nếu gạo hoặc lụa được sử dụng như một phương tiện trao đổi, chất lượng của nó như một loại hàng hóa có thể bị giảm giá trị một cách dễ dàng; gạo có thể không ăn được; lụa có thể bị mòn. Giá trị của vàng và bạc không xấu đi một cách dễ dàng. Tuy nhiên, chúng quá quý đối với các giao dịch nhỏ và có thể trở thành mục tiêu dễ dàng của bọn cướp.

Điều này giải thích tại sao tiền giấy được phát minh ngay sau khi trở thành một tiêu chuẩn kim loại quý được thành lập. Tiền gửi tiền đã được thông qua để tiết kiệm chi phí xử lý tiền mặt.

Như điều này cho thấy, một loại tiền tệ đã được phát triển để tiết kiệm chi phí giao dịch. Trong nói cách khác, việc lựa chọn 1 loại tiền tệ được xác định bằng cách so sánh chi phí giao dịch giữa tiền hiện có và một loại tiền thay thế có thể được phát triển mới.

***3.3 Tiền tệ Sổ cái và Chi phí Giao dịch***

Chi phí duy trì một loại tiền gửi là khá cao. Điều này có thể dễ dàng được hiểu khi nghĩ về số lượng ngân hàng, chi nhánh của họ và những người làm việc ở đó. Nhiều người hào hứng với tiền ảo vì họ mong đợi tiền ảo để tiết kiệm đáng kể chi phí đó. Điều này có thể được giải thích bằng cách so sánh bách khoa toàn thư truyền thống và Wikipedia.

Trước đây, nhiều gia đình có một bộ bách khoa toàn thư, trong đó các chuyên gia giải thích các chủ đề tương ứng của họ, bao gồm các hiện tượng xã hội, sự kiện lịch sử và hiểu biết khoa học. Quá trình ghép một bộ bách khoa toàn thư lại với nhau có thể được gọi là “xử lý tri thức tập trung”giống như tính toán mạng tập trung. Bài xã luận hội đồng quản trị bách khoa toàn thư chịu trách nhiệm kiểm soát tập trung việc lựa chọn tác giả cho mọi chủ đề. Mặc dù tất cả các chủ đề được giải thích bởi các chuyên gia, chúng được kiểm tra bởi ban biên tập, ban biên tập có trách nhiệm đảm bảo rằng tất cả các giải thích là đúng đắn và đáng tin cậy. Nói cách khác, ban biên tập hoạt động như thể máy chủ trung tâm của một mạng tập trung.

Ngược lại, Wikipedia dựa trên “xử lý kiến ​​thức phi tập trung”. Mỗi bài viết trên Wikipedia được viết bởi một chuyên gia hoặc nhiều chuyên gia. Tuy nhiên, không có thẩm quyền tồn tại những người đáng tin cậy để kiểm tra xem các bài báo có đúng hay không. Thay vào đó, tất cả người dùng kiểm tra các bài báo, bổ sung giải thích, nếu cần, và sửa lỗi nếu có.

Quá trình xử lý kiến ​​thức phi tập trung được Wikipedia giới thiệu có một điểm trở ngại. Đôi khi, chúng tôi thấy một số lỗi trong phần giải thích vì không có cơ quan đáng tin cậy kiểm tra các bài báo. Một số giải thích là quá kỹ thuật cho những người bình thường để hiểu.

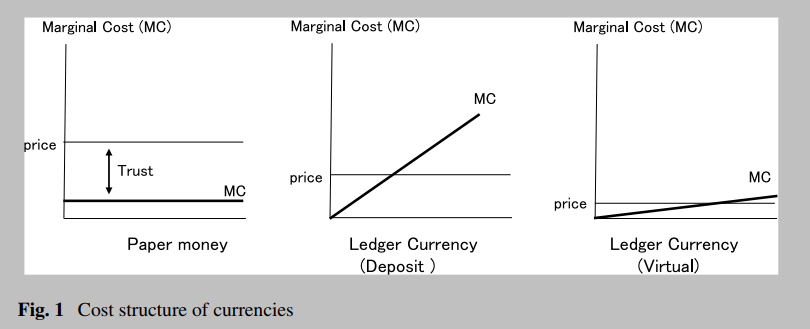
Điểm mạnh của Wikipedia là tận dụng lòng vị tha của con người hoặc sự thôi thúc chia sẻ thông tin chính xác để xây dựng một cái gì đó có ích cho xã hội. Nếu bạn có tư duy thiện chia sẻ thông tin chính xác với xã hội và bạn tự tin vào chuyên môn, bạn sẽ bị cám dỗ để viết một bài báo cho Wikipedia. Nó yêu cầu nỗ lực đáng kể để một người viết một bài báo mà người bình thường có thể hiểu được. Nếu bạn viết một bài báo giả mạo, người khác sẽ sớm phát hiện ra và viết lại nó. Điều này giảm thiểu khuyến khích đóng góp thông tin sai và / hoặc không chính xác.

Nói tóm lại, Wikipedia đã tận dụng hiệu quả sự thôi thúc của con người để giải thích và chia sẻ hiểu biết. Nhờ cơ chế này, nó đã thành công trong việc tạo ra một bách khoa toàn thư với một nội dung khổng lồ với chi phí rất nhỏ.

Theo nhiều khía cạnh, blockchain tương tự như Wikipedia. Nó không sử dụng tập trung

hệ thống quản lý. Ngoại trừ thiết lập giao thức tối thiểu, không có tập trung kiểm soát và đánh giá thông tin được phân cấp và để lại cho một số lượng lớn của những người tham gia ẩn danh. Nó tối đa hóa sự sẵn lòng của những người có thiện chí để tạo hồ sơ chính xác và phân quyền bảo vệ chống lại các cuộc tấn công độc hại. Thông qua thiết kế như vậy, tiền ảo cung cấp tiền với chi phí thấp hơn so với hệ thống tiền tệ tiền gửi tập trung.

***3.4 Cơ cấu chi phí của các đơn vị tiền tệ khác nhau***



Hình [1](https://translate.googleusercontent.com/translate_f#79) minh họa sự khác biệt giữa tiền giấy và tiền tệ trên sổ cái và giữa tiền gửi và tiền ảo. Đối với mỗi ô, trục tung thể hiện giá của tiền. Giá của tiền được biểu thị bằng lãi suất danh nghĩa.

Bảng điều khiển ngoài cùng bên trái giải thích chi phí (chi phí cận biên) của tiền giấy liên quan đến giá của nó. Chi phí in hóa đơn có thể được cho là không đáng kể. Dù cho như thế nào nhiều hóa đơn đô la được in, chi phí in thêm một hóa đơn có thể được giả định không đổi. Giá tiền giấy được xác định ở mức cao hơn nhiều so với chi phí biên.

Ở giữa và ngoài cùng bên phải của Hình [1](https://translate.googleusercontent.com/translate_f#79), đường chi phí cận biên để tạo ra sổ cái tiền tệ là một đường dốc lên. Điều này là do chi phí bổ sung của tăng cung tiền tệ, bằng tiền gửi hoặc tiền ảo, trở nên lớn hơn khi nguồn cung tăng lên. Tuy nhiên, như đã lưu ý ở trên, có thể giả định rằng chi phí của tạo ra một loại tiền ảo nhỏ hơn nhiều.

Trong những trường hợp đơn giản này, người ta biết rằng đường chi phí cận biên và đường cung là giống hệt nhau. Do đó, như được hiển thị trong bảng giữa và bên phải, nguồn cung cấp của một đơn vị tiền tệ trên sổ cái được xác định tại điểm giao nhau giữa giá của một loại tiền tệ và đường chi phí cận biên. Ngược lại, như bảng điều khiển bên trái của hình cho thấy, trong trường hợp tiền giấy, việc cung cấp tiền tệ được xác định bởi chính phủ chính sách tiền tệ; không có mối quan hệ giữa đơn giá tiền và đường chi phí cận biên.

**Chương 5**

**Ethereum, Hợp đồng thông minh, DApps**

**2 Ethereum**

Vitalik Buterin bắt đầu quan tâm đến Bitcoin dưới sự khuyến khích của cha mình. Sau

nghiên cứu về Bitcoin, anh ấy bắt đầu viết các bài báo để đổi lấy tiền điện tử và đã bắt đầu *Tạp chí Bitcoin* với một đồng nghiệp khác. Cuối cùng anh ấy đã có được sự tiết lộ rằng nền tảng có thể trở nên rất mạnh mẽ bằng cách được tổng quát hóa ngoài mức đơn giản trao đổi tiền tệ thành thứ gì đó có thể thực hiện *bất kỳ* loại xử lý nào.

Có thể dễ dàng nghĩ về Bitcoin như một mạng máy tính thay thế ngân hàng của bạn.

Nhưng sẽ phức tạp hơn một chút để tưởng tượng việc thêm quá trình xử lý phức tạp vào Bitcoin có thể như thế nào hữu ích. Vì vậy, hãy để chúng tôi tiếp cận nó từ một góc độ ngược lại và tưởng tượng ngân hàng của bạn như một loại máy tính. Nó có ba hướng dẫn: gửi tiền vào tài khoản của tôi, tiền rút từ tài khoản của tôi, gửi tiền từ tài khoản của tôi sang tài khoản khác.

Bây giờ, hãy tưởng tượng nếu bạn có thể cung cấp cho ngân hàng của mình các hướng dẫn đặc biệt để hoàn thành mục tiêu tiết kiệm: “trong năm tới, chỉ cho phép tôi rút tối đa 100 đô la mỗi

tuần." Hoặc giả sử bạn muốn tạo một tài khoản dùng chung cho doanh nghiệp khởi nghiệp của mình trong đó Giám đốc điều hành có toàn quyền kiểm soát nhưng muốn có thêm mức độ trách nhiệm đối với các sĩ quan khác. “Tạo một tài khoản với ba chủ sở hữu. Alice có thể rút càng nhiều càng tốt cô ấy muốn bất cứ lúc nào nhưng Bob và Charles chỉ có thể rút tiền nếu một trong những người khác cũng chấp thuận. ”

Bạn thậm chí có thể tự động hóa việc phân phối tiền thu được từ doanh nghiệp của mình "mọi

khi 20 đô la trở lên được gửi vào tài khoản, đưa 5 đô la mỗi người cho Alice, Bob và

Charles, và chia đều phần còn lại cho tất cả các tài khoản khác trên một tài khoản đặc biệt

danh sách." Mỗi tài khoản đó có thể có các hướng dẫn đặc biệt riêng! Có thể là Bob

muốn tất cả các khoản tiền được chuyển trực tiếp đến tổ chức từ thiện yêu thích của mình.

