TÌM HIỂU VỀ BLOCKCHAIN(sưu tầm)

Người sưu tầm và giới thiệu: PGS.TS Nguyên Hữu Công

Blockchain là gì?

Blockchain là một sổ cái kỹ thuật số được phân chia hay dễ hiểu hơn là cơ sở dữ liệu trong một mạng. Sổ cái được chia sẻ cho những người tham gia vào mạng lưới. Điều này cho thấy rằng trong toàn bộ hệ thống không phải chỉ có một vị trí duy nhất, một tài liệu có thể làm căn cứ đáng tin (authority) duy nhất, vì những lần sao chép cùng một phiên bản sổ cái được đặt ở nhiều nơi.

Tất cả các bản sao này được cập nhật khi dữ liệu hoặc giao dịch mới được ghi vào blockchain thông qua sự đồng thuận của tất cả mọi người tham gia. Người đào có trách nhiệm phê duyệt các giao dịch và giám sát mạng bằng cách giải quyết các công thức tinh vi với sự trợ giúp của máy tính. Nó là một hệ thống ngang hàng P2P, loại bỏ tất cả mọi khâu trung gian, làm tăng cường an ninh, minh bạch và sự ổn định cũng như giảm thiểu chi phí và lỗi do con người gây ra.

Bằng cách cho phép phân phối các thông tin kỹ thuật số nhưng không được sao chép, công nghệ blockchain đã tạo ra xương sống cho một loại hình Internet mới.

Trong cuốn sách Blockchain Revolution (2016), Don & Alex Tapscott đã nhận định rằng: "Blockchain là một sổ cái kỹ thuật số không thể bị phá hỏng của các giao dịch kinh tế, có thể được lập trình để ghi lại không chỉ những giao dịch tài chính mà có thể ghi lại tất cả mọi thứ có giá trị".

Blockchain làm việc như thế nào?

Công nghệ blockchain có lẽ là phát minh tốt nhất từ chính Internet. Nó cho phép trao đổi giá trị mà không cần sự tin tưởng hoặc chứng cứ làm tin. Hãy tưởng tượng bạn và tôi đặt cược 50$ cho thời tiết ngày mai ở San Francisco. Tôi đặt cược trời sẽ nắng, bạn cược là mưa. Hôm nay chúng ta có ba tùy chọn để quản lý giao dịch này:

- **Chúng ta có thể tin tưởng lẫn nhau.** Mưa hoặc nắng, người thua sẽ trả 50 đô la cho người chiến thắng. Nếu chúng ta là bạn, đây có thể là một cách hay để đặt cược. Tuy nhiên, dù là bạn bè hay người lạ thì vẫn không thể dễ dàng trả tiền cho người kia.
- **Chúng ta có thể biến tiền cược thành một hợp đồng.** Với một hợp đồng tại chỗ, cả hai bên sẽ dễ phải trả tiền hơn, tuy nhiên, nếu một trong hai người

quyết định không trả, người chiến thắng sẽ phải trả thêm tiền để trang trải chi phí pháp lý và bản án có thể mất một thời gian dài. Đặc biệt với một lượng tiền mặt nhỏ, điều này dường như không phải là cách tối ưu để quản lý giao dịch.

- **Chúng ta có thể nhờ đến một bên thứ ba trung lập.** Mỗi người trong chúng ta đưa 50 đô la cho một người thứ ba, cô ấy sẽ đưa tổng số tiền cho người chiến thắng. Nhưng, cô ấy cũng có thể bỏ trốn với tất cả số tiền. Vì vậy, chúng ta sẽ chọn một trong hai lựa chọn đầu tiên: tin tưởng hoặc hợp đồng.

Cả sự tin tưởng và hợp đồng đều không phải là giải pháp tối ưu. Chúng ta không thể tin tưởng vào người lạ và thực thi hợp đồng đòi hỏi thời gian và tiền bạc. Công nghệ blockchain là thú vị vì nó cung cấp cho chúng ta lựa chọn thứ ba, an toàn, nhanh chóng và rẻ tiền.

Blockchain cho phép viết một vài dòng code, chương trình chạy trên blockchain, mà cả hai chúng ta gửi 50 đô la vào đó. Chương trình này sẽ giữ 100 đô la an toàn và kiểm tra thời tiết ngày mai một cách tự động trên nhiều nguồn dữ liệu. Nắng hoặc mưa, nó sẽ tự động chuyển toàn bộ số tiền cho người chiến thắng. Mỗi bên có thể kiểm tra hợp đồng logic, và vì nó đang chạy trên blockchain nên nó không thể thay đổi hoặc ngừng lại. Nỗ lực này có thể là quá cao đối với một giao dịch 50 đô la, nhưng hãy tưởng tượng khi bán nhà hoặc công ty.

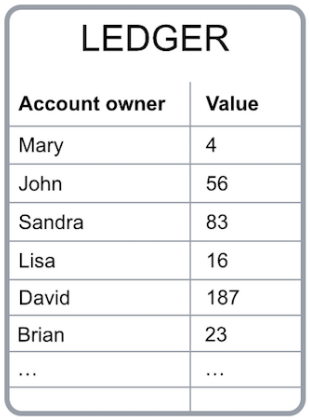
Mục tiêu của phần này là để giải thích cách blockchain hoạt động mà không thảo luận về các chi tiết kỹ thuật sâu, nhưng đủ để bạn có một ý tưởng chung về logic và cơ chế cơ bản.

Ứng dụng được biết đến và thảo luận nhiều nhất của công nghệ blockchain chính là Bitcoin. Một loại tiền tệ số có thể được sử dụng để trao đổi sản phẩm và dịch vụ, giống như đồng đô la Mỹ (USD), Euro (EUR), đồng (Việt Nam) và các loại tiền tệ quốc gia khác. Hãy sử dụng ứng dụng đầu tiên của công nghệ blockchain này để tìm hiểu cách hoạt động của nó.

Bitcoin là gì?

Một Bitcoin là một đơn vị tiền tệ kỹ thuật số của Bitcoin, giống như đô la, bản thân nó không có giá trị. Nó có giá trị vì chúng ta đồng ý trao đổi hàng hóa, dịch vụ để đổi lấy một lượng tiền lớn hơn dưới dự kiểm soát của chúng ta và chúng ta tin rằng người khác cũng sẽ làm như vậy.

