

CÔNG NGHỆ BLOCKCHAIN VÀ ỨNG DỤNG

Hoàng Xuân Thảo *

Tóm tắt: Sứ mạng của công nghệ là luôn đưa ra một công nghệ tốt hơn, đáp ứng nhu cầu của con người trong mọi hoạt động. Blockchain là một công nghệ như vậy. Nó là công nghệ nền trong nền công nghiệp 4.0, nó là Internet giai đoạn 2 và là môi trường giao dịch của tiền điện tử của tương lai.

Từ khóa: Blockchain, công nghệ Blockchain, xác nhận cộng đồng, khóa.

Abstract: The mission of technology is to always deliver a better technology that meets the needs of people in all activities. Blockchain is such a technology, it is the underlying technology in Industry 4.0, it is the second phase Internet and the environment for the cryptocurrency of the future.

Keywords: Blockchain, blockchain technology, public acknowledge, lock, key.

Trong mấy năm qua, chúng ta thường xuyên nghe thấy thuật ngữ “công nghệ Blockchain” có liên quan đến tiền điện tử Bitcoin. Blockchain là block (khối) và chain (chuỗi) dịch sang tiếng Việt là “chuỗi khối”. Vì không có mô hình trực quan thực sự nào để con người hiểu một cách dễ dàng, nên bắt buộc phải đặt câu hỏi: Blockchain là gì, công nghệ được sử dụng, cách thức hoạt động, và tại sao nó trở nên vô cùng quan trọng trong thế giới kỹ thuật số?

1. Công nghệ Blockchain là gì?

Để hình dung khái niệm “công nghệ Blockchain”, ta lấy một ví dụ đơn giản về quản lý điểm ở Trường Đại học Kinh doanh và Công nghệ Hà Nội (HUBT). Tập hợp các điểm sau khi thi kết thúc các học phần được tổ chức thành Cơ sở dữ liệu (CSDL) và gọi đó là Sổ cái. Sổ cái là khái niệm chung đại diện cho nhiều thứ, như sổ cái điểm, sổ cái về các công trình khoa học, sổ cái về tiền ảo, sổ cái về danh sách nhân sự, sổ cái về văn bằng, v.v. Ta

lưu Sổ cái điểm của HUBT trên 31 máy tính (Hình 1) có kết nối Internet (ứng với các khoa, phòng ban và một số lãnh đạo chủ chốt và gọi đó là 31 Nút). Mục đích của chúng ta là:

- Tạo thuận lợi cho cán bộ ở 31 Nút đó xem điểm dễ dàng;

- Một Nút muốn sửa điểm, phải có sự đồng thuận của cả 30 Nút còn lại, nếu không, sẽ bị khóa, không sửa được (đảm bảo quản lý chéo);

- Mỗi Nút có thể làm việc với Sổ cái để lọc điểm, xếp loại, in danh sách tốt nghiệp,... nhưng muốn sửa một cấu trúc hoặc một số điểm nào đó, phải được 30 Nút còn lại đồng thuận;

- Khi thêm điểm trong Sổ cái phải báo cho các Nút và được các Nút chấp thuận;

- Giả sử trên 31 Nút đó ta lưu 31 Sổ cái tiền ảo t_i của người n_i ; 31 Sổ cái của người $t_2, \dots, (t_p, t_2, \dots, t_{31})$ của 31 người và nếu một t_i nào đó muốn gửi tiền cho một t_k (i khác k), thì tất cả các Nút phải xác nhận và việc giao dịch mới được gọi là

* Khoa Công nghệ thông tin,
Trường ĐH KD&CN Hà Nội.

tồn tại và thành công. Cũng như bạn đến gửi tiền cho ai đó ở ngân hàng, thì bạn phải có hóa đơn của ngân hàng xác định bạn gửi để nếu mất thì ngân hàng đền. Ở đây không có khái niệm đền, vì “tập thể” đã xác nhận rồi và luôn đúng;



