ĐẠI HỌC KINH TẾ QUỐC DÂN

TRƯỜNG ĐẠI HỌC CÔNG NGHỆ - KHOA CÔNG NGHỆ THÔNG TIN

BÁO CÁO CÁC CÔNG NGHỆ HIỆN ĐẠI TRONG CÔNG NGHỆ THÔNG TIN

Tìm hiểu về Blockchain, các giải pháp Blockchain

Giảng viên hướng dẫn: Nguyễn Trung Tuấn

Lớp: Công nghệ thông tin 64B

Thành viên nhóm: Nguyễn Thị Yến – 11227076

Phạm Quang Tú – 11226675

Nguyễn Ngọc Vượng –11236236

Trần Duy Việt – 11226912

Nguyễn Trọng Vỹ – 11227025

Phạm Thành Vinh – 11226937

Hà Nội - 2024

MỤC LỤC

LỜI MỞ ĐẦU

Trong thế giới công nghệ phát triển mạnh mẽ và đa dạng hiện nay, Blockchain đã nổi lên như một trong những từ khóa quan trọng nhất, thu hút sự quan tâm không chỉ từ giới chuyên gia mà còn từ cả công chúng. Là nền tảng đằng sau sự phát triển vượt bậc của các loại tiền điện tử như Bitcoin, Blockchain đang được đánh giá là cuộc cách mạng công nghệ có thể thay đổi hoàn toàn cách chúng ta lưu trữ, quản lý và chia sẻ dữ liệu. Đặc biệt, với tính chất phi tập trung, minh bạch và an toàn, Blockchain đã trở thành nền tảng của các hệ thống lưu trữ dữ liệu trong nhiều lĩnh vực, từ tài chính, chuỗi cung ứng, đến giáo dục và năng lượng.

Tại Việt Nam, sự quan tâm đối với Blockchain đang gia tăng, kéo theo sự xuất hiện của nhiều dự án và ứng dụng dựa trên công nghệ này. Nhiều công ty công nghệ lớn trong nước và các doanh nghiệp khởi nghiệp đã bắt đầu tích hợp Blockchain vào sản phẩm và dịch vụ của mình nhằm nâng cao độ tin cậy và bảo mật cho người dùng. Ví dụ, trong lĩnh vực tài chính, Blockchain giúp cải thiện hiệu quả giao dịch, giảm chi phí trung gian và gia tăng độ minh bạch, giúp các ngân hàng và tổ chức tài chính hoạt động hiệu quả hơn. Trong chuỗi cung ứng, công nghệ này cho phép theo dõi nguồn gốc hàng hóa một cách minh bạch và bảo đảm tính xác thực, từ đó giảm thiểu các vấn đề liên quan đến hàng giả, hàng nhái.

Công nghệ Blockchain không chỉ giới hạn trong lĩnh vực kinh doanh mà còn có những ảnh hưởng tích cực đến đời sống xã hội. Trong giáo dục, Blockchain có thể được sử dụng để lưu trữ hồ sơ học tập của học sinh, sinh viên một cách an toàn và dễ dàng chia sẻ giữa các cơ sở giáo dục, giảm thiểu tình trạng giả mạo văn bằng. Trong ngành năng lượng, Blockchain còn giúp quản lý hiệu quả việc trao đổi và tiêu thụ năng lượng trong các hệ thống lưới điện thông minh, góp phần thúc đẩy phát triển bền vững.

Tuy nhiên, Blockchain không phải là một công nghệ đơn giản mà ai cũng có thể hiểu rõ. Để hiểu được tiềm năng và những ứng dụng thực tiễn của nó, chúng ta cần nắm vững nguyên lý hoạt động và cấu trúc của công nghệ này. Vậy, Blockchain là gì, và tại sao nó được đánh giá cao đến vậy? Trong báo cáo này, nhóm 10 chúng em xin trình bày chi tiết về bản chất của Blockchain, cách nó hoạt động, cũng như những tác động mà công nghệ này mang lại cho cuộc sống hàng ngày của chúng ta. Qua đó, chúng em hy vọng có thể cung cấp cái nhìn toàn diện và sâu sắc hơn về một trong những công nghệ đột phá nhất của thời đại.

I. CÁC KHÁI NIỆM CƠ BẢN TRONG BLOCKCHAIN

1. Khái niệm và sự ra đời của blockchain

Bitcoin là một loại đồng tiền ảo với hai đóng góp lớn: một hệ thống tiền tệ kỹ thuật số hoạt động liên tục và một mô hình cho công nghệ ứng dụng phi tập trung tự động được gọi là blockchain.

Bitcoin được một người hoặc nhiều người bí ẩn tự xưng là Satoshi Nakamoto tạo ra vào khoảng năm 2008, 2009. Bitcoin tạo nên một nền tảng sáng tạo để giao dịch ngang hàng mà không cần đến một cơ quan thẩm định trung ương nào. Như vậy thì làm thế nào để Bitcoin có được sự tin tưởng và bảo mật trong giao dịch? Bằng cách cài đặt các chương trình phần mềm dành cho kiểm chứng, xác thực, đồng thuận trong một cơ sở hạ tầng mới gọi là ***blockchain***.

Blockchain là "một cơ sở dữ liệu phân tán duy trì một danh sách các bản ghi được sắp xếp liên tục tăng lên, được gọi là các khối". Các khối này "được liên kết bằng mật mã". Mỗi khối chứa một mã băm của khối trước đó, dấu thời gian và dữ liệu giao dịch. Blockchain là một sổ cái kỹ thuật số phi tập trung, phân tán và công khai được sử dụng để ghi lại các giao dịch trên nhiều máy tính để bản ghi không bị thay đổi hồi tố mà không có sự thay đổi của tất cả các khối tiếp theo và sự đồng thuận của mạng.

Tại sao blockchain lại quan trọng? Trong bối cảnh thời kỳ công nghiệp 4.0, thông tin nhận được càng chính xác càng tốt. Blockchain rất lý tưởng để cung cấp thông tin vì nó cung cấp thông tin ngay lập tức, được chia sẻ và có thể quan sát được lưu trữ trên một sổ cái bất biến mà chỉ các thành viên mạng được cấp phép mới có quyền truy cập. Mạng blockchain có thể theo dõi đơn đặt hàng, thanh toán, tài khoản, sản xuất và nhiều hơn nữa.

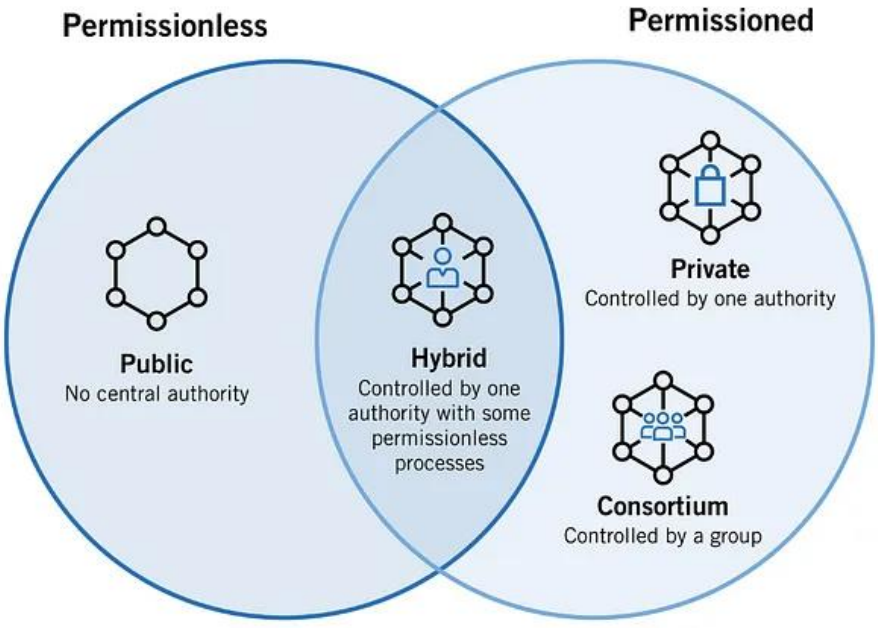
2. Phân loại blockchain

Hệ thống blockchain có 4 loại chính:

- Public blockchain:
  - Bất kỳ ai cũng có quyền đọc và ghi dữ liệu trên Blockchain. Quá trình xác thực giao dịch trên Blockchain này đòi hỏi phải có rất rất nhiều nút tham gia. Muốn tấn công được vào hệ thống Blockchain này cần chi phí rất lớn và thực sự không khả thi.
  - Blockchain công khai được thiết kế với mục đích phi tập trung hoàn toàn. Vì vậy sẽ không có sự kiểm soát của bất kỳ cá nhân hay tổ chức nào với các giao dịch được lưu trữ hoặc xử lý trên chuỗi khối.
  - Tuy nhiên, quá trình xác thực giao dịch blockchain sẽ diễn ra rất lâu bởi chúng cần nhiều nút tham gia.
  - Ví dụ điển hình nhất là Bitcoin và Ethereum.
- Private blockchain:

- Người dùng chỉ được quyền đọc dữ liệu, không có quyền ghi vì điều này thuộc về bên tổ chức thứ ba tuyệt đối tin cậy. Vì đây là một Private Blockchain, cho nên thời gian xác nhận giao dịch khá nhanh vì chỉ cần một lượng nhỏ thiết bị tham gia xác thực giao dịch.
- Private blockchain mang tính tập trung hoá hơn so với blockchain do thuộc quyền quản trị của một thực thể nhất định.
- Ví dụ: Ripple là một dạng Private Blockchain, hệ thống này cho phép 20% các nút là gian dối và chỉ cần 80% còn lại hoạt động ổn định là được.

- Hybrid blockchain:
  - Blockchain hỗn hợp, kết hợp các yếu tố từ cả mạng lưới riêng tư và mạng lưới công khai. Các công ty có thể thiết lập những hệ thống riêng tư, dựa trên quyền hạn bên cạnh một hệ thống công khai. Bằng cách này, họ kiểm soát quyền truy cập vào dữ liệu cụ thể được lưu trữ trong chuỗi khối trong khi vẫn công khai những dữ liệu còn lại.
- Consortium blockchain:
  - Blockchain liên hợp, các tổ chức được chọn từ trước chia sẻ trách nhiệm duy trì chuỗi khối và quyết định về quyền truy cập dữ liệu. Các ngành trong đó nhiều tổ chức có cùng mục tiêu và hưởng lợi từ trách nhiệm chung thường thích dùng mạng lưới chuỗi khối liên hợp.
  - Ví dụ: Các ngân hàng hay tổ chức tài chính liên doanh sẽ sử dụng Blockchain cho riêng mình.



Hình 1. Tính chất cho phép truy cập của các loại mạng blockchain chính.

3. Các phiên bản của blockchain

3.1. Blockchain 1.0 – Tiền tệ (Cryptocurrency)

Blockchain 1.0 được giới thiệu vào năm 2005 bởi Hall Finley, người triển khai DLT - Distributed Ledger Technology (Công nghệ sổ cái phân tán) đại diện cho ứng dụng đầu tiên dựa trên tiền điện tử. Điều này cho phép giao dịch tài chính dựa trên công nghệ Blockchain hoặc DTL được thực hiện một cách an toàn – ưu tiên số một trong các hoạt động tài chính.

Phiên bản này được xây dựng theo mô hình blockchain công khai, không có sự hạn chế nào và sự tham gia vào mạng không bị bất kì thực thể nào kiểm soát. Vì vậy bất kỳ ai cũng có khả năng gia nhập vào blockchain với đầy đủ quyền.

Vì các tính chất trên mà phiên bản này chủ yếu được sử dụng trong lĩnh vực tài chính tiền tệ. Blockchain 1.0 nhằm mục đích giới thiệu một hệ thống giao dịch phân tán, minh bạch, có thể truy cập công khai, bất biến trên thị trường tài chính toàn cầu.

Ứng dụng nổi bật nhất của công nghệ sổ cái phân tán – DTL là Bitcoin. Bitcoin đã trở thành "cash for the internet" và mở đường cho "Internet of Money". Sau khi ra mắt vào năm 2009, Bitcoin đã chứng minh tính ổn định, độ tin cậy, hiệu quả, đơn giản, độc lập và bảo mật để theo dõi giao dịch tài sản số và chuyển giao quyền sở hữu của những tài sản này từ người dùng này sang người dùng khác một cách trực tiếp. Về cơ bản, nó sử dụng cơ chế đồng thuận và khai thác để trao đổi tiền điện tử.

3.2. Blockchain 2.0 – Hợp đồng thông minh (Smart Contracts)

Phiên bản 2.0 của Blockchain ra đời vì có một số vấn đề trong phiên bản 1.0 như việc khai thác Bitcoin rất lãng phí và thiếu khả năng mở rộng mạng. Những vấn đề đó được cải thiện trong phiên bản 2.0. Trong phiên bản này, Blockchain không chỉ giới hạn ở tiền điện tử (Cryptocurrencies) mà còn mở rộng sang hợp đồng thông minh(Smart Contracts).

Ứng dụng xử lý tài chính và ngân hàng: mở rộng quy mô của Blockchain, đưa vào các ứng dụng tài chính và thị trường. Các tài sản bao gồm cổ phiếu, chi phiếu, nợ, quyền sở hữu và bất kỳ điều gì có liên quan đến thỏa thuận hay hợp đồng.

Ethereum (ETH) là biểu tượng tiên phong của Blockchain 2.0. Ý tưởng chủ đạo của công nghệ này là sử dụng sổ cái giao dịch phi tập trung của Blockchain để đăng ký, xác thực và chuyển giao mọi loại hợp đồng tài sản, bao gồm:

- Giao dịch tài chính
- Văn khố quốc gia
- Hồ sơ nhận dạng
- Hồ sơ chứng thực
- Tài sản vô hình
- Cổ phần hóa…

Điều này đồng nghĩa với việc khi bạn sở hữu một đồng coin trong hệ thống này, bạn đang nắm giữ tài sản của chính mình theo một phương thức bảo mật và minh bạch. Ứng dụng phổ biến nhất của Blockchain 2.0 hiện nay là việc sử dụng nền tảng Ethereum để mua bán các ICO (hình thức kêu gọi đầu tư bằng tiền điện tử).

3.3. Blockchain 3.0 - Ứng dụng phi tập trung (Decentrailzed Applications – dApps)

Trở ngại chính của các phiên bản blockchain 1.0 và 2.0 là chúng không thể mở rộng được, chủ yếu dựa trên Proof of Work và mất hàng giờ để xác nhận giao dịch. Tất cả điều này dẫn đến sự ra đời của thế hệ blockchain mới được gọi là Blockchain 3.0 nhằm mục đích làm cho tiền điện tử trở nên khả thi trên toàn cầu.

Ngoài các hợp đồng thông minh, thế hệ thứ ba của blockchain chủ yếu liên quan đến Ứng dụng phi tập trung (dApps). Chúng là các chương trình kỹ thuật số chạy trên mạng lưới các máy tính Blockchain thay vì một máy chủ đơn lẻ và do đó nằm ngoài tầm kiểm soát của bất kỳ một thực thể trung tâm nào. Do đó, thế hệ này có khả năng thúc đẩy các giao dịch liên chuỗi với sự hỗ trợ của các kỹ thuật như sharding. Sharding ngụ ý mỗi nút của Blockchain chỉ chứa một phần dữ liệu trên đó chứ không phải thông tin đầy đủ. Điều này giúp phân tán tải và giúp cho hệ thống trở nên khó xâm nhập, hiệu quả và nhanh chúng.

Blockchain 3.0 cũng sử dụng cơ chế đồng thuận Proof of Stake và Proof of Authority để tăng cường tốc độ và sức mạnh tính toán cho các hợp đồng thông minh mà không phải trả phí giao dịch riêng.

Mặc dù Blockchain 3.0 mới bắt đầu nhưng nhằm mục đích cải thiện khả năng mở rộng, khả năng tương tác, tính riêng tư và tính bền vững của các thế hệ trước vì chúng được thiết kế theo khái niệm "FFM", từ viết tắt của Fast, Feelless và Minerless. Do đó, Blockchain 3.0 loại bỏ sự phụ thuộc vào các "miner" để xác minh và xác thực các giao dịch và thay vào đó sử dụng các cơ chế sẵn có cho hoạt động tương tự. Do đó, chúng cực kỳ nhanh chóng để cho phép hàng nghìn giao dịch mỗi giây, không giống như các thế hệ trước.

3.4. Blockchain 4.0 – Blockchain cho doanh nghiệp (Blockchain for business)

Phiên bản thứ tư nhằm mục đích cung cấp công nghệ blockchain như một nền tảng có thể sử dụng cho doanh nghiệp để tạo và chạy các ứng dụng, từ đó đưa công nghệ này trở nên phổ biến và rộng rãi. Nó cũng mang lại khả năng tích hợp các công nghệ mạnh mẽ khác như trí tuệ nhân vạo với blockchain.

Blockchain 4.0 cho phép phát triển sự tích hợp liền mạch của các nền tảng khác nhau để hoạt động dưới một sự gắn kết duy nhất nhằm đáp ứng nhu cầu kinh doanh và công nghiệp.

Nền tảng giới thiệu để đưa ra các tiện ích Blockchain 4.0 là Unibright cho phép hợp nhất một số mô hình kinh doanh blockchain. Một ví dụ khác là Nền tảng SEELE. cho phép tích hợp trong không gian blockchain bằng cách cho phép giao tiếp chéo giữa các giao thức khác nhau trên các dịch vụ khác nhau một cách hài hòa. Thế hệ thứ tư có tiềm năng cho phép tốc độ giao dịch lên tới 1 triệu giao dịch mỗi giây, điều mà hiện tại không thể thực hiện được ở thế hệ hiện tại.

4. Các thành phần của blockchain

4.1. Node (Nút)

Bất kỳ một thiết bị nào được kết nối với blockchain đều được phân loại là một node (máy chủ, laptop, điện thoại di động,…), node là đơn vị cơ bản của mạng blockchain.

Mỗi nút lưu trữ một bản sao của sổ cái blockchain và tham gia xác thực và xác minh các giao dịch trên mạng. Tất cả các node đều được kết nối với blockchain một cách nào đó và liên tục cập nhật cho nhau những thông tin mới nhất để cập nhật vào blockchain. Các node là một thành phần quan trọng đối với cơ sở hạ tầng của một blockchain. Lợi ích cốt lõi của chúng là đảm bảo dữ liệu được lưu giữ trên blockchain là hợp lệ an toàn và có thể truy cập được cho các bên ủy quyền.

Mục tiêu của các node là duy trì độ tin cậy của dữ liệu được lưu trữ trên blockchain. Khi một block (khối) dữ liệu mới được thêm vào một blockchain, một node sẽ truyền đi block đó với các node khác trên mạng, các node có thể từ chối hoặc chấp nhận khối. Khi một khối mới được chấp nhận, thông tin sẽ được thêm vào đầu các khối đã tồn tại trước đó. Nói cách khác, node có vai trò là kiểm tra tính hợp lệ của một khối mới, lưu trữ một khối vào blockchain và cập nhật các node khác trong mạng blockchain để đảm bảo rằng thông tin trên các node đều là mới nhất.

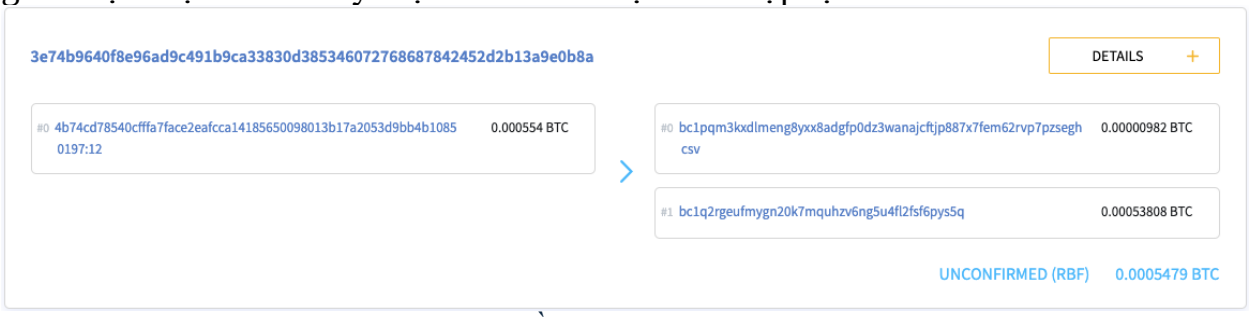
Node được phân làm nhiều loại, trong đó chúng ta quan tâm đến 3 loại chính:

- Full Node: Lưu trữ toàn bộ lịch sử giao dịch và khối của blockchain, có khả năng xác minh và truyền tải giao dịch.
- Lightweight Node: Chỉ lưu trữ một phần dữ liệu để tiết kiệm tài nguyên, nhưng vẫn tham gia vào mạng.
- Miner Node: Miner node chịu trách nhiệm xác minh các giao dịch và thêm các khối mới vào Blockchain. Các nút này thực hiện các phép tính phức tạp để giải các bài toán cho phép chúng tạo các khối mới và nhận phần thưởng dưới dạng tiền điện tử.

