

CÔNG NGHỆ CHUỖI KHỐI VÀ ỨNG DỤNG TRONG CUỘC SỐNG

● NGUYỄN THỊ NGỌC DIỄM

TÓM TẮT:

Chúng ta đang sống trong thời kỳ của cách mạng công nghệ, nơi sự sáng tạo không ngừng mở ra những tiềm năng đáng kể cho tương lai. Trong số những xu hướng đầy hứa hẹn, công nghệ chuỗi khối (Blockchain) đã thu hút sự quan tâm nhanh chóng và trở thành một yếu tố quan trọng trong lĩnh vực kỹ thuật số. Công nghệ chuỗi khối đã tạo ra những sản phẩm toàn cầu như tiền điện tử (ví dụ như Bitcoin) và NFT (Non Fungible Token), đồng thời thúc đẩy việc thực hiện giao dịch thông qua các hợp đồng thông minh và cải tiến hệ thống quản lý chuỗi cung ứng cũng như hệ thống tài chính. Blockchain ngày càng khẳng định vị trí của mình là công nghệ của tương lai. Tuy nhiên, thực tế cho thấy do sự thiếu hiểu biết về Blockchain, nhiều người có xu hướng phóng đại lợi ích của công nghệ này và không biết cách áp dụng nó vào công việc và cuộc sống. Bài viết giới thiệu những khái niệm cơ bản và cách hoạt động của Blockchain, trình bày các ứng dụng nổi bật của Blockchain trong cuộc sống cũng như thách thức mà công nghệ này đang đối mặt để cung cấp cái nhìn tổng quan.

Từ khóa: công nghệ chuỗi khối, Blockchain, hợp đồng thông minh.

1. Giới thiệu về công nghệ chuỗi khối (blockchain)

Blockchain, công nghệ nền tảng của Bitcoin và các loại tiền điện tử khác, là một cơ sở dữ liệu phân tán, công khai, cung cấp khả năng quản lý dữ liệu giao dịch phi tập trung. Điều làm cho blockchain trở nên độc đáo là nó hoạt động trên mạng ngang hàng (peer to peer network), nơi không có nút nào có thẩm quyền lớn hơn bất kỳ nút nào khác và là nơi bất kỳ người tham gia nào cũng có thể tham gia hoặc rời khỏi mạng theo ý muốn. Công nghệ blockchain đặc biệt phù hợp với các giao dịch yêu cầu đánh giá ngang hàng, xác định người tham gia, ra quyết định dân chủ, tạo sự đồng thuận hoặc các nguồn gốc xuất xứ và kiểm

toán vững chắc. Rõ ràng có rất nhiều ứng dụng tiềm năng trong lĩnh vực quản lý chất lượng (Tapscott và Tapscott, 2016).

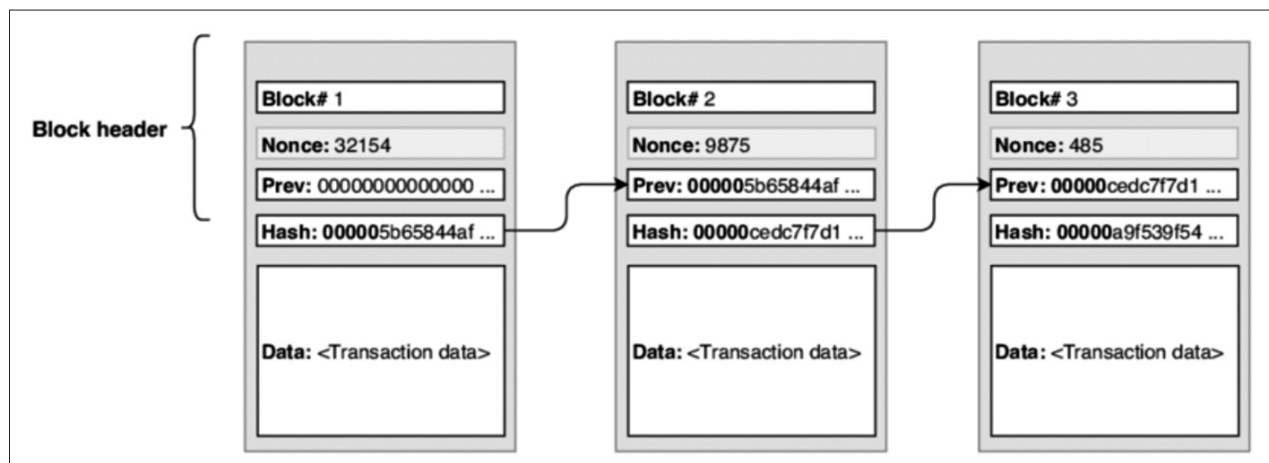
Blockchain = Block (khối) + Chain (chuỗi)