Đây là những ví dụ đơn giản nhưng sẽ rất khó đạt được

với một ngân hàng thực tế vì số lượng con người và các quy trình liên quan; họ

không được trang bị để cung cấp mức độ tùy chỉnh đó. Nó sẽ liên quan đến quyền lực của

luật sư với người mà bạn thực sự tin tưởng, một loạt các hợp đồng pháp lý phức tạp và

sổ sách kế toán độc lập, hoặc tất cả những điều trên. Với một vài dòng phần mềm, những

các ví dụ có thể được tạo và mô hình được nhân rộng cho bất kỳ ai khác muốn

đạt được cùng một kết quả.

Rất có thể Bitcoin có thể phát triển thành chiếc máy tính vô hạn này. Sự phát triển-

Tuy nhiên, những người mà Buterin đang làm việc với họ không tiếp thu ý tưởng tuyệt vời này

vì vậy anh quyết định tự mình bắt tay vào thực hiện dự án. Do đó, Ethereum đã được hình thành

vào khoảng năm 2014 và ra mắt vào năm 2015 để mở rộng khái niệm về Bitcoin. Ethereum có

tiền tệ của riêng nó là Ether (ETH), giống như Bitcoin (BTC), nhưng nền tảng này có thể chạy bất kỳ

tập hợp các hướng dẫn, không chỉ là “gửi và nhận Bitcoin (Hacket [2016](https://translate.googleusercontent.com/translate_f#103)). ”

***2.1 Hợp đồng thông minh***

Trở lại năm 1994, Nick Szabo, một nhà khoa học máy tính và học giả pháp lý, đã tạo ra thuật ngữ

“Hợp đồng thông minh” và định nghĩa nó là: “Hợp đồng thông minh là giao thức giao dịch được vi tính hóa thực thi các điều khoản của hợp đồng (Szabo [1994](https://translate.googleusercontent.com/translate_f#103)). ” Anh ấy đã hình dung ra một cách mang lại hiệu quả cho các thỏa thuận bằng văn bản theo cách thực thi chúng một cách tự động. Hãy nghĩ về một máy bán hàng tự động. Không có nhân viên cửa hàng, nó thực thi hợp đồng bán hàng đồ uống với giá được quảng cáo cho khách hàng đã nạp đủ số lượng tiền vào máy.

The Turing-complete (Cộng tác viên của Wikipedia [2019](https://translate.googleusercontent.com/translate_f#103)) động cơ máy tính được cung cấp

bởi Ethereum là giao thức giao dịch máy tính đầu tiên thực hiện nhiều những thứ mà Szabo đã hình dung trong các bài viết trước đây của mình. Các chương trình máy tính chạy trên nền tảng Ethereum được gọi là hợp đồng thông minh. Họ có thể thực thi *một số các loại* thỏa thuận giữa các bên, giống như một máy bán hàng tự động, nhưng chúng không có thực chất là quan hệ trực tiếp với hợp đồng pháp lý. Hợp đồng thông minh Ethereum trở nên phổ biến đến nỗi phiên bản Ethereum của hợp đồng thông minh đã làm lu mờ sử dụng ban đầu của thuật ngữ và thêm nhiều nhầm lẫn về những gì blockchain có thể làm.

Tại sao nó là một "hợp đồng"? Ý tưởng ban đầu là nó tạo thành một số loại thỏa thuận giữa các bên. Tại sao nó "thông minh"? Ý tưởng ban đầu là nó có thể tự thi hành mà không cần luật sư hoặc những người có liên quan. Vì vậy, một hợp đồng thông minh thực sự là gì? Kể từ khi Ethereum tự tuyên bố là “một nền tảng phi tập trung chạy các hợp đồng thông minh, ”nó thực sự chỉ đề cập đến một loại chương trình phần mềm đặc biệt. Nó có thể có hoặc không có ý nghĩa pháp lý và vẫn cần một khung pháp lý truyền thống xung quanh nó nếu nó cần được sử dụng như một phần của giao dịch hợp pháp. Ví dụ, nếu bạn viết hợp đồng thông minh để chứng khoán hóa bất động sản, phân chia quyền sở hữu một tài sản thành các mã thông báo ảo, bạn vẫn cần các hợp đồng pháp lý truyền thống (trong trường hợp thích hợp khu vực pháp lý) để ràng buộc các mã thông báo hợp đồng thông minh đó với tài sản thực tế.

***3.2 Tiền xu, Mã thông báo và DApps***

Các thuật ngữ “tiền xu”, “token”, “tiền điện tử”, “tiền ảo”, “tiền kỹ thuật số”

và gần đây hơn, "tài sản tiền điện tử" hiện thường được sử dụng trong các giao dịch tương tự hoặc những cách có thể. Chúng tôi có thể tiếp tục tạo ra các thuật ngữ kỳ lạ tương tự bằng cách ghép nối các tính từ "tiền điện tử" khác nhau với các từ đồng nghĩa "tiền xu" khác nhau! Nó đủ để làm tiêu tan ngay cả nhà ngôn ngữ tài chính siêng năng nhất. Do đó, có thể sẽ khá lâu

trước khi tất cả chúng ta đồng ý về ngôn ngữ chính xác để sử dụng, cả tình cờ và hợp pháp. Tuy nhiên, bây giờ, chúng tôi có một cách tiếp cận thực tế. Chúng tôi có thể phá vỡ các loại khác nhau

công nghệ và phân loại chúng theo các thuật ngữ được chấp nhận nhiều nhất mặc dù ở đó

có thể có một số trùng lặp trong việc sử dụng trong thế giới thực.

Sự khác biệt chính mà chúng tôi sẽ thực hiện là giữa “tiền xu” và “tokens”. Chúng ta có thể mô tả tiền xu như một loại tiền tệ cơ bản. Khi một mạng, chẳng hạn như Bitcoin, bao gồm tiền tệ là một phần không thể thiếu của phần mềm, chúng tôi nghĩ về đơn vị tiền tệ đó, trong trường hợp này Bitcoin, như một đồng xu. Như chúng ta đã biết, Bitcoin được tạo ra với mục đích chính là lưu trữ và trao đổi quỹ. Trong Ethereum, tiền tệ Ether cũng được tích hợp vào nền tảng và do đó là một đồng xu. Điều này áp dụng cho các nền tảng khác có nguồn gốc từ Bitcoin, chẳng hạn như Litecoin hoặc Monero. Tiền xu cũng được sử dụng để khuyến khích hành vi tốt và đảm bảo nền tảng. Tiền xu được sử dụng để thanh toán cho các tài nguyên tính toán và lưu trữ và được cung cấp khai thác các nút như phần thưởng cho công việc của họ.

Token, giống như tiền xu, không có bất kỳ đặc tính bẩm sinh nào ngoài khả năng ghi sổ kế toán của chúng. Tuy nhiên, chúng có một số thể loại cơ bản mà chúng thường thuộc. Bạn có thể đã nghe các thuật ngữ “token tiện ích” hoặc “token bảo mật”. Lý do này sự phân biệt được thực hiện liên quan đến cách các mã thông báo được sử dụng để huy động vốn cho dự án hoặc doanh nghiệp. Bất kỳ ai cũng có thể tạo mã thông báo từ không có gì và bán chúng. Cách Ethereum đã huy động tiền cho sự phát triển của nó là bằng cách bán tương lai của nền tảng tiền tệ (Ether) cho Bitcoin. Khái niệm cho rằng Ether có thể được sử dụng để thanh toán việc gửi, lưu trữ và thực hiện các hợp đồng thông minh và dữ liệu liên quan. Nó đã "tiện ích" này sẽ làm cho nó có giá trị trong tương lai và là một khoản đầu tư đáng giá. Tất nhiên, nó cũng có thể được sử dụng đơn giản như một phương tiện trao đổi như Bitcoin.

**4 Hợp đồng thông minh ở đâu *?***

Các giao dịch chuỗi khối được lưu trữ trên một máy tính, thường được gọi là một nút.

Các nền tảng blockchain phổ biến như Ethereum có hàng chục nghìn nút hoạt động tại bất kỳ thời điểm nào. Mỗi nút lưu trữ một bản sao giống hệt nhau của tất cả các hồ sơ giao dịch. Nút xác thực lô giao dịch tiếp theo, được gọi là một khối, được gọi là một nút khai thác. Các khối lần lượt được xác nhận bởi mỗi nút khai thác.

Mỗi nút trong mạng Ethereum đều lưu trữ một bản sao của tất cả phần mềm (thông minh

hợp đồng), dữ liệu, số dư tài khoản và trạng thái giao dịch (Buterin [2014a](https://translate.googleusercontent.com/translate_f#103)). nếu bạn

nghĩ rằng có vẻ như rất nhiều dữ liệu, đúng như vậy. Bản sao của nút Ethereum sản xuất

tại thời điểm viết bài là khoảng 179 GB dữ liệu. Một kho lưu trữ đầy đủ tất cả các giao dịch

đã xảy ra, bao gồm tất cả các trạng thái trung gian là 1,8 TB.[2](https://translate.googleusercontent.com/translate_f#95) Để so sánh, một điển hình

điện thoại thông minh hoặc máy tính xách tay có thể có tổng bộ nhớ 64–512 GB.