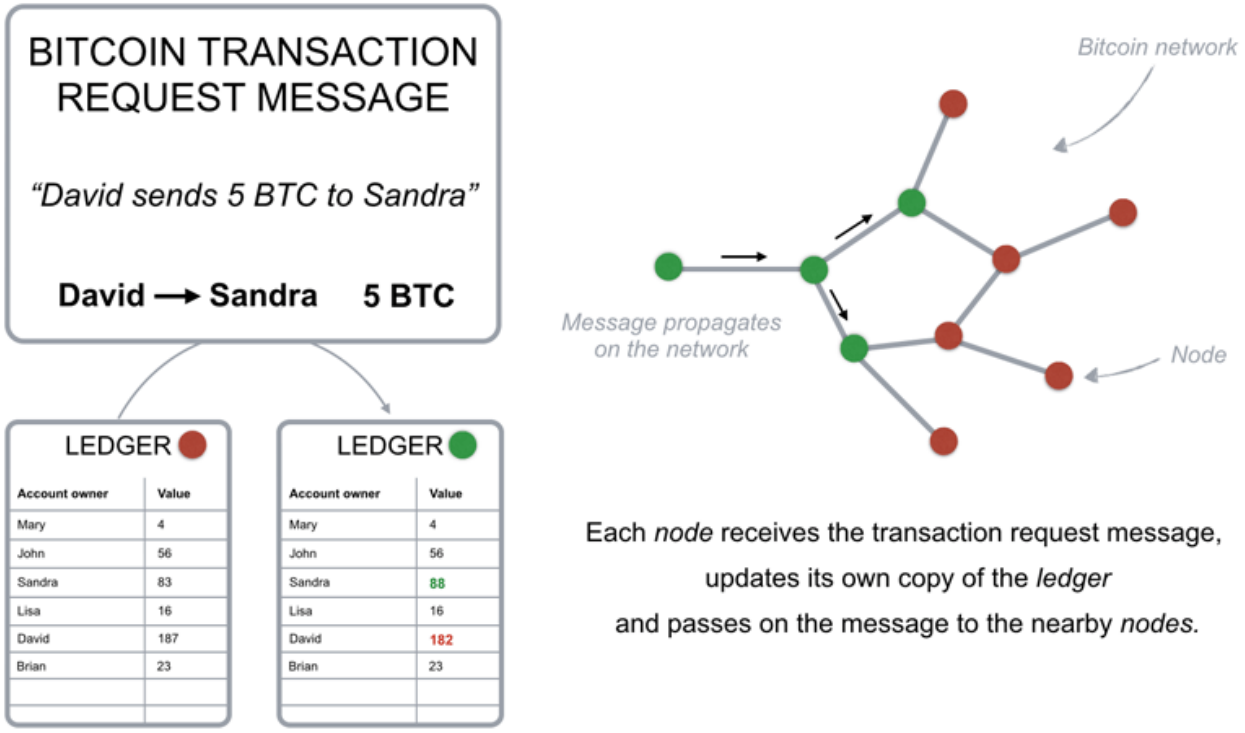
Để theo dõi lượng Bitcoin mỗi người trong chúng ta sở hữu, blockchain sử dụng một sổ cái - file kỹ thuật số - theo dõi tất cả các giao dịch của Bitcoin.



Tập tin kỹ thuật số của Bitcoin đã được đơn giản hoá

File này không được lưu trữ trên máy chủ tập trung, giống như ngân hàng hay trung tâm dữ liệu. Nó được phân tán trên toàn thế giới thông qua mạng máy tính, vừa lưu trữ dữ liệu, vừa thực hiện tính toán. Mỗi máy tính đại diện cho một nút của mạng blockchain và có một bản sao của file sổ cái.

Nếu David muốn gửi Bitcoin cho Sandra, anh ta sẽ phát một tin nhắn tới mạng nói rằng số lượng Bitcoin trong tài khoản của anh ta sẽ giảm xuống 5 BTC, và số tiền của tài khoản Sandra sẽ tăng lên theo cùng số lượng. Mỗi nút trong mạng sẽ nhận được thông báo và áp dụng giao dịch yêu cầu vào bản sao của sổ cái, do đó cập nhật số dư tài khoản.



Thực tế là sổ cái được duy trì bởi một nhóm các máy tính được kết nối chứ không phải là một thực thể trung lập như ngân hàng:

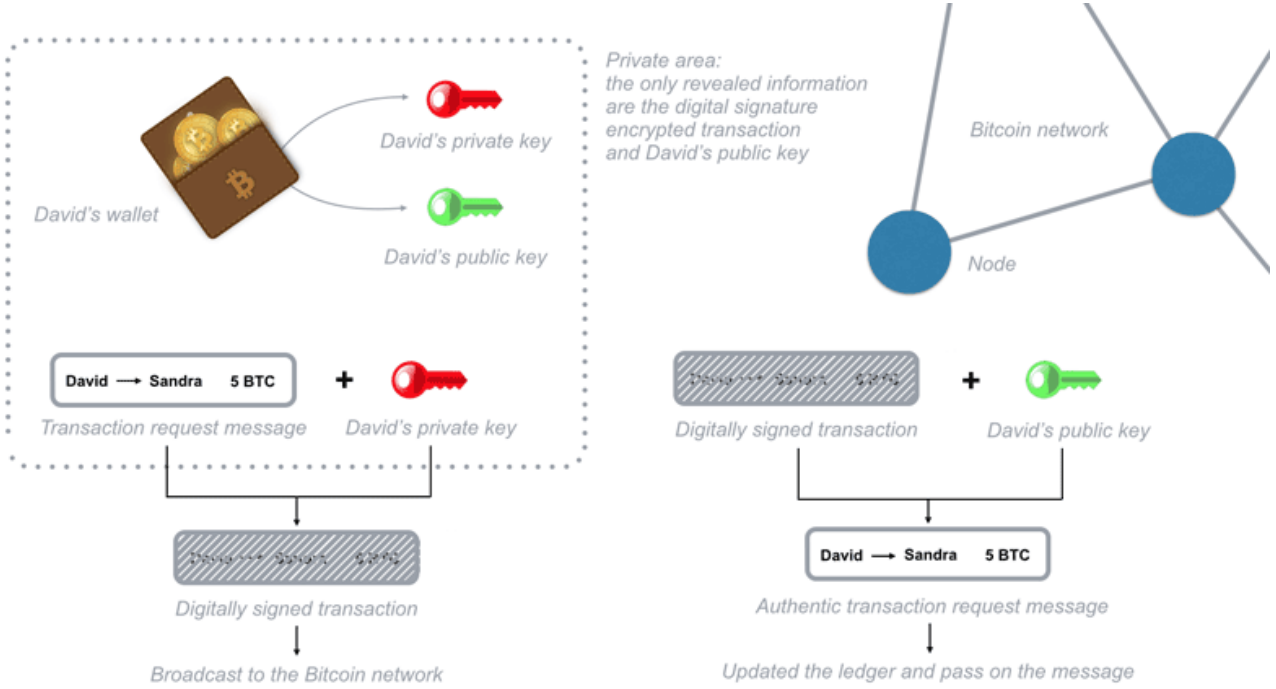
- Trong hệ thống ngân hàng, chúng ta chỉ biết các giao dịch và số dư tài khoản của riêng mình, trên blockchain mọi người có thể thấy mọi giao dịch khác của người khác.