Blockchain là công nghệ lưu trữ và truyền tải thông tin bằng các khối được liên kết với nhau và mở rộng theo thời gian bởi một mạng lưới ngang hàng các máy tính. Đặc điểm chính của blockchain là tính toàn vẹn, an toàn và không thể thay đổi dữ liệu đã được ghi lại. Điều này đảm bảo tính minh bạch và tin cậy cho các giao dịch được thực hiện trên nền tảng này. Các công nghệ cơ bản áp dụng trong Blockchain gồm: Mật mã học nhằm đảm bảo tính minh bạch, toàn vẹn và riêng tư; Mạng lưới ngang hàng (P2P) để đảm bảo quyền hành các

node; và Lý thuyết trò chơi nhằm đảm bảo luật chơi đồng thuận của các node. Thực tế, một block khá phức tạp với nhiều thông số, tùy vào code của hệ thống. Đối với Blockchain Bitcoin, thông tin sẽ được trình bày thành các phần: (1) Số thứ tự, (2) Số Nonce, (3) Dữ liệu, (4) Hash - mã băm của chính nó và của khối liền kề trước nó (Hình 1).

ta cũng không thể thay đổi dữ liệu bởi điều đó có nghĩa chúng ta đang giả mạo dữ liệu và sẽ làm sai lệch đi mục đích của Blockchain. Chúng ta có thể tự do thay đổi giá trị của Nonce, điều này sẽ cho phép chúng ta thay đổi một cách ngẫu nhiên giá trị băm. Từ "ngẫu nhiên" ở đây bởi trong thuật toán băm, chúng ta không thể dự đoán trước nó sẽ

Hình 1: Thông tin của 1 khối trong Blockchain

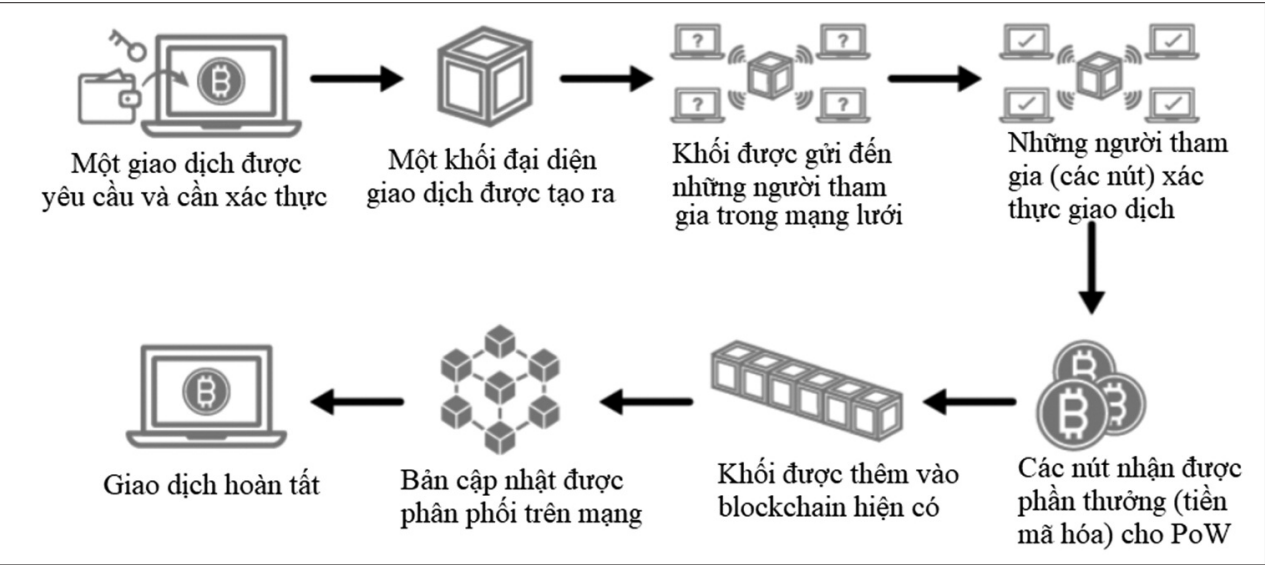


Nguồn: <https://anonystick.com/blog-developer/>

Trong một khối, giá trị băm của khối trước đó là một đặc điểm rất quan trọng trong Blockchain, vì đó là cách liên kết mật mã được tạo giữa các khối trong chuỗi. Nếu không có trường giá trị này, chuỗi khối sẽ không hoạt động. Và để có được giá trị băm của khối hiện tại chúng ta sẽ lấy tất cả 4 trường dữ liệu (bao gồm số khối, giá trị Nonce, giá trị của Data và giá trị băm của khối trước đó), và đưa chúng vào một thuật toán băm để thực hiện tính toán giá trị băm cho khối. Nonce (Number Only Used Once) là số được sử dụng một lần duy nhất (dài 32 bit) để giúp tạo ra mã băm thấp hơn mã chỉ tiêu để được chấp nhận đưa vào Blockchain. Trường Nonce sẽ giúp chúng ta kiểm soát giá trị băm của khối hiện tại và Nonce là ý tưởng chính trong hoạt động khai thác của máy đào (Mining). Hay nói cách khác, chúng ta có thể thay đổi giá trị băm (của khối hiện tại) bằng cách thay đổi Nonce để không phải thay đổi bất kỳ trường nào trong khối. Về nguyên tắc, chúng ta không thể thay đổi số khối, không thể thay đổi giá trị băm của khối trước đó, vì nó được liên kết trực tiếp với những gì đã có trong khối trước đó. Chúng