4.2. Transactions (Giao dịch)

Giao dịch là các hoạt động cơ bản trong mạng blockchain, chẳng hạn như chuyển tài sản kỹ thuật số, lưu trữ dữ liệu hoặc thực hiện hợp đồng thông minh. Chúng là những "viên gạch" để xây dựng nên chuỗi khối. Mỗi giao dịch chứa các

thông tin quan trọng như địa chỉ của người gửi và người nhận, số tiền giao dịch, thời gian thực hiện và chữ ký điện tử để xác thực tính hợp lệ.



Hình 2. Ví dụ về một transaction của Bitcoin.

4.3. Block (Khối)

Đơn vị cơ bản của một dự án blockchain là khối. Mỗi khối hoạt động như một nơi chứa dữ liệu là các giao dịch và các thông tin liên quan khác. Các khối được thêm tuần tự vào một chuỗi và trở thành chuỗi khối hay blockchain, tạo ra danh sách liên kết liên tục và theo trình tự thời gian của tất cả các giao dịch.

Mỗi khối bao gồm 3 phần chính là: Tiêu đề (The header), dữ liệu giao dịch (Transaction data) và nonce. Tiêu đề chứa siêu dữ liệu như mã băm của khối (Hash), dấu thời gian và mã băm của khối trước (Previous Block Hash). Siêu dữ liệu này rất quan trọng để liên kết các khối với nhau một cách an toàn. Dữ liệu giao dịch liệt kê tất cả các giao dịch được ghi lại trong khối, mỗi giao dịch được mã hóa để duy trì tính bảo mật và tính toàn vẹn. Cuối cùng, nonce là một số ngẫu nhiên được sử dụng trong các mã băm, đóng vai trò quan trọng trong quá trình khai thác, bao gồm việc giải các bài toán phức tạp để thêm các khối mới vào chuỗi.

Trong đó, mã băm (hash) được hiểu là mỗi khối có một mã băm duy nhất, là một chuỗi ký tự duy nhất được tạo ra dựa trên nội dung của khối. Mã băm này giúp nhận diện duy nhất khối và đảm bảo rằng không thể sửa đổi dữ liệu trong khối mà không làm thay đổi mã băm. Mỗi khối có một liên kết đến các khối trước đó thông qua mã băm của khối trước (Previous Block Hash). Điều này tạo ra các chuỗi liên kết giữa các khối, đảm bảo tính toàn vẹn của dữ liệu.

VD: Một khối trong blockchain của Bitcoin chứa khoảng 1MB dữ liệu giao dịch, thường bao gồm hàng nghìn giao dịch Bitcoin. Trong đó, mỗi khối Bitcoin có một mã băm độc nhất, giúp nhận dạng khối và liên kết của khối trước và mã băm của khối trước giúp tạo liên kết giữa các khối để tạo thành chuỗi blockchain.

4.4. Chain (Chuỗi)

Chuỗi là khái niệm trong đó tất cả các khối được kết nối với sự trợ giúp của một chuỗi trong toàn bộ cấu trúc chuỗi khối trên thế giới. Và các khối đó được kết nối với sự trợ giúp của mã băm khối trước đó và nó biểu thị cấu trúc chuỗi.

4.5. Mining (Khai thác – "Đào") và Miner (Người khai thác – "Thợ đào")

Đối với các mạng blockchain, quá trình "đào" là quá trình mà những người tham gia giành quyền ghi khối lên mạng blockchain, sau đó nhận phần thưởng (thường là tiền điện tử). Những người tham gia vào hoạt động khai thác này được gọi là miner – thợ đào.

VD: Mining trong Bitcoin là quá trình mà các thợ đào giải quyết các bài toán băm để thêm khối mới vào blockchain.

- Mining Reward: Thợ đào nhận phần thưởng khi họ tìm ra lời giải cho bài toán băm và tạo ra khối mới. Ban đầu phần thưởng là 50 BTC, hiện tại là 6.25 BTC sau khi quá trình halving (chia đôi phần thưởng) diễn ra vào năm 2020.
- Fees: Ngoài phần thưởng khối, các thợ đào còn nhận được phí giao dịch từ các giao dịch trong khối mà họ đã khai thác.

4.6. Distributed Ledger (Sổ cái phân tán)

Sổ cái phân tán là một hệ thống lưu trữ dữ liệu phi tập trung, trong đó thông tin và các bản ghi được phân phối trên nhiều máy chủ hoặc nút mạng khác nhau. Hệ thống này cho phép người dùng đồng thời truy cập, xác thực, và cập nhật dữ liệu trên một cơ sở kết nối mạng. Nhờ sử dụng mã hóa và các giao thức bảo mật, sổ cái phân tán ngăn chặn các can thiệp trái phép, đảm bảo tính toàn vẹn của dữ liệu trong quá trình giao dịch.

Một trong những ưu điểm lớn của sổ cái phân tán là nó không cần đến một cơ quan trung ương hoặc bên trung gian để xử lý và xác nhận giao dịch. Các bản ghi dữ liệu chỉ được thêm vào sổ cái khi đạt được sự đồng thuận giữa các bên liên quan. Mỗi người tham gia sẽ có một bản sao của sổ cái, bao gồm tất cả các bản ghi mới nhất. Đồng thời, tất cả những dữ liệu trong sổ đề sẽ được công khai, đảm bảo chính xác và minh bạch, bất cứ ai cũng có thể tra cứu.

VD: Sổ cái trong blockchain bitcoin là một bản ghi tập trung của tất cả các giao dịch Bitcoin đã diễn ra từ khối gốc đến hiện tại. Mọi node đều có bản sao của sổ cái này. Trong Bitcoin, mọi giao dịch đều công khai và có thể kiểm tra trên các trang web như Blockchain Explorer. Mọi người đều có thể xem lịch sử giao dịch của bất kỳ địa chỉ ví Bitcoin nào.

4.7. Consencus Mechanism (Cơ chế đồng thuận)

Cơ chế đồng thuận là một quy trình, được sử dụng để duy trì trạng thái nhất quán và thống nhất của hệ thống blockchain trên tất cả các nút. Cơ chế này đảm bảo rằng tất cả các nút xác thực và đồng ý về tính hợp lệ của các giao dịch cũng như thứ tự thêm chúng vào chuỗi khối.

Các cơ chế đồng thuận phổ biến bao gồm: Proof of Work (PoW), Proof of Stake (PoS) và Delegated Proof of Stake (DPoS). Các cơ chế này khác nhau trong việc xác định nút nào có quyền thêm khối mới vào chuỗi.

- Proof of Work (PoW): Dựa trên quá trình "đào" (mining), nơi các node cạnh tranh để giải một bài toán khó nhằm tạo ra khối mới. Người thành công sẽ nhận được phần thưởng, ví dụ như bitcoin.
- Proof of Stake (PoS): Không yêu cầu "đào", thay vào đó, các node (validators) sẽ được chọn ngẫu nhiên để xác thực khối mới dựa trên số lượng tài sản họ nắm giữ.
- Delegated Proof of Stake (DPoS): Là biến thể của PoS, nơi người dùng bỏ phiếu chọn ra những người đại diện (delegates) để xác thực giao dịch và thêm khối.

VD: Bitcoin sử dụng cơ chế **Proof of Work (PoW)**. Các thợ đào (miners) cạnh tranh để giải các bài toán băm phức tạp nhằm thêm khối mới vào blockchain. Người đầu tiên tìm ra lời giải hợp lệ sẽ nhận phần thưởng là số Bitcoin mới sinh ra (block reward) cùng với phí giao dịch. Các thợ đào cần thực hiện hàng triệu phép tính mỗi giây để tìm ra giá trị nonce phù hợp sao cho mã băm của khối mới thỏa mãn điều kiện (có một số lượng bit 0 nhất định).

4.8. Cryptography (Mật mã học)

Mật mã đóng một vai trò then chốt trong việc bảo mật các giao dịch và duy trì tính toàn vẹn của chuỗi khối. Mật mã khóa công khai thường được sử dụng để xác minh danh tính và tạo chữ ký số. Khóa riêng do cá nhân nắm giữ được sử dụng để ký các giao dịch. Mặt khác, khóa chung được sử dụng để xác minh tính xác thực của chữ ký. Bản chất an toàn và chống giả mạo của các kỹ thuật mã hóa đảm bảo tính bất biến của các giao dịch. Một số kỹ thuật mật mã chính bao gồm:

- Hashing: Tạo ra mã băm duy nhất từ dữ liệu, giúp bảo vệ dữ liệu trong khối.
- Chữ ký số (Digital Signature): Đảm bảo rằng người gửi giao dịch chính là chủ sở hữu hợp pháp tài sản đó.

Về cơ bản, mục tiêu chính của mật mã học bao gồm:

- Confidentiality (Tính bảo mật): Chỉ có các bên liên quan trong quá trình trao đổi, chủ sở hữu hoặc người có thẩm quyền mới có quyền truy cập các thông tin liên quan.
- Integrity (Tính toàn vẹn): Dữ liệu trong quá trình lưu trữ và trao đổi không được thay đổi hoặc bị mất.
- Authentication (Tính xác thực): Người nhận biết được thông điệp mà họ nhận được đến từ ai và xác thực được danh tính người gửi.

- Non-repudiation (Tính chống chối bỏ): Người gửi không thể chối bỏ được thông điệp mà họ đã gửi. Người gửi sẽ phải chịu toàn bộ trách nhiệm với thông tin mà họ đã gửi.

Nói chung, mật mã học đóng vai trò cực kỳ quan trọng trong việc chuyển giao thông tin giữa các thiết bị điện tử. Bất cứ lúc nào chúng ta truy cập vào mạng máy tính, mật mã đều có mặt.

VD: Bitcoin sử dụng các thuật toán mã hóa để bảo mật giao dịch và dữ liệu:

- Hashing (SHA-256): Thuật toán băm SHA-256 được sử dụng để tạo mã băm cho các khối và giao dịch, đảm bảo rằng dữ liệu không thể bị thay đổi mà không làm thay đổi mã băm.
- Public-key Cryptography: Bitcoin sử dụng cặp khóa công khai (public key) và khóa riêng tư (private key) để đảm bảo rằng chỉ chủ sở hữu của một địa chỉ Bitcoin mới có thể chi tiêu Bitcoin từ địa chỉ đó. Public key được sử dụng để tạo ra địa chỉ Bitcoin, và private key để ký vào giao dịch.

5. Các đặc tính nổi bật của blockchain

5.1. Decentralized (Tính phi tập trung)

Công nghệ chuỗi khối là một hệ thống phi tập trung, có nghĩa là không có một thực nào nắm vai trò trung tâm trong kiểm soát mạng. Thay vào đó, mạng được tạo thành từ một số lượng lớn các nút hoạt động cùng nhau để xác minh và xác thực các giao dịch. Mỗi nút trong mạng blockchain sẽ có cùng một bản sao sổ cái.

5.2. Consencus (Sự đồng thuận)

Mỗi blockchain đều có sự đồng thuận để giúp mạng đưa ra quyết định nhanh chóng và khách quan. Sự đồng thuận là thuật toán ra quyết định để nhóm các nút hoạt động trên mạng đạt được thỏa thuận nhanh chóng và nhanh hơn, để hệ thống hoạt động một cách trơn tru. Các nút không tin tưởng lẫn nhau nhưng chúng có thể tin tưởng thuật toán ở lõi của mạng để đưa ra quyết định. Có rất nhiều thuật toán đồng thuận, mỗi thuật toán đều có những ưu và nhược điểm riêng. Mỗi blockchain phải có một thuật toán đồng thuận, nếu không nó sẽ mất đi giá trị của mình.

Nói đơn giản, mỗi blockchain cần có một phương thức hay thuật toán để tất cả những thực thể tham gia vào mạng đều đồng thuận với dữ liệu có trên mạng blockchain đó.

5.3. Immutable (Tính bất biến)

Tính bất biến nghĩa là blockchain là một mạng lưới vĩnh viễn và không thể thay đổi. Sau khi một giao dịch được ghi lại trên blockchain, nó không thể bị sửa đổi hoặc xóa. Điều này làm cho blockchain trở thành một sổ cái không thể thay đổi và chống giả mạo, cung cấp mức độ tin cậy cao.

Mỗi nút trong mạng đều có một bản sao của sổ cái kỹ thuật số. Để thêm một giao dịch, mỗi nút sẽ kiểm tra tính hợp lệ của giao dịch và nếu hợp lệ thì giao dịch đó sẽ được thêm vào mạng. Điều này có nghĩa là nếu phần lớn các nút không chấp thuận thì không ai có thể thêm bất kỳ khối giao dịch vào vào sổ cái.

Bất kỳ bản ghi nào đã được xác thực đều không thể đảo ngược và không thể thay đổi. Điều này có nghĩa bất kỳ người dùng nào trên mạng sẽ không thể chỉnh sửa, thay đổi hay xóa nó.

VD: Mọi giao dịch Bitcoin đều tồn tại mãi mãi trong chuỗi khối và không thể thay đổi.

5.4. Liveness (Tính khả dụng)

Trong blockchain, tính khả dụng đề cập đến khả năng đảm bảo rằng mọi giao dịch và hành đông trên mạng đều sẽ được thực hiện. Nghĩa là mạng được đảm bảo hoạt động thông suốt mà không rơi vào trạng thái trì trệ hoặc ngừng hoạt động.

Liveness đảm bảo rằng miễn là hệ thống đang hoạt động, bất kỳ giao dịch hợp lệ nào cũng sẽ được đưa vào blockchain vào một thời điểm nào đó, ngay cả trong các điều kiện bất lợi như phân vùng mạng hoặc sự chậm trễ.

Tính khả dụng là một trong những thuộc tính quan trọng trong các hệ thống phân tán, cùng với tính an toàn và nó đảm bảo rằng blockchain sẽ không chỉ duy trì an toàn mà còn tiếp tục thêm các khối và xác nhận giao dịch.

Tính chất này còn đảm bảo rằng bất cứ người dùng nào cũng có khả năng tham gia vào một mạng blockchain, chỉ cần họ có internet và thiết bị điện tử phù hợp.

VD: Trong mạng Bitcoin, các giao dịch hợp lệ sẽ được các thợ đào đưa vào khối và cuối cùng sẽ được thêm vào blockchain, miễn là có đủ sức mạnh tính toán (hash power). Mặc dù có thể mất thời gian nếu mạng bị tắc nghẽn, tính liveness của Bitcoin đảm bảo rằng các giao dịch sẽ không bị bỏ qua hoàn toàn. Trong trường hợp mạng bị tấn công hoặc chia rẽ, khi kết nối được khôi phục, các giao dịch vẫn sẽ được xử lý.

5.5. Transparency (Tính minh bạch)

Tính minh bạch của chuỗi khối đề cập đến tính năng đặc trưng của chuỗi khối nhằm đảm bảo tất cả các giao dịch và dữ liệu trên mạng đều có sẵn cho mọi người có quyền truy cập vào hệ thống. Với tính minh bạch của blockchain, bất kỳ ai cũng có thể xem và xác thực tính xác thực của các giao dịch và dữ liệu trên mạng. Đây là cách tiếp cận mà nhiều blockchain công khai như Bitcoin và Ethereum đã thực hiện khi phát triển các mạng khác nhau của họ.

Tính minh bạch là điều cần thiết vì nó cho phép mọi người tin tưởng vào thông tin có trong mạng blockchain. Nó cũng cho phép các thành viên của mạng xác minh rằng các giao dịch mà họ đang thực hiện là hợp pháp. Tính minh bạch của mạng

blockchain là một trong những điểm mạnh chính của nó. Nó mang lại sự công bằng, tin cậy và độ tin cậy và là một tính năng chính giúp công nghệ blockchain hiệu quả hơn các hệ thống lưu trữ dữ liệu khác.

VD: Mọi giao dịch trên mạng Bitcoin đều có thể kiểm tra công khai qua các trình duyệt blockchain.

5.6. Security and privacy (Tính bảo mật và quyền riêng tư)

Từ các tính chất trên, cùng với kĩ thuật bổ sung như mã hoá, băm,… blockchain cung cấp một cơ chế xác thực và bảo mật rất cao và đáng tin cậy.

Mặc dù có tính chất minh bạch và công khai, điều này không có nghĩa rằng mọi dữ liệu của người dùng đều có thể bị tra cứu hay hiển thị một cách dễ dàng và trực tiếp. Quyền riêng tư vẫn có thể được đảm bảo bởi blockchain qua nhiều cách. Đầu tiên là danh tính người dùng không được xác định bằng thông tin cá nhân của họ mà được xác định qua địa chỉ ví. Hay kĩ thuật mật mã Zero-Knowledege Proofs, một kĩ thuật cho phép xác minh thông tin mà không cần tiết lộ nội dung chi tiết. Ngoài ra, các nền tảng blockchain có thể triển khai các "hợp đồng thông minh" - được xem như các luật lệ được áp dụng trên mạng về bảo vệ quyền riêng tư, che giấu thông tin…

II. NGUYÊN LÝ HOẠT ĐỘNG CỦA BLOCKCHAIN

1. Cơ chế phi tập trung

Phi tập trung có nghĩa là mạng sẽ hoạt động trên hình thức peer-to-peer (ngang hàng) giữa 2 người trực tiếp (user-to-user).

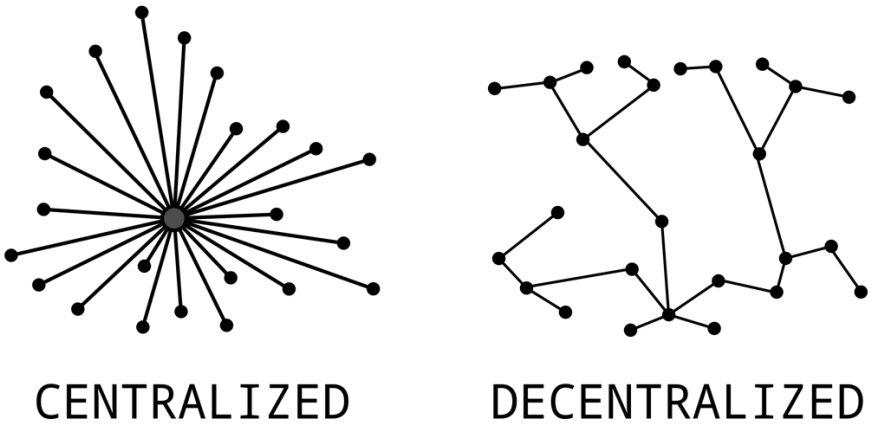
Phi tập trung (Decentralization) trong blockchain là chỉ việc chuyển quyền kiểm soát và ra quyết định từ một thực thể nhất định (cá nhân, tổ chức hoặc nhóm) sang một mạng lưới phân tán gồm nhiều thực thể tham gia. Các mạng lưới blockchain phi tập trung sử dụng tính minh bạch để giảm nhu cầu phải có sự tin tưởng giữa những người tham gia. Các mạng lưới này cũng ngăn cản những người tham gia sử dụng quyền hạn hoặc quyền kiểm soát lên lẫn nhau theo những cách làm suy yếu chức năng của mạng lưới.

Phi tập trung cung cấp môi trường khôi đòi hỏi sự tin tưởng, mỗi người không cần phải biết hoặc tin tưởng bất cứ ai khác. Mỗi thành viên trong mạng đều có bản sao của cùng dữ liệu chính xác dưới dạng sổ cái phân tán. Nếu sổ cái của thanh viên nào bị thay đổi hoặc bị lỗi theo bất kỳ cách nào, số cái đó sẽ bị đa số thành viên trong mạng từ chối. Ngoài ra, phi tập trung còn cải thiện đối chiếu dữ liệu, giảm điểm yếu trong các hệ thống nơi mà có thể phụ thuộc quá nhiều vào những tác nhân cụ thể và tối ưu hóa phân phối tài nguyên để cung cấp các dịch vụ đã cam kết với hiệu năng và tính nhất quán cao hơn.

Để dễ hiểu hơn ta sẽ lấy một ví dụ so sánh mạng tập trung (centralized) với phi tập trung (decentralized). Với phương pháp truyền thống: khi 2 người muốn giao dịch với nhau sẽ đều phải thông qua một bên trung gian thứ 3 là ngân hàng, và rất nhiều người khác cũng sẽ phải làm tương tự nếu muốn giao dịch. Vì vậy đây sẽ là một mạng tập trung khi mọi giao dịch của tất cả các user đều tập trung hướng về ngân hàng để đến được bên đích người nhận.

Giờ ta sẽ so sánh sự khác biệt với mạng phi tập trung. Trong mạng này các bên sẽ giao dịch trực tiếp với nhau mà vị trí của họ đang ở đâu không quan trọng. Các chức năng của các bên trung gian trong mạng tập trung được chuyển sang ngoại vi cho nhưng người tham gia ngang hàng khác trong cơ sở hạ tầng blockchain.

VD: Bitcoin hoạt động dựa trên hàng ngàn node toàn cầu mà không có bất kỳ tổ chức hoặc chính phủ nào điều hành.



Hình 3. Khác biệt giữa mạng tập trung và mạng phi tập trung.

2. Cơ chế tạo giao dịch (transactions)

Một hợp đồng, thỏa thuận, chuyển nhượng, hoặc trao đổi tài sản giữa hai hoặc nhiều bên được gọi là một giao dịch. Thông thường, tài sản ở đây có thể là tiền mặt hoặc tài sản bất động sản.