- Trong khi bạn có thể tin tưởng vào ngân hàng của mình, mạng Bitcoin sẽ được phân phối và nếu có vấn đề gì đó không có sự trợ giúp để gọi hoặc bất cứ ai để kiện.
- Hệ thống blockchain được thiết kế theo cách mà không cần sự tin tưởng, độ an toàn và độ tin cậy thu được thông qua các chức năng toán học đặc biệt và code.

Để có thể thực hiện các giao dịch trên blockchain, bạn cần một ví, một chương trình cho phép bạn lưu trữ và trao đổi Bitcoin. Vì chỉ có bạn mới có thể chi tiêu được Bitcoin của mình, mỗi chiếc ví được bảo vệ bởi một phương pháp mật mã đặc biệt, sử dụng một cặp khóa riêng biệt khác nhau nhưng có kết nối: một khoá riêng tư (private) và công khai (public).

Nếu một thông điệp được mã hoá bằng khóa công khai cụ thể, chỉ chủ nhân của khóa riêng tư đã ghép nối mới có thể giải mã và đọc tin nhắn. Mặt khác, nếu bạn mã hóa tin nhắn bằng khóa cá nhân của bạn, chỉ có thể sử dụng khóa công khai được ghép nối để giải mã nó. Khi David muốn gửi Bitcoin, anh ta cần phát một tin nhắn được mã hóa bằng khoá riêng của ví của anh ta, vì vậy anh ta và chỉ có anh ta mới có thể sử dụng Bitcoin mà anh ta sở hữu, vì David là người duy nhất biết chìa khóa riêng của anh ta cần để mở ví của mình. Mỗi nút trong mạng có thể kiểm tra chéo yêu cầu giao dịch đến từ David bằng cách giải mã thông báo yêu cầu giao dịch với khóa công khai của ví của anh ta.

Khi mã hóa yêu cầu giao dịch với khóa riêng tư của ví của bạn, bạn sẽ tạo ra một chữ ký số được sử dụng bởi các máy tính trong mạng blockchain để kiểm tra lại nguồn và tính xác thực của giao dịch. Chữ ký số là một chuỗi văn bản, là kết quả của việc kết hợp yêu cầu giao dịch và khóa riêng tư của bạn, vì vậy nó không thể được sử dụng cho các giao dịch khác. Nếu bạn thay đổi một ký tự trong thông báo yêu cầu giao dịch, chữ ký số sẽ thay đổi, do đó không kẻ tấn công tiềm ẩn nào có thể thay đổi yêu cầu giao dịch của bạn hoặc thay đổi lượng Bitcoin bạn đang gửi.



Mã hoá giao dịch chữ ký số đơn giản hóa

Để gửi Bitcoin, bạn cần phải chứng minh rằng mình sở hữu khóa riêng của một ví cụ thể, vì cần sử dụng nó để mã hóa thông báo yêu cầu giao dịch. Lưu ý rằng, bạn chỉ phát thông báo sau khi nó đã được mã hóa, nên không bao giờ phải tiết lộ khóa riêng.

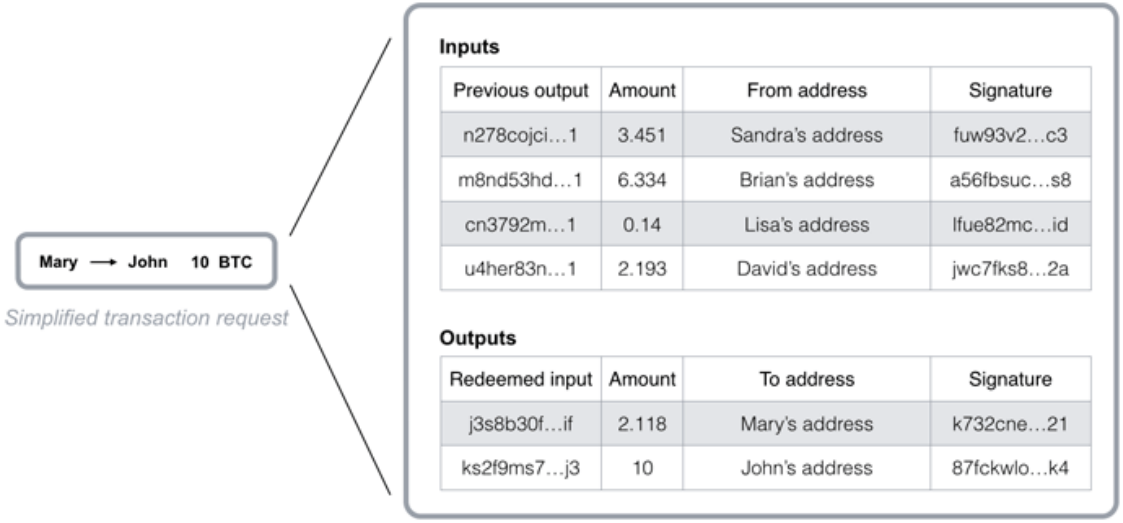
Mỗi nút trong blockchain đang giữ một bản sao của sổ cái. Vì vậy, làm thế nào một nút biết số dư tài khoản của bạn là bao nhiêu? Hệ thống blockchain không theo dõi các số dư tài khoản, nó chỉ ghi lại từng giao dịch được yêu cầu. Sổ sách trên thực tế không theo dõi số dư, nó chỉ theo dõi mọi giao dịch được phát đi trong mạng Bitcoin. Để biết số dư trong ví của bạn, bạn cần phải phân tích và xác minh tất cả các giao dịch đã từng diễn ra trên toàn bộ mạng kết nối với ví của mình.

LEDGER

Transactions	Value
Mary → John	10.000
John → Lisa	0.345
Sandra → David	18.4332
Lisa → Sandra	7.156
David → Mary	12.3402
Brian → Lisa	3.029381
…	…

Sổ cái Bitcoin

Xác minh số dư này được thực hiện nhờ liên kết đến các giao dịch trước đó. Để gửi 10 Bitcoin cho John, Mary phải tạo yêu cầu giao dịch bao gồm các liên kết tới các giao dịch đến (số tiền nhận được) trước đó có tổng số dư bằng hoặc vượt quá 10 Bitcoin. Các liên kết này được gọi là đầu vào, các nút trong mạng sẽ xác minh rằng tổng số tiền của các giao dịch này bằng hoặc vượt quá 10 Bitcoin và các đầu vào này chưa được chi tiêu. Trên thực tế, mỗi lần bạn tham chiếu các đầu vào trong một giao dịch được xem là không hợp lệ trong bất kỳ giao dịch nào trong tương lai. Tất cả được thực hiện tự động trong ví của Mary và kiểm tra lại bởi các nút mạng Bitcoin, cô ấy chỉ gửi một giao dịch 10 BTC đến ví của John sử dụng khóa công khai của anh ấy.