đưa ra giá trị gì. Nonce là số ngẫu nhiên, để tìm ra số Nonce phù hợp cho hàm băm thì thợ đào sẽ sử dụng phương pháp thử và sai hàng nghìn, thậm chí hàng triệu lần bằng cách sử dụng những siêu máy tính, thiết bị và phần mềm chuyên dụng để tìm ra số Nonce. Thợ đào không chỉ chịu áp lực tìm ra số Nonce mà còn phải nhanh hơn các thợ đào khác. Do đó, hệ thống máy móc không chỉ cần khả năng tính toán tốt mà còn xử lý với tốc độ nhanh nhất có thể. Mạng lưới Bitcoin được thiết kế để bổ sung một khối vào Blockchain cứ 10 phút một lần nên khi có thêm nhiều máy tính được thêm vào mạng lưới (đồng nghĩa công suất tính toán trên mạng lưới càng tăng khiến thời lượng ước đoán con số phù hợp khả dụng cho mỗi khối càng giảm), thì độ khó sẽ được điều chỉnh bằng cách giảm bớt chỉ tiêu mạng lưới (điều này đồng nghĩa với việc sẽ có ít mã băm hợp lệ được chấp nhận và loạt số cần ước đoán nhiều hơn mới có thể tạo nên một khối với mã băm hợp lệ). Chỉ tiêu độ khó được điều chỉnh mỗi 2.016 khối bằng cách điều chỉnh các số nhỏ nhất và số lớn nhất để đưa vào một khối. (Hình 2)

Hình 2: Cách giao dịch trong Blockchain Bitcoin



Nguồn: Euromoney Learning (2020)

Để giao dịch được xác thực (hay khối mới được thêm vào chuỗi) phải thỏa mãn điều kiện là thuật toán đồng thuận. Thuật toán đồng thuận trong blockchain là cơ chế giúp cho tất cả các nút trong mạng lưới đều đạt được một sự thống nhất. Có rất nhiều loại thuật toán đồng thuận, mỗi thuật toán sẽ có cách thức vận hành khác nhau. Hai thuật toán phổ biến nhất là bằng chứng công việc (PoW - Proof of Work) áp dụng trong Bitcoin và bằng chứng cổ phần (PoS - Proof of Stake) áp dụng trong Ethereum (trong đó Ethereum là chuyển đổi từ cơ chế PoW sang PoS). Sự khác biệt giữa hai thuật toán được trình bày trong Bảng 1.

Công nghệ Blockchain có rất nhiều lợi ích:

Tính minh bạch: Blockchain cung cấp nhiều

bước tiến to lớn trong việc cải thiện tính minh bạch khi so sánh với cách thức ghi chép hồ sơ và sổ cái hiện hành trong nhiều ngành công nghiệp. Công nghệ xây dựng dựa trên nền tảng Blockchain cung cấp sự rõ ràng tới toàn bộ mọi người trong mạng lưới, nhờ các giao dịch được thông báo tới mọi máy tính kết nối trong mạng lưới. Đa số các máy tính được liên kết trong Blockchain phải chấp nhận giao dịch hoặc sự thay đổi ở Blockchain, vì thế tránh được tình trạng che giấu hoặc ngụy tạo giao dịch.

Loại bỏ đơn vị trung gian: Các hệ thống xây dựng dựa trên công nghệ Blockchain cho phép loại bỏ các đơn vị trung gian liên quan đến hoạt động lập hồ sơ và chuyển giao tài sản. Blockchain đặc

Bảng 1. So sánh PoW và PoS

Bằng chứng công việc (PoW)	Bằng chứng cổ phần (PoS)
• Là thuật toán đồng thuận đầu tiên; • Hoạt động bằng cách khiến cho tất cả các nút thi nhau giải thuật toán để xác thực giao dịch; • Nút giải được thuật toán sẽ xác nhận giao dịch và nhận được phần thưởng là tiền mã hóa mới tạo; • Các nút tham gia vào việc xác thực sẽ được gọi là các thợ đào (Miners).	• Là thuật toán đồng thuận sau PoW; • Hoạt động bằng cách tất cả các nút đặt cược một lượng coin nhất định để được xác thực giao dịch; • Nút được chọn sẽ xác nhận giao dịch và nhận được phần thưởng là phí từ các giao dịch; • Các nút tham gia vào việc xác thực sẽ được gọi là các nhà xác thực (Validators).