Tương tự, một giao dịch blockchain chỉ đơn giản là việc truyền dữ liệu qua mạng máy tính của hệ thống blockchain. Các giao dịch (transactions) là phần tử cơ bản nhất của một blockchain. Thông thường, dữ liệu được truyền đi trong các giao dịch có thể là giá trị của token, đồng tiền kĩ thuật số… đi từ nơi lưu trữ của người dùng này sang người dùng khác.

Các thành phần chính của transaction trong blockchain:

- **Địa chỉ người gửi:** Mỗi giao dịch xuất phát từ địa chỉ ví tiền điện tử của người gửi. Địa chỉ này đóng vai trò là một định danh duy nhất và được tạo ra từ khóa công khai của người gửi.

- **Địa chỉ người nhận:** Địa chỉ người nhận là đích đến nơi tài sản kỹ thuật số sẽ được gửi. Tương tự như địa chỉ người gửi, nó là sản phẩm của khóa công khai của người nhận.
- **Số lượng:** Số lượng tiền điện tử hay tài sản được chuyển trong giao dịch, là một thành phần quan trọng của bất kỳ giao dịch nào. Nó xác định số lượng tài sản kỹ thuật số đang được chuyển giao.
- **Phí giao dịch:** Để khuyến khích các thợ đào đưa các giao dịch của họ vào blockchain, người dùng đính kèm một khoản phí giao dịch. Các thợ đào ưu tiên những giao dịch có phí cao hơn, vì họ nhận được các khoản phí này như phần thưởng cho nỗ lực của họ.
- **Chữ ký:** Trước khi một giao dịch được thêm vào blockchain, nó phải được xác nhận bởi mạng. Người gửi ký giao dịch bằng khóa riêng của họ, chứng minh quyền sở hữu tài sản đang được chuyển nhượng.
- **Dấu thời gian:** Mỗi giao dịch đều có dấu thời gian, cung cấp một bản ghi theo thứ tự thời gian về thời điểm giao dịch xảy ra. Điều này góp phần vào tính minh bạch và không thể thay đổi của blockchain.

Vì mỗi mạng blockchain sẽ có một cơ chế thực thi và lưu trữ giao dịch khác nhau nên trước hết ta phân tích Bitcoin làm ví dụ về các giao dịch trong một mạng blockchain cụ thể. Một khái niệm cơ bản của một mạng Bitcoin là **Unspent Transaction Output (UTXO)**, tập hợp tất cả các UTXOs trên mạng Bitcoin sẽ xac định chung trạng thái của Bitcoin Blockchain. UTXOs có thể được hiểu là **đầu vào (input)** và **đầu ra (output)** của một giao dịch. Đầu ra của giao dịch này có thể làm đầu vào của một giao dịch khác.

Một ví dụ đơn giản về giao dịch trong Bitcoin như sau: Giả sử, A chuyển cho B một lượng 2BTC nhưng chia làm 2 lần, mỗi lần có giá trị 1BTC.2 lần giao dịch đó của A tạo ra 2 UTXOs thuộc quyền sở hữu của B, mỗi UTXO có giá trị là 1BTC. Ban đầu khi B và C chưa tiêu thụ số Bitcoin trên, các UTXOs đầu ra của các giao dịch vừa rồi vẫn sẽ nằm yên trong cơ sở dữ liệu và chưa thay đổi. Cho tới khi B chuyển tiếp 2BTC này cho một bên khác để tiêu thụ, ví dụ B muốn mua một chiếc xe hơi giá 2BTC, thì các UTXOs nói trên sẽ trở thành đầu vào trong giao dịch mới của B với đại lý ô tô. Đây là lý do tại sao nó được gọi là **Unspent Transaction Output** (nó sẽ chỉ là đầu ra của một giao dịch nào đó, được giữ nguyên khi mà lượng tiền trong nó vẫn chưa được tiêu – unspent).

Cấu trúc của một UTXO rất đơn giản. Nó chứa một định danh duy nhất của giao dịch đã tạo ra nó, một chỉ số nêu vị trí của nó trong danh sách đầu ra của giao dịch và giá trị hoặc lượng tiền nó đại diện. Cuối cùng là một script không bắt buộc phải có, để nêu ra điều kiện cần thỏa mãn thì đầu ra này mới được sử dụng tiếp.

Bản thân giao dịch chứa một số tham chiếu tới chính nó, tham chiếu tới một hoặc nhiều hoặc không có UTXO đầu vào nào, tham chiếu tới một hoặc nhiều hoặc không có UTXO đầu ra được tạo bởi nó, cuối cùng là lượng tiền đầu vào và đầu ra.

Các người tham gia trên mạng có thể kiểm chứng các nội dung của giao dịch - đầu vào UTXO của giao dịch này có thực sự tồn tại trên trạng thái mạng bây giờ không ? Đây chỉ là 1 trong rất nhiều điều kiện để kiểm chứng giao dịch. Thao tác này giống như Alice cho Amy vay 10000$ và Amy nhờ Kevin đếm tiền để kiểm chứng xem có thật sự là 10000$ hay không - trên mạng Blockchain thì giao dịch sẽ có rất nhiều "Kevin" để kiểm chứng (rất nhiều thợ đào) vì vậy rất khó để gian lận trong giao dịch, từ đó sự an toàn, tin tưởng và bảo mật được thiết lập trong blockchain.

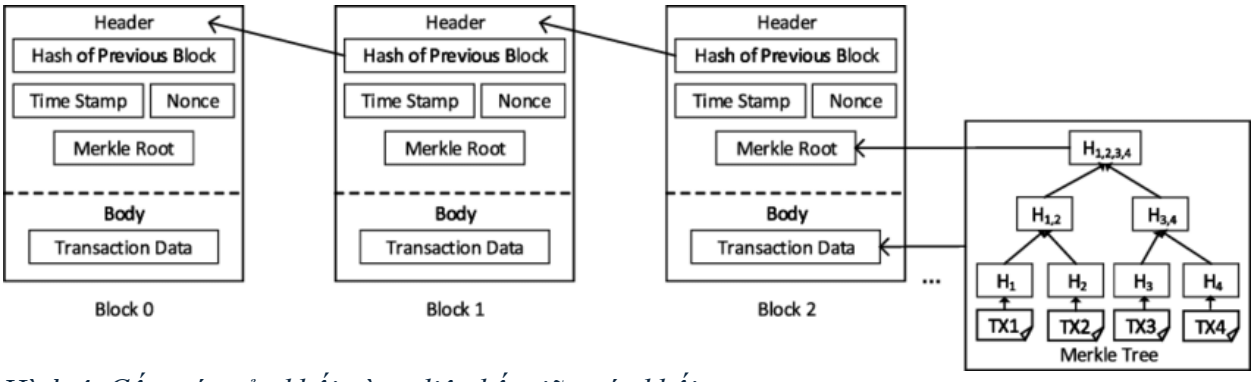
Bitcoin và nhiều giao thức dựa trên UTXO lưu trữ dữ liệu, giao dịch và số dư tài khoản người dùng trong dạng Unspent Transactions Output, được hiểu như là danh sách lượng bitcoin được gửi tới người dùng mà "chưa tiêu" (unspent). Tổng các đầu ra này sẽ tạo thành số dư của người dùng. Trên blockchain, chúng được coi như là tập hợp các lượng bitcoin trên nhiều địa chỉ khác nhau, và vai trò của ví điện tử (wallet) ở đây là xác định xem những địa chỉ nào người dùng có quyền truy cập tới (có khóa của địa chỉ). Một bitcoin độc lập được theo dõi dễ dàng vì chúng được ký gửi từ người này sang người khác. Một giao dịch được coi là hợp lệ nếu một người có thể chứng minh quyền sở hữu của những bitcoin mà họ đang cố gửi đi.

Cách thức này khác với mô hình tài khoản của Ethereum, nơi lưu trữ toàn bộ thông tin số dư của tài khoản người dùng. Người dùng gửi và nhận token (tiền) từ tài khoản của họ và các đồng tiền ETHs khó theo dõi hơn vì chúng chỉ được cộng và trừ khỏi số dư. Một giao dịch được coi là hợp lệ nếu người dùng chứng minh được số dư tài khoản của họ đủ cao để thực hiện.

3. Cơ chế ghi khối vào mạng blockchain

Giao dịch là phần tử cơ bản nhất của Bitcoin Blockchain, các giao dịch được kiểm chứng và truyền đi (broadcast). Nhiều giao dịch sẽ tạo thành 1 khối (block). Nhiều khối tạo thành một chuỗi thông qua các liên kết dữ liệu kỹ thuật số (blockchain).

3.1. Cấu trúc chi tiết của một khối



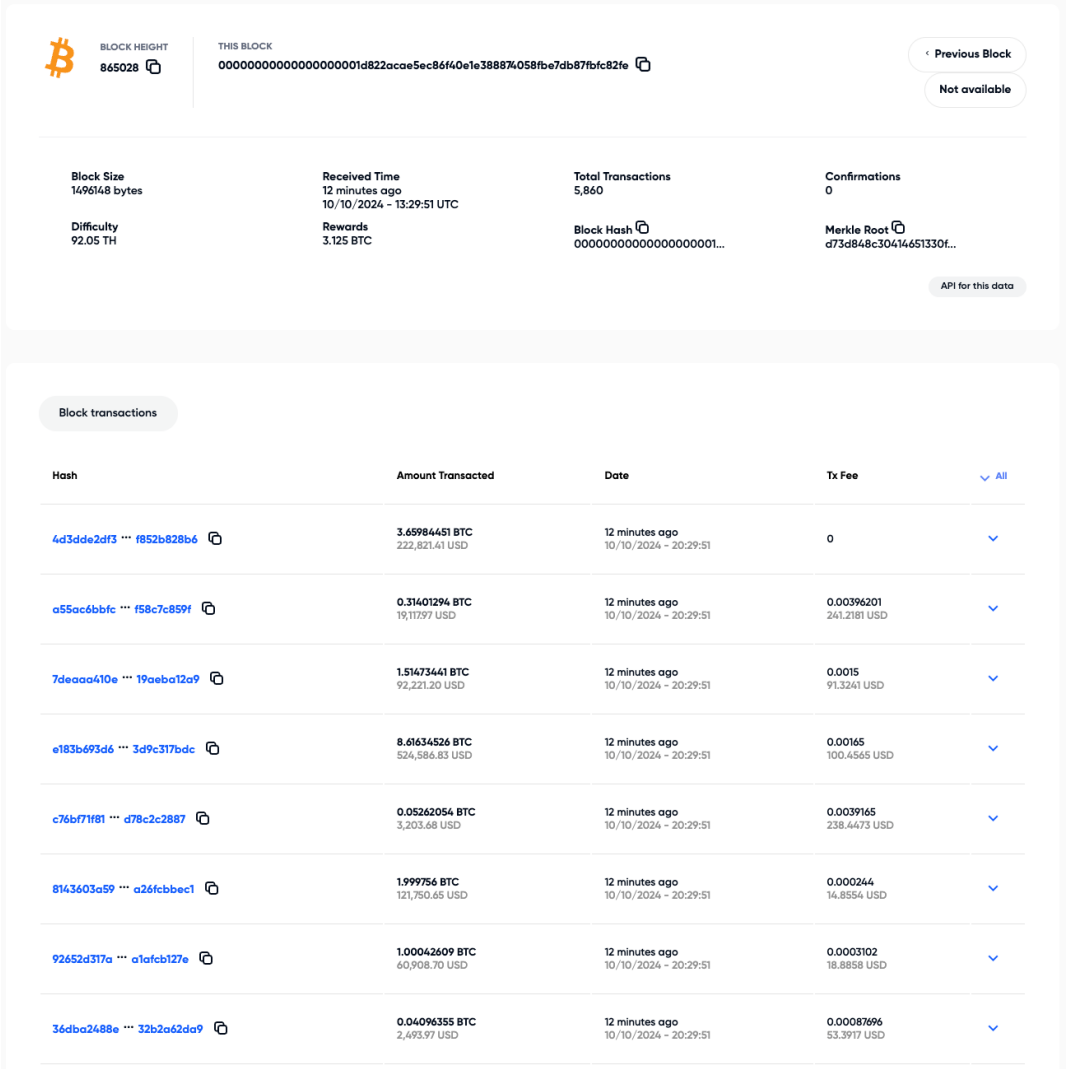
Hình 4. Cấu trúc của khối và sự liên kết giữa các khối

3.1.1. Phần đầu (Block header)

- Chiều cao khối (Block height): Số thứ tự cho mỗi khối được thêm vào mạng blockchain. Không có khối nào có cùng số chiều cao.
- Timestamp: Đây là thời điểm khối được khai thác. Nó thường là trong thời gian Unix.
- Mã băm của khối trước đó: Đây là mã băm của khối trước đó. Giá trị này có vai trò xâu chuỗi các khối lại với nhau và làm cho dữ liệu trong các khối trước đó không thay đổi. Nếu dữ liệu trong các khối trước đó bị thay đổi, thì mã băm của khối đó sẽ thay đổi, dẫn đến việc chuỗi khối này không được chấp nhận bởi những node khác.
- Nonce: Đây là một số nguyên mà người khai thác thay đổi để thay đổi mã băm của khối nhằm đạt được độ khó của mạng.
- Giá trị băm gốc Merkel: Mã băm với đầu vào là dữ liệu của tất cả các giao dịch được truyền đi trong khối.

3.1.2. Phần thân (Block body)

- Dữ liệu giao dịch (Transaction data): Bao gồm tất cả các giao dịch có trong khối.
- VD: Mỗi khối Bitcoin chứa khoảng 2000 giao dịch. Kích thước của mỗi khối là khoảng 1 MB. Kích thước và số lượng giao dịch trong một khối khác nhau tùy theo chuỗi khối. Nó được quyết định dựa trên tình trạng tắc nghẽn mạng và chi phí liên lạc.



Hình 5. Thông tin của một khối trên mạng Bitcoin

3.2. Cơ chế ghi khối vào blockchain

Mỗi khối được tiến hành ghi vào blockchain khi đã đạt tới một dung lượng dữ liệu nhất định, hoặc ghi theo thời gian định kỳ.

Blockchain mining về cơ bản là quá trình người khai thác ghi một khối lên mạng blockchain sau khi khối đó đạt yêu cầu để được phép ghi lên mạng. Thao tác chèn thêm khối mới lên mạng blockchain không hề khó, vấn đề của những "thợ đào" là làm cách nào để giành được quyền chèn khối tiếp theo lên mạng. Nếu như các mạng blockchain chọn một cách ngẫu nhiên người khai thác, có thể sẽ xảy ra một số vấn đề tiềm ẩn như sybil attack, tấn công 51%, không công bằng,…Vậy nên buộc các blockchain phải có cơ chế để chọn người khai thác dự trên một số tiêu chí và điều kiện nhất định, các cơ chế đó còn được gọi là cơ chế đồng thuận.

Hiện tại có khá nhiều các cơ chế đồng thuận khác nhau tuỳ theo từng mạng blockchain, nhưng trong bài báo cáo này sẽ tập trung vào 2 loại chính hiện nay: ***proof of work*** và ***proof of stake***.

3.2.1. Proof of work – PoW

(a) Định nghĩa và cách hoạt động

PoW là một khái niệm được sử dụng trong một số các mạng blockchain công khai để chứng minh rằng một chương trình đã thực hiện công việc cần thiết để có thể nhận được quyền ghi thêm một khối mới lên chuỗi. Điều này có nghĩa rằng, hệ thống sẽ yêu cầu các người khai thác, hay thợ đào, sử dụng sức mạnh tính toán của những thiết bị điện tử mà họ có, để giải một bài toán phức tạp và gửi đáp án đúng đến toàn mạng lưới. Bất cứ ai có được đáp án nhanh nhất sẽ giành được quyền thêm khối vào chuỗi và nhận được phần thưởng.

PoW sử dụng các hàm băm, là các thuật toán mật mã một chiều chuyển đổi dữ liệu đầu vào thành các chuỗi ký tự có độ dài cố định. Các thợ đào cần tìm một giá trị chuỗi băm phù hợp với một mẫu cụ thể, được gọi là mục tiêu, bằng cách liên tục thay đổi giá trị nonce cho đến khi thu được giá trị chuỗi băm mong muốn.

Để duy trì thời gian tạo khối nhất quán, mạng điều chỉnh độ khó của các câu đố dựa trên tổng sức mạnh tính toán của mạng. Khi nhiều thợ đào tham gia hoặc rời khỏi mạng, độ khó được thay đổi linh hoạt để điều chỉnh tốc độ tạo khối.

Bitcoin là một trong những ví dụ về việc sử dụng cơ chế PoW.

(b) Ưu điểm và nhược điểm của PoW

- Ưu điểm:
    - **Bảo vệ chống tấn công DDoS:** PoW đặt ra giới hạn cao đối với mạng lưới. Điều này yêu cầu bất kỳ hành động nào trước hết cần phải vượt qua. Do đó, để tấn công mạng lưới, người tấn công cần phải sử dụng một lượng lớn năng lực máy tính và mất nhiều thời gian tính toán. Mặc dù có thể tấn công, nhưng với chi phí rất lớn.
    - **Khả năng đào block:** Điều quan trọng không phải là số tiền trong ví, mà là khả năng năng lực máy tính để giải quyết bài toán đào block. Vì vậy, trên mạng lưới blockchain, người có tiền không chắc chắn có quyền.
- Nhược điểm:
    - **Chi phí đắt đỏ:** Đào tiền yêu cầu thiết bị máy tính chuyên dụng với thuật toán rất phức tạp, với chi phí rất lớn đối với cá nhân. Vì vậy, hoạt động này chủ yếu được thực hiện bởi nhóm thợ đào. Nhóm này sử dụng thiết bị tiêu tốn nhiều năng lượng, tăng chi phí khai thác.
    - **Sự lãng phí của năng lực máy tính:** Thợ đào tạo ra block mới thông qua sức lao động cật lực, tiêu tốn rất nhiều điện năng. Tuy nhiên, công việc tính toán này không áp dụng ở các lĩnh vực khác.

- **Tấn công 51%:** Tấn công 51% xảy ra khi một nhóm người dùng kiểm soát đa số năng lực khai thác.
- **Tốn thời gian:** Người khai thác phải kiểm tra nhiều giá trị nonce để tìm ra giải pháp phù hợp cho bài toán phải giải để khai thác block, đây là một quá trình tốn thời gian.

3.2.2. Proof of Stake – PoS

(a) Định nghĩa và cách hoạt động

Những hạn chế của PoW – cơ chế đồng thuận đầu tiên cho các mạng blockchain, đã thúc đẩy việc khám phá ra những cơ chế mới mạng blockchain có thể hoạt động hiệu quả hơn. Một trong số những cơ chế mới đó là proof-of-stake (PoS).

Thay vì giải mã các bài toán mật mã sử dụng sức mạnh tính toán để xác minh các giao dịch, Proof-of-Stake đạt được sự đồng thuận bằng cách yêu cầu người dùng đóng góp một lượng token của họ để có cơ hội được chọn để xác thực các block giao dịch và được thưởng vì đã làm như vậy.

Trong cơ chế đồng thuận PoS (Proof of Stake), các block được "rèn" thay vì "khai thác" như trong PoW (Proof of Work). Yếu tố quan trọng đầu tiên trong quá trình lựa chọn người xác thực block là lượng cổ phần (stake) mà người dùng nắm giữ.

Những người muốn tham gia vào quá trình này cần sở hữu một phần cổ phần trong mạng. "Staking" là hành động khóa một số tiền nhất định vào mạng để làm bằng chứng cho cổ phần của họ. Càng nhiều người dùng khóa cổ phần, cơ hội của họ được chọn làm người xác thực càng cao. Số lượng cổ phần mà một node sở hữu sẽ quyết định cơ hội được chọn để rèn block kế tiếp; cổ phần càng lớn thì xác suất được chọn càng cao so với những người có cổ phần ít hơn.

Trong PoS, phần thưởng cho việc tham gia xác thực các block đến từ phí giao dịch, khác với hệ thống PoW, nơi phần thưởng là tiền tệ mới được tạo ra.

Để tránh việc chỉ các node giàu có liên tục được chọn và ngày càng giàu hơn, các phương thức bổ sung được áp dụng trong quá trình lựa chọn người xác thực. Mục tiêu là đảm bảo cơ hội ngẫu nhiên để không phải người dùng giàu nhất lúc nào cũng được chọn. Hai phương thức phổ biến nhất là:

- **Lựa chọn khối ngẫu nhiên**: Người xác thực được chọn dựa trên việc tìm kiếm các node có giá trị băm thấp nhất kết hợp với cổ phần lớn nhất.
- **Lựa chọn Coin Age**: Các node được chọn dựa trên thời gian mà token của họ đã được giữ làm cổ phần. "Tuổi coin" được tính bằng cách nhân số ngày các coin được giữ làm cổ phần với số lượng coin đó.

Ví dụ điển hình cho việc sử dụng cơ chế PoS là Ethereum.

(b) Ưu điểm và nhược điểm của PoS

- Ưu điểm:

- **Năng lượng**: Thuật toán PoS tiết kiệm năng lượng – đặc biệt là khi so sánh với PoW.
- **Bảo mật**: Để kiểm soát mạng lưới và phê duyệt giao dịch gian lận. Một node phải sở hữu phần lớn cổ phần trong mạng, còn được gọi là tấn công 51%. Điều này sẽ không thực tế vì để giành quyền kiểm soát mạng. Bạn cần phải chiếm hữu được 51% số lượng tiền đang được lưu hành.
- **Phân cấp**: Nếu người dùng trên mạng dựa trên PoS đầu tư gấp đôi so với người dùng khác. Họ sẽ có quyền kiểm soát gấp đôi. Kịch bản tương tự trên PoW sẽ cấp cho người dùng quyền kiểm soát theo cấp số nhân.