Cấu trúc yêu cầu giao dịch Bitcoin

Vậy, làm thế nào hệ thống có thể tin tưởng giao dịch đầu vào và xem xét chúng có giá trị? Nó kiểm tra tất cả các giao dịch trước đó có tương quan với ví bạn sử dụng để gửi Bitcoin thông qua các tham chiếu và đầu vào. Để đơn giản hóa và đẩy nhanh quá trình xác minh, một bản ghi đặc biệt về các giao dịch không được sử dụng sẽ được giữ bởi các nút mạng. Nhờ kiểm tra bảo mật này, bạn không thể tiêu gấp đôi số Bitcoin nhận được.

Tất cả các code để thực hiện giao dịch trên mạng Bitcoin là mã nguồn mở, điều này có nghĩa là bất cứ ai có máy tính xách tay và một kết nối Internet đều có thể thực hiện giao dịch. Tuy nhiên, nếu có một lỗi trong code được sử dụng để phát thông báo yêu cầu giao dịch, Bitcoin liên quan sẽ bị mất vĩnh viễn. Hãy nhớ rằng vì mạng được phân phối, nên không có dịch vụ hỗ trợ khách hàng nào để gọi cũng như bất cứ ai có thể giúp bạn khôi phục lại giao dịch bị mất hoặc mật khẩu ví bạn đã quên. Vì lý do này, nếu bạn quan tâm đến giao dịch trên mạng Bitcoin, bạn nên sử dụng mã nguồn mở và phiên bản chính thức của phần mềm ví Bitcoin (chẳng hạn như Bitcoin Core) và để lưu mật khẩu của ví của bạn hoặc khóa riêng tư vào kho lưu trữ rất an toàn.

- Cách tạo và dùng Ví Bitcoin, Ví Ethereum trên Blockchain

Những đặc điểm chính của BlockChain

Một cơ sở dữ liệu phân tán

Hãy tưởng tượng một bảng tính được nhân đôi hàng ngàn lần thông qua mạng lưới máy tính, mạng lưới này được thiết kế để cập nhật thường xuyên bảng tính đó là bạn đã có thể hiểu được cơ bản về blockchain.

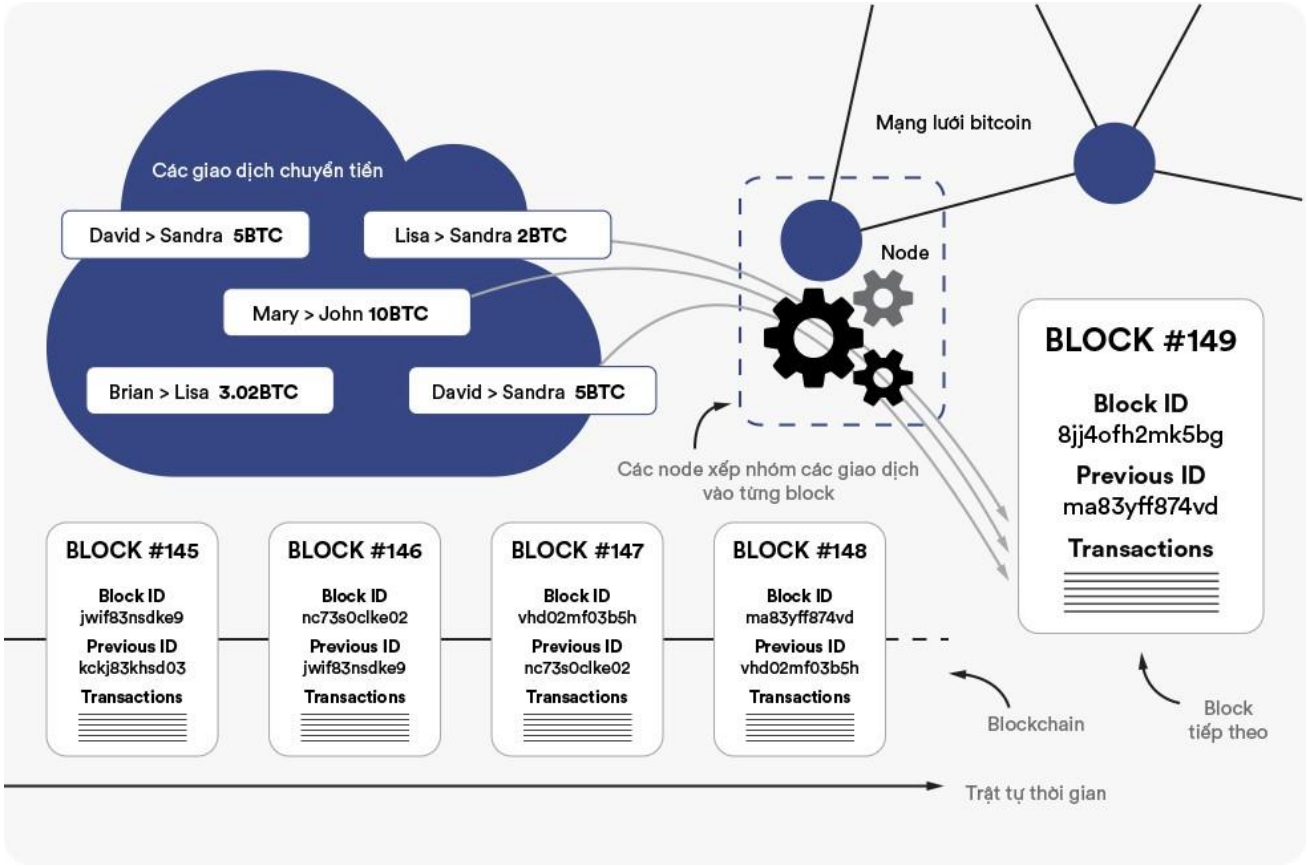
Thông tin được tổ chức trên một blockchain tồn tại dưới dạng cơ sở dữ liệu được chia sẻ và hòa hợp liên tục. Đây là cách để sử dụng mạng với những lợi ích rõ ràng. Cơ sở dữ liệu blockchain không được lưu trữ ở duy nhất một vị trí nào, nghĩa là các bản ghi được lưu trữ một cách công khai, dễ kiểm chứng. Không có một phiên bản tập trung nào của cơ sở dữ liệu này tồn tại, nên hacker cũng chẳng có cơ hội nào để tấn công nó. Blockchain được lưu trữ bởi hàng triệu máy tính cùng lúc, dữ liệu của nó có thể truy cập bởi bất cứ ai trên Internet.