Nguồn: S6kLabs (2022)

biệt hữu dụng trong những trường hợp khi mà niềm tin vào các đơn vị trung gian không tồn tại và hoạt động giao dịch trực tiếp giữa mọi người quá khó khăn hoặc rủi ro cao.

Phi tập trung: Các hệ thống xây dựng dựa trên công nghệ Blockchain có thể hoạt động trên mạng lưới máy tính phi tập trung, từ đó giảm thiểu rủi ro bị tấn công, thời gian chết trên máy chủ và thất thoát dữ liệu.

Độ bảo mật: Dữ liệu khi đã được đưa vào Blockchain sẽ bất khả sửa đổi, tức là không thể thay đổi hoặc chỉnh sửa do đó tránh được tình trạng gian lận qua việc ngụy tạo giao dịch và lịch sử dữ liệu. Một khối dữ liệu trên Blockchain đều có thể được truy ngược về “khối nguyên thủy”, tức khối đầu tiên và vì vậy cho phép dễ dàng thẩm tra và kiểm kê mọi giao dịch.

Tiềm năng ứng dụng rộng: Đa phần mọi giá trị đều có thể được lập hồ sơ dựa trên Blockchain và nhiều công ty trong nhiều lĩnh vực công nghiệp đã phát triển các hệ thống dựa trên công nghệ Blockchain. Gần như mọi giá trị đều có thể ghi lại trong Blockchain, cụm từ “mọi giá trị” không nhất thiết phải là giá trị tài chính; mà có thể là biên bản quyền sở hữu, chứng nhận bản quyền, tài liệu kỹ thuật số hoặc bất cứ thứ gì có thể được ghi vào cơ sở dữ liệu ngày nay.

Công nghệ dễ tiếp cận: Công nghệ Blockchain giúp việc tạo lập các ứng dụng dễ dàng hơn, nhờ các bước tiến hiện nay như nền tảng Ethereum và hợp đồng thông minh, mà không cần phải đầu tư quá nhiều vào cơ sở hạ tầng.

Tăng tốc độ giao dịch: Khả năng loại bỏ đơn vị trung gian và thiết lập trên sổ cái phân tán cho phép tăng tốc độ giao dịch cao hơn so với nhiều hệ thống hiện có (Mark Gates, 2017).

2. Ứng dụng blockchain trong cuộc sống

Ngày 27/01/2021, Chính phủ Việt Nam đã ban hành Quyết định số 130/QĐ-TTg về “Chương trình quốc gia phát triển công nghệ cao đến năm 2030”. Trong đó, có 4 công nghệ được đề cập đầu tiên chính là Trí tuệ nhân tạo, Internet kết nối vạn vật, Dữ liệu lớn và phân tích dữ liệu lớn, và Chuỗi khối. Đã có rất nhiều ứng dụng ra đời trên nền tảng chuỗi khối như tiền mã hóa (nổi bật nhất là Bitcoin), NFT (một loại token đại diện cho một tài

sản duy nhất, có thể là tài sản hoàn toàn kỹ thuật số hoặc phiên bản token hóa của tài sản trong thế giới thực), tài chính phi tập trung (DeFi)... Hay hợp đồng thông minh (Smart Contract) kế thừa các thuộc tính của chuỗi khối cơ bản. Không giống như các hợp đồng giấy truyền thống dựa vào người trung gian và bên thứ ba để thực hiện, hợp đồng thông minh tự động hóa các thủ tục hợp đồng, giảm thiểu tương tác giữa các bên và góp phần giảm chi phí hành chính so với mô hình tài chính truyền thống (Wang và cộng sự, 2020).

Bên cạnh đó, Blockchain còn được áp dụng trong rất nhiều ngành nghề để tăng cường tính hiệu quả và giảm thiểu chi phí, tiêu biểu như:

Quản lý chuỗi cung ứng: Blockchain cho phép theo dõi và xác minh toàn bộ quá trình sản xuất, vận chuyển và phân phối hàng hóa. Điều này giúp giảm thiểu rủi ro gian lận và làm giả dữ liệu trong chuỗi cung ứng, đồng thời tăng cường tính minh bạch và đáng tin cậy.

Ngành y tế: Blockchain có thể cung cấp quyền kiểm soát dữ liệu y tế cho người dùng và cải thiện quy trình chia sẻ thông tin giữa các nhà cung cấp dịch vụ y tế. Nó cũng có thể giúp theo dõi và quản lý chuỗi cung ứng dược phẩm, đảm bảo tính minh bạch và chống giả mạo.