Các giao dịch được truyền trên Internet giữa các nút trong một mạng ngang hàng

thời trang. Nghĩa là, các nút có kết nối với một số nhưng không phải tất cả các nút trong

mạng. Mất khoảng 40 giây để 95% các nút nhìn thấy một giao dịch nhất định

trong chuỗi khối Bitcoin có thể so sánh được (Decker và Wattenhofer [2013](https://translate.googleusercontent.com/translate_f#103)). Một phí giao dịch

được gửi cùng với giao dịch và nút khai thác nhận được phí cho các giao dịch mà nó nhóm vào khối. Khai thác đề cập đến việc đoán giải pháp cho một vấn đề toán học (duy nhất đối với

nhóm các giao dịch) mà không thể được tính toán trực tiếp. Đoán đó là xong

trên phần cứng có thể đưa ra hàng triệu lần đoán mỗi giây. Có một dự kiến

số lần phỏng đoán trung bình sẽ cần đến giải pháp và do đó, nút khai thác

đã chứng minh một cách hiệu quả rằng nó đã thực hiện một số phỏng đoán. Do đó khai thác cũng

được gọi là bằng chứng công việc (PoW).

Khối đã khai thác được phân phối trở lại mạng qua Internet và mỗi

nút sẽ xác minh tất cả các giao dịch chứa trước khi chấp nhận nó và chuyển nó

dọc theo. Cuối cùng, tất cả các nút sẽ lưu trữ một bản sao của trạng thái hệ thống mà tất cả chúng

thỏa thuận. Theo cách này, nó không phải là một máy tính phân tán nhiều như người ta nghĩ

theo nghĩa truyền thống. Nó giống như một máy tính có nhiều bản sao chạy trong

song song và lưu trữ thông tin giống nhau để đảm bảo không ai gian lận.

**Chương 6**

**DEX: DApp cho phân cấp**

**Thương trường**

**Chris Dai**

**2 mã hóa ở các lớp khác nhau của chuỗi khối**

Blockchain đôi khi còn được gọi là “chuỗi giá trị”. Hầu hết các tài sản

giá trị đại diện có thể được đại diện và sở hữu trên blockchain dưới dạng

"Mã thông báo". Vì mã thông báo được phát hành trên các lớp khác nhau của chuỗi khối, nên trước tiên, chúng tôi

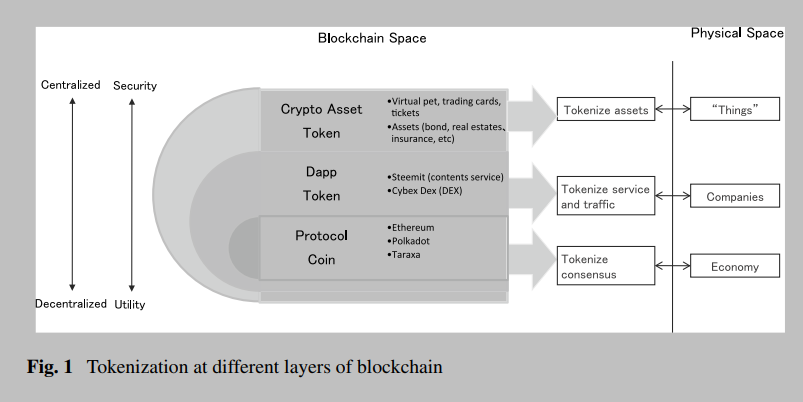
cần hiểu các giá trị mà mã thông báo đại diện ở mỗi lớp của chuỗi khối.

Có ba lớp blockchain có thể phát hành mã thông báo hoặc “mã hóa” (xem Hình [1](https://translate.googleusercontent.com/translate_f#107)).

***2.1 Mã thông báo tài sản tiền điện tử và giá trị của nó***

Mã thông báo tài sản tiền điện tử có thể đại diện cho bất kỳ thứ gì từ vé xem phim đến một gallon dầu hoặc một giờ do ai đó quyên góp. Bởi vì những mã thông báo này thực sự đại diện cho tài sản hoặc các giá trị trong thế giới vật chất, mã hóa ở lớp này rất giống với chứng khoán hóa

trong thế giới tài chính nơi các công ty có thể chứng khoán hóa một tài sản thực hoặc một số hình thức quyền đối với mục tiêu giao dịch.



**Hình 1** Mã hóa ở các lớp khác nhau của chuỗi khối

Việc phát hành các mã thông báo này yêu cầu một tổ chức trung tâm duy trì bảo tồn tài sản thực tế, phát hành mã thông báo đại diện trên blockchain và đảm bảo rằng bất kỳ ai nắm giữ mã thông báo đều có thể đổi tài sản cơ bản bất kỳ lúc nào. Chuỗi khối cho phép dễ dàng phát hành mã thông báo tài sản tiền điện tử và có nhiều tiêu chuẩn chung được cung cấp bởi các giao thức blockchain như Ethereum, EOS, v.v. Lợi ích của phát hành mã thông báo tài sản tiền điện tử là khả năng tạo chứng từ công khai kỹ thuật số không thể được giả mạo và đại diện cho một số hình thức quyền liên quan đến tài sản thực cơ bản.

Ngoài ra, chi phí phát hành cho mã thông báo tài sản tiền điện tử thấp vì không có bên thứ ba

hoặc trung gian là cần thiết. Chi phí chỉ phản ánh chi phí lưu giữ hồ sơ trong

sổ cái công khai, rất thấp. Hơn nữa, bản thân mã thông báo hoặc chứng từ kỹ thuật số có thể

chứa logic sẽ được thực thi tự động và do đó giảm bớt việc quản lý

chi phí của mã thông báo. Ví dụ: nếu một mã thông báo tài sản tiền điện tử đại diện cho một vé sự kiện, nó có thể được lập trình để sau một ngày nhất định (ví dụ: ngày diễn ra sự kiện), mã thông báo sẽ xóa chính nó. Các yêu cầu về sự chấp thuận của nhiều bên cũng có thể được kết hợp

(ví dụ: chuyển nhượng vé cho một cá nhân hoặc tổ chức khác), do đó thực hiện các quy tắc cho

quản trị.

***2.3 Cho phép Trao đổi Thực sự Hiệu quả và Công bằng***

Một loại thị trường mới được gọi là sàn giao dịch phi tập trung (DEX) đặc biệt

hữu ích vì nó cung cấp trao đổi ngang hàng an toàn cho các mã thông báo tài sản tiền điện tử. DEX

cung cấp thị trường hoàn hảo để giao dịch mã thông báo tài sản tiền điện tử giữa các chủ sở hữu mã thông báo.

Thị trường tập trung là một hộp đen dựa vào tất cả các bên tham gia tin tưởng thị trường là hiệu quả và công bằng. Tuy nhiên, điều này không phải lúc nào cũng trường hợp. Các nền tảng giao dịch ngoại hối ở Nhật Bản kiếm lợi nhuận dựa trên sự chênh lệch giữa giá mua và giá bán thay vì phí giao dịch. Điều này có nghĩa là nhà điều hành thị trường cũng tham gia với tư cách là một bên quầy giao dịch có lợi thế là biết tất cả giá hỏi và giá đặt mua và có thể phản ứng với thị trường trước tất cả người chơi. Điều này lợi thế không công bằng mang lại cho nhà điều hành sàn giao dịch trung tâm lợi nhuận giao dịch liên tục.

Mặt khác, một sàn giao dịch phi tập trung chỉ có hai bên tham gia; đó là, người mua và người bán. Bản thân thị trường chỉ là một tập hợp các hướng dẫn chương trình đảm bảo rằng khi một giao dịch được khớp giữa người mua và người bán, không ai có thể trở lại sau khi cả hai bên đã ký kết. Bản thân giao dịch được ghi lại trên blockchain, vì vậy nó dễ dàng được truy tìm. Thay vì tin tưởng một bên thứ ba để lưu trữ tất cả dữ liệu giao dịch, an toàn hơn và tốt hơn nếu lưu nó trên blockchain để không ai có thể thay đổi nó sau (tính bất biến) và mọi người có thể kiểm tra nó để chứng minh tính hợp pháp của giao dịch (minh bạch).

Bằng cách cho phép giao dịch ngang hàng, tính thanh khoản cũng được thêm vào thị trường nơi tài sản có thể không có bất kỳ giao dịch vật chất nào hoặc tính hợp pháp của quyền sở hữu là khó chứng minh trực tuyến. Trong trường hợp của tác phẩm nghệ thuật, số lượng trao đổi trung tâm (ví dụ, các nhà đấu giá) bị hạn chế và chỉ một nhóm nhỏ khách hàng / nhà đầu tư giàu có có thể tham gia vào thị trường. Những đặc điểm này làm cho thị trường rất kém thanh khoản. Tuy nhiên, nếu mã thông báo tác phẩm nghệ thuật được phát hành trong một sàn giao dịch phi tập trung, mỗi mã thông báo có thể đại diện cho quyền sở hữu một phần tác phẩm nghệ thuật và những người quan tâm đến nghệ thuật có thể mua và bán mã thông báo và kiếm lợi nhuận từ nó ngay cả khi họ không có tiền để mua một tác phẩm nghệ thuật toàn bộ. Bởi vì sàn giao dịch phi tập trung được chạy trên tự động mã máy tính, phí của nó thấp hơn nhiều so với một nhà đấu giá, và do đó có thể thu hút nhiều giao dịch mua và bán hơn. Cho phép nhiều người chơi hơn và nhiều giao dịch hơn trong này thị trường cho phép thanh khoản và thanh khoản tạo ra giá trị. Về bản chất, tiền điện tử giá trị mã thông báo tài sản được tính từ giá trị của tài sản cơ bản của nó, cộng với tính thanh khoản phí bảo hiểm được tạo ra từ việc giảm chi phí giao dịch.

***2.5 Tiền xu lớp giao thức và giá trị của nó***

Nếu chúng ta đánh đồng giá trị mã thông báo tài sản tiền điện tử với việc đại diện cho những thứ trong thế giới vật chất, và mã thông báo Dapp được định giá như cổ phiếu của các công ty, sau đó giá trị của token lớp giao thức hay “đồng xu” như hầu hết mọi người gọi chúng trong cộng đồng blockchain?

Đầu tiên, lớp giao thức blockchain là nơi chứa sổ cái (hồ sơ công khai) và thuật toán đồng thuận (các quy tắc về người ghi vào sổ cái) được xác định. Trong mạng blockchain, các nút khai thác và các nút đầy đủ cung cấp cơ sở hạ tầng của blockchain công khai duy trì việc ghi chính xác các giao dịch vào blockchain và ngăn chặn các cuộc tấn công vào blockchain. Chức năng của giao thức trong chuỗi khối thế giới tương tự như chức năng của hiến pháp và hệ thống pháp luật của một quốc gia hoặc kinh tế trong thế giới vật chất. Các mã chạy trên tất cả các nút trong một chuỗi khối tương tự như tập hợp các quy tắc mà chúng ta tạo ra trong thế giới vật chất của chúng ta dưới dạng luật.