- Nhược điểm:
  - **Ưu tiên số lượng stake lớn:** PoS tập trung vào số lượng stake của người kiểm định. Stake lớn hơn đưa người kiểm định vào vị trí tốt hơn, được chọn nhiều hơn những nút mạng ít tiền, tạo ra một vấn đề xung quanh việc ưu tiên.
  - **Vấn đề Nothing at stake**: Người kiểm định (thợ đào) không cần bất kỳ phần cứng nào để tạo lập và có thể tạo khối bằng cách tăng số token stake của họ lên. Trong trường hợp chuỗi phụ, người kiểm định có thể tối đa hóa phần thưởng của họ bằng cách tạo khối xung quanh các nhánh khác nhau của blockchain, nó được coi là một vấn đề 'Nothing at stake'. Do vậy, blockchain sử dụng giao thức PoS đồng thuận cần những quy tắc đặc biệt hoặc biện pháp an ninh để chống lại điều này.

3.2.3. Một số cơ chế đồng thuận khác

(a) Delegated Proof of Stake (DPoS)

Cách hoạt động: DPoS là một phiên bản cải tiến của PoS, trong đó người dùng trong mạng có thể bỏ phiếu để chọn ra một nhóm delegate (đại biểu) hoặc validator thay mặt họ xác nhận giao dịch và tạo block.

Cách chọn validator: Các validator được chọn thông qua một quá trình bỏ phiếu. Những người có nhiều phiếu bầu nhất sẽ được quyền xác nhận giao dịch và tạo block. Quy trình này làm tăng tính dân chủ và cải thiện hiệu suất.

Ví dụ: EOS, TRON, Steem.

(b) Proof of Authority (PoA)

Cách hoạt động: PoA chọn validator dựa trên danh tiếng và độ tin cậy của họ, thay vì số lượng coin nắm giữ hoặc sức mạnh tính toán. Những người được chọn làm validator thường là các tổ chức hoặc cá nhân uy tín.

Cách chọn validator: Một nhóm nhỏ validator đáng tin cậy được chọn để xác nhận giao dịch và tạo block mới. Điều này giúp mạng hoạt động nhanh và hiệu quả, nhưng có thể tạo ra sự tập trung quyền lực.

Ví dụ: VeChain, Binance Smart Chain.

(c) Proof of Burn (PoB)

Cách hoạt động: Để được chọn làm miner, người tham gia cần phải "đốt" (tức là tiêu hủy) một lượng coin nhất định bằng cách gửi chúng đến một địa chỉ không thể sử dụng. Điều này tạo ra bằng chứng rằng họ sẵn sàng hy sinh tài nguyên để có quyền tạo block mới.

Cách chọn miner: Người dùng càng đốt nhiều coin thì cơ hội được chọn để tạo block càng cao.

Ví dụ: Slimcoin.

(d) Proof of Space (PoSpace) hoặc Proof of Capacity (PoC)

Cách hoạt động: PoSpace chọn miner dựa trên lượng dung lượng lưu trữ mà họ có thể cung cấp cho mạng. Người tham gia phải dành ra một lượng lớn không gian lưu trữ để tham gia vào quá trình khai thác block.

Cách chọn miner: Miner nào cung cấp nhiều dung lượng lưu trữ hơn sẽ có cơ hội lớn hơn được chọn để tạo block.

Ví dụ: Chia, Burstcoin.

(e) Proof of Elapsed Time (PoET)

Cách hoạt động: PoET là một cơ chế đồng thuận được phát triển bởi Intel, sử dụng phần cứng đặc biệt để chọn ngẫu nhiên validator bằng cách sử dụng thời gian chờ ngẫu nhiên. Người tham gia nào có thời gian chờ ngắn nhất sẽ được chọn để tạo block.

Cách chọn validator: Các validator được yêu cầu chờ một khoảng thời gian ngẫu nhiên. Người nào có thời gian chờ thấp nhất sẽ được chọn để tạo block.

Ví dụ: Hyperledger Sawtooth.

(f) Proof of Activity (PoA)

Cách hoạt động: PoA là một cơ chế kết hợp giữa PoW và PoS. Đầu tiên, các miner sử dụng PoW để tạo ra block, nhưng block này chỉ chứa thông tin cơ bản mà không có giao dịch. Sau đó, một nhóm các validator PoS sẽ được chọn ngẫu nhiên để xác thực và hoàn thiện block.

Cách chọn validator: Miner sử dụng PoW để tạo block đầu tiên, sau đó các validator PoS được chọn ngẫu nhiên dựa trên số lượng coin họ nắm giữ.

Ví dụ: Decred.

(g) Proof of Importance (PoI)

Cách hoạt động: PoI chọn validator dựa trên mức độ quan trọng của họ trong mạng, đánh giá dựa trên các yếu tố như số lượng coin nắm giữ, tần suất giao dịch và mạng lưới liên kết với các node khác.

Cách chọn validator: Validator có chỉ số "quan trọng" cao hơn (dựa trên hành vi tham gia mạng và giao dịch) sẽ có cơ hội cao hơn để tạo block.

Ví dụ: NEM.

4. Các thuật toán và kỹ thuật được sử dụng

4.1. Mã hóa khóa công khai

Hai phương pháp chính được sử dụng để bảo mật chuỗi và đảm bảo việc xác thực là băm (hashing) và mã hóa bằng khóa bất đối xứng (asymmetric key encryption). Cả hai phương pháp này đều dựa trên các thuật toán phức tạp đã được kiểm chứng. Báo cáo này sẽ cung cấp một cái nhìn tổng quát về việc áp dụng các thuật toán này, cũng như vai trò quan trọng của chúng trong việc bảo mật chuỗi phi tập trung, cụ thể là: mã hóa khóa công khai, băm an toàn, đảm bảo tính toàn vẹn của giao dịch và của blockchain. Phần này sẽ bắt đầu bằng việc thảo luận về mã hóa khóa bất đối xứng, tiếp theo là định nghĩa về khái niệm băm và các thuật toán băm được sử dụng trong giao thức blockchain. Sau đó, sẽ giải thích cách sử dụng các kỹ thuật này để quản lý tính toàn vẹn của giao dịch và các block trong chuỗi.

Trong mạng phi tập trung blockchain, các thành viên không nhất thiết phải biết nhau, vì thế việc xác thực danh tính bằng các phương pháp truyền thống như kiểm tra giấy tờ cá nhân là không khả thi. Các thành viên có thể tham gia hoặc rời khỏi mạng bất cứ lúc nào, hoạt động mà không dựa trên lòng tin giữa nhau. Trong tình huống này, làm thế nào để nhận diện các thành viên, ủy quyền giao dịch, và phát hiện các giao dịch giả mạo hoặc có lỗi? Đáp án nằm ở việc sử dụng mã hóa khóa công khai. Trong mã hóa đối xứng, cùng một khóa được dùng để mã hóa và giải mã, nhưng nó có hạn chế là dễ bị lộ khóa bí mật từ dữ liệu mã hóa và vấn đề phân phối khóa trong một mạng phi tập trung.

Mã hóa khóa công khai khắc phục các vấn đề này bằng cách sử dụng một cặp khóa, gồm khóa công khai và khóa riêng. Khóa công khai có thể được chia sẻ công khai, trong khi khóa riêng phải được giữ kín. Ví dụ, A mã hóa dữ liệu giao dịch bằng khóa riêng của mình và sau đó bằng khóa công khai của B. Thành viên B sẽ giải mã dữ liệu bằng khóa riêng của họ và dùng khóa công khai của A để xác minh rằng chỉ có A mới có thể gửi dữ liệu này.

Một trong những thuật toán mã hóa phổ biến là RSA (Rivest Shamir Adleman), được dùng rộng rãi cho việc xác thực không cần mật khẩu. Tuy nhiên, blockchain yêu cầu một thuật toán mạnh hơn và hiệu quả hơn, đó là mã hóa đường cong elliptic (ECC), được sử dụng trong Bitcoin và Ethereum để sinh ra cặp khóa. Với cùng số bit, ECC mạnh hơn RSA, ví dụ, khóa ECC 256 bit tương đương với khóa RSA 3072 bit.

4.2. Băm (Hashing)

Để bảo vệ tài sản trong blockchain, việc giữ khóa riêng an toàn là quan trọng. Băm là gì? Hàm băm chuyển đổi và ánh xạ dữ liệu đầu vào có độ dài bất kỳ thành một giá trị cố định. Ngay cả sự thay đổi nhỏ trong dữ liệu đầu vào cũng sẽ tạo ra một

giá trị băm hoàn toàn khác. Hàm băm phải có hai thuộc tính cơ bản: nó phải là hàm một chiều và có khả năng tránh trùng lặp (hoặc trùng lặp rất thấp).

Yêu cầu thứ nhất đảm bảo không ai có thể khôi phục dữ liệu gốc từ giá trị băm. Yêu cầu thứ hai đảm bảo rằng mỗi giá trị băm là duy nhất cho một bộ dữ liệu cụ thể, với xác suất rất thấp để hai bộ dữ liệu khác nhau cho cùng một giá trị băm. Những yêu cầu này đạt được bằng cách chọn một thuật toán mạnh như hash bảo mật (secure hash), và bằng cách sử dụng số lượng bit lớn thích hợp cho giá trị hash. Kích thước băm phổ biến nhất là 256 bit, với các thuật toán phổ biến như SHA-256, SHA-3 và Keccak-256.

Giá trị băm 256 bit rất mạnh, với số lượng tổ hợp lên tới 10^77. Tỷ lệ tạo ra giá trị băm trùng lặp gần như không thể xảy ra. Có hai phương pháp chính để tính toán giá trị băm: phương pháp hash đơn giản (simple hash) và Merkle tree hash. Phương pháp hash đơn giản sắp xếp các mục dữ liệu theo thứ tự tuyến tính, trong khi Merkle tree hash tổ chức dữ liệu theo cấu trúc cây, băm theo cặp lá để đi đến giá trị cuối cùng.

Ethereum sử dụng hàm băm để sinh ra địa chỉ tài khoản, chữ ký số và băm các giao dịch, trạng thái và header của block.

4.3. Tính toàn vẹn của giao dịch

Quản lý tính toàn vẹn của giao dịch trong blockchain yêu cầu ba yếu tố chính: bảo mật địa chỉ tài khoản duy nhất, ủy quyền giao dịch thông qua chữ ký số và xác minh rằng nội dung giao dịch không bị thay đổi. Để đạt được điều này, blockchain sử dụng sự kết hợp giữa mã hóa khóa công khai và băm.

Địa chỉ tài khoản được sinh ra từ cặp khóa công khai/bí mật. Một số ngẫu nhiên 256 bit được sinh ra làm khóa riêng, sau đó sử dụng thuật toán ECC để tạo khóa công khai tương ứng. Từ đó, áp dụng hàm băm cho khóa công khai để sinh ra địa chỉ tài khoản, có kích thước ngắn hơn (160 bit). Khi thực hiện giao dịch, người gửi mã hóa dữ liệu băm bằng khóa riêng của họ để tạo chữ ký số, và người nhận có thể sử dụng khóa công khai của người gửi để xác minh tính toàn vẹn của giao dịch.

4.4. Bảo mật Blockchain

Các thành phần chính của block trong Ethereum bao gồm header, giao dịch, giá trị băm của giao dịch và trạng thái. Tính toàn vẹn của block được đảm bảo thông qua băm các thành phần trong header. Blockchain là một chuỗi không thể thay đổi, với mỗi block băm liên kết với block trước đó. Khi một block bị giả mạo, giá trị băm sẽ thay đổi, khiến chuỗi bị mất tính toàn vẹn, và các block sau đó sẽ bị từ chối bởi các miner.

Trong Ethereum, các giao dịch được tổ chức trong cấu trúc cây Merkle để tính toán giá trị băm của trạng thái và biên nhận. Cây Merkle cũng giúp tính toán lại giá trị băm khi có sự thay đổi trạng thái mà không cần tính toán lại toàn bộ cây. Bằng

cách sử dụng sự kết hợp giữa băm và mã hóa khóa công khai/bí mật, blockchain đảm bảo tính bảo mật và toàn vẹn của các giao dịch và block trong chuỗi.

III. SMART CONTRACT

1. Smart contract là gì?

Hợp đồng thông minh là các hợp đồng kỹ thuật số được lưu trữ trên một blockchain, tự động thực thi khi đáp ứng các điều khoản và điều kiện đã được xác định trước.

Hợp đồng thông minh là một tính năng cực kỳ mạnh mẽ của Blockchain, nó là phần tử tính toán của chuỗi khối. Mạng Bitcoin có một tính năng gọi là script để chứa những luật lệ và chính sách (rule and policies). Bitcoin sử dụng script được đính kèm với giao dịch để thêm những điều kiện cần thực hiện khi chuyển giao tài sản. Nhưng những script này khá đơn giản và có khả năng giới hạn. Sau đó Ethereum xuất hiện và mở rộng và cải thiện hơn so với Bitcoin. Một sự đóng góp to lớn của Ethereum chính là hợp đồng thông minh nơi hỗ trợ thực thi bất kỳ code nào trên Blockchain. Từ đó nó sẽ giúp người dùng thực hiện những hoạt động có độ phức tạp lớn hơn, tăng khả năng tương thích của Ethereum Blockchain để trở thành một hệ thống tính toán phi tập trung mạnh mẽ.

Một hợp đồng thông minh đại diện cho một lớp business logic, với một logic cụ thể được lập trình trong một ngôn ngữ bậc cao. Một hợp đồng thông minh chứa những hàm có thể kích hoạt chạy bằng những tin nhắn hoạt động như function calls. Những tin nhắn này cùng tham số dành cho hàm chứa trong tin nhắn được nêu cụ thể trong các giao dịch.

Hợp đồng thông minh thường được sử dụng để tự động hóa việc thực hiện một thỏa thuận sao cho tất cả những người tham gia đều có thể chắc chắn ngay lập tức về kết quả, mà không cần sự can thiệp của bên thứ ba hoặc mất thời gian. Chúng cũng có thể tự động hóa một quy trình công việc, kích hoạt hành động tiếp theo khi đáp ứng các điều kiện đã xác định trước. Tính minh bạch của người dùng được bảo vệ nhờ vào các giao dịch thực hiện nhưng không cần phải cung cấp danh tính trước đó.

Ví dụ chúng ta có thể hẹn giờ tự động giao dịch, hoặc trả góp cho một món hàng hàng tháng với một lãi suất cụ thể. Những việc này mang đến những điều kiện, điều luật, chính sách mà những giao thức chuyển giao tiền mã hóa cần phải xử lý được. Hợp đồng thông minh đáp ứng nhu cầu này cho những ứng dụng xác thực cụ thể cho Blockchain.

Khi đã được triển khai trên Blockchain, hợp đồng thông minh là một đoạn code không thể thay đổi. Chúng ta sẽ cần phải triển khai lại một hợp đồng thông minh mới, hoặc bằng cách nào đó chuyển hướng tin nhắn gọi từ hợp đồng cũ sang hợp đồng mới.

2. Cách hoạt động của Smart Contract

2.1. Cơ chế hoạt động

Smart Contract hoạt động dựa trên các câu lệnh điều kiện dạng "if / when… then…" được mã hóa và lưu trữ trên blockchain. Khi các điều kiện định sẵn được đáp ứng và xác thực, mạng lưới sẽ tự động thực thi các hành động đã lập trình.

Các hành động này có thể bao gồm việc gửi tiền/tài sản/token cho các bên, đăng ký tài sản, gửi thông báo, hoặc tạo chứng từ như hóa đơn và vé điện tử. Một khi giao dịch được thực hiện, thông tin sẽ được ghi lại trên blockchain, đảm bảo tính bất biến và chỉ các bên được cấp quyền mới có thể truy cập kết quả.

Để thiết lập các điều khoản của Smart Contract, các bên cần xác định chi tiết dữ liệu giao dịch trên blockchain, thống nhất về các quy tắc và ngoại lệ của hợp đồng, đồng thời xây dựng phương án xử lý cho các trường hợp tranh chấp. Tất cả các quy tắc sẽ được lập trình trực tiếp vào hợp đồng nhằm đảm bảo thực hiện chính xác và minh bạch các cam kết đã thỏa thuận giữa các bên.

2.2. Các yếu tố cần

Chủ thể hợp đồng: Các bên tham gia thực hiện giao kết hợp đồng, trong đó có những bên được cấp quyền truy cập, theo dõi tình hình xử lý và nội dung hợp đồng.

Điều khoản hợp đồng: Các điều khoản quy định ở dạng chuỗi, được lập trình đặc biệt mà các bên tham gia phải đồng ý với các điều này.

Chữ ký số: Các bên tham gia hợp đồng thông minh đồng thuận triển khai thỏa thuận về chữ ký số và phải thực hiện thao tác thông qua chữ ký số.

Nền tảng phân quyền: Bước vào giai đoạn hoàn tất, smart contract cần được tải lên blockchain. Chuỗi blockchain tiếp tục phân phối dữ liệu về các node và lưu lại, không thể điều chỉnh.

2.3. Quy trình hoạt động

Bước 1: Các bên tham gia giao kết smart contract bằng cách sử dụng chữ ký số để xác nhận danh tính và sự đồng ý của mình. Hợp đồng thông minh được viết bằng ngôn ngữ lập trình và được mã hóa chuyên biệt.

Bước 2: Hợp đồng thông minh được tải lên blockchain và được phân phối, sao chép bằng các node trong mạng lưới. Mỗi node sẽ kiểm tra tính hợp lệ của hợp đồng và xác nhận nó vào một khối mới.

Bước 3: Khi có lệnh triển khai, hợp đồng sẽ tự động thực thi đúng như các điều khoản đã lập trình. Một mạng máy tính sẽ thực hiện các hành động khi đáp ứng được điều kiện xác minh. Các hành động có thể là: chi trả tiền, đăng ký phương tiện, xuất hóa đơn, gửi thông báo…

Bước 4: Sau khi hoàn thành các hành động, kết quả sẽ được ghi lại và cập nhật trên blockchain. Các bên có quyền truy cập có thể xem kết quả và không thể tự ý thay đổi giao dịch.

3. Ưu điểm và nhược điểm của Smart Contract

3.1. Ưu điểm

- **Tốc độ, hiệu quả và chính xác cao:** Vì hợp đồng thông minh là kỹ thuật số và tự động, không có thủ tục giấy tờ để xử lý và không mất thời gian để điều chỉnh các lỗi thường xảy ra khi điền tài liệu theo cách thủ công. Nên khi một điều kiện được đáp ứng, hợp đồng được thực hiện ngay lập tức.
- **Đáng tin cậy và minh bạch:** Vi không có bên thứ 3 tham gia và các bản ghi chép mã hóa về các giao dịch đều được chia sẻ giữa những người tham gia giao dịch. Do đó bạn không cần phải lo lắng về giao dịch có đến được với người bên kia hay không? Hay lo lắng về tài sản mình giao dịch bị thất thoát hay không? Tất cả đều rất minh bạch, rõ ràng và đáng tin.
- **Bảo mật:** Các bản ghi giao dịch trong chuỗi khối được mã hóa, điều này khiến chúng rất khó bị hack. Hơn nữa, bởi vì mỗi bản ghi được kết nối với các bản ghi trước đó và sau đó trên một sổ cái phân tán, điều này sẽ rất tốn thời gian và công sức khi tin tặc sẽ phải thay đổi toàn bộ chuỗi để thay đổi một bản ghi duy nhất.
- **Áp dụng trong nhiều lĩnh vực:** Hợp đồng thông minh có thể được phát triển trên rất nhiều lĩnh vực khác nhau như: tiền điện tử, xuất nhập khẩu, bất động sản, bầu cử…
- **Tiết kiệm:** Hợp đồng thông minh sẽ loại bỏ nhu cầu về các bên trung gian để xử lý các giao dịch bằng cách mở rộng, rút ngắn thời gian và phí liên quan của chúng.

3.2. Nhược điểm

- **Khó sửa chữa**: Hợp đồng thông minh khi đã được tải lên blockchain thì không thể được sửa đổi hay hủy bỏ. Điều này có thể gây ra những vấn đề khi có sự thay đổi trong điều kiện hoặc mong muốn của các bên tham gia.
- **Khó giải quyết tranh chấp**: Hợp đồng thông minh không có cơ chế giải quyết tranh chấp khi có xảy ra những tình huống ngoài dự kiến hoặc không rõ ràng. Các bên tham gia có thể phải tìm đến các tổ chức hoặc cá nhân khác để giải quyết, nhưng điều này có thể mất nhiều thời gian và chi phí.
- **Phụ thuộc vào công nghệ blockchain**: Hợp đồng thông minh hoạt động dựa trên công nghệ blockchain, do đó nó cũng phải chịu những hạn chế của công nghệ này, ví dụ như: khả năng mở rộng, hiệu suất, tiêu thụ năng lượng, v.v.

- **Thiếu pháp lý**: Hợp đồng thông minh hiện nay vẫn chưa được công nhận và quy định rõ ràng bởi các luật pháp của các quốc gia. Điều này có thể gây ra những khó khăn và rủi ro khi áp dụng hợp đồng thông minh trong các giao dịch quốc tế hoặc liên quan đến các quyền và nghĩa vụ pháp lý.