Ngành tài chính: Blockchain có 8 chức năng vàng tác động sâu rộng đến lĩnh vực tài chính (Bảng 2).

3. Tầm nhìn và thách thức

Công nghệ chuỗi khối đã mang lại nhiều lợi ích đáng kể cho cuộc sống và các ngành công nghiệp. Tuy nhiên, cũng cần nhìn nhận và đối mặt với những thách thức hiện tại và tương lai. Một số thách thức này bao gồm vấn đề về bảo mật, quyền riêng tư, quy định pháp lý và khả năng mở rộng của công nghệ... Cụ thể như sau:

Những lo ngại về bảo mật: Các hệ thống dựa trên công nghệ Blockchain sử dụng mật mã học và mã hóa cao cấp an toàn hơn các mật khẩu tiêu chuẩn trên mạng Internet hay mã số truy cập. Vì tính minh bạch trong Blockchain, nếu khách hàng có khóa công khai, họ có thể xem số dư tài khoản và giá trị của nó nhưng không thể truy cập được. Và trong vài năm qua, có hàng tỷ USD tiền ảo bị mất do bị tấn công, gian lận hoặc bảo vệ kém.

Bảng 2. Cách mạng Blockchain của ngành dịch vụ tài chính

Chức năng	Ảnh hưởng của Blockchain	Các bên liên quan
1. Xác thực danh tính và giá trị	Các danh tính có thể xác thực và rõ ràng, an toàn mật mã.	Các cơ quan đánh giá, các phân tích dữ liệu người dùng, marketing, ngân hàng bán lẻ, ngân hàng bán buôn, mạng lưới thẻ thanh toán, các nhà quản lý.
2. Chuyển giao tài sản - Thực hiện thanh toán, chuyển tiền, mua bán hàng hóa và dịch vụ	Chuyển giao tài sản từ rất lớn tới rất nhỏ mà không qua trung gian sẽ làm giảm đáng kể chi phí và tốc độ thanh toán.	Ngân hàng bán lẻ, ngân hàng bán buôn, các mạng lưới thẻ thanh toán, các dịch vụ chuyển tiền, viễn thông, các nhà quản lý.
3. Lưu trữ tài sản - tiền tệ, hàng hóa và tài sản tài chính là những hình thức lưu trữ tài sản. Kết sắt, tài khoản tiết kiệm, hoặc tài khoản thanh toán. Quỹ thị trường tiền tệ hoặc tín phiếu kho bạc.	Cơ chế thanh toán kết hợp với hình thức lưu trữ đáng tin cậy và an toàn giúp giảm nhu cầu về các dịch vụ tài chính điển hình; tài khoản tiết kiệm và thanh toán ngân hàng sẽ trở nên lỗi thời.	Ngân hàng bán lẻ, ngành môi giới, ngân hàng đầu tư, doanh nghiệp quản lý tài sản, viễn thông, các nhà quản lý.
4. Cho vay tài sản - nợ thẻ tín dụng, thế chấp, trái phiếu doanh nghiệp, trái phiếu chính quyền địa phương, trái phiếu chính phủ, chứng khoán bảo đảm bằng tài sản và các hình thức tín dụng khác.	Các khoản vay có thể được phát hành, giao dịch và thanh toán trên Blockchain; tăng hiệu quả, giảm thiểu sự cản trở, cải thiện rủi ro hệ thống. Người tiêu dùng có thể dựa vào uy tín xã hội để tiếp cận với khoản vay từ thành viên ngang hàng; điều này có ý nghĩa quan trọng đối với những người không sử dụng ngân hàng và doanh nhân.	Ngân hàng bán buôn, ngân hàng thương mại, ngân hàng bán lẻ, tài chính công, hình thức cho vay vi mô, hình thức kêu gọi vốn cộng đồng, các nhà quản lý, các cơ quan xếp hạng tín dụng, các công ty phần mềm cho điểm tín dụng.
5. Giao dịch tài sản - đầu cơ, bảo hiểm rủi ro và kiểm soát chênh lệch giá. Khớp lệnh, xác minh giao dịch, quản lý tài sản thế chấp và định giá, thanh toán và lưu ký.	Blockchain cắt giảm thời gian giải quyết các giao dịch tốn nhiều ngày và tuần thành phút và giây. Tốc độ và hiệu quả sẽ mang lại cơ hội cho những người không sử dụng hoặc không đủ điều kiện sử dụng ngân hàng tạo lợi nhuận.	Đầu tư, ngân hàng bán buôn, các giao dịch viên trao đổi ngoại hối, quỹ phòng vệ, quỹ lương hưu, ngành môi giới bán lẻ, phòng thanh toán bù trừ, chứng khoán, các công cụ phái sinh, trao đổi hàng hóa; các nhà môi giới hàng hóa, các NHTW, các nhà quản lý.
6. Tài trợ và đầu tư tài sản, công ty, các công ty khởi nghiệp - tăng trị giá vốn, cổ tức, lãi suất, tiền thuê, hoặc một số hình thức kết hợp.	Tạo mô hình mới cho hệ thống tài chính ngang hàng, ghi lại các hoạt động của công ty cũng như cổ tức được trả tự động thông qua các hợp đồng thông minh. Đăng ký để tự động hóa việc nhận thu nhập và các hình thức sinh lợi khác.	Ngân hàng đầu tư, đầu tư mạo hiểm, pháp lý, kiểm toán, doanh nghiệp quản lý tài sản, chứng khoán, gọi vốn cộng đồng, các nhà quản lý.
7. Bảo đảm giá trị tài sản và quản lý rủi ro - bảo vệ tài sản, nhà cửa, mạng sống, sức khỏe, các sản phẩm phái sinh, tài sản kinh doanh và hoạt động kinh doanh.	Sử dụng hệ thống uy tín, các công ty bảo hiểm sẽ đánh giá tốt hơn những rủi ro kinh tế, tạo ra thị trường không tập trung cho bảo hiểm. Sản phẩm phái sinh sẽ trở nên minh bạch hơn.	Ngành bảo hiểm, quản lý rủi ro, ngân hàng bán buôn, ngành môi giới, phòng thanh toán bù trừ, các nhà quản lý.