Hình 1. Blockchain

Ta thấy 31 máy trên như là một mạng quy ước của 31 người để thực thi một công việc nào đó. Vậy Blockchain là một công nghệ sổ cái phân tán được phát triển từ Internet. Trong khi kỷ nguyên đầu tiên của internet là trao đổi thông tin, thì Blockchain hứa hẹn sẽ trao đổi giá trị thực. Blockchain xuất hiện vào cuối năm 2008, giữa cuộc khủng hoảng tài chính toàn cầu. Satoshi Nakamoto đã phát hành một giao thức mới cho “hệ thống tiền điện tử” và tạo ra một loại tiền kỹ thuật số hoặc tiền điện tử gọi là Bitcoin dựa trên công nghệ chuỗi khối, với giao dịch bitcoin đầu tiên được thực hiện vào ngày 12 tháng 1 năm 2009. Tiền điện tử khác với tiền truyền thống ở chỗ, nó không được phát hành bởi một quốc gia. Chúng không được lưu trữ trong kho tiền ngân hàng hoặc tín dụng được ghi trong một tệp điện tử ở đâu đó; nó là một sổ cái của tất cả các giao dịch, sử dụng tài nguyên của một mạng lớn để xem xét và phê duyệt từng giao dịch Bitcoin. Blockchain không chỉ là tiền điện tử, mà có nhiều ứng dụng

hơn và các nhà đầu tư nhận ra tiềm năng thương mại của nó với tốc độ nhanh.

Blockchain có năm đặc tính, khiến nó trở thành một công nghệ có khả năng biến đổi và đột phá:

1) Phân phối

Một giao thức thiết lập một tập hợp các quy tắc dưới dạng các phép tính toán học phân tán để đảm bảo tính toàn vẹn của dữ liệu được trao đổi giữa một số lượng lớn các công trình điện toán, không cần thông qua một bên thứ ba. Mỗi chuỗi khối được chạy trên các máy tính do các sổ cái trên khắp thế giới cung cấp. Điều này có nghĩa là những thứ có giá trị cao như tiền, cổ phiếu, trái phiếu, quyền sở hữu trí tuệ, âm nhạc, xe hơi và thậm chí cả phiếu bầu,... đều có thể được lưu trữ và trao đổi mà không cần tổ chức hoặc người trung gian.

2) Được mã hóa

Blockchain sử dụng hệ thống xác thực hai khóa để duy trì bảo mật ảo.

3) Toàn diện và minh bạch

Trong trường hợp Blockchain công khai, bất kỳ ai cũng có thể xem tất cả các giao dịch tồn tại trên mạng, do đó không một người hoặc tổ chức nào có thể ẩn giao dịch. Blockchain là mã nguồn mở, nên bất kỳ ai cũng có thể tải xuống và sử dụng nó. Satoshi Nakamoto đã tưởng tượng ra một thế giới, trong đó, bất kỳ người nào cũng có thể giao tiếp với chuỗi khối thông qua “chế độ xác minh thanh toán đơn giản” có thể được sử dụng trên thiết bị di động. Không cần tài liệu hoặc bản trình bày về bằng chứng tin cậy để có được quyền truy cập.

4) Bất biến

Trong thời gian ngắn, tất cả các giao dịch được xác minh, xóa và lưu trữ trong một khối được liên kết với khối trước đó, do đó tạo ra một chuỗi. Mỗi khối tham

chiều đến khối trước đó mới hợp lệ. Cấu trúc này đánh dấu thời gian vĩnh viễn và lưu trữ các trao đổi giá trị, ngăn không cho bất kỳ ai thay đổi sổ cái.