Blockchain giống như Google Docs

Cách chia sẻ tài liệu thông thường khi cộng tác là gửi tài liệu Microsoft Word cho một người khác qua email và yêu cầu họ sửa nó. Vấn đề trong trường hợp này là bạn cần phải đợi cho đến khi nhận được một bản sao lưu được gửi trở lại thì mới có thể xem hoặc thực hiện những thay đổi khác, vì đã bị khóa quyền chỉnh sửa cho đến khi người cộng tác của bạn hoàn tất việc chỉnh sửa. Đó là cách cơ sở dữ liệu hiện tại đang hoạt động. Hai chủ sở hữu không thể cùng chỉnh sửa một bản ghi cùng một lúc. Đó là cách các ngân hàng duy trì số dư và

số chuyển khoản, họ nhanh chóng khóa quyền truy cập (hoặc giảm số dư) trong khi thực hiện chuyển khoản, rồi sau đó cập nhật tài khoản và mở lại quyền truy cập (hoặc cập nhật lại). Với Google Docs thì khác, cả hai bên đều có quyền truy cập đồng thời vào cùng một tài liệu và phiên bản duy nhất của tài liệu đó luôn hiển thị cho cả hai. Nó giống như sổ cái được chia sẻ, nhưng nó là một tài liệu được chia sẻ. Phần phân tán chỉ hoạt động khi chia sẻ liên quan đến một số người.

Lược dịch từ ý kiến của William Mougayar, cố vấn liên doanh, nhà kinh doanh 4x, nhà tiếp thị, chuyên gia chiến lược và chuyên gia blockchain.



Tính bền vững của blockchain

Công nghệ blockchain giống như Internet vì nó có một sức mạnh được tích hợp sẵn. Bằng cách lưu trữ những khối thông tin giống nhau trên mạng lưới của mình, blockchain không thể:

- Bị kiểm soát bởi bất kỳ một thực thể nào
- Không có điểm thiếu sót, lỗi duy nhất nào.

Bitcoin được phát hành vào năm 2008, kể từ đó, blockchain Bitcoin được vận hành, hoạt động mà không có sự gián đoạn đáng kể nào. Đến này, bất kỳ vấn đề nào liên quan đến Bitcoin là do hack hoặc quản lý kém. Nói cách khác, những vấn đề này đến từ ý định xấu và lỗi của con người, không phải là những sai sót tự thân của Bitcoin.

Internet đã chứng minh được độ bền trong gần 30 năm. Đây là bản ghi theo dõi tốt cho công nghệ blockchain khi nó tiếp tục được phát triển.

Minh bạch và không thể bị phá vỡ

Mạng lưới blockchain tồn tại trong trạng thái của sự thỏa thuận, tự động kiểm tra 10 phút một lần. Một loại hệ sinh thái tự kiểm soát giá trị kỹ thuật số, mạng lưới sẽ điều hòa mọi giao dịch xảy ra trong khoảng 10 phút. Mỗi nhóm giao dịch này được gọi là khối. Hai đặc tính quan trong được rút ra từ đây:

- Minh bạch: Dữ liệu được nhúng trong mạng như một khối, công khai.

- Nó không bị thể bị hỏng: Khi thay đổi bất kỳ đơn vị thông tin nào trên blockchain có nghĩa là sử dụng một lượng lớn máy tính để ghi đè lên toàn bộ mạng.

Về lý thuyết, điều này có thể xảy ra. Trong thực tế, nó không xảy ra. Ví dụ, việc kiểm soát hệ thống để chiếm lấy Bitcoin sẽ khiến giá trị của nó bị hủy hoại.

Một mạng lưới các nút

Một mạng lưới các nút tính toán tạo thành blockchain. Nút ở đây là máy tính được kết nối với mạng blockchain, sử dụng client để thực hiện nhiệm vụ xác nhận và chuyển tiếp các giao dịch. Nút sẽ nhận được một bản sao của blockchain, được tải tự động khi tham gia mạng lưới blockchain.

Các nút này cùng nhau tạo ra một mạng lưới cấp 2 mạnh mẽ, một góc nhìn hoàn toàn khác về cách mà Internet có thể hoạt động. Mỗi nút là một "quản trị viên" của mạng blockchain và tự động tham gia vào mạng, động lực cho việc tham gia này chính là cơ hội giành được Bitcoin.

Nút còn được gọi là đào Bitcoin, nhưng thuật ngữ này có chút nhầm lẫn. Trong thực tế, mỗi người đang cạnh tranh để giành Bitcoin bằng cách giải quyết những câu đố. Bitcoin là "lẽ sống" của blockchain ngay từ khi nó được hình thành. Bitcoin mới chỉ được công nhận như một phần rất nhỏ trong số những tiềm năng của công nghệ blockchain.

Có khoảng 700 loại tiền kỹ thuật số tương tự như Bitcoin, ngoài ra còn có rất nhiều những biến thể của khái niệm blockchain ban đầu hiện đang hoạt động hoặc đang được phát triển.

Ý tưởng về phân quyền

Theo thiết kế, blockchain là một công nghệ được phân quyền. Bất cứ điều gì xảy ra trên đó đều là chức năng của mạng. Một số gợi ý quan trọng bắt nguồn từ điều này. Nhờ tạo ra cách mới để xác nhận giao dịch mà những khía cạnh của thương mại truyền thống có thể trở nên không cần thiết. Ví dụ như những giao dịch trên thị trường chứng khoán có thể thực hiện cùng lúc trên blockchain, hoặc có thể lưu trữ tài liệu giống như sổ đỏ, hoàn toàn công khai. Và sự phân quyền đã trở thành hiện thực.

Mạng máy tính toàn cầu sử dụng công nghệ blockchain để cùng quản lý cơ sở dữ liệu, ghi lại các giao dịch của Bitcoin. Tức là, Bitcoin được quản lý bởi mạng của nó và không một ai là trung tâm cả. Phân quyền có nghĩa là mạng lưới hoạt động dựa trên cơ sở người dùng hay P2P. Các hình thức hợp tác tập thể có thể thực hiện chỉ mới bắt đầu được nghiên cứu.