Việc sử dụng giao thức không miễn phí vì các ưu đãi phải được trao cho các cá nhân để chia sẻ

tài nguyên của họ như một phần của cơ sở hạ tầng. Do đó, mọi giao dịch sẽ trả một khoản phí giao dịch để ghi lại một giao dịch vào sổ cái. Điều này tương tự với thuế đánh vào về các cá nhân và công ty trong thế giới vật chất. Tiền trong giao thức là thường được sử dụng để thanh toán phí giao dịch bằng giao thức.

Giá trị của đồng xu là gì? Điều này giống như việc hỏi giá trị của đồng đô la Mỹ. Nhiều

lập luận rằng đồng đô la Mỹ được hỗ trợ bởi Chính phủ Hoa Kỳ và do đó có giá trị, nhưng

tiền xu được phát hành trên blockchain không được hỗ trợ bởi bất kỳ ai và do đó không nên

giá trị. Điều thú vị là trên mỗi tờ đô la Mỹ đều có một câu: "TRONG ĐỨC CHÚA TRỜI

CHÚNG TÔI TIN TƯỞNG ”(Trang web của Bộ Ngân khố [2011](https://translate.googleusercontent.com/translate_f#116)). Theo một cách nào đó, nó sẽ là

thích hợp hơn để nói “vào Chính phủ Hoa Kỳ mà chúng tôi tin tưởng” hoặc “trong Cục Dự trữ Liên bang chúng tôi tin." Điều này cho chúng ta biết rằng giá trị của đô la Mỹ phụ thuộc nhiều hơn vào cá nhân niềm tin vào một trí tưởng tượng tập thể hơn là vào một cơ quan trung ương. Niềm tin của tiền vào một nền dân chủ và nền kinh tế thị trường xuất phát từ sự đồng thuận của mọi thành viên xã hội mà người đó đồng ý trao đổi giá trị thành tiền đó bất kỳ lúc nào. Điều này sự tin tưởng là sự tin tưởng tập thể và sự tin tưởng này được thực hiện trên blockchain bằng cách sử dụng các đồng tiền và mã thông báo. Về bản chất, tiền xu là một phương tiện trao đổi nhưng cũng đại diện cho sự tin cậy của những người tham gia vào hệ sinh thái. Không giống như thế giới thực, nơi các cá nhân có thể không thể chọn quốc gia của họ hoặc nền kinh tế, việc chọn một blockchain dễ dàng hơn nhiều và chỉ cần mua mã thông báo hoặc tiền xu để giao dịch với người khác. Loại thanh khoản này cho phép cạnh tranh giữa các giao thức blockchain, và cuối cùng, sẽ dẫn đến việc cải thiện giao thức blockchain. Ở lớp giao thức, không nên có chủ sở hữu thực sự của

giao thức vì nó là một cơ sở hạ tầng. Giao thức phi tập trung hơn DApp, điều này giới hạn phương thức kiếm tiền của nhóm phát triển chủ yếu là bán mã thông báo.

**3 DEX là gì?**

Cho đến nay, chúng tôi đã giải thích cách các mã thông báo blockchain có thể được sử dụng để đại diện và ghi lại giá trị dữ liệu và xây dựng các mô hình kinh doanh mới mở ra dữ liệu đó cho tất cả những người tham gia hệ thống. Tuy nhiên, nếu chỉ phát hành mã thông báo trên blockchain sử dụng mô hình phân tán trong khi việc trao đổi mã thông báo được thực hiện một cách tập trung, thì toàn bộ tiềm năng của mô hình phân tán blockchain không thể đạt được. Khi Adam Smith đề xuất khái niệm về bàn tay vô hình, anh ấy vẫn hình dung chính thị trường sẽ được điều hành bởi một thực thể trung tâm (Smith [1776](https://translate.googleusercontent.com/translate_f#116)). Ngày nay chúng ta thấy nhiều thị trường trên thế giới: thị trường cho các sản phẩm tiêu dùng như Amazon hoặc thị trường chứng khoán như Sở giao dịch chứng khoán New York hoặc Sở giao dịch chứng khoán Tokyo, và các thị trường trao đổi hàng hóa như Chicago Mercantile Exchange, v.v. Các thị trường này cùng nhau tạo nên xương sống của nền kinh tế thị trường của chúng ta, phân luồng và tối ưu hóa dòng tiền đến đúng ngành và tài sản. Tuy nhiên, hầu hết những trao đổi này không hiệu quả như chúng ta nghĩ. Có nhiều trung gian giữa người mua và người bán và một số giao dịch rất phức tạp và quy trình giải quyết thủ công mất nhiều ngày để giải quyết. Với blockchain, một loại Dapp [1](https://translate.googleusercontent.com/translate_f#112) được gọi là “DEX” (viết tắt của “trao đổi phi tập trung”) để thay đổi cách chúng ta giao dịch với nhau.

Một sàn giao dịch phi tập trung trên blockchain có các đặc điểm sau:

• Cho phép trao đổi ngang hàng các tài sản mã thông báo / tiền điện tử mà không cần bên trung gian.

• Mỗi người tham gia kiểm soát tài sản riêng của mình (khóa riêng).

• Tất cả các giao dịch được viết trên blockchain và minh bạch cho công chúng thấy.

• Tất cả các giao dịch sau khi xác nhận là bất biến.

***3.1 Cốt lõi kỹ thuật chính của DEX***

Trong phần trước, chúng tôi đã tranh luận về lợi ích của DEX và xem xét các loại

tài sản có thể được giao dịch trên DEX. Nó cũng đáng giá để xem xét kỹ hơn

các tính năng kỹ thuật của DEX và cách nó được triển khai. Cốt lõi của DEX là

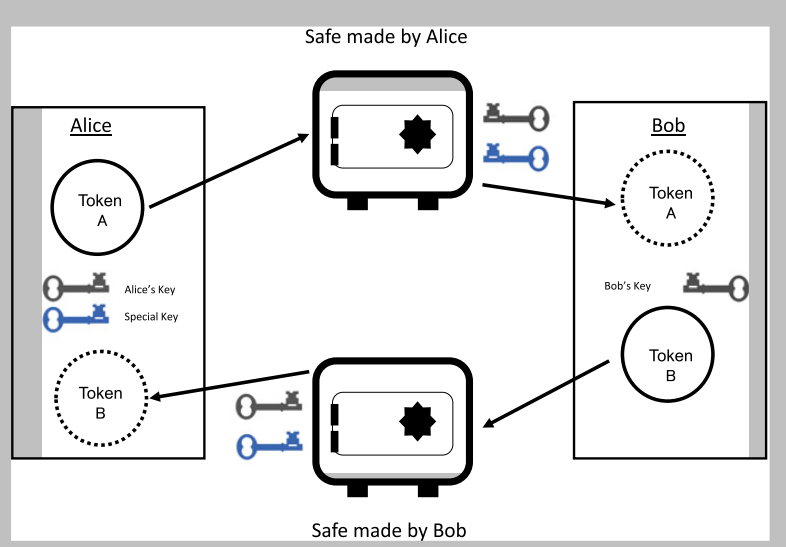
tính năng được gọi là "hoán đổi nguyên tử", là mã trên blockchain cho phép hai bên

để trao đổi mã thông báo / tài sản tiền điện tử mà không liên quan đến bên trung gian và tránh

một bên mặc định giao dịch, điều này sẽ gây thiệt hại cho bên truy cập. Trong

một DEX, không giống như một sàn giao dịch tập trung, những người tham gia quản lý tài sản tiền điện tử của riêng họ trong ví của chính họ. Khi có sự trao đổi giữa hai bên, sự trao đổi

xảy ra trực tiếp giữa hai ví thay vì đi qua một thứ ba đáng tin cậy bữa tiệc. Quá trình trao đổi trực tiếp này được gọi là hoán đổi nguyên tử. Có nhiều cách để thực hiện hoán đổi nguyên tử và Hình [2](https://translate.googleusercontent.com/translate_f#113) cho thấy phương pháp được đề xuất bởi Charlie Lee, người sáng lập Litecoin.



**Hình 2** Một ví dụ về hoán đổi nguyên tử

Hình [2](https://translate.googleusercontent.com/translate_f#113) cho thấy một trường hợp với hai người tham gia, Alice và Bob, những người muốn

hoán đổi mã thông báo trên hai blockchain khác nhau với nhau. Alice giữ mã thông báo A

của chuỗi khối A và Bob nắm giữ mã thông báo B của chuỗi khối B. Đầu tiên, Alice và Bob đồng ý

theo tỷ giá hối đoái của 1 mã thông báo A cho 1 mã thông báo B. Đàm phán giá trao đổi

xảy ra trên một bảng mua / bán hoặc một bảng trò chuyện. Sau khi tỷ giá hối đoái được đồng ý, Alice

tạo một két an toàn kỹ thuật số trên chuỗi A có thể được mở bằng chìa khóa của Bob và một chìa khóa đặc biệt do Alice tạo ra và Bob chưa biết. Alice đặt 1 mã thông báo A trong két và gửi két

thông tin cho Bob, chia sẻ các thông số kỹ thuật của khóa cho chìa khóa đặc biệt mà không có

chia sẻ chìa khóa. Bob sau đó cũng tạo một két an toàn kỹ thuật số trên chuỗi B và đặt 1 mã thông báo B trong két sắt. Két sắt của Bob chỉ có thể được mở bằng chìa khóa của Alice và chìa khóa đặc biệt được sử dụng cùng nhau, nhưng khi Alice sử dụng chìa khóa đặc biệt để mở két trên chuỗi B, chìa khóa đặc biệt sẽ được tiết lộ cho Bob. Tương tự, Bob sử dụng khóa riêng của mình và chìa khóa đặc biệt để mở két an toàn trên chuỗi A và giao dịch hoàn tất. Các khóa trên cả hai hộp an toàn đều có giới hạn thời gian và nếu Alice không mở hộp an toàn trên chuỗi B hoặc Bob không tạo hộp an toàn trên chuỗi B và gửi thông tin cho Alice, sau đó các mã thông báo trong két sắt sẽ được trả lại cho chủ sở hữu ban đầu mà không gây tổn thất cho một trong hai bên. Trong trường hợp này, sau khi Alice mở két ở chuỗi B, ở đó không quay lại và giao dịch sẽ được thực hiện. Đây là lý do tại sao quá trình được gọi là "hoán đổi nguyên tử", bởi vì nó tuân theo khái niệm ban đầu rằng nguyên tử không thể phân chia và quy trình này được thiết kế để giao dịch giữa hai chuỗi có thể được toàn bộ và không thể phân chia sau khi cả hai bên cam kết. Hoán đổi nguyên tử cung cấp khả năng dự đoán và trao đổi minh bạch các mã thông báo trên các blockchain khác nhau trên cơ sở mã và không dựa trên sự tin tưởng của một bên thứ ba. Trong phần tiếp theo, chúng tôi xem xét các tác động của nó và tác động thông qua các trường hợp thực tế.