Chức năng	Ảnh hưởng của Blockchain	Các bên liên quan
8. Kiểm toán tài sản - hệ thống quản trị công ty mới.	Công nghệ sổ cái phi tập trung của blockchain sẽ làm cho kiểm toán và báo cáo tài chính minh bạch và thực hiện trong thời gian thực, cải thiện đáng kể năng lực cho các nhà quản lý và các bên liên quan khác để kiểm soát các hoạt động tài chính trong một công ty.	Kiểm toán, doanh nghiệp quản lý tài sản, giám sát cổ đông, các nhà quản lý.

Nguồn: Tapscott và Tapscott (2016)

Nếu có người giành được quyền truy cập khóa cá nhân của bạn, họ có thể rút toàn bộ số tiền ra khỏi tài khoản của bạn và không có cách nào đảo ngược giao dịch đó hoặc yêu cầu đền bù. Vấn đề quan trọng là bạn không thể đặt lại mật khẩu trong trường hợp quên hoặc làm mất nó. Mọi tiến bộ trong mật mã học khiến người ta phải chép lại khóa cá nhân vào đâu đó, rồi giấu ở nhà hoặc trong máy tính, tất cả điều đó gây sụt giảm tính bảo mật nếu so sánh với phương thức bảo mật truyền thống. Còn nếu sử dụng các ví dựa trên nền tảng web do bên thứ ba cung cấp, mọi người phải hy sinh những lợi ích bảo mật của Blockchain chẳng hạn như khóa cá nhân để đổi lấy các mật khẩu truyền thống mà họ có thể đặt lại nếu chẳng may quên mất.

Thiếu tính riêng tư: Nhiều Blockchain phi tập trung không có tính riêng tư. Số dư tài khoản và các giao dịch đều có thể bị mọi người trên mạng lưới xem xét. Việc xác định danh tính một tài khoản trên Blockchain Bitcoin sau khi nhận được khoản thanh toán từ người đó tương đối dễ dàng. Nếu bạn đến một cửa hàng và thực hiện thanh toán, chủ cửa hàng có thể thấy giao dịch đó trên Blockchain. Thông tin trong giao dịch sẽ cho thấy khoản tiền được gửi từ ví nào, họ còn có thể kiểm tra tài khoản đó và biết được bạn sở hữu bao nhiêu tiền, cũng như toàn bộ các giao dịch xuất nhập từ tài khoản đó của bạn. Ý nghĩ về một Blockchain phi tập trung cung cấp rõ ràng từng giao dịch đơn lẻ, từ đó công khai mạng lưới để trở thành nỗi lo lắng của nhiều người, đặc biệt trong trường hợp mua sắm tại những cửa hàng nơi danh tính có thể liên kết trực tiếp tới tài khoản và giao dịch. Có nhiều Blockchain phi tập trung cung cấp mức độ bảo mật giao dịch cao hơn hoặc giới hạn người có thể truy cập để theo dõi thông tin. Tuy nhiên,

Bitcoin, Ethereum và nhiều đồng tiền ảo Blockchain quy mô lớn khác không vận hành theo cách đó và hiện tại không có kế hoạch tăng cường tính riêng tư cho giao dịch hay tài khoản.