Tăng cường bảo mật

Nhờ lưu trữ dữ liệu trên mạng của mình, blockchain loại bỏ những rủi ro đi kèm với dữ liệu được tổ chức tập trung. Mạng của nó không có những điểm dễ bị tổn thương. Trong khi đó, vấn đề bảo mật trên Internet thì ngày càng trở nên phức tạp. Chúng ta đều dựa vào hệ thống username/password để bảo vệ danh tính và tài sản của mình trên mạng, nhưng hệ thống này vẫn có nhiều khả năng bị phá vỡ. Phương pháp bảo mật của blockchain sử dụng công nghệ mã hóa với cặp khóa public/private. Khóa public (một chuỗi dài các số ngẫu nhiên) là địa chỉ của người dùng trên blockchain. Bitcoin gửi qua mạng sẽ được ghi nhận thuộc về địa chỉ đó. Khóa private giống như mật khẩu, cho phép chủ sở hữu truy cập vào Bitcoin hoặc các tài sản kỹ thuật số khác. Lưu trữ dữ liệu trên blockchain và nó sẽ không bị hư hỏng. Điều này là sự thật, mặc dù bảo vệ tài sản kỹ thuật số của bạn sẽ yêu cầu bảo mật khóa private bằng cách in ra, tạo ví kỹ thuật số để đựng giống như ví đựng tiền giấy.

Blockchain có thể dùng ở đâu?

Danh sách này được lấy từ bài viết "What is Blockchain Technology? A Step-by-Step Guide For Beginners" trên blockgeeks.com, mình đã lược bớt một số vì quá dài và khó hiểu, dưới đây là những gì còn lại:

Hợp đồng thông minh

Các sổ cái được phân chia cho phép mã hóa các hợp đồng đơn giản, sẽ được thực thi khi những điều kiện nhất định được thỏa mãn. Ethereum là một dự án blockchain mã nguồn mở, được xây dựng đặc biệt để đáp ứng yêu cầu này. Tuy nhiên, trong giai đoạn đầu phát triển, Ethereum có tiềm năng để tận dụng lợi thế của blockchain trên một quy mô lớn hơn như thế rất nhiều.

Ở cấp độ phát triển hiện tại của công nghệ, hợp đồng thông minh có thể được lập trình để thực hiện những chức năng đơn giản. Ví dụ, một giao dịch phát sinh có thể được thanh toán khi công cụ tài chính đáp ứng một số tiêu chuẩn, với việc sử dụng công nghệ blockchain và Bitcoin cho phép thanh toán tự động, không cần sự tham gia của con người hay bên trung gian làm chứng.

Kinh tế chia sẻ

Với những công ty như Uber, AirBnB, nền kinh tế chia sẻ đã chứng minh được những thành công ban đầu. Tuy nhiên, ở thời điểm hiện tại, người dùng muốn thuê dịch vụ chia sẻ xe phải dựa vào một trung gian là Uber. Bằng cách cho phép thanh toán ngang hàng, blockchain mở ra một cánh cửa mới để tạo sự tương tác trực tiếp giữa các bên, kết quả sẽ dẫn tới kinh tế chia sẻ được thực sự phân quyền.

Ví dụ, OpenBazaar sử dụng blockchain để tạo eBay ngang hàng. Tải ứng dụng về máy tính, bạn có thể giao dịch với nhà cung cấp OpenBazaar mà không phải

trả lệ phí giao dịch. Phong cách "không có quy tắc" của giao thức nghĩa là danh tiếng cá nhân trong tương tác kinh doanh còn quan trọng hơn cả bản thân tương tác đó trên eBay.

Mở rộng thị trường gọi vốn

Các sáng kiến thu hút vốn đầu tư như Kickstarter và Gofundme đang "dọn đường" cho nền kinh tế ngang hàng mới nổi này. Những trang web kể trên đã cho thấy mọi người muốn có tiếng nói trực tiếp trong việc phát triển sản phẩm. Blockchain đưa công việc này lên một cấp độ mới nhờ có khả năng tạo ra nguồn vốn mạo hiểm nhiều hơn cho các startup.

Năm 2016, đã có một minh chứng cho điều này. DAO (Decentralized Autonomous Organization), dựa trên Ethereum, đã gây vốn được 200 triệu USD chỉ trong vòng 2 tháng. Những người tham gia mua DAO được vote trên một hợp đồng thông minh về đầu tư mạo hiểm (quyền vote dựa trên số DAO họ đang nắm giữ). Số tiền mà dự án thu được đã chứng minh, dự án được đưa ra không cần thẩm định rủi ro. Như vậy, có thể thấy rằng, blockchain có tiềm năng để mở ra một mô hình mới cho hợp tác kinh tế.

Quản trị

Bằng cách tạo ra những kết quả minh bạch và có thể truy cập công khai, công nghệ cơ sở dữ liệu phân tán có thể mang lại sự minh bạch đầy đủ cho cuộc bầu cử hay bất cứ hình thức thăm dò nào khác. Những hợp đồng thông minh dựa trên Ethereum sẽ giúp tự động hóa toàn bộ quá trình.

Ứng dụng như Boardroom, cho phép tổ chức ra quyết định trên blockchain, nhờ đó giúp quá trình quản trị công ty trở nên minh bạch, kiểm chứng được tài sản số, sự công bằng hay những thông tin nội bộ.

Kiểm tra chuỗi cung ứng

Người tiêu dùng ngày càng muốn biết rằng có bao nhiêu phần trăm sự thật trong những tuyên bố về tiêu chuẩn sản phẩm của các công ty. Blockchain cung cấp cách thức xác nhận dễ dàng rằng những sản phẩm chúng ta mua là chính hãng. Tính minh bạch đi kèm với dấu thời gian dựa trên blockchain của ngày tháng, vị trí - ví dụ, trên viên kim cương, sẽ tương ứng với số sản phẩm.

Ở Anh có thể kiểm tra nguồn gốc xuất xứ của những mặt hàng tiêu dùng thông qua chuỗi cung ứng. Sử dụng blockchain Ethereum, dự án thí điểm kiểm tra chất lượng đảm bảo rằng cá được bán trong các nhà hàng Sushi của Nhật đã được các nhà cung cấp cá ở Indonesia khai thác đúng cách.

Lưu trữ file

Việc lưu trữ phân quyền trên Internet mang lại những lợi ích rõ rệt. Phân phối dữ liệu trong toàn mạng giúp bảo về các file không bị tấn công hoặc bị mất.

Inter Planetary File System (IPFS) giúp dễ dàng khái niệm hóa cách thức một trang web phân tán có thể hoạt động. Tương tự như cách bittorrent di chuyển dữ liệu trên Internet, IPFS sẽ loại bỏ nhu cầu về các mối quan hệ giữa máy chủ, máy khách. Một mạng Internet được tạo thành từ những trang web phân tán hoàn toàn có khả năng tăng tốc độ truyền file và thời gian stream. Sự cải tiến này không chỉ thuận tiện mà còn là một nâng cấp cần thiết cho những hệ thống phân phối nội dung trên web hiện đang quá tải.