***3.2 Hàm ý của DEX: Cuộc cách mạng do khả năng mang lại***

***phát hành, giao dịch và ghi lại tài sản tiền điện tử***

Mặc dù giá trị của hoán đổi nguyên tử là rất rõ ràng đối với việc giao dịch tài sản tiền điện tử, nhưng chức năng của DEX vượt xa mức trao đổi. So với trao đổi tập trung, chỉ có thể được sử dụng để trao đổi tài sản tiền điện tử, một DEX có thể sử dụng chuỗi của nó để phát hành tài sản tiền điện tử mới, giao dịch tài sản tiền điện tử đó và ghi lại hoạt động kinh doanh các giao dịch liên quan đến tài sản tiền điện tử. Chúng tôi không có nền tảng tập trung nào có thể làm cả ba cùng nhau. Binance cung cấp một nền tảng trung tâm để giao dịch tài sản tiền điện tử, nhưng,

bởi vì nó là tập trung và không sử dụng blockchain để chạy trao đổi của nó, nó phải phát hành thủ công tài sản tiền điện tử mới trong sàn giao dịch của nó. Tương tự, DApp sử dụng tiền điện tử tài sản không thể ghi lại các giao dịch trên nền tảng giao dịch trung tâm của Binance. Cái gì là

lợi ích của việc thực hiện cả ba quy trình phát hành, giao dịch và ghi lại các giao dịch trên một chuỗi khối duy nhất? Nếu tất cả các hoạt động liên quan đến một tài sản tiền điện tử duy nhất được ghi lại trên cùng một blockchain, khi đó người dùng và nhà đầu tư có thể xem đầy đủ việc sử dụng / giao dịch và hồ sơ giao dịch của bên phát hành. Điều này tạo ra sự minh bạch hơn và thêm độ tin cậy đối với tài sản tiền điện tử. Với sự minh bạch về dữ liệu giao dịch, một DEX

thực sự có thể trở thành một hệ sinh thái để lưu trữ các dịch vụ và cho phép thanh khoản cho các tài sản tiền điện tử được hỗ trợ bằng hàng hóa và dịch vụ.

Giá trị của một DEX được thể hiện rõ ràng trong RECIKA's[2](https://translate.googleusercontent.com/translate_f#114)  dự án thị trường dữ liệu người tiêu dùng nhằm dân chủ hóa việc giao dịch dữ liệu mua hàng của người tiêu dùng. Bằng cách sử dụng DEX làm hệ thống cốt lõi, RECIKA cho phép các cá nhân tải lên bản quét biên lai mua hàng của họ để nhận mã thông báo trong khi các doanh nghiệp muốn truy cập dữ liệu người tiêu dùng đã tải lên có thể thanh toán mã thông báo để lấy dữ liệu. Trong mô hình kinh doanh hiện tại, dữ liệu mua hàng của người tiêu dùng được lưu trữ trong cơ sở dữ liệu của nhà bán lẻ nhưng nhà bán lẻ

không được khuyến khích chia sẻ dữ liệu này. Đó là khó khăn cho các nhà sản xuất nhỏ hơn và các công ty khởi nghiệp để truy cập dữ liệu mua hàng của người tiêu dùng. Bằng cách ghi nhận quyền sở hữu của người tiêu dùng đối với dữ liệu tiêu dùng của họ và đạt được sự đồng ý của họ để chia sẻ dữ liệu, dữ liệu đó có thể được luân chuyển giữa người tiêu dùng, nhà bán lẻ và nhà sản xuất. Tất cả các giao dịch dữ liệu được ghi lại trên chuỗi khối DEX để cho phép chuyển đổi tính minh bạch trong hệ thống. Bất kỳ người tham gia nào cũng có thể kiểm tra lượng dữ liệu đang được tải lên và bao nhiêu dữ liệu được trao đổi. Ngoài ra, các nhà sản xuất có thể phát hành

hệ thống điểm thưởng bằng cách phát hành mã thông báo của riêng họ cho bất kỳ người tiêu dùng nào đã tải lên một biên lai có chứa sản phẩm của nhà sản xuất. Điểm đã phát hành (mã thông báo) của tất cả các nhà sản xuất cũng có thể được giao dịch trên DEX, vì vậy người tiêu dùng có thể chuyển đổi điểm từ các nhà sản xuất khác nhau đến nhà sản xuất mong muốn khi cần thiết. Tất cả điều này có thể đạt được trong hệ thống tập trung, nhưng nói chung là người tiêu dùng và / hoặc nhà sản xuất không tin tưởng vào dữ liệu của họ và chỉ đến một bên trung gian. Thay vì tin tưởng một bên thứ ba có thể làm rò rỉ dữ liệu quyền riêng tư của người tiêu dùng hoặc lạm dụng quyền lực mà họ nắm giữ đối với người tiêu dùng và các nhà sản xuất, một hệ sinh thái phi tập trung sẽ nhận được nhiều hỗ trợ hơn từ các bên liên quan khác nhau.

Một trường hợp sử dụng khác được xây dựng trên DEX là phát hành vé. Một DEX cho phép ứng dụng để phát hành mã thông báo có thể thay thế và không thể thay thế và chuyển giao ngang hàng và giao dịch các mã thông báo đó. Các chức năng này rất tiện lợi cho các nhà tổ chức sự kiện và các công ty phát hành vé. Ở Nhật Bản, hầu hết các vé sự kiện không được số hóa và nhiều vé nhỏ để các nhà tổ chức sự kiện quy mô vừa vẫn sử dụng fax để xác nhận đặt chỗ. Vé lớn

các nền tảng tính một khoản phí đáng kể mà các công ty vừa và nhỏ không thể mua được. Bằng cách phát hành vé dưới dạng mã thông báo trên chuỗi DEX, chi phí phát hành vé được hạ xuống nhưng nó cũng cho phép một thị trường thứ cấp nơi giao dịch vé có thể, và tính hợp pháp của vé có thể xác minh được. Mã thông báo vé được phát hành trên blockchain trở thành nhận dạng kỹ thuật số mà những người tham dự sự kiện có thể hiển thị tại quầy tiếp tân sự kiện.

***3.3 Những thách thức đối với DEX***

Mặc dù giao dịch dữ liệu và vé trên DEX có vẻ lành mạnh đối với quy định tài chính

cơ quan, giao dịch tiền điện tử và các chứng khoán tài chính khác trên mạng ngang hàng

cơ sở đặt ra những lo ngại nghiêm trọng trong lĩnh vực rửa tiền và tài trợ cho tội phạm

và khủng bố. Mối quan tâm này không chỉ đối với DEX mà còn đối với toàn bộ tiền điện tử.

Do thiếu xác thực trung tâm, nhiều DEX không yêu cầu "biết khách hàng của bạn ”(KYC) hoạt động và không có một tổ chức trách nhiệm rõ ràng để liên lạc với các cơ quan quản lý của chính phủ. Để DEX được sử dụng rộng rãi hơn, đúng là các chức năng như KYC và trách nhiệm giải trình cần được tích hợp vào mã, có thể dẫn đến hoạt động tập trung hơn của DEX. DEX cũng cung cấp

cơ hội cho các cơ quan quản lý và toàn xã hội giám sát để phát hiện giao dịch và hoạt động trong một mô hình khác biệt rõ rệt. Blockchain cung cấp một đại dương dữ liệu giao dịch tài chính toàn cầu minh bạch cho tất cả mọi người. Nó cho phép bất cứ ai để truy xuất và phân tích dữ liệu, điều rất khó đạt được trong nền tài chính hiện tại,ngành mà mọi ngân hàng đều ẩn giao dịch trong các máy chủ bảo mật cao. Sử dụng công nghệ AI với dữ liệu lớn này cho phép phát triển công nghệ quy định để có thể tìm, giám sát và theo dõi hoạt động bất hợp pháp trên blockchain với hiệu quả rất cao.

Bên cạnh những thách thức về quy định, cơ sở người dùng DEX hiện tại không phát triển nhanh chóng mặc dù lợi ích rõ ràng của nó vì hiệu suất thấp của công nghệ blockchain. Tốc độ giao dịch của một sàn giao dịch tập trung là 100 × hoặc 1000 × so với DEX hoạt động tốt nhất hiện tại, mang đến cho người dùng trải nghiệm tốt hơn nhiều. Còn nhiều việc phải làm để giải quyết vấn đề khả năng mở rộng của blockchain và hy vọng nó sẽ mang lại sự phát triển mạnh mẽ của DEX.

Cuối cùng, thách thức lớn nhất của chúng ta là chính chúng ta. Chúng tôi quá thoải mái khi dựa vào về quyền lực tập trung để quản lý những gì có giá trị nhất và thân yêu nhất đối với chúng ta, có thể dữ liệu cá nhân của chúng tôi hoặc tài sản sở hữu. Trong quá trình này, chúng tôi có nguy cơ mất không chỉ quyền riêng tư của chúng tôi mà còn bị lợi dụng bởi các cơ quan trung ương có khả năng sử dụng dữ liệu của chúng tôi để tác động đến hành vi của chúng tôi. DEX hỗ trợ chuỗi khối giúp mọi người đứng ở ngã tư một lần nữa, cung cấp cho chúng tôi tùy chọn để lựa chọn và tham gia kiểm soát một lần nữa.