Quy định và kết hợp: Các hệ thống dựa trên nền tảng Blockchain sẽ phải đối mặt với những vấn đề về luật định cùng với việc tốn kém thời gian và chi phí trong vấn đề phối hợp với các hệ thống hiện hành. Các chính phủ và ngân hàng phản đối thay đổi vì quy mô và chi phí thay thế hệ thống hiện thời quá lớn. Hội đồng Giám sát Độ Ổn định Tài chính (Financial Stability Oversight Council - FSOC) còn lo ngại rằng một số hệ thống dựa trên nền tảng Blockchain dễ bị gian lận hơn so với những nhận định thu được gần đây qua thử nghiệm trên quy mô nhỏ. Nhiều tổ chức tài chính lớn sẽ rất thận trọng với việc chuyển đổi sang bất cứ hệ thống nào mà các quy định của chính phủ chưa rõ ràng. Rủi ro kinh doanh và tài chính sẽ quá cao nếu các chính phủ không đưa ra quy định cụ thể về cách thức ứng xử đối với các tài sản dựa trên nền tảng Blockchain. Quan ngại về luật định, chi phí tích hợp cùng với việc thiếu thốn các ứng dụng hệ thống dựa trên nền tảng Blockchain trên quy mô lớn sẽ dẫn tới việc áp dụng chậm chạp công nghệ này vào các chính phủ và tổ chức tài chính lớn.

Không tồn tại quyền quản lý tập trung: Với một mạng Blockchain như Bitcoin, những sự thay đổi phải nhận được đồng thuận của một đa số nào đó trong mạng lưới, con số này có thể hơn 50% nhưng cũng có thể đạt tới 70% hoặc 80% mạng lưới. Không một tổ chức đơn lẻ nào kiểm soát các thay đổi hoặc định hướng trong Blockchain phi tập trung, điều này khiến các tổ chức sử dụng có nguy cơ gặp rủi ro khi giao dịch, vì họ không thể kiểm soát được thay đổi nào trong hệ thống.

Rủi ro từ tấn công quá bán: Nhiều máy tính vận hành Blockchain trên quy mô toàn cầu được đặt tại các quốc gia nơi mà người dân không an tâm vì vấn đề tội phạm, hệ thống pháp luật và tình trạng thiếu các quy định. Chi phí điện thấp và chi phí máy tính tại nhiều quốc gia đã tạo nên nhiều trung tâm khai thác khối lớn trên Blockchain. Nếu những trung tâm dữ liệu này liên kết lại với nhau, chúng có khả năng kiểm soát hơn 50% mạng lưới và chiếm quyền quản lý mạng lưới. Nếu tận dụng được quyền kiểm soát trên mạng lưới tiền ảo này, theo lý thuyết, họ có thể khiến các giao dịch mới không được xác nhận, đảo chiều giao dịch và cho phép “giao dịch lặp chi” tại hai xảy ra. Một cuộc tấn công quá bán trên mạng lưới Blockchain thường được coi là lý thuyết vì để kiểm soát một số lớn trên mạng lưới rất khó khăn. Tuy nhiên, có nhiều trang trại khai thác khổng lồ đặt tại Trung Quốc, Nga và nhiều nơi khác trên thế giới nắm quyền kiểm soát phần lớn công suất tính toán trong mạng lưới Blockchain. Nếu những trang trại khai thác khổng lồ này liên kết lại với nhau, họ có khả năng chiếm dụng mạng lưới Blockchain và thao túng mạng lưới vì lợi ích riêng.

Công nghệ chưa được kiểm chứng: Các công nghệ Blockchain là công nghệ mới chưa được chứng thực và được sử dụng chủ yếu trong các loại tiền ảo. Điều này vẫn hạn chế các công ty hoặc phần mềm thực tế sử dụng công nghệ Blockchain để chứng minh hiệu quả cao hơn các hệ thống hiện có.

Chi phí: Cần lượng điện năng lớn để vận hành. Theo ước tính, cứ nửa giờ mạng Blockchain tiêu thụ lượng điện bằng lượng điện mà các hộ gia đình thông thường tại Mỹ sử dụng trong trọn 1 năm. Các tính toán về lượng tiêu thụ điện năng dựa trên lượng tiêu thụ điện hộ gia đình thông thường tại Mỹ vào khoảng 10.000 - 12.000 kWh. Số lượng này bằng với lượng điện để sản sinh ra 4 khối trên Blockchain Bitcoin. Do chi phí điện năng vận hành máy tính trên mạng Blockchain sử dụng thuật toán PoW rất cao, nên rất lợi thế cho những quốc gia có nguồn điện giá rẻ hoặc cho các tổ chức có những thỏa thuận với các công ty năng lượng. Vì độ khó của các mảnh ghép trên Blockchain tăng, nên lượng tiêu thụ điện năng cũng sẽ tăng, điều này

khiến chi phí càng cao và đòi hỏi càng nhiều nguồn lực để vận hành Blockchain sử dụng thuật toán PoW trên quy mô lớn.