4. Triển khai Smart Contract trên mạng Etherum

Về cơ bản, hợp đồng thông minh là một đoạn code bất biến được chạy trên mạng blockchain.

Hợp đồng thông minh có thể chứa các biến bên trong nó và gọi là các biến trạng thái. Ta có thể lấy dữ liệu các biến này và quan sát các biến thay đổi qua các block như thế nào. Một hợp đồng thông minh của Ethereum Blockchain có những thành phần sau:

- Pragma directive để chỉ phiên bản ngôn ngữ Solidity cho Compiler
- Tên của hợp đồng
- Dữ liệu hoặc các biến trạng thái tạo nên trạng thái của hợp đồng
- Tập hợp các hàm phục vụ mục đích tạo ra hợp đồng

Ở phần này, báo cáo sẽ sử dụng ngôn ngữ Solidity và IDE Remix - một môi trường phát triển phổ biến nhất dành cho Solidity nói riêng và hợp đồng thông minh nói chung.

4.1. Remix IDE

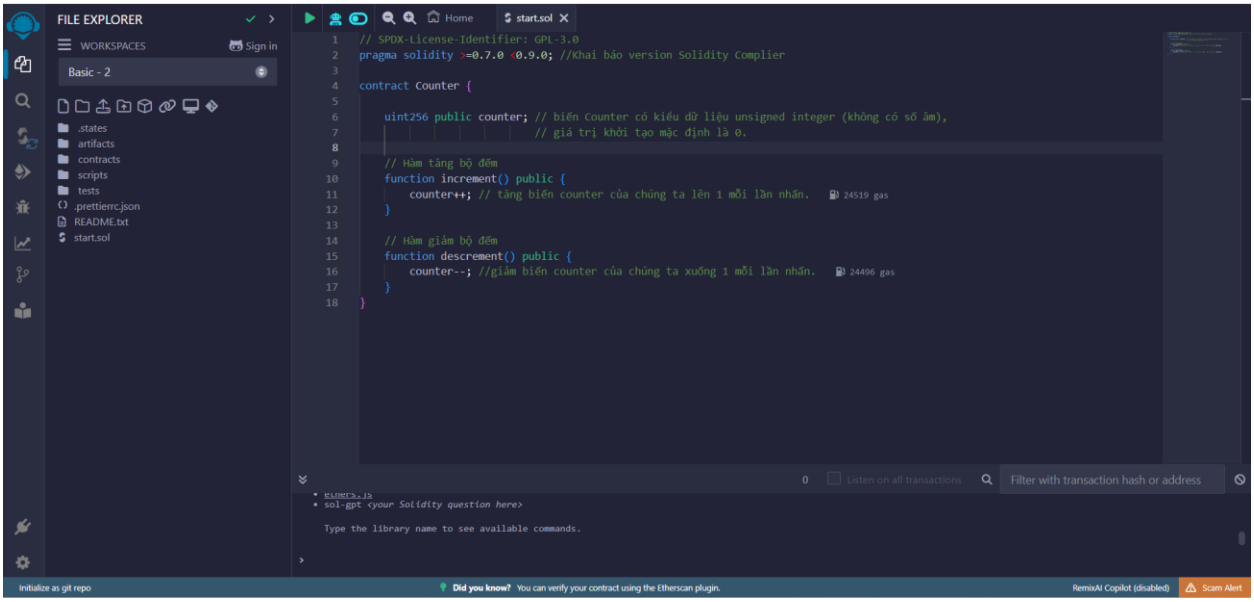
Remix IDE là một môi trường phát triển tích hợp (IDE) dựa trên web, chuyên dùng để viết, biên dịch, triển khai và kiểm thử các hợp đồng thông minh trên nền tảng Ethereum. Remix IDE là công cụ phổ biến nhất để phát triển các hợp đồng thông minh bằng ngôn ngữ Solidity và có thể chạy trực tiếp trên trình duyệt mà không cần cài đặt phần mềm.

Các tính năng chính của Remix IDE:

- **Soạn thảo mã nguồn (Code Editor):** Cung cấp giao diện đơn giản để viết và quản lý mã Solidity. Soạn thảo mã có tính năng hỗ trợ cú pháp, làm nổi bật các lỗi và cảnh báo trong thời gian thực.
- **Trình biên dịch (Compiler):** Remix tích hợp trình biên dịch Solidity giúp chuyển đổi mã nguồn thành mã máy để triển khai lên mạng blockchain Ethereum. Người dùng có thể chọn phiên bản Solidity mà họ muốn sử dụng.
- **Triển khai hợp đồng (Deployment):** Remix hỗ trợ việc triển khai hợp đồng thông minh lên Ethereum Mainnet, Ropsten, Rinkeby, và nhiều mạng test khác. Ngoài ra, có thể triển khai cục bộ bằng cách sử dụng JavaScript VM.
- **Trình mô phỏng giao dịch (Transaction Simulation):** Remix cho phép người dùng kiểm thử các giao dịch và tương tác với hợp đồng thông minh

mà không cần kết nối trực tiếp với blockchain thực. Điều này giúp giảm thiểu chi phí và thời gian thử nghiệm.

- **Debugging (Gỡ lỗi):** Remix có công cụ gỡ lỗi mạnh mẽ giúp theo dõi và phân tích các giao dịch, kiểm tra các thay đổi về trạng thái và bộ nhớ trong hợp đồng thông minh.
- **Tích hợp với các công cụ khác:** Remix tích hợp dễ dàng với các công cụ phát triển khác như Metamask, Ganache, và Truffle, giúp việc quản lý và triển khai hợp đồng thông minh trở nên tiện lợi hơn.



Hình 6. Giao diện của REMIX IDE

4.2. Ngôn ngữ lập trình Solidity

Solidity là một ngôn ngữ lập trình hướng đối tượng, high-level, curly-bracket được phát triển bởi team Ethereum Network.

Ngôn ngữ này ra đời nhằm để xây dựng và thiết kế các Smart Contracts (hợp đồng thông minh) trên các nền tảng của blockchain.

Nó có rất nhiều điểm tương đồng với C và C ++. Solidity khá đơn giản để học và dễ hiểu. ***Ví dụ:*** main trong C tương đương với contract trong Solidity.

Giống như các ngôn ngữ lập trình khác, Solidity cũng có biến, hàm, classes, Toán tử số học, thao tác chuỗi và nhiều khái niệm khác.

4.3. Các bước lập trình và triển khai Smart Contract

4.3.1. Code minh họa

```solidity
// SPDX-License-Identifier: MIT
pragma solidity ^0.8.0;

contract SimpleWallet {
    // Địa chỉ chủ sở hữu ví
    address public owner;

    // Sự kiện cho việc gửi và rút tiền
    event Deposit(address indexed sender, uint amount);
    event Withdraw(address indexed receiver, uint amount);

    // Khởi tạo hợp đồng và đặt chủ sở hữu là người triển khai
    constructor() {
        owner = msg.sender;
    }

    // Hàm để gửi tiền vào hợp đồng (payable)
    function deposit() external payable {
        require(msg.value > 0, "Phải gửi một số tiền lớn hơn 0");
        emit Deposit(msg.sender, msg.value);
    }

    // Hàm rút tiền chỉ có chủ sở hữu có thể thực hiện
    function withdraw(uint _amount) external {
        require(msg.sender == owner, "Chỉ chủ sở hữu có thể rút tiền");
        require(_amount <= address(this).balance, "Số dư không đủ");

        payable(owner).transfer(_amount);
        emit Withdraw(owner, _amount);
    }

    // Hàm để lấy số dư của hợp đồng
    function getBalance() external view returns (uint) {
        return address(this).balance;
    }
}
```

Hình 7. Code Solidity minh họa

(a) Cấu trúc dữ liệu và biến

- **Biến** owner:
  - Kiểu dữ liệu: address
  - Chức năng: Lưu trữ địa chỉ của chủ sở hữu ví, chỉ người này có quyền rút tiền.
  - Khởi tạo trong hàm constructor với giá trị là msg.sender (người triển khai hợp đồng).
- **Sự kiện** Deposit **và** Withdraw:
  - Deposit: Ghi lại thông tin khi có người gửi tiền vào hợp đồng. Chứa các tham số sender (người gửi) và amount (số tiền gửi).

- Withdraw: Ghi lại thông tin khi chủ sở hữu rút tiền khỏi hợp đồng. Chứa các tham số receiver (người nhận tiền) và amount (số tiền rút).

(b) Hàm deposit()

- **Chức năng**: Cho phép gửi tiền vào hợp đồng.
  - Hàm deposit() có từ khóa payable, cho phép nhận tiền Ether.
  - Kiểm tra giá trị msg.value lớn hơn 0 để đảm bảo có tiền được gửi vào.
  - Sau khi gửi tiền thành công, phát ra sự kiện Deposit để ghi lại thông tin giao dịch.
- **Gas**: Hàm này tạo một transaction vì nó thay đổi số dư của hợp đồng, gây ra việc ghi dữ liệu lên blockchain.

(c) Hàm withdraw()

- **Chức năng**: Rút tiền từ hợp đồng, chỉ dành cho chủ sở hữu.
  - Kiểm tra msg.sender để đảm bảo chỉ có chủ sở hữu (owner) có quyền rút tiền.
  - Kiểm tra số dư hợp đồng (address(this).balance) để đảm bảo có đủ tiền cho giao dịch rút.
  - Thực hiện chuyển tiền với lệnh payable(owner).transfer(_amount).
  - Sau khi rút tiền thành công, phát ra sự kiện Withdraw để ghi lại thông tin giao dịch.
- **Gas**: Đây là một transaction vì nó thay đổi số dư và cập nhật dữ liệu blockchain.

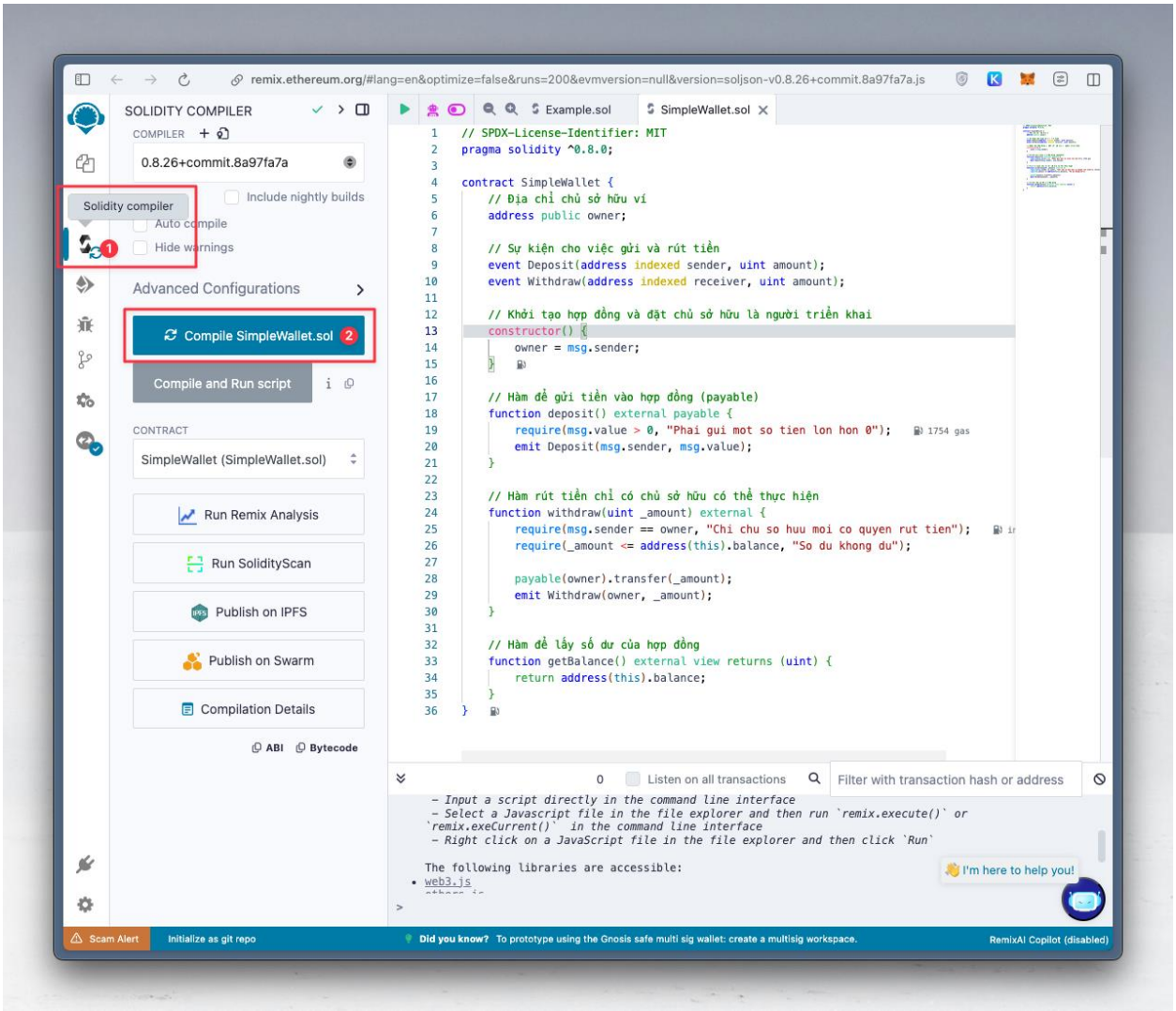
(d) Hàm getBalance()

- **Chức năng**: Trả về số dư hiện tại của hợp đồng.
  - Đây là hàm view, chỉ đọc dữ liệu (số dư hợp đồng) mà không thay đổi trạng thái blockchain.
- **Gas**: Vì là hàm view, getBalance() không tạo transaction và có thể được gọi miễn phí, không tiêu tốn gas.

4.3.2. Triển khai Smart Contract lên blockchain

- **Bước 1:** ***Biên dịch (Compile)***

Sau khi hoàn thành một đoạn code, ta truy cập vào thẻ “Solidity Compiler”của Remix IDE và chọn biên dịch file .sol.

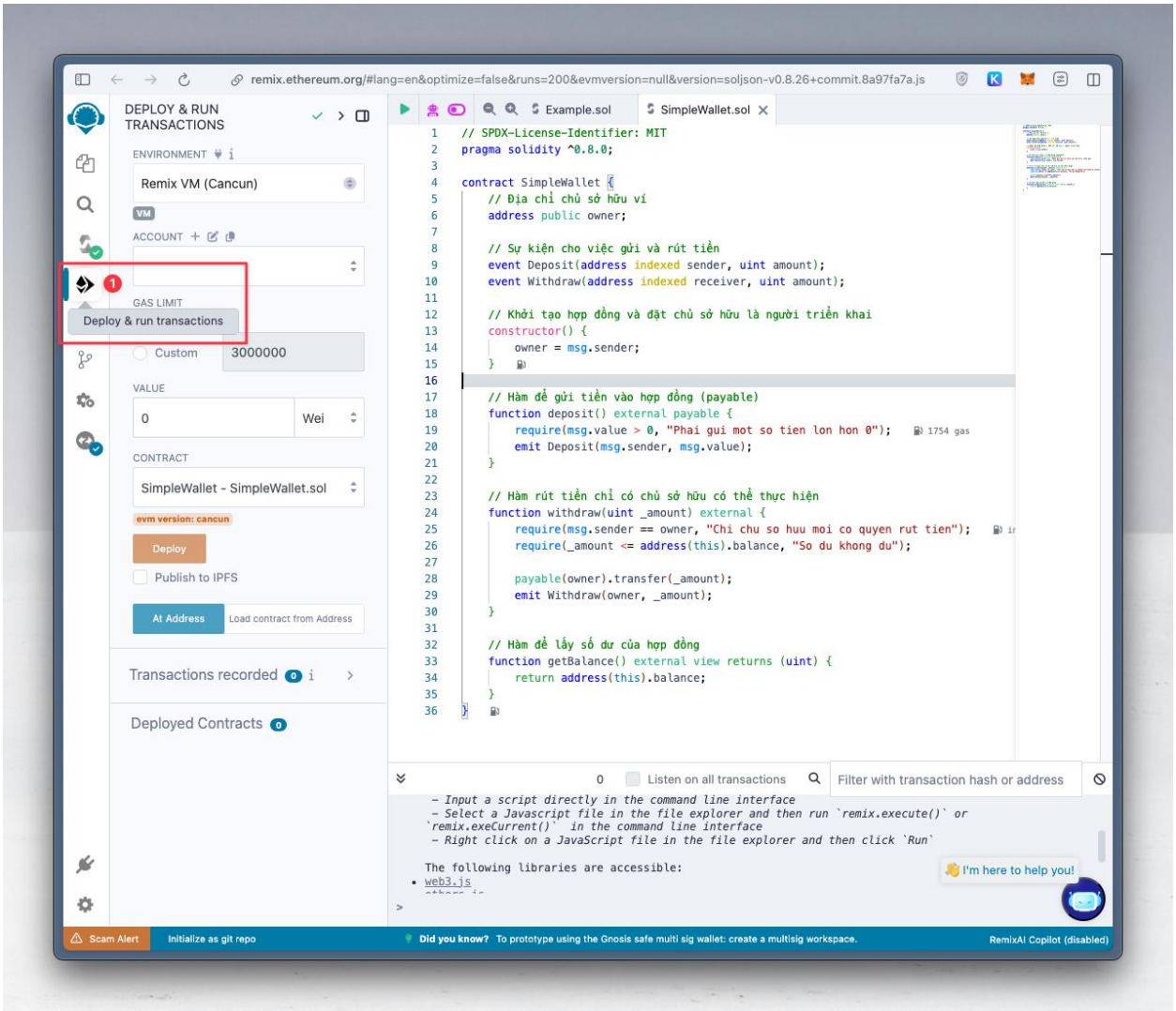


Hình 8. Giao diện trang biên dịch của Remix IDE

IDE sẽ thông báo bằng tích xanh hoặc dấu "x" đỏ khi biên dịch thành công hoặc thất bại.

- **Bước 2: *Triển khai***

Sau khi biên dịch thành công, chuyển sang thẻ "Deploy & Run Transactions" để bắt đầu thực hiện triển khai smart contract.



Hình 9. Giao diện trang triển khai và thực thi giao dịch Remix IDE

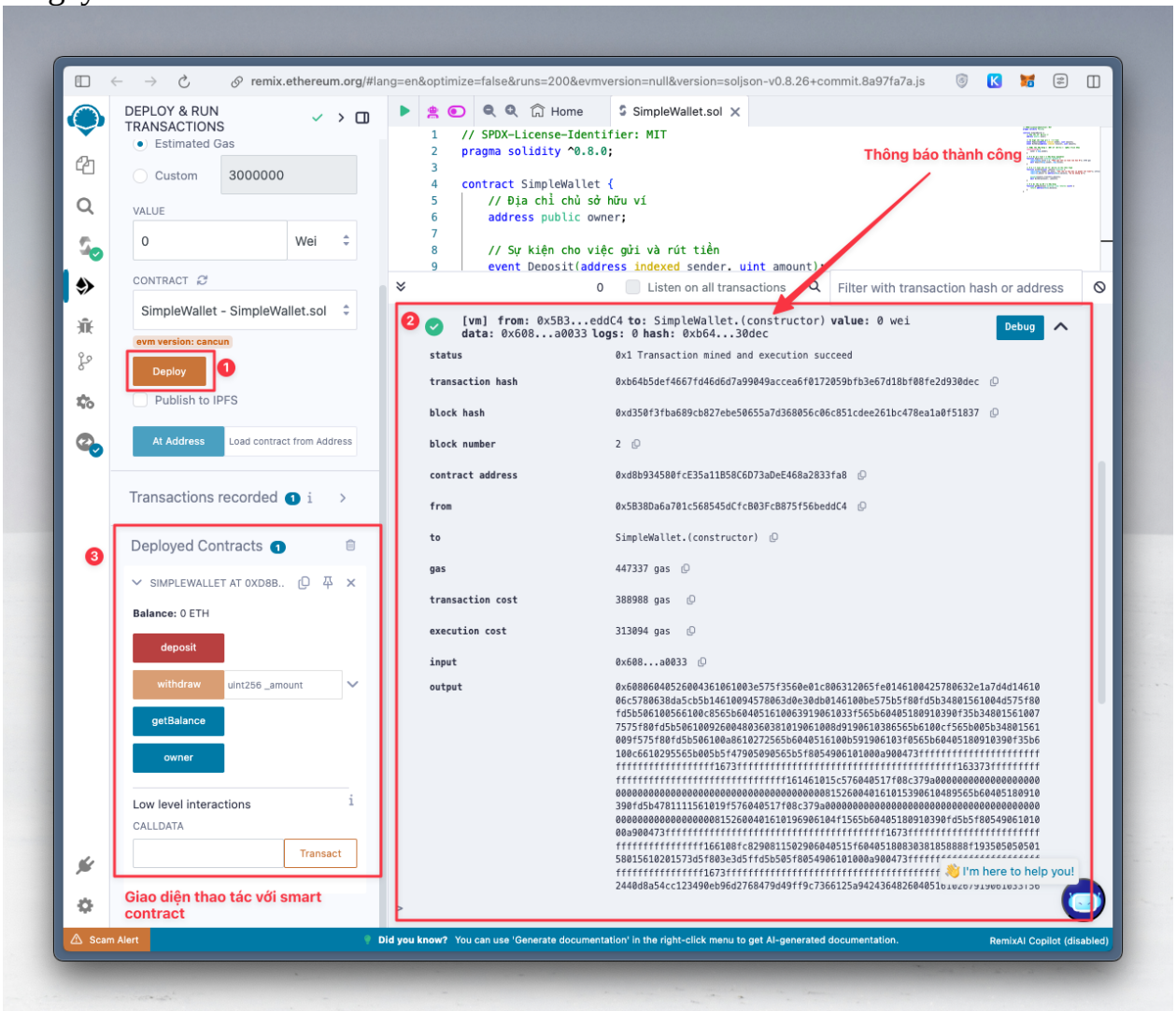
Tại đây, người dùng cần lựa chọn các cấu hình yêu cầu trước khi thực hiện triển khai:

- Môi trường (Environment): Môi trường triển khai
    - **JavaScript VM**: Deploy hợp đồng trên một blockchain giả lập trong trình duyệt, không mất phí gas.
    - **Injected Web3**: Kết nối với MetaMask để triển khai trên một testnet hoặc mạng chính của Ethereum.
    - **Web3 Provider**: Kết nối với một nút từ xa (ví dụ: Infura hoặc Alchemy).
- Tài khoản (Account): Chọn tài khoản (có số dư) sẽ thực hiện hành động triển khai.
- Giới hạn Gas: Cấu hình giới hạn lượng gas mà hành động triển khai sẽ tiêu tốn.