**Chương 7**

**Kinh doanh Blockchain và Quy chế của nó**

**Makoto Yano, Chris Dai, Kenichi Masuda và Yoshio Kishimoto**

Để thiết kế một hệ thống tài chính mong muốn cho ngành công nghiệp blockchain, chúng ta nên

kiểm tra các ứng dụng blockchain từ bốn quan điểm sau đây.

1. So sánh giữa các thiết bị tài chính phi tập trung và thông thường.

2. Các phương pháp gây quỹ khác nhau cho các dự án blockchain.

3. Các quy định mong muốn cho các ứng dụng blockchain hiện tại.

4. Quy định và tự điều chỉnh của ngành công nghiệp blockchain trong tương lai.

Trước khi bắt đầu cuộc thảo luận của chúng ta, cần nhấn mạnh rằng các chuyên gia coi một hợp đồng blockchain phi tập trung trở nên lý tưởng. Trong một chuỗi khối như vậy, mặc dù ai đó có quyền kiểm soát trung tâm trong giai đoạn phát triển, không có pháp nhân nào bị tính phí hợp pháp có trách nhiệm duy trì và cải thiện một chuỗi khối (mặc dù có các tổ chức chẳng hạn như nền tảng Ethereum tự nguyện duy trì và cải thiện các blockchains khác nhau). Việc bảo trì và cải tiến còn lại để phát triển thành viên cộng đồng (rất có thể là chuyên gia máy tính), những người đóng góp tự nguyện. Điều này rõ ràng khác với các doanh nghiệp thông thường, có chủ sở hữu và thậm chí cách các công ty được thành lập.

Chúng tôi thảo luận về các quy định về blockchain cho tiền tệ chẳng hạn như Bitcoin và Bitcoin Cash. Để hiểu lý do tại sao blockchain tiền tệ nên được đối xử riêng biệt với các dự án kinh doanh, điều quan trọng đầu tiên là phải hiểu sự khác biệt giữa tiền bạc và các doanh nghiệp tiêu chuẩn và cách họ được xử lý trong một hệ sinh thái tài chính thông thường. Sau đó, chúng tôi sẽ đề cập đến các quy định về blockchain tiền tệ.

***1.3 Tiền và Token***

Trong các ICO (hoặc gây quỹ cho các dự án blockchain), tiền thường được cung cấp để trao đổi

cho chứng chỉ được gọi là mã thông báo hoặc tiền xu chứ không phải là chứng chỉ bảo mật. Nói chung, tiền xu tham khảo sang tiền tệ cơ sở trong hệ thống blockchain. Ví dụ như Bitcoin và Ethereum. Token là tiền tệ kỹ thuật số có thể được phát hành và phân phối bằng các hợp đồng thông minh và Dapps dựa trên blockchain. Tuy nhiên, trong nhiều trường hợp, mã thông báo và tiền xu không rõ ràng phân biệt.

Theo truyền thống, mã thông báo là một từ đồng nghĩa với vé; ví dụ, một vé đến New York

Subway từng được gọi là mã thông báo, là một miếng kim loại hình đồng xu. Token là

cũng được sử dụng trong nhiều khu vui chơi giải trí.

Trong hệ thống tàu điện ngầm hoặc trong một khu vui chơi giải trí, mã thông báo không có rủi ro

tài sản. Nếu phí tàu điện ngầm là 25 xu, một phần tư có thể được sử dụng thay vì mã thông báo

được bán với giá 25 xu. Nói cách khác, mã thông báo và tiền rất giống nhau trong xe điện ngầm.

Ở một số khía cạnh, có ý nghĩa tốt rằng chứng chỉ đầu tư cho các ICO là được gọi là mã thông báo, thay vì chứng khoán. Đầu tiên, các dự án blockchain dựa trên sự huấn luyện, theo nghĩa đó, chúng hoàn toàn khác với được quản lý tập trung doanh nghiệp thông thường về bản chất của chúng. Thứ hai, rất tốn kém để phát hành một bảo mật để người gây quỹ tuân thủ các quy định về chứng khoán.

**2 ICO**

Như đã nói ở trên, nhiều chức năng khác nhau được cung cấp bởi cái được gọi là ảo

tiền tệ. Một số loại tiền ảo nhất định cung cấp chức năng tiền tệ, như Bitcoin. Khác

hoạt động giống như chứng khoán mà lợi nhuận được liên kết với kết quả hoạt động kinh doanh.

Ví dụ: một trong những sàn giao dịch tiền ảo, Binance, đã phát hành một loại tiền ảo

được gọi là BNB vào năm 2017. Ngoài phí chiết khấu khi giao dịch bằng BNB, Binance

hứa hẹn mua lại mã thông báo BNB bằng cách chi 20% lợi nhuận hàng năm của Binance.

**4 Hướng tới Xây dựng một Hệ sinh thái Blockchain lành mạnh**

Bởi vì công nghệ blockchain được giới thiệu với Bitcoin, nhiều quốc gia đang đồng hành cùng việc áp dụng các quy định tài chính cho ngành công nghiệp blockchain. Nhật Bản là không ngoại lệ.

Mọi hoạt động kinh doanh mới đều gắn liền với những rủi ro mới. Khi Edison bắt đầu một công ty năng lượng, người dân bị mất điện, cháy nổ do rò rỉ điện; một số người đã bị điện giật trong những tai nạn bất cẩn có thể tránh được.

Mục đích của cuốn sách này không chỉ là giải thích về tiền ảo mà còn để nghiên cứu về chuỗi khối

công nghệ, bằng cách tạo ra các sổ cái phân tán giúp nó có thể an toàn và hiệu quả sử dụng tốt dữ liệu cá nhân và dữ liệu công nghiệp trong quá trình sản xuất. Ví dụ có thể bao gồm dữ liệu nông nghiệp từng cây trồng của một nông dân nhỏ, dữ liệu sức khỏe liên quan đến các bệnh liên quan đến lối sống và dữ liệu về tắc nghẽn giao thông trong thành phố. Công nghệ chuỗi khối sẽ làm cho nó có thể sử dụng các loại dữ liệu này mà không xâm phạm cá nhân quyền riêng tư và bí mật thương mại. Nếu dữ liệu như vậy có sẵn, lượng nông phế phẩm văn hóa có thể được giảm bớt, người trung niên trở lên có thể sử dụng dữ liệu để sửa đổi thói quen lối sống để đạt được lợi ích về sức khỏe và dự báo về tình trạng tắc nghẽn giao thông có thể trở nên sẵn sàng cho các trình điều khiển. Hơn nữa, công nghệ blockchain sẽ mở ra khả năng rằng nhiều tài sản kỹ thuật số và mã thông báo tiện ích sẽ được tạo ra có sẵn bởi DApps. Hơn nữa, công nghệ này có thể tạo ra một loại tiền ảo ổn định điều đó làm cho các khoản thanh toán vi mô khác nhau có thể thực hiện được.

**Chương 8**

**Công nghệ Bitcoin và Blockchain**

Sổ cái có thể được định nghĩa là “sổ ghi chép vĩnh viễn”. Với thông tin hiện đại

công nghệ, dữ liệu đã trở thành tài nguyên kinh tế nếu chúng được kết hợp với

sive chủ sở hữu và đưa vào một sổ cái.

Blockchain là một công nghệ đưa dữ liệu vào một sổ cái như vậy mà không có trung tâm thẩm quyền như ngân hàng quản lý tiền gửi. Thay vào đó, nhiều người độc lập với kiến ​​thức kỹ thuật góp phần tạo ra một sổ cái liên kết dữ liệu với nhau mảnh với chủ sở hữu của họ. Trong chương này, chúng tôi giải thích công nghệ này bằng cách tập trung vào blockchain ban đầu cho Bitcoin.

Chuỗi khối Bitcoin là sổ cái phi tập trung đầu tiên biến dữ liệu thành một tài nguyên kinh tế. Một sổ cái như vậy phải có một số tính năng cơ bản:

1. Dấu thời gian

2. Tính bất biến

3. Độ chính xác

4. Tính độc đáo

5. Tính xác thực

Dấu thời gian là một điểm đánh dấu chỉ định thời gian và ngày mà tại đó một bản ghi được thực hiện. Đặt dấu thời gian trên mỗi phần dữ liệu là quan trọng nếu quyền sở hữu dữ liệu

mảnh thay đổi ngoài giờ. Ví dụ: nếu sổ cái dùng để ghi lại quyền sở hữu của tài sản, sẽ không thể biết ai sở hữu một tài sản cụ thể tại một thời điểm cụ thể mà không có dấu thời gian.

Bởi tính bất biến, chúng tôi muốn nói rằng dữ liệu không thể bị giả mạo hoặc thay đổi bởi cuộc tấn công độc hại. Điều này ngụ ý rằng không ai có thể tạo ra một phiên bản giả mạo của một

sổ cái.

Độ chính xác ngụ ý rằng sổ cái phải ghi dữ liệu một cách chính xác và đáp ứng mọi yêu cầu

áp đặt trên sổ cái. Ví dụ: sổ cái cho các giao dịch tiền tệ phải đảm bảo rằng đối với mỗi giao dịch, không ai có thể chi tiêu nhiều hơn số dư hiện có trong tài khoản của anh ấy / cô ấy.

Tính duy nhất ngụ ý rằng mỗi sổ cái phải là một sổ ghi chép duy nhất cho mục đích cụ thể. Nếu hai sổ ghi chép khác nhau được tạo ra, nó sẽ dẫn đến tranh chấp; ví dụ, nếu sổ cái ghi lại quyền sở hữu đất, thì mỗi mảnh đất phải được liên kết với một chủ sở hữu duy nhất. Trong lịch sử, nhiều cuộc tranh chấp lãnh thổ đã dẫn đến từ việc không duy trì được một cuốn sổ ghi chép duy nhất về quyền sở hữu đất đai.