5) Truy xuất đa chiều

Vì Blockchain là một sổ cái phân tán đại diện cho sự đồng thuận mạng của mọi giao dịch đã từng xảy ra, nên chuỗi khối phải được bảo toàn. Nó cho phép dễ dàng truy xuất nguồn gốc của các đối tượng trong sổ cái. Giá trị công nghệ mới này cho phép các giao dịch xảy ra trực tiếp giữa hai hoặc nhiều người lạ, được xác thực bởi sự cộng tác hàng loạt các thiết bị liên kết với nhau và được thúc đẩy bởi lợi ích tập thể. Nói tóm lại, Blockchain loại bỏ những người trung gian. Thuộc tính này cho phép các nhà phát triển xây dựng các ứng dụng cho một số mục đích khác nhau.

2. Ứng dụng thực tế và tiềm năng

1) Các dịch vụ tài chính

Bitcoin do Satoshi Nakamoto tạo ra là ứng dụng đầu tiên và nổi bật nhất của công nghệ Blockchain như một hệ thống thanh toán điện tử. Đây là một loại tiền kỹ thuật số độc lập với bất kỳ cơ quan ngân hàng nào, có thể chuyển nhượng điện tử với chi phí giao dịch thấp. Bên cạnh Bitcoin, còn có các loại tiền điện tử khác, như Litecoin, Ethereum, Ripple, Peercoin và Namecoin. Một loại tiền điện tử ổn định và được chấp nhận rộng rãi sẽ tạo nên cuộc cách mạng chuyển tiền và thậm chí cả thư tín dụng, thách thức đối với ngân hàng truyền thống. Hiện nay, tiền điện tử được giao dịch có giá trị hàng trăm tỷ đô-la trên phạm vi toàn cầu.

2) Bán lẻ và dịch vụ

Blockchain được sử dụng trong bán lẻ và dịch vụ. Bất kỳ người bán nào chấp nhận thanh toán bằng tiền kỹ thuật số đều có thể trao đổi hàng hóa và dịch vụ

này. Những cá nhân và công ty tham gia vào chuỗi giá trị cung ứng có thể sử dụng Blockchain riêng để giảm chi phí giao dịch trong các mối quan hệ kinh doanh của họ và thực hiện thanh toán và chuyển khoản một cách rất minh bạch, cho phép tiếp thị trực tiếp sản phẩm của mình, giảm vi phạm bản quyền phương tiện điện tử và đảm bảo thanh toán nhanh chóng và chính xác.

3) Nhận dạng kỹ thuật số

Phát hiện tệ nạn, phòng ngừa và chống lại hành vi trộm cắp, khôi phục danh tính sau khi bị xâm phạm là một hoạt động kinh doanh trị giá hàng chục tỷ đô-la hàng năm. Sử dụng công nghệ blockchain sẽ giúp theo dõi và quản lý hiệu quả và chi phí thấp. Danh tính có thể được xác thực duy nhất không thể chối cãi, bất biến và an toàn như hộ chiếu, cư trú điện tử, giấy khai sinh, giấy chứng nhận khác,...

4) Bỏ phiếu kỹ thuật số

Hai trong số những trở ngại lớn nhất đối với phiếu bầu điện tử và bỏ phiếu trực tuyến là bảo mật có thể bị vi phạm và phiếu bầu có thể bị thao túng. Bằng cách sử dụng Blockchain, một cử tri có thể xác minh xem phiếu bầu của mình có được chuyển đổi thành công hay không, mà vẫn ẩn danh, vì sổ cái phân tán trên toàn mạng, nên sẽ không thể thay đổi một phiếu bầu sau khi đã bỏ phiếu. Khả năng tổ chức bỏ phiếu điện tử có thể giúp giảm tỷ lệ thời gian đi lại và chờ đợi.

5) Hợp đồng pháp lý và công chứng

Các hợp đồng số hóa có thể lập trình ràng buộc về mặt pháp lý, có thể được ký kết trên một chuỗi khối và có thể được lập trình để giải phóng tiền bằng cách sử dụng mạng Bitcoin khi các điều khoản được đáp ứng, cho phép giảm nhu cầu về luật sư và các tổ chức trung gian khác. Các

cơ quan công chứng có thể được thay thế bằng cách có bằng chứng tồn tại kỹ thuật số, cho phép người dùng tải tệp lên và trả phí giao dịch và có bằng chứng mật mã về nó trên Blockchain. Dấu thời gian của khối trở thành dấu thời gian của văn bản ghi.