- Giá trị (Value): Giá trị token (ether) sẽ được gửi kèm lệnh triển khai.
- Hợp đồng (Contract): Lựa chọn hợp đồng sẽ muốn triển khai lên mạng blockchain trong trường hợp có nhiều hợp đồng có sẵn.

Thao tác triển khai hợp đồng lên mạng blockchain cũng sẽ làm thay đổi dữ liệu trên mạng nên nó cũng sẽ được coi là một giao dịch, vì vậy tuỳ vào môi trường người dùng lựa chọn để deploy, sẽ có các quy trình khác nhau để có thể gửi lệnh triển khai và thực hiện giao dịch đó. Để đơn giản hoá trong phạm vi báo cáo, ví dụ sẽ sử dụng môi trường giả lập của Remix IDE.

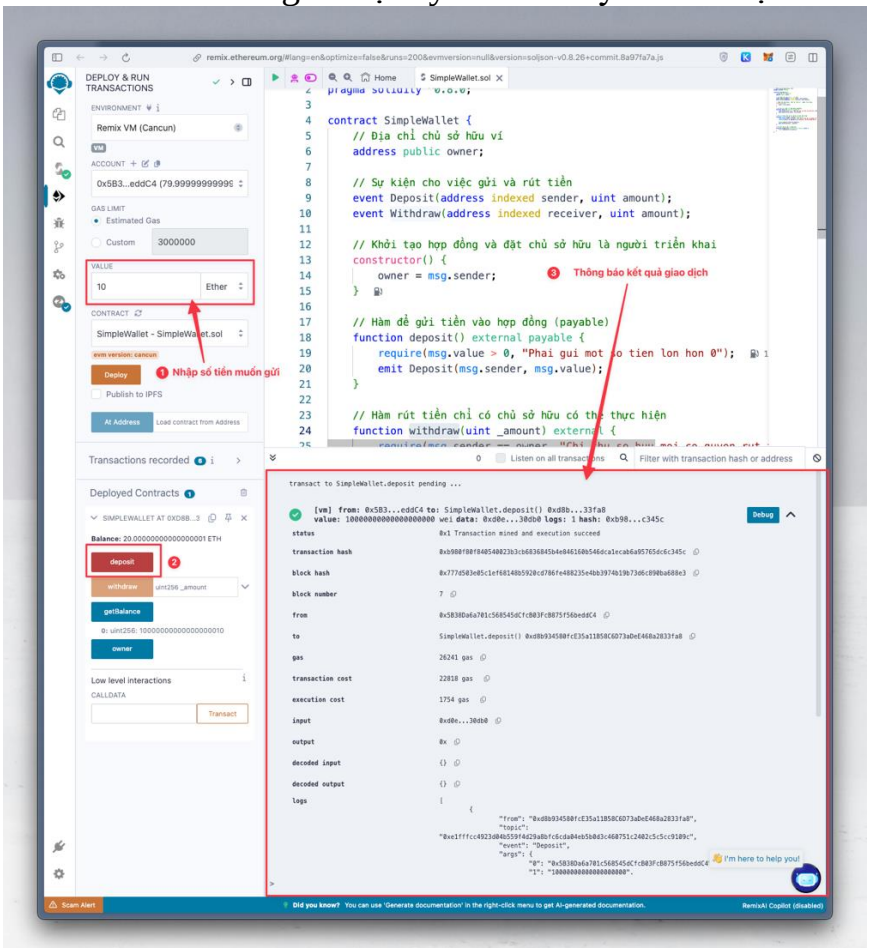
Sau khi cấu hình xong các tuỳ chọn và nhấn "Deploy", giao dịch yêu cầu triển khai hợp đồng sẽ được gửi lên mạng blockchain để xử lí. Sau khi triển khai thành công, ta có thể thấy được giao diện để thực hiện giao tiếp với hợp đồng thông minh ở ngay trên IDE.



Hình 10. Giao diện sau khi triển khai smart contract thành công

4.3.3. Thực hiện thao tác với Smart Contract

- **Bước 1:** Xem các hàm và trạng thái của smart contract
  - Sau khi triển khai thành công, hợp đồng của bạn sẽ xuất hiện dưới phần **Deployed Contracts**.
  - Tại đây, người dùng sẽ thấy danh sách các hàm đã được định nghĩa trong smart contract. Ví dụ:
    - Các hàm ***public*** và ***external*** sẽ hiển thị như các nút bấm để bạn có thể tương tác.
    - Các biến ***public*** sẽ hiển thị để bạn xem trực tiếp giá trị của chúng.
- **Bước 2:** Gọi các hàm
  - Với các hàm view hoặc pure, người dùng có thể gọi hàm mà không tốn phí gas. Ví dụ, hàm ***getBalance()*** có thể được gọi để lấy số dư đang có trong hợp đồng bằng cách nhấn ***getBalance***.
  - Với các hàm thay đổi trạng thái (ví dụ: ***deposit, withdraw***), người dùng sẽ cần trả phí gas để gọi chúng vì các hàm trên thực hiện sẽ tạo ra giao dịch yêu cầu thay đổi dữ liệu trên mạng blockchain.



Hình 11. Giao diện khi thực hiện gọi hàm và kết quả giao dịch

- Ở thông báo kết quả của giao dịch trong console, các thông tin của giao dịch sẽ được hiển thị:
  - Trạng thái (Status): Trạng thái của giao dịch (thành công hay thất bại).
  - Mã băm của giao dịch (transaction hash).
  - Mã băm của khối mà giao dịch được chèn vào (block hash).
  - Số khối (Block number).
  - Địa chỉ gửi (from): Địa chỉ ví thực hiện thao tác gọi hàm.
  - Địa chỉ nhận (to).
  - Gas, transaction cost, execution cost: phí gas cần sử dụng để có thể thực hiện giao dịch.
  - Đầu vào (input): input đã qua hàm băm.
  - Đầu ra (output): output đã qua hàm băm.
  - Đầu vào được giải mã (decoded input).
  - Đầu ra được giải mã (decoded output).

IV. CÁC ỨNG DỤNG TRONG BLOCKCHAIN

1. Tổng quát

Tổng quát các ứng dụng của Blockchain trong các lĩnh vực và ví dụ minh họa:

STT	Lĩnh vực	Ví dụ
1	Quản lý chuỗi cung ứng	Theo dõi việc cung cấp sản phẩm,nguồn gốc và điểm đến. Cuối cùng, nó giúp xác định nguồn gốc xuất xứ của sản phẩm. Các công ty như IBM, Wallmart đang tận dụng công nghệ này. IBM Blockchain, Blockverify, Origin Trail, De Bia, v.v.
2	Đá quý	De Beers- Đế chế kim cương hùng mạnh nhất thế giới đóng góp vào 30% của thị trường cung cấp kim cương. Hiện đang sử dụng Tracr là blockchain-backed đầu tiên trên thế giới để truy xuất và tìm nguồn kim cương ngay từ các mỏ, giúp lưu vết thông tin kim cương trên trang sức thành phẩm. Blockverify_ Nó cũng tập trung vào giải pháp chống hàng giả sử dụng Blockchain để tìm ra nếu có bất kỳ sản phẩm giả mạo.
3	Bán lẻ	Một phân khúc khác mà Blockchain có thể chứng minh là cực kỳ có lợi là bán lẻ. Warranteer-- Nó là một ứng dụng Blockchain cho phép người tiêu dùng truy cập thông tin về sản phẩm họ đã mua.

		Blockpoint- Nó đơn giản hóa việc tạo ra hệ thống thanh toán và cho phép thanh toán khác nhau các nền tảng như chương trình khách hàng thân thiết, thẻ quà tặng, ví di động để hoạt động
4	Giải trí & Truyền thông	Công nghệ Blockchain hứa hẹn sẽ thay đổi cách cung cấp, sử dụng và thanh toán nội dung giải trí, chẳng hạn như phim, video, âm nhạc, v.v. Ngoài ra, nó bổ sung tính bảo mật và kiểm soát minh bạch để cải thiện chuỗi cung ứng của ngành và giảm vi phạm bản quyền.
5	Âm nhạc	Spotify- Ứng dụng nghe nhạc nổi tiếng đã được mua lại khởi động Phòng thí nghiệm Medichain. Sự thống nhất là để phát triển các giải pháp thông qua cơ sở dữ liệu phi tập trung để hỗ trợ kết nối tốt hơn các nghệ sĩ và cấp phép thỏa thuận với các bản nhạc trên Spotify.
6	Chăm sóc sức khỏe	Một lĩnh vực khác mà Blockchain đang được sử dụng rộng rãi trong lĩnh vực chăm sóc sức khỏe. Ở đây nền tảng Blockchain có thể được sử dụng để giữ tất cả các hồ sơ y tế, và các dữ liệu khác liên quan đến bệnh sử của bệnh nhân, có thể dễ dàng truy cập bởi y tế các chuyên gia. MedicalChian- Đó là công ty chăm sóc sức khỏe đầu tiên sử dụng công nghệ Blockchain để quảng bá lưu trữ và sử dụng hồ sơ sức khỏe điện tử, và điều này đã được sử dụng để cung cấp dịch vụ y tế từ xa. SimplyVital Health- Đây là một ứng dụng phổ biến khác Nền tảng chuỗi khối cho phép chăm sóc sức khỏe các nhà cung cấp và bệnh nhân để truy cập, chia sẻ và di chuyển dữ liệu chăm sóc sức khỏe của họ.
7	Bất động sản	Blockchain đã được chứng minh là cực kỳ có lợi, ngay cả trong lĩnh vực bất động sản. Vấn đề minh bạch, quá nhiều thủ tục giấy tờ và kiện tụng ám ảnh cơ chế hoạt động truyền thống của bất động sản. Nhưng, với sự trợ giúp của Blockchain, những vấn đề này có thể dễ dàng vượt qua. BitProperty- Nó dân chủ hóa bất động sản, bằng cách cho phép mọi người từ bất kỳ nơi nào trên thế giới đầu tư vào bất động sản
8	Tài chính-Ngân hàng	Blockchain đóng vai trò tiên phong trong cuộc cách mạng kỹ thuật số củalĩnh vực tài chính Ví dụ: Trust Wallet, Binance Tại Việt Nam như BIDV, MB, VPBank, Vietcombank, Bảo Việt, AIA,…
9	Giáo dục	Nền tảng Hyperledger Fabric để lưu trữ dữ liệu sinh viên như điểm số, đề tài, văn bằng, chứng chỉ trong suốt quá trình học

10	Giao thông	Blockchain giúp quản lý phương tiện, tuyến đường, hỗ trợ theo dõi tình huống giao thông từ đó đưa ra thông báo về tình trạng của các tuyến đường

2. Những thành tựu áp dụng Blockchain trên thế giới

Blockchain với sự khởi đầu chính thức từ năm 2008, đã ngày càng phát triển ở khắp mọi nơi trên thế giới, được ngày càng nhiều các quốc gia ứng dụng trong nhiều lĩnh vực. Công nghệ này luôn là tâm điểm của nhiều bài báo, nghiên cứu, và là một trong những chủ đề được thảo luận nhiều nhất ở Diễn đàn Kinh tế thế giới Davos tại Thụy Sĩ vào năm 2018. Cho đến thời điểm hiện tại, công nghệ này đã được ứng dụng ở rất nhiều khu vực cũng như ở mọi lĩnh vực khác nhau như y tế, giáo dục, tài chính...

Hiện tại, Blockchain áp dụng trong 6 lĩnh vực được chi tiết dưới đây và được sử dụng ở khắp mọi nơi trên thế giới. Trong đó Estonia là một trong những quốc gia đi đầu trong việc sử dụng Blockchain cho hầu hết các hoạt động trong nước. Những cường quốc như Mỹ, Anh, Nhật, Liên minh châu Âu đã sử dụng công nghệ này trong hầu hết các hoạt động tài chính, nông nghiệp, y tế, giáo dục và logistic...

2.1. Hợp đồng thông minh

Hợp đồng thông minh, sản phẩm của blockchain, mang đến giải pháp về sự minh bạch cho các doanh nghiệp, tổ chức. Các yếu tố của hợp đồng truyền thống được ghi lại toàn bộ trên hợp đồng thông minh, nhưng được viết bằng ngôn ngữ lập trình trong hệ thống máy tính áp dụng công nghệ Blockchain. Yếu tố khác biệt của hợp đồng thông minh so với hợp đồng giấy là khả năng tự thực thi. Tự thực thi nghĩa là khi các điều kiện trong mã của các hợp đồng này được đáp ứng, chúng sẽ tự động được triển khai và hợp đồng sẽ tự có hiệu lực.

Hợp đồng thông minh được sử dụng trong nhiều mảng như bầu cử, logistic..., ví dụ như:

- Về việc bầu cử, nếu dùng Blockchain thì việc bầu cử được diễn ra rất công bằng, mọi phiếu bầu đều như nhau với danh tính được giấu kín. Vì vậy, Estonia là quốc gia đầu tiên ứng dụng công nghệ Blockchain trong quá trình bầu cử. Ireland cũng là một trong những đất nước tiên phong đưa Blockchain vào hệ thống bầu cử.
- Trong logistic, Blockchain đang đóng vai trò vô cùng quan trọng trong quá trình từ vận chuyển đến truy xuất nguồn gốc. Walmart, thương hiệu bán lẻ lớn của Mỹ, đã sử dụng Blockchain từ năm 2016 để theo dõi nguồn thịt lợn nhập từ Trung Quốc đến Mỹ. Hay Maersk, nhà vận tải giao nhận hàng đầu thế giới, cũng đã phát triển 'lịch sử số' ứng dụng Blockchain cho tất cả các lô hàng từ đầu năm 2018.

2.2 Tài chính

Từ trước đến nay, Ngân hàng với hệ thống cồng kềnh và phức tạp sẽ tốn hàng ngày giờ để xác nhận các giao dịch cơ bản. Ứng dụng Blockchain vào tài chính được xem là một cách để cắt giảm chi phí và thay vì mất hàng ngày hàng giờ thì thời gian thanh toán bù trừ giao dịch liên ngân hàng, cũng như tạo ra hệ thống giao dịch an toàn hơn các định chế xưa cũ.

Bên cạnh sự thành công của Barclays trong việc tiết kiệm chi phí khi ứng dụng công nghệ mới này, còn rất nhiều những ngân hàng khác, những tổ chức tài chính đã và đang áp dụng công nghệ này để cải thiện bộ máy cũng như tiết kiệm chi phí.

Ví dụ như:

- Ba ngân hàng lớn của Nhật Bản gồm Mizuho Bank, Sumitomo Mitsui Banking và MUFG Bank cũng đã công bố việc áp dụng công nghệ Blockchain trong hoạt động của mình.
- Tập đoàn ngân hàng lớn nhất Tây Ban Nha - Grupo Santander đã tiên phong trong ứng dụng công nghệ Blockchain vào hoạt động. Họ đã xây dựng một hệ thống thanh toán One Pay FX trên nền tảng Blockchain. Mục tiêu chính của hệ thống này là tối ưu hóa việc thanh toán giữa châu Âu và Nam Mỹ bằng việc sử dụng sổ cái phân tán.

2.3 Y tế

Trong y tế, một hệ thống Blockchain hỗ trợ lưu trữ dữ liệu bệnh nhân liên quan có thể truy cập ngay lập tức mà không mắc phải giới hạn bởi địa lý đã được sử dụng. Sự riêng tư của bệnh nhân sẽ được duy trì trên một mạng lưới phân quyền an toàn, nơi quyền truy cập chỉ được cấp cho những người được ủy quyền y tế và chỉ trong một khoảng thời gian cấp thiết. Đã có rất nhiều ứng dụng đã được phát triển dựa trên công nghệ này.

Một trong những ứng dụng kho dữ liệu y tế ban đầu hiện được nhiều chuyên gia y tế tín nhiệm là DNA.bits. Ứng dụng này mã hóa bản ghi AND/DNA của các bệnh nhân vào Blockchain và cung cấp cho các nhà nghiên cứu bằng khóa bí mật, đồng thời các nhà nghiên cứu có thể tiếp tục cập nhật công trình hay phân tích của mình trên đó.

MedicalChain - công ty chăm sóc sức khỏe đầu tiên sử dụng công nghệ blockchain để tạo điều kiện thuận lợi cho việc lưu trữ và sử dụng các hồ sơ sức khỏe điện tử nhằm mang lại trải nghiệm từ xa tuyệt vời. Công ty gồm những bác sĩ đang thực hành trong mảng cấu trúc sức khỏe ở Anh mở ra với mong muốn thay đổi hệ thống từ bên trong.

2.4 Giáo dục

Việc quản lý các chứng chỉ, bằng cấp, sinh viên của các trường đại học nói chung hay các cơ sở đào tạo nghề nói riêng nếu được áp dụng công nghệ Blockchain sẽ góp phần minh bạch hóa hồ sơ học viên cũng như giúp các nhà tuyển dụng dễ dàng truy xuất nguồn gốc cơ sở đào tạo hay quá trình học tập của các ứng viên từ thấp đến cao.

Tại San Francisco, trường Holberton - một trường đào tạo kỹ sư phần mềm đã thông báo dự án quản lý sinh viên dựa trên nền tảng blockchain vào năm học mới. Bên cạnh đó, MIT là trường đai học tiên phong trong việc cấp chứng chỉ dựa trên blockchain.

2.5 Xác minh nhận dạng số

Một hệ thống quản lý nhận dạng cá nhân là rất cần thiết ở thời điểm hiện tại. Công nghệ sổ cái phân tán được sử dụng trong Blockchain cung cấp phương pháp mã hóa công khai tiên tiến bằng cách có thể chứng minh danh tính và số hóa tài liệu của mình. Việc nhận dạng này sẽ giúp người dùng yên tâm và tránh rủi ro khi giao dịch tài chính hay tương tác trực tuyến trong nền kinh tế chia sẻ. Hơn nữa, các cơ quan chính phủ và các tổ chức tư nhân khác nhau sẽ gần nhau hơn thông qua giải pháp nhận dạng trực tuyến phổ quát mà Blockchain có thể cung cấp.

Đã có rất nhiều quốc gia ứng dụng thành công việc nhận dạng danh tính như Estonia. Đây là quốc gia đi đầu trong việc áp dụng công nghệ Blockchain, trong đó việc đưa hoạt động nhận diện dựa trên nền tảng Blockchain rất được đón nhận.

2.6 Năng lượng

Một trong những thách thức lớn nhất đối với ngành công nghiệp năng lượng là các công ty cung cấp rất cần lưu giữ thông tin ở mức chính xác tuyệt đối. Việc theo dõi phân bổ năng lượng trong thời gian thực, và đảm bảo phân phối hiệu quả thông qua chuỗi cung ứng đòi hỏi nhiều điểm dữ liệu, và cũng yêu cầu hợp tác chặt chẽ giữa tất cả các thực thể. Sử dụng Blockchain giúp cho việc lưu trữ các dữ liệu ví dụ như giá thị trường, giá nhiên liệu, chi phí cận biên, việc tuân thủ các quy định về năng lượng tái tạo... được chặt chẽ rõ ràng hơn.

IBM (Tập đoàn máy tính quốc tế) đã hợp tác với TenneT để tạo ra một platform thí điểm sử dụng công nghê Blockchain để cân bằng giữa cung và cầu của điện để đảm bảo cho nguồn cung về điện.

ElectricChain đã tạo ra SolarCoin - một loại tiền mã hóa dựa trên tiền thưởng cho một mạng lưới của các máy phát năng lượng mặt trời liên kết. Cho mỗi một MWh điện được sản xuất, bạn sẽ nhận được 1 SolarCoin - tương đương 0.50 USD.

3. Những thành tựu áp dụng Blockchain tại thị trường Việt Nam

Công nghệ blockchain tại Việt Nam đang dần được nhiều cơ quan/công ty nhận thấy lợi ích và tầm quan trọng trong bối cảnh nền kinh tế số ngày càng tăng trưởng. Trong những năm gần đây, công nghệ này đã được mạnh dạn ứng dụng trong nhiều lĩnh vực.