Theo tính xác thực, chúng tôi muốn nói rằng mỗi phần dữ liệu trên sổ cái phải mô tả

ý định chính xác của chủ nhân của nó. Nếu nó là sổ cái cho các giao dịch tiền tệ mà một ngân hàng duy trì, ghi chép về các khoản tiền gửi đến hoặc rút tiền từ tài khoản phải được tiến hành

theo cách chính xác mà chủ sở hữu dự định. Nếu một giao dịch được thực hiện thông qua một

máy rút tiền tự động (ATM), điều này có thể đạt được bằng cách sử dụng mật khẩu thích hợp

cho tài khoản, đảm bảo rằng đơn đặt hàng là xác thực.

Sổ cái thông thường đã được duy trì bởi các cơ quan trung ương; hồ sơ trên ngân hàng giao dịch của các ngân hàng và những giao dịch về tình trạng hôn nhân của chính quyền địa phương, v.v. Công nghệ chuỗi khối giúp bạn có thể xây dựng một sổ cái như vậy một cách phi tập trung mà không có bất kỳ cơ quan trung ương nào. Thay vào đó, một chuỗi khối dựa trên các thuật toán mà máy tính có thể làm theo.

Nó không phải là một nhiệm vụ dễ dàng để đưa ra các thuật toán như vậy. Trong những gì sau đây, chúng tôi giải thích việc triển khai một thuật toán như vậy bằng cách tập trung vào chuỗi khối Bitcoin, cái đầu tiên cho thấy tiềm năng của sổ cái dựa trên thuật toán phi tập trung

hệ thống.

Thuật toán Bitcoin thông qua bốn ý tưởng quan trọng trong việc thiết kế sổ cái tiền tệ.

Họ đang:

1. Chuỗi khối

2. Bằng chứng công việc

3. Thuật toán đồng thuận phi tập trung

4. Tài khoản mật mã khóa mở

**1 chuỗi khối**

Trong một chuỗi khối, một khối là một tệp chứa dữ liệu có dấu thời gian. Chuỗi khối bitcoin

là một chuỗi kết nối các khối trong một hàng duy nhất. Mỗi khi một khối mới được xây dựng,

cái này được đính kèm với khối gần đây nhất trên chuỗi.

**2 Bằng chứng công việc**

Để xây dựng một sổ cái, một khối mới phải được "dán" vào khối gần đây nhất. Một câu đố mật mã đóng vai trò là chất keo kết nối vĩnh viễn một khối với khối trước đó khối. Cần một lượng lớn sức mạnh tính toán (tức là điện) để giải quyết câu đố này. Quá trình này được gọi là bằng chứng công việc, ngụ ý rằng một khối được nhúng vào một chuỗi khối cho thấy rằng một lượng đủ sức mạnh tính toán đã được sử dụng cho việc tạo ra khối đó .

Sau khi một khối được xây dựng, nó sẽ được chuyển đổi thành một câu đố mật mã. Hiểu

câu đố này, cần phải biết một thuật toán mật mã được gọi là băm an toàn thuật toán (SHA). SHA biến bất kỳ dữ liệu kỹ thuật số nào có độ dài bất kỳ thành dữ liệu duy nhất dãy các chữ số dường như ngẫu nhiên với độ dài cố định. Một số SHA có còn phát triển. Thuật toán phổ biến nhất hiện nay được gọi là SHA 256, biến bất kỳ câu nào thành một số có 256 chữ số trong hệ thống chữ số nhị phân.Ví dụ, SHA 256 chuyển từ “blockchain” thành

SHA (chuỗi khối)

= EF7797E13D3A75526946A3BCF00DAEC9

FC9C9C4D51DDC7CC5DF888F74DD434D1 (1)

được thể hiện trong hệ thống chữ số thập lục phân (với các chữ số 0-9 và

chữ cái A – F). Giá trị này được SHA 256 gọi là giá trị băm của từ “blockchain”.

SHA được thiết kế theo cách thực tế không thể đoán được câu gốc từ một giá trị băm. Một câu cụ thể luôn được dịch thành cùng một giá trị băm. Hơn nữa, cơ hội mà hai câu khác nhau là

được liên kết với một giá trị băm giống hệt nhau trên thực tế bằng không. Một công dụng của SHA là lưu trữ mật khẩu. Ví dụ: mật khẩu cho máy ATM phải được lưu trữ cùng với số tài khoản. Nếu mật khẩu đã được lưu trữ trong các giá trị trần mà chủ sở hữu tài khoản chọn, nó sẽ tạo ra một vấn đề lớn nếu mật khẩu đã bị đánh cắp. Thuật toán băm an toàn rất hữu ích để ẩn mật khẩu khỏi bất kỳ ai khác ngoài chủ sở hữu tài khoản được liên kết. Ngay cả khi ai đó nhìn thấy giá trị băm của mật khẩu được liên kết với tài khoản, anh ấy / cô ấy không bao giờ có thể tìm thấy mật khẩu. Đồng thời, liệu mật khẩu nhập vào máy ATM có thể xác thực , có thể được xác định dễ dàng bằng cách chuyển đổi mật khẩu đã nhập bởi SHA được ngân hàng thông qua hay không.

Câu đố mật mã được gọi là bằng chứng công việc yêu cầu một chuỗi các chữ số có thể được gắn vào cuối một câu cụ thể để giá trị băm của câu cụ thể cộng với chuỗi đính kèm bắt đầu bằng X số không cái mà được yêu cầu bởi thuật toán. Nếu câu đố bằng chứng công việc yêu cầu tìm một chuỗi các chữ số để đính kèm vào "blockchain" để số đầu tiên của giá trị băm bằng 0,

một giải pháp là chuỗi 34 số không ở cuối từ “blockchain”. Đó là

để nói,

SHA (chuỗi khối0000000000000000000000000000000000)

= 088C389A0BC33DE6A7D8DD9012DBD6

C5E9276B94C2639E72725F40E98A7163AA (2)

Nếu giá trị băm gồm 16 chữ số là một chuỗi các chữ số được chọn ngẫu nhiên từ 1

đến F (thực ra không phải vậy), xác suất mà số đầu tiên bằng 0 là 1/16, và giá trị đó của hai số đầu tiên là 1/16^2 . Như vậy, rõ ràng là có nhiều giải pháp cho từng câu đố bằng chứng công việc. Hơn nữa, vì số lượng số không bắt buộc tăng lên, ngày càng khó tìm ra giải pháp trong đó chuỗi các chữ số được gắn vào một câu nhất định để các số không sẽ xếp hàng ở đầu của giá trị như thuật toán yêu cầu.

Nếu thuật toán này được sử dụng để lưu trữ một phần thông tin (hoặc nếu "blockchain" là mảnh được nộp), nó có thể dùng như một bằng chứng đơn giản cho thấy một thời gian tính toán nhất định được chi tiêu trước khi nộp thông tin. Điều này là do cần có thời gian để tìm ra một chuỗi các chữ số để đính kèm vào một tin nhắn và rất dễ dàng để kiểm tra xem trình tự đính kèm là đúng. Vì lý do này, thuật toán được coi là cung cấp một bằng chứng công việc. Một thuật toán bằng chứng công việc được phát minh vào năm 1997 cho phần mềm có tên là Hashcash.

Phần mềm này tách các email có ý nghĩa khỏi các thư rác. Ví dụ, nếu mọi thư nonspam được yêu cầu bao gồm một giải pháp xếp hàng một số số không nhất định ở đầu giá trị băm của câu email, nó có độ dài nhất định là thời gian tính toán trước khi người gửi gửi email. Vì tính toán tốn kém

thời gian, không có người gửi thư rác nào dám giải câu đố do Hashcash đặt ra và không có thư rác được gửi kèm theo lời giải cho câu đố. Do đó, người nhận thư có thể tách các thư thực (có giải pháp cho câu đố) khỏi thư rác.

Chuỗi khối Bitcoin sử dụng thuật toán bằng chứng công việc. Để tạo và đính kèm khối mới cho chuỗi hiện tại, cần phải tìm một giải pháp sao cho số lượng các số 0 ở đầu giá trị băm của giải pháp được thêm vào những gì được viết trong khối hiện có và viết lời giải trong khối mới. Các

số lượng số không mà chuỗi khối Bitcoin yêu cầu được đặt theo cách mà nó cần, trung bình, khoảng 10 phút để một máy tính nhanh chóng tìm ra giải pháp. Điều này xóa sạch mọi động cơ giả mạo chuỗi khối vì viết lại một phần hoặc tất cả các khối trên một chuỗi yêu cầu phải giải lại tất cả các câu đố, điều này cực kỳ tốn kém. Nói tóm lại, một blockchain được xây dựng trên thuật toán bằng chứng công việc là bất biến.

**3 Thuật toán đồng thuận phi tập trung**

Công nghệ chuỗi khối giúp bạn có thể xây dựng một sổ cái chính xác bằng cách không dựa vào trên một cơ quan trung ương nhưng trên một thuật toán liên quan đến nhiều người độc lập hoặc các máy tính được gọi là các nút mạng. Thuật toán này được gọi là đồng thuận (phi tập trung) Để tạo sổ cái theo cách phi tập trung, điều quan trọng là phải cung cấp các biện pháp khuyến khích để mọi người sẵn sàng đóng góp vào việc xây dựng sổ cái. Trong chuỗi khối Bitcoin, điều này khuyến khích được tạo ra bằng cách tách những người sử dụng sổ cái (người dùng), ghi lại chuyển tiền giữa các tài khoản người dùng, từ những người thêm hồ sơ mới vàosổ cái. Một cá nhân muốn ghi lại chuyển tiền sẽ đăng một giao dịch với một khoản phí giao dịch được đề xuất. Vì kích thước tối đa của mỗi khối là cố định, 1 máy ghi chỉ có thể chọn một số từ nhóm giao dịch và đặt chung vào khối mới. Đối với một máy ghi cụ thể để đặt khối của mình vào chuỗi khối hiện có, như đã thảo luận ở trên, anh ấy / cô ấy phải là người đầu tiên giải được câu đố mật mã được tạo ra từ khối mới nhất của chuỗi. Để thu hút một số lượng đủ lớn người ghi, một số tiền cố định được trao như một giải thưởng cho bất kỳ người ghi nào thực sự thêm một khối vào chuỗi. Nếu giải thưởng này đủ lớn, nhiều người sẽ tham gia tạo khối mới. Bất kể có bao nhiêu người ghi tham gia vào việc tạo ra một khối mới tại một thời điểm cụ thể, chỉ một người ghi có thể nhận được giải thưởng. Điều này quá trình tương tự như tìm kiếm vàng trong mỏ vàng và do đó được gọi là

"khai thác mỏ." Những người điều hành hoạt động khai thác và duy trì máy tính ghi lại các khối mới được gọi là "thợ đào".