3. Tại sao Blockchain lại phổ biến?

Giả sử bạn đang chuyển tiền cho gia đình hoặc bạn bè từ tài khoản ngân hàng của mình. Bạn sẽ đăng nhập vào ngân hàng trực tuyến và chuyển số tiền cho người khác bằng số tài khoản của họ. Khi giao dịch được thực hiện, ngân hàng của bạn cập nhật hồ sơ giao dịch. Nó có vẻ đơn giản? Có một vấn đề tiềm ẩn mà hầu hết chúng ta đều bỏ qua. Các loại giao dịch này có thể bị giả mạo rất nhanh chóng. Những người quen thuộc với sự thật này thường cảnh giác với việc sử dụng các loại giao dịch truyền thống, do có sự phát triển của các ứng dụng thanh toán của bên thứ ba trong những năm gần đây. Những lỗ hổng này về cơ bản là lý do tại sao công nghệ Blockchain được tạo ra.

Về mặt công nghệ, Blockchain là một số cái kỹ thuật số đang được rất nhiều người chú ý và thu hút gần đây. Nhưng tại sao nó lại trở nên phổ biến như vậy?

Lưu trữ hồ sơ dữ liệu và giao dịch là một phần quan trọng của doanh nghiệp. Thông thường, thông tin này được xử lý tại nhà hoặc thông qua một bên thứ ba, như nhà môi giới, chủ ngân hàng hoặc luật sư, sẽ làm tăng thời gian, chi phí hoặc cả hai, cho doanh nghiệp. May mắn thay, Blockchain tránh được quá trình kéo dài này và tạo điều kiện cho giao dịch di chuyển nhanh hơn, do đó tiết kiệm cả thời gian và tiền bạc.

Hầu hết mọi người đều cho rằng Blockchain và Bitcoin có thể được sử dụng thay thế cho nhau, nhưng trên thực tế, không phải vậy. Blockchain là công

nghệ có khả năng hỗ trợ các ứng dụng khác nhau liên quan đến nhiều ngành, như tài chính, chuỗi cung ứng, sản xuất, v.v., còn Bitcoin là một loại tiền tệ dựa vào công nghệ Blockchain để được bảo mật.

Blockchain là một công nghệ mới nổi với nhiều ưu điểm trong thế giới kỹ thuật số:

1) An toàn cao

Nó sử dụng tính năng chữ ký điện tử để thực hiện các giao dịch không gian lận, không thể làm hỏng hoặc thay đổi dữ liệu của một cá nhân bởi những người dùng khác mà không có chữ ký số cụ thể.

2) Hệ thống phi tập trung

Thông thường, bạn cần sự chấp thuận của các cơ quan quản lý, như chính phủ hoặc ngân hàng, cho các giao dịch. Nhưng với Blockchain, các giao dịch trực tiếp được thực hiện với sự đồng thuận lẫn nhau của người dùng nên suôn sẻ hơn, an toàn hơn và nhanh hơn.

3) Khả năng tự động hóa

Nó có thể lập trình và có thể tự động tạo ra các hành động, sự kiện và thanh toán có hệ thống khi các tiêu chí của trình kích hoạt được đáp ứng.