Dự đoán thị trường

Sự chính xác của một sự kiện sẽ cao hơn khi có càng nhiều dự đoán về xác suất của sự kiện đó, điều này đã được chứng minh. Những sai lệch chưa được khảo sát có thể dẫn đến những phán đoán sai lầm. Việc lấy ý kiến trung bình từ những dự đoán sẽ giúp triệt tiêu bớt những sai lệch đó. Đã có những ứng dụng đầu tiên áp dụng blockchain trong việc dự đoán thị trường. Ví dụ như Augur, ứng dụng dự đoán thị trường còn đang trong giai đoạn phát triển. Nó đưa ra lời đề nghị chia sẻ về kết quả của các sự kiện trong thế giới thực. Người tham gia có thể kiếm tiền bằng cách mua vào những dự đoán chính xác. Càng nhiều cổ phiếu được mua vào theo dự đoán đúng, số tiền nhận được càng cao. Với một

khoản đầu tư nhỏ (ít hơn 1$), bất kỳ ai cũng có thể đặt câu hỏi, tạo một thị trường dựa trên kết quả dự đoán và thu được một nửa tổng số phí giao dịch mà thị trường tạo ra.

Bảo vệ quyền sở hữu trí tuệ

Như bạn đã biết, thông tin kỹ thuật số có thể bị sao chép vô hạn và phân phối rộng rãi nhờ Internet. Điều này đã giúp người dùng web trên toàn cầu có một mỏ vàng nội dung miễn phí. Tuy nhiên, chủ sở hữu bản quyền thì không may mắn như vậy, họ mất quyền kiểm soát sở hữu trí tuệ và số tiền lẽ ra phải thuộc về họ từ quyền đó. Hợp đồng thông minh có thể bảo vệ bản quyền và tự động hóa việc bán các tác phẩm trực tuyến, loại bỏ nguy cơ sao chép, phân phối lại.

Mycelia sử dụng blockchain để tạo một hệ thống phân phối nhạc ngang hàng. Được sáng lập bởi ca sĩ kiêm nhạc sĩ người Anh, Imogen Heap, Mycelia cho phép nhạc sĩ bán bài hát trực tiếp cho khán giả cũng như những mẫu giấy phép cho người sản xuất và chia lợi nhuận cho nhạc sĩ, ca sĩ, tất cả những chức năng này được thực hiện tự động hóa bằng những hợp đồng thông minh.

Internet of Things (IoT)

Nếu chưa biết về Internet of Things, bạn đọc tại đây nhé (Internet of Things - IoT hay Mạng lưới vạn vật kết nối là gì?). Hiểu nôm na, IoT là việc quản lý mạng lưới kiểm soát của một số loại thiết bị điện tử, ví dụ như nhiệt độ không khí

trong nhà kho. Hợp đồng thông minh có thể tự động hóa việc quản lý hệ thống này từ xa. Một sự kết hợp của phần mềm, cảm biến và mạng sẽ tạo điều kiện trao đổi dữ liệu giữa các đối tượng và cơ chế vận hành. Kết quả làm tăng hiệu quả làm việc của hệ thống và cắt giảm chi phí theo dõi.

Các nhà sản xuất lớn nhất trong lĩnh vực sản xuất, công nghệ và viễn thông đều đang tranh giành ngôi vị thống trị của IoT. Hãy nghĩ đến Samsung, IBM, AT&T. Việc mở rộng cơ sở hạ tầng hiện có được kiểm soát bởi con người bằng ứng dụng IoT sẽ thực hiện nhiệm vụ từ dự đoán các bộ phận cơ khí đến thống kê dữ liệu và quản lý hệ thống tự động trên quy mô lớn.

Quản lý danh tính

Nhu cầu xác thực danh tính trên web ngày càng trở nên bức thiết, nhất là đối với những giao dịch tài chính trực tuyến. Những giải pháp hiện có để phục vụ nhu cầu này chưa thực sự hoàn hảo. Với blockchain, chúng ta sẽ có những phương pháp nâng cao để chứng minh mình là ai, cùng với khả năng số hóa tài liệu cá nhân. Như trên đã nói, trong nền kinh tế chia sẻ hay các giao dịch kinh doanh, một danh tính tốt là vô cùng quan trọng.

Phát triển các tiêu chuẩn nhận diện kỹ thuật số là một quá trình rất phức tạp. Bên cạnh các thách thức về kỹ thuật, một giải pháp nhận diện trực tuyến phổ quát đòi hỏi sự hợp tác giữa các cá nhân và chính phủ. Thêm vào đó là cần

phải điều hướng hệ thống pháp luật ở các quốc gia khác nhau và vấn đề trở nên khó khăn theo cấp số nhân. Thương mại điện tử trên Internet hiện tại dựa trên chứng nhận SSL (khóa màu xanh lá cây nhỏ trên trình duyệt) cho những giao dịch bảo mật trên web. Nếu blockchain được áp dụng thì mọi việc sẽ trở nên dễ dàng hơn rất nhiều.

AML và KYC

Blockchain có tiềm năng mạnh mẽ trong vấn đề Anti-money laundering (AML) - chống rửa tiền và know your customer (KYC) - biết khách hàng của bạn. Hiện tại, các tổ chức tài chính phải thực hiện quy trình nhiều bước, đòi hỏi nhiều lao động để tìm kiếm khách hàng mới. Chi phí cho KYC có thể giảm xuống thông qua việc xác minh khách hàng đồng thời nâng cao hiệu quả giám sát và phân tích.

Polycoin, một startup có AML và KYC, liên quan đến việc phân tích các giao dịch. Những giao dịch được xác định là đáng ngờ được chuyển tiếp tới các bộ phận liên quan. Tradle, một startup khác đang phát triển ứng dụng có tên Trust in Motion (TiM). Được mô tả như "Instagram cho KYC", TiM cho phép khách hàng chụp ảnh nhanh các tài liệu chính (hộ chiếu, hóa đơn điện nước, v.v...). Sau khi được ngân hàng xác minh, dữ liệu này sẽ được lưu trữ như mật mã trên blockchain.

Giao dịch chứng khoán

Khả năng của blockchain trong thị trường chứng khoán đang được kiểm tra mạnh mẽ. Khi thực hiện ngang hàng, xác nhận giao dịch trở nên gần như tức thời. Nhờ vậy, những khâu trung gian như kiểm toán viên, người lưu ký,... có thể được loại bỏ.

Hệ thống lưới vi mô lân cận (Neighbourhood Microgrid)

Công nghệ blockchain cho phép mua và bán năng lượng tái tạo, được tạo ra bởi các lưới vi mô lân cận. Khi các tấm pin mặt trời làm cho năng lượng dư thừa, những hợp đồng thông minh dựa trên Ethereum sẽ tự động phân phối lại nó.