Vấn đề về khả năng mở rộng: Mạng lưới Blockchain chưa được chứng minh rằng có hiệu quả sánh ngang với các hệ thống hiện có. Mạng lưới Bitcoin chỉ có thể xử lý khoảng 7 giao dịch một giây, trong khi mạng lưới Visa có thể xử lý trên 20.000 giao dịch một giây. Một giao dịch trên Blockchain Bitcoin sẽ cần tối thiểu 10 phút mới được bổ sung vào Blockchain nên các công ty có thể sẽ phải chờ nhiều khối được thêm vào hơn trước khi xác nhận giao dịch (đối với Bitcoin là 6 khối được thêm vào), để đảm bảo rằng giao dịch sẽ không bị đảo chiều. So sánh sự khác biệt giữa hai phương thức này, nếu khách hàng định mua hàng và thanh toán bằng Bitcoin, chủ cửa hàng có thể sẽ phải chờ một tiếng để chắc chắn rằng giao dịch đã được xác nhận sau khi nhiều khối khác phía trên khối chứa giao dịch đã được bổ sung vào chuỗi. Có những mạng Blockchain nhanh hơn mạng Bitcoin nhiều nhưng lại không được phổ biến hoặc được chấp nhận là một hình thức thanh toán như Bitcoin. Nhưng ngay cả những Blockchain và các loại tiền ảo sở hữu thời gian xác nhận giao dịch nhanh hơn cũng không có khả năng sánh được với trình độ của các mạng thanh toán tài chính đương thời như Visa hay MasterCard.

Sự thiếu hiểu biết về công nghệ Blockchain: Cách thức Blockchain hoạt động và lợi ích của nó rất khó hiểu với nhiều người. Nhiều người còn lo ngại về các phương diện trên mạng lưới Blockchain như số dư và giao dịch của họ bị công khai. Ngay cả khi hiểu được các lợi ích, nhiều người vẫn thích các hệ thống hiện hành hơn. Blockchain chỉ là một hình thức dữ liệu mới, không phải một giải pháp quyền năng như thường bị phóng đại.

4. Kết luận

Công nghệ chuỗi khối đã trở thành một tiền đề quan trọng cho sự tiến bộ của xã hội và kinh tế. Ứng dụng của nó trong cuộc sống hàng ngày đang mở ra những cơ hội mới và tiềm năng vô tận. Song bên cạnh những lợi ích hay đặc tính tuyệt vời của blockchain, vẫn còn khá nhiều những khiếm khuyết và thách thức cần được tiếp tục nghiên cứu, khám phá và khắc phục ■

TÀI LIỆU THAM KHẢO:

1. Euromoney Learning. (2020). How does a transaction get into a blockchain? Truy cập tại link <https://www.euromoney.com/learning/insights/blockchain/blockchain-explained/how-transactions-get-into-the-blockchain>
2. S6kLabs. (2022). Ứng dụng đầu tiên. Truy cập tại link <https://www.youtube.com/watch?v=-5Eat0cQnKU>
3. Tapscott, D. và Tapscott, A. (2016). Blockchain Revolution: How the Technology Behind Bitcoin is Changing Money, Business, and the World. New York: Penguin Random House.
4. Wang, Y., Kim, D. K., và Dongwon J. (2020). A Survey of the Application of Blockchain in Multiple Fields of Financial Services. Journal of Information Processing Systems, 16(4), 935-958.
5. Mark Gates. (2017). Blockchain - Bản chất của Blockchain, Bitcoin, tiền điện tử, hợp đồng thông minh và tương lai của tiền tệ. NXB Lao Động, Thành Dương dịch.

Ngày nhận bài: 4/3/2024

Ngày phản biện đánh giá và sửa chữa: 16/3/2024

Ngày chấp nhận đăng bài: 6/4/2024

Thông tin tác giả:

TS. NGUYỄN THỊ NGỌC DIỄM

Khoa Tài chính Kế toán, Trường Đại học Sài Gòn

THE BLOCKCHAIN TECHNOLOGY AND ITS PRACTICAL APPLICATION

● Ph.D **NGUYEN THI NGOC DIEM**

Faculty of Finance - Accounting

Saigon University

ABSTRACT:

We are in a technological revolution with promising technological innovations that significantly change socio-economic aspects and open great opportunities for the future. Among these technology trends, blockchain technology has attracted rapid interest and has become an important factor in the digital sector. Blockchain technology has created global products such as cryptocurrencies (e.g., Bitcoin) and NFTs (non-fungible tokens). It also facilitates transactions through smart contracts and improves supply chain management systems as well as financial systems. However, due to a lack of understanding about blockchain, many people tend to exaggerate the benefits of this technology and do not know how to apply it to work and life. This paper introduced the basic concepts and how blockchain works, presented outstanding applications of blockchain in life, and discussed the challenges this technology is facing.

Keywords: blockchain technology, Blockchain, smart contracts.