4. Công nghệ Blockchain hoạt động như thế nào?

Trong những năm gần đây, nhiều doanh nghiệp trên thế giới sử dụng công nghệ Blockchain. Nhưng thật ra, công nghệ này hoạt động như thế nào? Là một thay đổi đáng kể hay chỉ là sự bổ sung đơn giản? Blockchain vẫn còn non trẻ và có tiềm năng mang tính cách mạng trong tương lai, vì vậy, hãy làm sáng tỏ đôi điều về nó. Blockchain là sự kết hợp của các công nghệ hàng đầu:

1) Khóa mật mã

Mạng ngang hàng có chứa số cái được chia sẻ. Máy tính để lưu trữ các giao dịch và hồ sơ của mạng, khóa mật mã bao gồm

hai khóa: Khóa riêng và Khóa công khai. Các khóa này giúp thực hiện các giao dịch thành công giữa hai bên. Mỗi cá nhân có hai khóa này, họ sử dụng để tạo ra một tham chiếu nhận dạng kỹ thuật số an toàn. Danh tính được bảo mật là khía cạnh quan trọng nhất của công nghệ blockchain. Trong thế giới tiền điện tử, danh tính này được gọi là “chữ ký số” và được sử dụng để ủy quyền và kiểm soát các giao dịch.

2) Chữ ký số được hợp nhất với mạng

Một số lượng lớn các cá nhân đóng vai trò là cơ quan chức năng sử dụng chữ ký số để đạt được sự đồng thuận trong các giao dịch, trong số các vấn đề khác, khi họ cho phép một giao dịch, giao dịch đó được xác nhận bởi một xác minh toán học, dẫn đến giao dịch bảo đảm thành công giữa hai bên được kết nối mạng. Vì vậy người dùng Blockchain sử dụng các khóa mật mã để thực hiện các tương tác kỹ thuật số khác nhau qua mạng.

3) Hợp đồng thông minh

Một bộ quy tắc, gọi là hợp đồng thông minh, được lưu trữ trên Blockchain và được thực thi tự động. Một hợp đồng thông minh có thể xác định các điều kiện để chuyển nhượng trái phiếu công ty, bao gồm các điều khoản về thanh toán bảo hiểm du lịch và hơn thế nữa.

4) Lợi ích của Blockchain

Các hoạt động thường bị lãng phí do lưu trữ hồ sơ trùng lặp và xác nhận của bên thứ ba. Hệ thống lưu trữ hồ sơ có thể dễ bị lừa đảo và tấn công mạng. Tính minh bạch có thể làm chậm quá trình xác minh dữ liệu, với sự xuất hiện của IoT, khối lượng giao dịch đã bùng nổ. Tất cả những điều này làm chậm lại hoạt động kinh doanh, giảm lợi nhuận, có nghĩa là chúng ta cần một cách khác tốt hơn. Với Blockchain, với tư cách là thành viên của mạng, bạn có thể yên tâm rằng bạn đang

nhận được dữ liệu chính xác và kịp thời; các bản ghi Blockchain bí mật của bạn sẽ chỉ được chia sẻ với các thành viên mạng mà bạn đã cấp quyền truy cập cụ thể. Tất cả các thành viên mạng đều có sự đồng thuận về độ chính xác của dữ liệu và tất cả các giao dịch đã được xác thực là không thay đổi, vì chúng được ghi lại vĩnh viễn. Không ai, ngay cả quản trị viên hệ thống, có thể xóa một giao dịch. Với sổ cái phân tán được chia sẻ giữa các thành viên trong mạng, việc điều chỉnh hồ sơ dẫn đến lãng phí thời gian, sẽ bị loại bỏ. Để tăng tốc độ giao dịch, hợp đồng thông minh được lưu trữ trên Blockchain và được thực thi tự động.

5. Các loại mạng Blockchain

Có một số cách để xây dựng mạng Blockchain. Nó có thể là công cộng, tư nhân, được ủy quyền hoặc được xây dựng bởi một tập đoàn.

1) Mạng Blockchain công cộng

Blockchain công cộng là một Blockchain mà bất kỳ ai cũng có thể tham gia, chẳng hạn như Bitcoin. Hạn chế có thể bao gồm yêu cầu tốc độ tính toán đáng kể, ít hoặc không có quyền riêng tư cho các giao dịch và bảo mật yếu. Đây là những cân nhắc quan trọng đối với các trường hợp sử dụng Blockchain của doanh nghiệp.