3.1 Sàn giao dịch NFT về tín chỉ carbon

Mỗi tín chỉ carbon đại diện cho quyền phát thải một tấn CO2. Những doanh nghiệp nào vượt quá lượng phát thải quy định, họ cần mua tín chỉ carbon để bù vào. Nếu dư, họ có thể bán quyền phát thải đó cho doanh nghiệp khác đang cần chúng. Nguồn cung của tín chỉ này đến từ những dự án phát triển tín chỉ (như trồng rừng, tái tạo năng lượng…) tuân theo quy định và tiêu chuẩn quốc tế.

Những năm gần đây, Chính Phủ thể hiện quan tâm đặc biệt đến thị trường tín chỉ carbon. Điều 17 Nghị định 06/2022/NĐ-CP quy định về thời điểm triển khai và phát triển thị trường carbon tại Việt Nam cho biết hết 2017 sẽ xây dựng quy định và quy chế vận hành sàn giao dịch tín chỉ carbon, đến 2028 sẽ tổ chức vận hành sàn giao dịch tín chỉ carbon.

Tháng 4 vừa qua, Tập đoàn Tín Thành ký kết hợp tác toàn diện với Trung tâm Chứng nhận chất lượng và Phát triển doanh nghiệp (QCC), để thương mại hoá tín chỉ carbon trên sàn giao dịch Singapore, đặt nền tảng cho việc mua bán, giao dịch tín chỉ carbon trên thị trường quốc tế của doanh nghiệp Việt Nam. Tập đoàn Tín Thành cho biết việc giao dịch dưới dạng NFT.

Công ty CP Vietnam Blockchain cũng là đơn vị cung cấp giải pháp Tín chỉ carbon ứng dụng công nghệ blockchain NFT. Việc giao dịch tín chỉ carbon bằng NFT được dự đoán rất tiềm năng ở Việt Nam khi Việt Nam có diện tích xanh lớn (rừng, lúa…). Năm 2023, Việt Nam đã bán được hơn 10 triệu tín chỉ carbon với tổng giá trị 51.5 triệu USD.

3.2 Giải pháp truy xuất nguồn gốc sản phẩm áp dụng công nghệ Blockchain

Người tiêu dùng Việt Nam ngày càng quan tâm hơn đến vấn đề nguồn gốc của một sản phẩm mình mua. Do đó, việc truy xuất nguồn gốc sản phẩm đáng tin cậy vừa tạo lòng tin cho người tiêu dùng, vừa tránh thiệt hại cho doanh nghiệp. Khảo sát của Mobifone cho biết 80% người tiêu dùng sẵn sàng trả giá cao hơn cho sản phẩm được truy xuất nguồn gốc và thông tin xác thực.

Từ đây, nhiều ứng dụng truy xuất nguồn gốc sản phẩm sử dụng công nghệ blockchain đã ra đời. Có thể liệt kê một vài cái tên trong ngách này như: mTrace của Tổng Công ty Viễn thông MobiFone, iCheck Trace của công ty cổ phần Icheck Trade, Agridential của công ty cổ phần Viet Nam Blockchain… Tất cả đều ứng dụng blockchain trong dịch vụ truy xuất của mình.

Vì sao blockchain lại hữu dụng trong lĩnh vực này? Đó là vì yêu cầu chính xác, không thể làm giả, không thể thay đổi đối với dữ liệu nguồn gốc và vận chuyển của hàng hóa. Khi tất cả được ghi vào blockchain với sự xác nhận của nhiều bên liên quan, thì sự xác nhận đó là đảm bảo.

3.3 Chia sẻ doanh thu bản quyền nhạc số bằng NFT

Việc một ca sĩ phát hành album kèm NFT không phải là điều mới thế thế giới. Tháng 5 vừa qua, siêu sao bóng đá người Bồ Đào Nha Cristiano Ronaldo vừa ra mắt bộ sưu tập token không thể thay thế (NFT) thứ 4 trong chiến dịch hợp tác với sàn điện tử Binance. Hay cũng trong tháng 5, BlackPink cũng ra mắt bộ sưu tập NFT lấy cảm hứng từ Pink Venom – một ca khúc của nhóm.

Nhưng tại Việt Nam, BinZ là một trong những nghệ sĩ tiên phong ra mắt bộ sưu tập NFT cùng với album của mình, mang tên "Don't Break My Heart", hồi đầu năm 2022.

Điều thú vị trong việc bán bộ sưu tập NFT của một ca khúc đó là người mua có thể nhận về tỷ lệ chia sẻ doanh thu bản quyền nhạc số tùy vào loại NFT mà họ mua. Trong trường hợp ca khúc Don't Break My Heart của BinZ, người mua NFT có thể nhận từ 0.05% đến 1% doanh thu bản quyền nhạc số của ca khúc.

Tuy nhiên, theo quan sát của BeInCrypto, NFT của BinZ không gây được nhiều tiếng vang. Và chưa đủ để dấy lên một làn sóng trong giới nghệ sĩ Việt Nam quan tâm đến xu hướng này.

3.4 Địa phương xây dựng blockchain riêng để phục vụ cho quản lý và du lịch

Đà Nẵng đã địa phương đầu tiên ở Việt Nam và cả Đông Nam Á tiên phong trong việc xây dựng một blockchain riêng để ứng dụng trong nhiều lĩnh vực của thành phố. Trước mắt, DanangChain đã được thí điểm trong lĩnh vực du lịch bằng việc token hóa và giao dịch NFT. Và sản phẩm địa phương OCOP Đà Nẵng được quản lý, giao dịch bằng công nghệ blockchain trên nền tảng DanangChain.

Xa hơn, DanangChain được kỳ vọng có thể ứng dụng để phục vụ cho chính quyền điện tử giúp quản lý văn bản số, bảo tàng số, truy xuất nguồn gốc thực phẩm, quản lý đất đai. Đến nay, DanangChain vẫn đang trong giai đoạn thí điểm để báo cáo và đánh giá. Dự kiến, DanangChain sẽ ra mắt vào cuối năm 2024.

Có thể nói, DanangChain là một bước đi táo bạo mang quy mô lớn mà Việt Nam từng triển khai. Nếu Chính phủ ban hành cơ chế, chính sách, quy định pháp lý hướng dẫn cụ thể… sẽ làm cơ sở để nhân rộng mô hình này trên những khu vực khác.

→ Dù đã có những ứng dụng thực tiễn, nhưng số lượng vẫn còn rất hạn chế. Nhiều ứng dụng đã nhanh chóng bị quên lãng và không thể tiếp tục phát triển hơn được, ví

dụ dự án NFT Cổng Trời, CovidPass…Nhiều ứng dụng vẫn đang chờ đợi phản ứng từ công chúng.
→ Dự đoán, cùng với tầm nhìn rằng sự phát triển nền kinh tế số Việt Nam sẽ tiếp tục dẫn đầu Đông Nam Á, thì các ứng dụng blockchain sẽ xuất hiện nhiều hơn trong đa dạng các lĩnh vực hơn thời gian tới, như y tế, logistic, hành chính, giải trí… Công chúng sẽ không chỉ tiếp cận blockchain như một cơ hội đầu tư, mà còn là một ứng dụng hữu ích trong đời sống.

4. Bitcoin

4.1 Bitcoin là gì?

Về cơ bản, Bitcoin là tiền kỹ thuật số. Bitcoin là loại tiền mã hóa đầu tiên từng được tạo ra, được công bố vào năm 2008 (và ra mắt vào năm 2009). Bitcoin cho phép người dùng gửi và nhận tiền kỹ thuật số gọi là đồng bitcoin (chữ b viết thường hoặc viết tắt là BTC).

Không giống như các loại tiền pháp định truyền thống do chính phủ phát hành (như đô la hoặc euro), Bitcoin có tính phi tập trung, nghĩa là không chịu sự kiểm soát của bất kỳ tổ chức, chính phủ hoặc pháp nhân đơn lẻ nào. Các giao dịch được thực hiện ngang hàng (P2P), không cần đến các ngân hàng hay tổ chức tài chính đóng vai trò trung gian.

Điều khiến Bitcoin trở nên hấp dẫn là khả năng chống kiểm duyệt vốn có của đồng tiền này, đặc tính không thể lặp chi và khả năng thực hiện giao dịch mọi lúc, mọi nơi.

4.2 Bitcoin hoạt động như thế nào?

Bitcoin hoạt động trên công nghệ blockchain, một sổ cái công khai ghi lại tất cả các giao dịch. Điều này nghĩa là mọi giao dịch Bitcoin đều minh bạch, có thể xác minh và an toàn.

Hãy tưởng tượng blockchain như một chuỗi các block, trong đó mỗi block đều chứa thông tin về các giao dịch. Mỗi khi ai đó sử dụng Bitcoin, giao dịch của họ sẽ được thêm vào blockchain và hồ sơ này được lưu trữ trên một mạng lưới máy tính toàn cầu (được gọi là các node).

Mạng lưới phân bổ này đảm bảo rằng không bên nào có thể thao túng dữ liệu. Bất kỳ ai cũng có thể tham gia vào hệ sinh thái bằng cách tải xuống phần mềm mã nguồn mở của Bitcoin.

- **Phi tập trung**: Blockchain của Bitcoin được duy trì bởi một mạng lưới máy tính phân bổ, đảm bảo không có cơ quan trung ương nào kiểm soát sổ cái.
- **Tính bất biến**: Sau khi thêm một giao dịch vào blockchain, không ai có thể thay đổi hoặc xóa giao dịch này.

- **Bảo mật**: Các giao dịch được mã hóa bằng mật mã và việc xác minh từng block đòi hỏi phải giải các câu đố toán học phức tạp. Quá trình này được gọi là đào.

Ví dụ về giao dịch BTC

Khi Alice gửi giao dịch BTC cho Bob, cơ sở dữ liệu blockchain sẽ cập nhật số dư của họ (ví dụ: trừ 1 BTC từ số dư của Alice và thêm 1 BTC vào số dư của Bob). Việc này giống như Alice đang viết trên một tờ giấy (mà mọi người đều có thể thấy) rằng cô ấy sẽ gửi cho Bob 1 BTC.

Khi Bob gửi số tiền tương tự cho Carol, mạng lưới có thể dễ dàng kiểm tra xem anh ta có đủ số dư BTC hay không. Blockchain này hoạt động giống như một sổ cái kỹ thuật số theo dõi tất cả các giao dịch Bitcoin và cập nhật số dư của người dùng.

Do mạng lưới có tính phi tập trung nên tất cả những bên tham gia (các node) đều có một bản sao cơ sở dữ liệu giống hệt nhau (sổ cái blockchain) được lưu trữ trên các thiết bị của họ. Vì vậy, các node phải giao tiếp liên tục để đồng bộ hóa thông tin mới.

Đào Bitcoin

Đào Bitcoin là quá trình bảo mật mạng lưới Bitcoin và xác nhận các giao dịch. Khi người dùng thực hiện một giao dịch BTC, họ sẽ phát giao dịch lên mạng lưới, nơi giao dịch được xác minh bởi các node khác gọi là "thợ đào".

Nói cách khác, đào là quá trình xác minh các giao dịch và ghi lại các giao dịch này vào cơ sở dữ liệu blockchain (sổ cái). Để làm được như vậy, các thợ đào cạnh tranh để giải quyết một vấn đề toán học phức tạp, đòi hỏi nhiều sức mạnh tính toán.

Thợ đào đầu tiên giải được câu đố sẽ thêm được một block giao dịch mới vào blockchain. Đổi lại, họ được thưởng bằng các bitcoin mới. Chi phí đào cao là một trong những yếu tố giữ an toàn cho mạng lưới và phần thưởng khối trao cho những thợ đào là nguồn bitcoin "mới" duy nhất. Mỗi block được đào sẽ thêm một lượng coin nhất định vào nguồn cung token.

Bằng chứng công việc (PoW)

Để duy trì tính bảo mật và tính toàn vẹn của blockchain, Bitcoin sử dụng cơ chế đồng thuận gọi là Bằng chứng xử lý (Proof of Work- PoW). Cơ chế này là một phần thiết yếu của quá trình đào được mô tả ở trên.

Bằng chứng xử lý (PoW) là một cơ chế được tạo ra cùng với Bitcoin để ngăn chặn việc lặp chi trong các hệ thống thanh toán kỹ thuật số. Bên cạnh Bitcoin, nhiều loại tiền mã hoá sử dụng PoW như một phương pháp để bảo mật mạng lưới blockchain của mình.

Khi chúng ta nói về một "vấn đề toán học phức tạp" mà các thợ đào phải giải quyết, về cơ bản chúng ta đang nói về PoW. PoW được thiết kế để việc tạo block trở nên tốn kém, nhưng việc xác minh block hợp lệ lại rẻ. Giả sử ai đó cố gắng gian lận bằng một block không hợp lệ. Trong trường hợp đó, mạng lưới ngay lập tức từ chối block đó và thợ đào không thể thu hồi chi phí đào.

4.3 Bitcoin dùng để làm gì?

Bitcoin chủ yếu được sử dụng như một loại tiền kỹ thuật số và lưu trữ giá trị. Bitcoin có thể được sử dụng để mua hàng trực tuyến hoặc trực tiếp, tương tự như các loại tiền tệ truyền thống. Ngày càng có nhiều doanh nghiệp chấp nhận Bitcoin làm phương thức thanh toán. Từ các nhà bán lẻ trực tuyến đến các cửa hàng truyền thống.

Bạn cũng có thể sử dụng Bitcoin để gửi tiền cho bất kỳ ai trên toàn cầu một cách nhanh chóng và với phí giao dịch tương đối thấp so với các ngân hàng và dịch vụ chuyển tiền truyền thống.

Là một khoản đầu tư, nhiều người mua Bitcoin với hy vọng giá trị của nó sẽ tiếp tục tăng. Mặc dù giá BTC có thể biến động, nhưng một số nhà đầu tư coi đó là cách để đa dạng hóa danh mục đầu tư của mình và phòng ngừa lạm phát trong dài hạn.

V. RỦI RO, HẠN CHẾ VÀ GIẢI PHÁP

1. Rủi ro

- Công nghệ blockchain bảo mật tốt như vậy nhưng tại sao các vụ tấn công vào các dự án ứng dụng blockchain vẫn xảy ra? Theo các chuyên gia an ninh mạng, nguyên nhân là do các lỗ hổng bảo mật bắt nguồn từ quá trình xây dựng và triển khai ứng dụng blockchain.
- Ví dụ: Cho đến nay, đã có hơn 40 vụ tấn công vào các sàn giao dịch tiền điện tử (ứng dụng phổ biến nhất của blockchain), gây thiệt hại hơn 1,8 tỷ đô. Trong đó, vụ tấn công gây tổn thất nặng nề nhất là vụ tấn công sàn giao dịch Coincheck. Các nhà đầu tư đã bị đánh cắp 500 triệu token NEM, tương đương 530 triệu USD. Một vụ tấn công nghiêm trọng khác là vào sàn giao dịch Mt.Gox. Sàn Mt.Gox đã phải tuyên bố đóng cửa sau khi bị thất thoát 460 triệu USD.

Như vậy, có thể thấy, các dự án ứng dụng blockchain vẫn tiềm ẩn các nguy cơ mất an toàn. Thậm chí, nhiều dự án triển khai công nghệ blockchain đã sớm lọt vào tầm ngắm của tin tặc. Do blockchain đóng vai trò quan trọng với nền kinh tế nên chúng hiển nhiên trở thành “miếng mồi ngon” cho các hành vi phá hoại an ninh mạng.

2. Hạn chế

2.1. Chi phí công nghệ

Mặc dù Blockchain có thể giúp người dùng tiết kiệm chi phí giao dịch, nhưng công nghệ này còn lâu mới có thể miễn phí.

Ví dụ: hệ thống PoW mà mạng Bitcoin sử dụng để xác thực các giao dịch, tiêu thụ một lượng lớn sức mạnh tính toán.

Trong thế giới thực, năng lượng từ hàng triệu máy tính trên mạng Bitcoin gần bằng lượng điện năng tiêu thụ hàng năm của Đan Mạch.

Bất chấp chi phí khai thác Bitcoin, người dùng vẫn tiếp tục tăng hóa đơn tiền điện để xác minh các giao dịch trên Blockchain. Đó là bởi vì khi các thợ đào thêm một khối vào chuỗi khối Bitcoin, họ sẽ nhận đủ số Bitcoin để thưởng cho thời gian và nổ lực của họ.

Tuy nhiên, khi nói đến các Blockchain không sử dụng tiền điện tử, các thợ đào sẽ cần được trả tiền hoặc được khuyến khích để xác thực các giao dịch.

Một số giải pháp cho những vấn đề này bắt đầu nảy sinh. Ví dụ: các trang trại khai thác Bitcoin thành lập và sử dụng năng lượng mặt trời, khí tự nhiên dư thừa từ các địa điểm khai thác mỏ hoặc năng lượng từ các trang trại gió.

2.2. Tốc độ và dữ liệu kém hiệu quả

Bitcoin là một nghiên cứu điển hình hoàn hảo cho sự kém hiệu quả của Blockchain. Hệ thống PoW của Bitcoin mất khoảng 10 phút để thêm một khối mới vào Blockchain. Ở tốc độ đó, người ta ước tính rằng hệ thống Blockchain chỉ có thể quản lý khoảng bảy giao dịch mỗi giây (TPS). Mặc dù các loại tiền điện tử khác như Ethereum hoạt động tốt hơn Bitcoin, nhưng chúng vẫn bị giới hạn bởi Blockchain.

Các giải pháp cho vấn đề này vẫn đang được phát triển trong nhiều năm. Hiện tại Blockchain đang tự hào có hơn 30.000 TPS.11

Vấn đề khác là mỗi khối chỉ có thể chứa rất nhiều dữ liệu. Cuộc tranh luận về kích thước khối đã và đang tiếp tục là một trong những vấn đề cấp bách nhất đối với khả năng mở rộng của các Blockchain trong tương lai.

2.3. Hoạt động bất hợp pháp

Trong khi tính bảo mật trên hệ thống Blockchain bảo vệ người dùng khỏi các vụ tấn công và quyền riêng tư, nó cũng cho phép các giao dịch và hoạt động bất hợp pháp trên hệ thống Blockchain.

Ví dụ: được biết đến nhiều nhất về việc Blockchain được sử dụng cho các giao dịch bất hợp pháp có lẽ là Con đường tơ lụa (Silk Road), một thị trường buôn bán ma túy và rửa tiền trực tuyến trên Dark web hoạt động từ tháng 2 năm 2011 đến tháng 10 năm 2013 bị đóng cửa bởi FBI.

Dark web cho phép người mua và bán hàng hóa bất hợp pháp mà không bị theo dõi bằng cách sử dụng trình duyệt Tor và thực hiện các giao dịch này bằng Bitcoin hoặc các loại tiền điện tử khác. Các quy định hiện hành của Hoa Kỳ yêu cầu các nhà cung cấp dịch vụ tài chính phải lấy thông tin khách hàng khi họ mở tài khoản, xác minh danh tính của từng khách hàng và xác nhận rằng khách hàng không xuất hiện trong bất kỳ danh sách nào của các tổ chức khủng bố hoặc bị nghi ngờ.

Hệ thống này có thể được xem là vừa chuyên nghiệp vừa gian lận. Nó cho phép bất kỳ ai cũng có thể truy cập vào các tài khoản tài chính nhưng cũng cho phép tội phạm giao dịch dễ dàng hơn.

Mặc dù Bitcoin đã sớm biết được sử dụng cho các mục đích như vậy, nhưng bản chất minh bạch và thời gian trưởng thành của nó như một tài sản tài chính đã thực sự chứng kiến hoạt động bất hợp pháp chuyển sang các loại tiền điện tử khác như Monero và Dash. Ngày nay, hoạt động bất hợp pháp chỉ chiếm một phần rất nhỏ trong tổng số Bitcoin giao dịch.

2.4. Những rào cản từ chính phủ

Nhiều người tham gia tiền điện tử đã bày tỏ lo ngại về quy định của chính phủ. Mặc dù ngày càng khó khăn và gần như không thể kết thúc một thứ như Bitcoin khi mạng lưới phi tập trung của nó đang phát triển, các chính phủ về mặt lý thuyết có thể khiến việc sở hữu tiền điện tử hoặc tham gia vào hệ thống này là bất hợp pháp.

Mối quan tâm này đã giảm dần theo thời gian, khi các công ty lớn như PayPal bắt đầu cho phép quyền sở hữu và sử dụng tiền điện tử trên nền tảng của nó.

3. Một số vấn đề điển hình trong việc ứng dụng blockchain và một số cách khắc phục

3.1. Các cuộc tấn công từ chối dịch vụ phân tán (Distributed Denial of Service - DDoS) – Sybil attack

- Các cuộc tấn công từ chối dịch vụ phân tán xảy ra khá phổ biến trên internet. Trong một cuộc tấn công DDoS, tin tặc khiến cho node độc hại "đánh cắp" danh tính của các node khác, tạo ra và phát tán nhiều danh tính giả dẫn đến việc quá tải các đường dẫn và phá hủy hệ thống.