Những bất lợi khi sử dụng Blockchain

Blockchain không phải là một phép màu hay toàn là những điều quyến rũ, nó cũng có những trở ngại nhất định mà trong tương lai gần chúng ta cần phải khắc phục. Những quảng cáo hoặc lời thổi phồng xung quanh blockchain có thể khiến nhiều người mù quáng, không nhận ra sự thật rất rõ ràng rằng, blockchain tồn tại những bất lợi khi sử dụng khiến các ngành công nghiệp phải tìm cách giảm thiểu nó trước khi có thể áp dụng trên quy mô lớn.

Rất tốn điện

Vì mỗi blockchain đã sao chép chính mình đến mọi nút trên blockchain nên đã tạo ra một số lượng lớn những sự dư thừa. Mỗi lần giao dịch Bitcoin được thực hiện, nó được xác nhận nhiều lần vì có nhiều nút trên mạng. Quy trình này sử dụng rất nhiều điện. Các blockchain tư nhân có thể không bị ảnh hưởng nhiều vì họ có thể giới hạn các blockchain đến một số ít máy tính. Tuy nhiên, nếu là ngân hàng, phải xử lý hàng nghìn giao dịch mỗi phút trên toàn cầu, thì đây sẽ là vấn đề lớn.

Tốn không gian lưu trữ

Ngay bây giờ, để vận hành một nút trên blockchain Bitcoin, bạn phải tải xuống 60GB dữ liệu. Sẽ như thế nào nếu dữ liệu là 1 Terabyte? Nếu thị trường Bitcoin phát triển mạnh, sẽ có nhiều blockchain với dung lượng hàng Terabyte xuất hiện trong thực tế. Khi đó, chỉ có các trang trại máy chủ và những người thực sự quan tâm đến việc thương mại hóa tiền kỹ thuật số quy mô lớn, mới có thể vận hành toàn bộ các nút. Điều này sẽ tạo ra một mạng lưới tập trung, vốn được coi là một sự phân quyền kỳ lạ.

Tính không thể bị phá vỡ cũng có nhược điểm của nó

Giả sử bạn có một chiếc ví trên mạng, bạn bị mất chìa khóa chứng thực để mở ví đó. Không có liên kết để reset mật khẩu, không có hotline hỗ trợ. Bạn mất toàn bộ số tiền trong ví. Không có sự thu hồi. Bạn mất trắng.

Nếu biết cách xử lý dữ liệu một cách có trách nhiệm, bạn sẽ không gặp phải điều giả sử ở trên. Tiền của bạn vẫn sẽ ở trong túi của bạn, và tất nhiên, bạn có toàn quyền kiểm soát nó. Nhưng quyền lực luôn đi đôi với trách nhiệm, điều mà không phải ai cũng hiểu được. Những người như thế chính là nguyên nhân khiến cho 1/4 số Bitcoin trên trái đất biến mất mãi mãi.

Nếu bạn đặt một thứ gì đó lên blockchain, bạn phải thật chắc chắn là mình sẽ không hối hận. Vì giao dịch một khi được thực hiện sẽ không thể đảo ngược, hay làm lại. Nó sẽ ở trên blockchain mãi mãi, theo đúng nghĩa đen luôn.

Blockchain và Internet

Ngày nay chúng ta có thể phân chia thời đại công nghệ hiện đại thành hai giai đoạn đặc biệt: Trước Internet và sau Internet, đây là cách mà World Wide Web bị phá vỡ. Sự bùng nổ Internet đã làm thay đổi cách chúng ta thực hiện những giao dịch, liên lạc, chia sẻ thông tin, quảng bá kinh doanh, giải trí, nghiên cứu,...

Bạn sẽ nghĩ rằng tất cả mọi thứ chúng ta đang làm bây giờ gần như là phải kết nối Internet. Vâng, nhiều chuyên gia thích suy nghĩ rằng công nghệ blockchain có tiềm năng để tạo ra một cuộc cách mạng giống như Internet đã từng.

Dưới đây là một số khía cạnh của blockchain mà rất giống với Internet vào những năm trước 2000:

- Các chuyên gia đồng ý và hướng chúng ta chú ý đến blockchain, rằng nó có tiềm năng để thay đổi hầu hết mọi thứ.
- Những công ty lớn đang đầu tư vào blockchain và thử nghiệm nó cho những trường hợp sử dụng khác nhau, với những phản hồi rất tích cực về khả năng sử dụng của nó.
- Người ta đầu tư vào hầu hết các dự án liên quan đến blockchain. Ví dụ, Bioptix, một công ty niêm yết trên NASDAQ đã đổi tên thành Riot Blockchain và ngay lập tức giá cổ phiếu đã tăng lên 20%. Ở Anh, một công ty đầu tư đã đổi tên từ On-line Plc thành On-line Blockchain và giá cổ phiếu của nó đã có lúc nhảy lên đến 394%.
- Không có cơ sở hạ tầng blockchain ở cấp độ toàn cầu hay quốc tế, nhưng sự thu hút và số lượng người lao vào thí điểm thì rất lớn.
- Mọi người không thực sự hiểu nó là gì, nhưng họ chắc chắn nó có thể thay đổi cuộc sống của chúng ta.

Liệu lịch sử có lặp lại?

Một số chuyên gia đã đưa ra danh sách dài những điểm tương đồng giữa hai thời đại và hai hiện tượng, một số chuyên gia lại cảnh báo rằng blockchain có thể sẽ có kết cục giống như bong bóng dot com vào năm 1999, sau đó mới đạt đến thời điểm

chín muồi khi nó được chấp nhận rộng rãi. Điều này có nghĩa rằng, blockchain tạo điều kiện cho những tài sản bị định giá quá cao, có thể gây ra sự điều chỉnh thị trường trong tương lai, làm ảnh hưởng đến nhiều công ty và toàn bộ ngành.

Chúng ta không biết trước tương lai sẽ như thế nào, nhưng bất chấp sự thay đổi, khủng hoảng từ năm 1999, Internet đã không biến mất, nó vẫn tiếp tục con đường của mình bằng cách định hình toàn bộ ngành công nghiệp. Điều tương tự rất có thể cũng sẽ xảy ra với công nghệ blockchain.

Blockchain thực sự có thể biến đổi thị trường, vì chúng ta có thể kiểm soát được mọi giao dịch, hợp đồng hoặc bất kỳ sự di chuyển nào trong mạng. Chúng ta có thể làm cho các giao dịch và quy trình P2P trở nên minh bạch, được bảo mật với sự trợ giúp của mật mã, có dấu thời gian và dễ theo dõi. Điều này khác với Internet ngày nay, nơi các trung gian đóng vai trò quan trọng. Các công ty như Facebook, Google, chính phủ, ngân hàng, công ty công nghệ cao đều là những trung gian ảnh hưởng đến thông tin và quy trình trong mạng Internet. Blockchain loại bỏ những trung gian như vậy vì lợi ích của tất cả mọi người.