2) Mạng Blockchain riêng

Mạng Blockchain riêng, tương tự mạng Blockchain công cộng, là một mạng ngang hàng phi tập trung. Tuy nhiên, một tổ chức quản lý mạng kiểm soát ai được phép tham gia, thực thi giao thức đồng thuận và duy trì sổ cái được chia sẻ. Tùy thuộc vào trường hợp sử dụng, có thể tăng đáng kể sự tin cậy giữa những người tham gia. Một Blockchain riêng có thể được chạy sau tường lửa của công ty và thậm chí được lưu trữ tại cơ sở.

3) Các mạng Blockchain được phép

Các doanh nghiệp thiết lập một Blockchain riêng thường sẽ thiết lập một mạng Blockchain được cấp phép. Cần lưu ý là, các mạng Blockchain công cộng cũng có thể được cấp phép. Điều này đặt ra những hạn chế đối với những người được phép tham gia vào mạng và các giao dịch nhất định. Người tham gia cần nhận được lời mời hoặc sự cho phép tham gia.

4) Blockchain liên hợp

Nhiều tổ chức có thể chia sẻ trách nhiệm duy trì một Blockchain. Các tổ chức được chọn trước xác định ai có thể gửi giao dịch hoặc truy cập dữ liệu. Một chuỗi khối liên hợp là lý tưởng cho kinh doanh khi tất cả những người tham gia cần được cấp phép và có trách nhiệm chung đối với chuỗi khối.

5) Bảo mật chuỗi khối

Khi xây dựng một ứng dụng Blockchain doanh nghiệp, điều quan trọng là phải có một chiến lược bảo mật toàn diện sử dụng các khuôn khổ an ninh mạng, dịch vụ đảm bảo và các phương pháp tốt nhất để giảm rủi ro, chống lại các cuộc tấn công và gian lận. Blockchain là một phát minh lớn không thể phủ nhận, một đứa con tinh thần của một người hoặc

một nhóm người được biết đến với biệt danh Satoshi Nakamoto. Nhưng kể từ đó, nó đã phát triển thành một thứ gì đó vĩ đại hơn và câu hỏi chính mà mọi người đang quan tâm là: Công nghệ Blockchain có phải là dạng Internet mới? Bằng cách cho phép thông tin kỹ thuật số được phân phối, nhưng không được sao chép, công nghệ Blockchain đã tạo ra xương sống của một loại hình Internet mới. Ban đầu được phát minh cho tiền kỹ thuật số, chuỗi khối Bitcoin (mua Bitcoin), cộng đồng công nghệ hiện đã tìm thấy những ứng dụng tiềm năng khác cho công nghệ này. Hiểu một cách đơn giản hơn, Blockchain là một chuỗi các bản ghi dữ liệu không thay đổi được đóng dấu thời gian và quản lý bởi một nhóm máy tính không thuộc sở hữu của bất kỳ thực thể nào. Mỗi khối dữ liệu này được bảo mật và ràng buộc với nhau bằng cách sử dụng các nguyên tắc mật mã. Mạng lưới Blockchain không có cơ quan trung ương, nó là một sổ cái được chia sẻ và bất biến, thông tin trong đó được mở cho bất kỳ ai và mọi người đều có thể xem. Do đó, bất kỳ thứ gì được xây dựng trên Blockchain, về bản chất, đều là minh bạch và mọi người liên quan đều phải chịu trách nhiệm về hành động của mình./

Tài liệu tham khảo

1. Một số trang web nói về Blockchain.
2. Dr.H. Heler: Technology Blockchain.
3. Dr. Roner. Blockchain.
4. Prof. Dr. Shuman. Industry 4.0.
5. Prof. Dr. Shuman. BigData.
6. Dr. Hoàng Xuân Thảo. Lập trình mạng và các giáo trình tin học khác có liên quan.

Ngày nhận bài: **26/01/2021**

Ngày phản biện: **23/01/2021**

Ngày duyệt đăng: **01/03/2021**