- Tấn công DDoS diễn ra với nhiều loại hình đa dạng khác nhau vì không phải tất cả các thiết bị và mạng đều dễ bị tổn thương theo cùng một cách. Kẻ tấn công thường đòi hỏi phải sáng tạo trong kỹ thuật tấn công để có thể khai thác các lỗ hổng trong cấu hình hệ thống.

- Tổng quan lại, chúng ta có 3 loại tấn công DDOS cơ bản như sau:

- **Volume-based attacks:** Loại tấn công sử dụng lưu lượng truy cập cao để làm ngập băng thông mạng.
- **Protocol attacks:** Loại tấn công tập trung vào việc khai thác nguồn tài nguyên máy chủ.

- **Application attacks:** Tấn công nhắm vào các ứng dụng web và được coi là một loại tấn công tinh vi và nghiêm trọng nhất.

Trong đó, Volume-based attacks là loại hình tấn công phổ biến nhất. Tấn công này dựa vào việc gửi đi yêu cầu truy cập đến mục tiêu với lưu lượng nhiều hơn mức được các nhà phát triển ban đầu xây dựng cho hệ thống để xử lý, từ đó khiến người dùng bình thường không vào được các trang web đó.

* Ví dụ thực tế:

- Tấn công vào AWS (2020): Amazon Web Services phải đối mặt với cuộc tấn công có quy mô lớn nhất từ trước đến nay, với lưu lượng 2,3 Tbps. Kẻ tấn công dùng giao thức CLDAP để khuếch đại lưu lượng và gây ra gián đoạn trong ba ngày. Điều đáng sợ là khối lượng và độ phức tạp của cuộc tấn công, mặc dù AWS đã có các biện pháp giảm thiểu hiệu quả.

- Tấn công vào Google (2017): Cuộc tấn công kéo dài 6 tháng với tốc độ đạt 2,5 Tbps, sử dụng các phương pháp DDoS khuếch đại UDP nhắm vào hàng nghìn IP của Google. Các hacker dùng 180.000 máy chủ để tạo ra 167 triệu gói tin mỗi giây, gây thiệt hại lớn. Đây là một trong những cuộc tấn công được cho là do các hacker được nhà nước tài trợ.

- Tấn công vào GitHub (2018): Hacker khai thác hệ thống bộ nhớ phân tán memcache, khuếch đại lưu lượng lên 1,35 Tbps. GitHub bị ngắt kết nối trong 5 phút và gián đoạn trong 4 phút, mặc dù đã có hệ thống bảo mật mạnh mẽ.

- Tấn công vào 6 ngân hàng Hoa Kỳ (2012): Cuộc tấn công làm gián đoạn dịch vụ của các ngân hàng lớn trong vài giờ với tốc độ 60 Gbps. Các botnet (Brobot) gây tê liệt dịch vụ nhằm xác định các điểm yếu. Cuộc tấn công này có thể liên quan đến các tổ chức khủng bố, gây ảnh hưởng đến uy tín và doanh thu của các ngân hàng.

- Tấn công vào Spamhaus (2013): Hacker nhắm vào dịch vụ chặn spam mail của Spamhaus với lưu lượng 300 Gbps, gây gián đoạn truy cập internet trên diện rộng ở châu Âu trong khoảng hai tuần.

* Giải pháp:

- Thường xuyên rà soát hệ thống, bởi DDoS có thể sửa đổi các giao dịch của những khối mới.

- Sử dụng các thuật toán đồng thuận khác nhau: Bằng chứng về công việc (PoW), Bằng chứng cổ phần (PoS), Bằng chứng cổ phần được ủy quyền (DPoS)

+ Bằng chứng về công việc (PoW)

Đây là thuật toán lâu đời và chiếm ưu thế nhất, được phát triển như một cơ chế để ngăn chặn chi tiêu gấp đôi.

Proof of Work (Proof of Work, hay PoW) đảm bảo rằng điều này không xảy ra. Nó được thiết kế để sử dụng sức mạnh tính toán để băm dữ liệu của một khối

nhằm kiểm tra xem hàm băm có phù hợp với một số điều kiện nhất định hay không. Nếu các điều kiện được đáp ứng, bạn sẽ được thưởng tiền điện tử và phí giao dịch từ khối được khai thác. Tuy nhiên, sức mạnh tính toán này sẽ khiến bạn phải trả giá bằng một thứ gì đó (ví dụ: năng lượng điện)—cũng như nhiều nỗ lực thất bại trong việc băm dữ liệu sẽ khai thác khối.

Ngoài ra, phần cứng (Mạch tích hợp dành riêng cho ứng dụng, được gọi là ASIC) được sử dụng để duy trì mạng lưới các nút khai thác rất đắt đỏ. Proof of Work đã được giới thiệu với Bitcoin vào năm 2008 bởi Satoshi Nakamoto và vẫn là thuật toán an toàn nhất trong tất cả các thuật toán.

+ Bằng chứng cổ phần (PoS)

Là một giải pháp thay thế cho Proof of Work, Proof of Stake (PoS) yêu cầu bạn phải đặt cọc tiền thay vì sử dụng sức mạnh tính toán. Trong khi PoW chiếm ưu thế nhất (vì được coi là an toàn và đáng tin cậy nhất), PoS hiện đang được sử dụng phổ biến nhất bởi các mạng blockchain.

Nó được giới thiệu vào năm 2011 như một giải pháp cho các vấn đề của PoW: người dùng phải trải qua rất nhiều tính toán để chứng minh công việc của họ nhằm khai thác các khối. Mặt khác, PoS chỉ yêu cầu bạn đưa ra bằng chứng bằng cách sử dụng tiền đặt cược của mình, do đó giải quyết vấn đề lớn nhất của PoW—chi phí khai thác.

Hệ thống của cơ chế này sử dụng Thời gian đặt cọc, Yếu tố ngẫu nhiên và Sự giàu có của nút làm yếu tố để chọn người xác nhận. Những người xác nhận này sau đó phải đặt một lượng tiền nhất định vào mạng để có thể khai thác các khối.

PoS có thể cải thiện bảo mật vì kẻ tấn công phải sở hữu 51% số tiền nên chúng sẽ phải trả giá đắt, đặc biệt là trong trường hợp thất bại.

Nó cũng cải thiện khả năng phân cấp và khả năng mở rộng, tức là giới hạn số lượng giao dịch mỗi giây.

+ Bằng chứng cổ phần được ủy quyền (DPoS)

Được giới thiệu vào năm 2014, Bằng chứng cổ phần được ủy quyền (Delegated Proof of Stake, hay DPoS) là một giải pháp thay thế phổ biến cho PoS. DPoS được coi là phiên bản hiệu quả hơn của PoS vì nó có khả năng mở rộng hơn, đồng nghĩa với việc xử lý nhiều giao dịch hơn mỗi giây.

DPoS sử dụng một hệ thống bỏ phiếu cho phép người dùng thuê các đại biểu (còn gọi là nhân chứng) để làm công việc của họ. Những người này sau đó sẽ thay mặt họ bảo mật mạng. Các bên liên quan có thể bỏ phiếu cho các đại biểu dựa trên số tiền mà mỗi người dùng có.

Những đại biểu này đảm bảo sự đồng thuận trong việc khai thác và xác thực các khối mới. Phần thưởng được chia theo tỷ lệ giữa các bên liên quan và đại biểu của họ.

Vì thuật toán này dựa trên hệ thống bỏ phiếu dân chủ nên nó phụ thuộc vào danh tiếng của các đại biểu, những người này sẽ bị trục xuất khỏi mạng (network) nếu các nút của họ không hoạt động hiệu quả hoặc có đạo đức.

3.2. Cuộc tấn công 51%

- Hash rate là một chỉ số quan trọng trong mạng blockchain. Nó đại diện cho sức mạnh tính toán của thành viên trong mạng. Sức mạnh tính toán cần phải được phân phối tương đối đồng đều giữa các node. Nó không được tập trung vào một thực thể riêng lẻ nào cả. Một cuộc tấn công 51% là một kiểu xâm nhập chuỗi blockchain có thể gây ra gián đoạn mạng và cuối cùng là độc quyền khai thác. Cuộc tấn công này xảy ra khi một thợ đào, một tổ chức hoặc một thực thể duy nhất giành được hơn 50% quyền kiểm soát hash rate hoặc năng lượng tính toán chạy trên mạng của chuỗi blockchain.

- Vì chuỗi blockchain sử dụng cơ chế đồng thuận Proof-of-Work (PoW) để xác thực các giao dịch, cho nên những gián đoạn này làm chậm quá trình xác nhận và sắp xếp các khối theo thứ tự thời gian của những thợ đào. Vì vậy, nếu như năng lượng tính toán của thợ đào bị giảm xuống, thì việc xác nhận giao dịch được sắp xếp trong một khối sẽ bị gián đoạn theo. Do, mạng chuỗi blockchain bị can thiệp, nên chúng cho phép các kẻ tấn công giải các phương trình nhanh hơn một thợ đào.

Kết quả là kẻ tấn công giành được quyền kiểm soát để đảo ngược một giao dịch chưa được xác nhận từ đó gây ra chi tiêu hai lần cho một coin, điều này có thể dẫn đến mức chi tiêu tăng gấp đôi. Ngoài ra, kẻ tấn công còn nhận được phần thưởng của thợ đào. Phần thưởng này bù đắp cho các thợ đào đã cập nhật chuỗi blockchain.

* Ví dụ thực tế:

- Bitcoin Gold (BTG): Vào tháng 5 năm 2018, Bitcoin Gold đã trải qua một cuộc tấn công 51% cho phép kẻ tấn công chi tiêu gấp đôi BTG trị giá khoảng 18 triệu đô la. Sự kiện này đã gây ra thiệt hại đáng kể cho danh tiếng và giá trị thị trường của đồng tiền.

- Ethereum Classic (ETC): Có lẽ là blockchain được nhắm mục tiêu thường xuyên nhất, Ethereum Classic đã phải chịu một cuộc tấn công lớn vào tháng 8 năm 2020, nơi kẻ tấn công đã chi tiêu gấp đôi ETC trị giá 5,6 triệu đô la.

- Vertcoin (VTC): Vertcoin, mặc dù ít được biết đến hơn, đã trải qua một cuộc tấn công 51% vào tháng 12 năm 2018. Kẻ tấn công đã chi gấp đôi 603 VTC, tương đương khoảng 100.000 USD.

* Giải pháp:

- Tấn công 51% nhắm thẳng vào tiền điện tử bằng cách sử dụng thuật toán đồng thuận dựa trên Proof-of-Work (PoW). Trong khi cách phòng thủ tốt nhất đối với cuộc tấn công này là sử dụng đồng thuận Proof-of-Stake (PoS).

- Khi sử dụng thuật toán PoS, trình xác thực có thể giảm thiểu nguy cơ xâm nhập bằng cách duy trì khả năng tồn tại của mạng. Ví dụ: PoS giúp giới hạn số lượng tiền điện tử có thể stake. Do đó, ngay cả khi tấn công 51% xảy ra, thực thể cần một số tiền định danh lớn được chia sẻ với tiền điện tử ban đầu để kiểm soát hệ thống. Xem xét kỹ lưỡng tấn công 51%, tiền điện tử PoS khó có khả năng bị nhắm đến do lợi nhuận không hấp dẫn.

3.3. Các cuộc tấn công lừa đảo

- Trong một cuộc tấn công lừa đảo, mục đích của tin tặc là lấy được thông tin đăng nhập của người dùng. Chúng có thể gửi email trông có vẻ đáng tin cậy và hợp pháp đến chủ sở hữu khóa ví. Các email này yêu cầu người dùng cung cấp thông tin đăng nhập thông qua một siêu liên kết đính kèm.

- Số lượng các cuộc tấn công lừa đảo này ngày càng tăng lên trong các mạng blockchain, tạo ra vấn đề nhức nhối cho các doanh nghiệp.

- Các cuộc tấn công lừa đảo thường nhắm vào cá nhân, nhân viên công ty. Vì vậy, các biện pháp ngăn chặn tấn công kiểu này cần hướng tới giáo dục cá nhân và giải pháp diện rộng.

* Ví dụ:

Vào tháng 6/2022, cầu nối Horizon của Harmony cũng bị hack mất 100 triệu USD. Ngay đầu tháng 8, tin tặc đã khai thác lỗ hổng trên cầu nối Nomad, đánh cắp 190 triệu USD khỏi ví điện tử và chỉ để lại 651,54 USD. Đây là cuộc tấn công lớn thứ 8 trong lịch sử tiền số, đồng thời là vụ trộm thứ 7 kể từ đầu năm đến nay. Theo đó, tin tặc đã loại bỏ token blockchain một cách bất thường khi những mã bị bỏ đều có mệnh giá tương đương, ví dụ giao dịch có giá trị chính xác 202.440,725413 được thực hiện hơn 200 lần. Không giống các vụ khai thác lỗ hổng vốn ngày càng phổ biến trong năm 2022, sự cố lần này có tới hàng trăm địa chỉ nhận token trực tiếp từ cầu nối.

* Giải pháp:

- Bảo mật thiết bị: Cài đặt các phần mềm phát hiện link độc hại; phần mềm diệt virus đáng tin cậy.

- Bảo mật trình duyệt: Cài đặt tiện ích bổ sung (đã được chứng nhận) để cảnh báo về web không an toàn.

- Thường xuyên cập nhật các thủ đoạn đánh lừa thông tin đăng nhập, không phản hồi các đường link lạ.

- Xác nhận lại với đối tác khi nhận được email liên quan vấn đề yêu cầu cung cấp thông tin đăng nhập.

3.4. Các cuộc tấn công định tuyến

- Một mạng lưới/ứng dụng blockchain hoạt động dựa trên việc truyền tải một khối lượng dữ liệu khổng lồ trong thời gian thực. Tin tặc có thể lợi dụng đặc tính ẩn danh của tài khoản để đánh chắn dữ liệu trong quá trình truyền tải dữ liệu tới các nhà cung cấp dịch vụ internet.

- Mối đe dọa này thường khó nhận ra bởi việc truyền dữ liệu và các hoạt động vẫn diễn ra bình thường. Điểm nguy hiểm là các cuộc tấn công này thường sẽ làm rò rỉ dữ liệu bí mật mà các thành viên không hề biết.

*Ví dụ:

- Vụ tấn công "BGP hijacking" (chiếm đoạt định tuyến) từng xảy ra với sàn giao dịch tiền mã hóa MyEtherWallet vào năm 2018:

Tin tặc đã lợi dụng lỗ hổng trong giao thức định tuyến BGP (Border Gateway Protocol) để chuyển hướng lưu lượng truy cập của người dùng từ MyEtherWallet sang một trang web giả mạo do chúng kiểm soát. Các gói dữ liệu của người dùng truy cập vào trang này vẫn được truyền tải bình thường, nhưng thay vì đến đúng đích, chúng đã bị điều hướng sang một máy chủ khác mà tin tặc kiểm soát.

Người dùng không nhận ra rằng mình đang bị chuyển hướng. Họ vẫn nghĩ mình đang truy cập vào trang web thật của MyEtherWallet, và do đó, họ vô tình cung cấp thông tin nhạy cảm như khóa riêng (private key) và mật khẩu. Tin tặc đã lợi dụng điều này để đánh cắp tài sản tiền mã hóa của người dùng.

Cuộc tấn công này rất khó nhận ra vì người dùng vẫn thấy các hoạt động trên giao diện diễn ra bình thường. Tuy nhiên, thông tin bí mật của họ đã bị rò rỉ do lưu lượng mạng đã bị điều hướng mà họ không hề biết.

Vụ tấn công này là một minh chứng cho thấy các cuộc tấn công định tuyến có thể gây thiệt hại nghiêm trọng và khó phát hiện, đặc biệt trong các hệ thống yêu cầu bảo mật cao như blockchain.

* Giải pháp:

- Mã hóa dữ liệu
- Thay đổi mật khẩu thường xuyên; mật khẩu có độ mạnh cao
- Phân quyền tài khoản nhân viên
- Giáo dục nhân viên về các rủi ro bảo mật thông tin.

3.5. Rủi ro từ điểm cuối của mạng blockchain

- Điểm cuối của mạng blockchain là nơi con người tương tác với blockchain – trên các thiết bị điện tử như máy tính, điện thoại di động,… Tin tặc có thể quan sát

thói quen của người dùng, tấn công vào các thiết bị để đánh cắp khóa của người dùng.

* Ví dụ:

Trong nhiều vụ tấn công, tin tặc đã sử dụng phần mềm độc hại hoặc các ứng dụng giả mạo để xâm nhập vào thiết bị của người dùng. Một ví dụ điển hình là phần mềm độc hại Cerberus - một loại Trojan được thiết kế đặc biệt để đánh cắp thông tin đăng nhập, mật khẩu, và đặc biệt là mã xác thực hai lớp (2FA) từ thiết bị di động.

- Cách thức hoạt động

Giả mạo ứng dụng hợp pháp: Tin tặc tạo ra các ứng dụng trông giống hệt các ứng dụng hợp pháp, ví dụ như ví tiền mã hóa hoặc các ứng dụng quản lý tài sản. Người dùng tải xuống ứng dụng từ các nguồn không đáng tin cậy hoặc từ các quảng cáo giả mạo.

Đánh cắp thông tin quan trọng: Khi ứng dụng giả mạo được cài đặt, nó có thể truy cập vào các thông tin nhạy cảm trên thiết bị của người dùng, bao gồm khóa cá nhân, mật khẩu, hoặc mã OTP dùng để xác thực giao dịch trên blockchain. Tin tặc có thể ghi lại các thao tác bàn phím, chụp màn hình, hoặc lấy dữ liệu từ các ứng dụng khác.

Chiếm đoạt tài sản: Với thông tin đã đánh cắp, tin tặc có thể đăng nhập vào tài khoản của người dùng, chiếm đoạt các khóa cá nhân, từ đó chuyển tài sản tiền mã hóa của người dùng mà không cần sự xác nhận của họ.

- Hậu quả

Người dùng có thể mất hoàn toàn quyền kiểm soát đối với tài sản tiền mã hóa của mình. Vì các giao dịch trên blockchain là không thể đảo ngược, việc lấy lại tài sản sau khi bị đánh cắp là rất khó hoặc gần như không thể.

Các vụ tấn công vào điểm cuối như thế này rất nguy hiểm vì chúng lợi dụng chính thói quen sử dụng và sự bất cẩn của người dùng khi tương tác với blockchain trên thiết bị cá nhân.

* Giải pháp:

- Không lưu khóa blockchain dưới các dạng tệp văn bản của máy tính.
- Cài đặt phần mềm chống virus cho thiết bị điện tử.
- Thường xuyên rà soát hệ thống, giám sát thời gian, địa điểm và thiết bị truy cập.

KẾT LUẬN

Blockchain, với tính chất phi tập trung, minh bạch và bảo mật cao, đã và đang mở ra một kỷ nguyên mới trong công nghệ thông tin, từ tài chính, chuỗi cung ứng đến giáo dục và năng lượng. Qua báo cáo này, chúng ta đã cùng tìm hiểu về các khái niệm cơ bản, nguyên lý hoạt động, các thành phần cấu thành, cũng như những ứng dụng thực tiễn của Blockchain trong các lĩnh vực khác nhau. Đặc biệt, công nghệ Smart Contract và các giải pháp triển khai trên nền tảng Ethereum đã cho thấy sự đổi mới đáng kể trong cách thức giao dịch và hợp tác.

Dù có những tiềm năng to lớn, Blockchain vẫn không thiếu các thách thức và rủi ro, từ chi phí công nghệ cao, tốc độ giao dịch chậm, cho đến các vấn đề về bảo mật và tấn công mạng. Tuy nhiên, các giải pháp và cải tiến kỹ thuật đang được phát triển liên tục để khắc phục những hạn chế này, hứa hẹn sẽ mở rộng ứng dụng của Blockchain trong tương lai gần.

Ở Việt Nam, Blockchain đang dần được áp dụng vào nhiều lĩnh vực như sàn giao dịch NFT, truy xuất nguồn gốc sản phẩm, và chia sẻ doanh thu bản quyền nhạc số. Điều này cho thấy tiềm năng phát triển mạnh mẽ của Blockchain trong thị trường nội địa, đồng thời cũng đặt ra nhu cầu nâng cao nhận thức và đào tạo nhân lực về công nghệ này.

Blockchain không chỉ là một xu hướng công nghệ mà là một cuộc cách mạng trong quản lý dữ liệu và giao dịch. Để khai thác tối đa tiềm năng của nó, các doanh nghiệp và chính phủ cần tiếp tục nghiên cứu và áp dụng Blockchain một cách sáng tạo và hiệu quả, đồng thời đảm bảo tính bảo mật và minh bạch trong mọi hoạt động.

Trong bối cảnh đó, báo cáo của nhóm 10 chúng em đã cung cấp cái nhìn tổng quan và chi tiết về công nghệ Blockchain, từ các khái niệm cơ bản, nguyên lý hoạt động, cho đến các ứng dụng thực tiễn trong nhiều lĩnh vực. Chúng em hy vọng rằng những thông tin và phân tích trong báo cáo sẽ giúp bạn đọc hiểu rõ hơn về tiềm năng to lớn cũng như những thách thức mà Blockchain mang lại, đặc biệt trong việc áp dụng vào các lĩnh vực kinh tế và xã hội tại Việt Nam. Qua đó, nhóm cũng mong muốn góp phần nâng cao nhận thức và thúc đẩy sự phát triển công nghệ Blockchain trong tương lai.

-END-