Một cách khác để nhìn vào quá trình này là nghĩ về nhóm thợ đào như một mạng máy tính kết nối qua Internet. Thợ mỏ là các nút mạng. Các toàn bộ chuỗi khối được lưu trữ trên mỗi nút. Mỗi nút hoạt động độc lập theo theo ý muốn của nút.

Yêu cầu chính đối với sổ cái là tính chính xác. Mặc dù một bằng chứng công việc thuật toán ngăn sổ cái bị spam, nó không đủ để duy trì độ chính xác của sổ cái. Nếu một khối chứa thông tin sai, nó không được thêm vào một chuỗi khối. Đối với một sổ cái thông thường như một loại tiền gửi, có một trung tâm thẩm quyền duy trì độ chính xác một mình.

Chuỗi khối Bitcoin thông qua một thuật toán đồng thuận phi tập trung. Khi một nút cụ thể tham gia mạng, nó được liên kết ngẫu nhiên với một số nút hiện có. Khi một nút cụ thể đặt một khối mới lại với nhau và giải câu đố, nó sẽ thông báo khối mới cho các nút được liên kết. Các nút liên kết đó kiểm tra độc lập nếu khối mới có bất kỳ lỗi nào. Nếu họ không tìm thấy lỗi, họ sẽ thông báo chặn toàn bộ mạng. Nếu các nút được liên kết tìm thấy lỗi, chúng sẽ bỏ qua khối, trong trường hợp đó không có nút nào khác sẽ biết khối mới. Thông qua quá trình này,độ chính xác của các khối có thể được duy trì.

Một yêu cầu quan trọng khác đối với sổ cái là tính duy nhất của nó; Nếu có thể rằng nhiều sổ ghi chép đã được tạo, chúng không thể phục vụ như một sổ cái. Tuy nhiên, chuỗi khối bitcoin có khả năng có nhiều chuỗi được xây dựng. Do đó, có nhiều khả năng là nhiều hơn một nút sẽ giải quyết câu đố hiện tại.

Nếu có nhiều hơn một nút thành công, một chuỗi khối sẽ chia đôi; chuỗi trên một số nút sẽ trở nên khác với ở các nút khác sau điểm phân đôi. Đến khắc phục tình huống như vậy và để duy trì một chuỗi duy nhất, thuật toán Bitcoin thiết lập quy tắc rằng chuỗi hiện có dài nhất được coi là chuỗi hợp lệ. Nếu một chuỗi chia đôi thành hai, tại điểm phân đôi, hai chuỗi có cùng chiều dài, rất có thể, với các khối khác nhau ở cuối trình bày các câu đố khác nhau. Bởi vì chiều dài của

thời gian cần thiết để giải một câu đố là hoàn toàn ngẫu nhiên, độ dài của một chuỗi sẽ nhanh chóng trở nên dài hơn cái khác. Ngay sau khi điều này xảy ra, hầu hết các nút sẽ bắt đầu giải câu đố được trình bày bởi chuỗi dài hơn và chuỗi ngắn hơn chuỗi sẽ nhanh chóng bị bỏ qua.

Điều này ngụ ý rằng ngay cả khi một khối được tạo bằng cách giải câu đố bằng chứng công việc,

nó không ngụ ý rằng khối (và các giao dịch trong khối) sẽ được ghi lại vĩnh viễn. Nghĩa là, những giao dịch đó có thể được ghi lại trong một chuỗi mà sau này sẽ trở nên ngắn hơn cái khác, và kết quả là bị lãng quên.

**4 tài khoản mật mã khóa mở**

Một vấn đề quan trọng khác trong việc xây dựng sổ cái cho hoạt động của các cá nhân là đảm bảo rằng việc ghi âm được thúc đẩy bởi ý chí của các cá nhân tiến hành các hoạt động. Nếu sổ cái ghi lại việc chuyển tiền từ tài khoản này sang tài khoản khác, bản ghi phải phản ánh chính xác những gì chủ sở hữu tài khoản muốn. Tuy nhiên, làm thế nào có thể thợ đào cho biết rằng một ứng dụng để ghi lại chuyển tiền từ một tài khoản là thực sự được thực hiện bởi chủ sở hữu của tài khoản? Trong trường hợp chuyển khoản ngân hàng, rất dễ dàng; ngân hàng có thể chỉ cần kiểm tra xem người yêu cầu chuyển khoản có biết mật khẩu của tài khoản. Tuy nhiên, nhiệm vụ này không đơn giản nếu bản ghi được tạo ra trong một cách thức phân tán.

Công nghệ chuỗi khối khắc phục khó khăn này bằng cách sử dụng “mã hóa khóa công khai” cung cấp một cặp khóa để mã hóa và giải mã một văn bản. Nếu một văn bản được mã hóa

bằng một trong hai khóa, văn bản được mã hóa kết quả có thể được giải mã thành văn bản gốc

văn bản bằng khóa còn lại. Nó được thiết kế theo cách mà không thể xác định được chìa khóa từ chìa khóa khác.

Tất nhiên, hai bên có thể sử dụng mật mã khóa công khai để giao tiếp chỉ giữa chúng bằng cách gán một trong hai khóa cho một bên và chìa khóa khác cho bên kia. Tuy nhiên, cách sử dụng phổ biến hơn là tạo một trong những hai khóa công khai, giải thích thuật ngữ của mật mã khóa công khai.

Một cách sử dụng của mật mã khóa công khai là nhận thông điệp một cách bí mật. Vì mục đích đó, người nhận tin nhắn có thể tạo một cặp khóa, đặt một trong các khóa ở chế độ công khai và giữ khóa khác ở chế độ riêng tư. Nếu người gửi tin nhắn mã hóa tin nhắn bằng khóa công khai và gửi nó đến người nhận, người nhận có thể nhận được tin nhắn bằng cách giải mã nó bằng khóa riêng.

Một cách sử dụng khác là đính kèm chữ ký điện tử để chứng minh rằng một tin nhắn được gửi từ người gửi chứ không phải từ một cá nhân khác. Vì mục đích này, người gửi có thể mã hóa

một tin nhắn có khóa riêng tư và gửi cả tin nhắn được mã hóa bởi cặp khóa công khai và tin nhắn gốc. Bằng cách sử dụng khóa công khai đã nhận, người nhận có thể giải mã tin nhắn đã mã hóa. Nếu thông báo được giải mã kết quả giống nhau là tin nhắn gốc, được gửi riêng, người nhận có thể chắc chắn rằng người gửi thư là người biết khóa cá nhân được ghép nối với khóa công khai.

Phương pháp chữ ký điện tử này được sử dụng bởi chuỗi khối Bitcoin. Trong việc tạo ra

một tài khoản mới cho Bitcoin, một số ngẫu nhiên được chọn đầu tiên. Bằng cách sử dụng khóa công khai mật mã, số ngẫu nhiên này được chuyển thành khóa riêng. Khóa riêng tư này là sau đó được chuyển thành khóa công khai được ghép nối. Một tài khoản Bitcoin được tạo ra từ khóa công khai. Khóa công khai được thông báo trên toàn mạng Internet. Về bản chất, khóa công khai đóng vai trò là cơ sở cho tài khoản của người dùng trong khi khóa riêng tư phục vụ làm mật khẩu cho tài khoản. Chủ sở hữu tài khoản mã hóa các giao dịch với khóa cá nhân và gửi cả giao dịch được mã hóa và giao dịch ban đầu, từ đó các thợ đào có thể xác nhận tính xác thực của giao dịch.

**5 Nhận xét Kết luận**

Chuỗi khối Bitcoin là công cụ đầu tiên chứng minh rằng sổ cái, một thứ bất biến, sổ sách ghi chép chính xác và duy nhất, có thể được xây dựng trên Internet một cách phi tập trung cách thức. Mặc dù quá trình này đã được nhiều người nhiệt tình chấp nhận, nhưng một số điểm yếu cũng đã được bộc lộ. Hiện tại, Bitcoin và các loại tiền ảo khác tiền tệ hoạt động như công cụ đầu cơ hơn là phương tiện trao đổi.

Chúng thường được sử dụng để buôn bán các mặt hàng bất hợp pháp như ma túy và để lấy tiền giặt giũ. Những vấn đề này có thể được giải quyết khi xã hội trở nên thông tin hơn về những gì blockchain có thể làm và những gì chúng không thể làm.

Một vấn đề cơ bản hơn có thể là các blockchains bằng chứng công việc yêu cầu lượng điện lớn để giải các câu đố về tiền điện tử; một số lượng cực kỳ lớn các thợ đào sử dụng máy tính của họ để giải các câu đố về blockchain. Tuy nhiên, như đã thảo luận trong Chap. [5](https://translate.googleusercontent.com/translate_f#88), điều hấp dẫn về tiền ảo là sản xuất không tốn kém, điều này làm cho nó có thể đánh đồng chi phí biên của tiền với mức thoả dụng biên của tiền bạc. Đây là điều kiện cần để sử dụng hàng hóa tư nhân có hiệu quả; theo truyền thống, tiền đã được đưa ra ngoài việc xem xét hiệu quả này bởi vì hàng hóa không có giá trị (như giấy) đã được sử dụng như tiền. Chuỗi khối Bitcoin rất quan trọng vì nó đã chứng minh rằng một khoản tiền gửi tiền tệ có thể được tạo ra khá rẻ theo cách phi tập trung. Một khi khả năng một công nghệ như vậy được hiện thực hóa, nhiều công nghệ mới khác sẽ được được phát triển có thể cung cấp nhiều thứ hơn là chỉ tiền với chi phí rẻ hơn nhiều.