|  |
| --- |
| BAN CƠ YẾU CHÍNH PHỦ  **HỌC VIỆN KỸ THUẬT MẬT MÃ**  ¯¯¯¯¯¯¯¯¯¯¯¯¯¯¯¯ |
| ĐỒ ÁN TỐT NGHIỆP  **Nghiên cứu Fungible Token trên Corda** |
| Ngành: An toàn thông tin  Mã số: 7.48.02.02  *Sinh viên thực hiện*:  **Mai Đức Hướng**  Lớp: AT16A  *Người hướng dẫn 1*:  **TS. Lê Quang Huy**  Cục Chứng thực số & Bảo mật thông tin |
| **Hà Nội, 2023** |

1. Công nghệ sổ cái phân tán và DAG
   1. Công nghệ sổ cái phân tán
      1. Khái niệm

Sổ cái phân tán (Hay sổ cái chia sẻ - DLT – distributed ledger technology) là một kỹ thuật đồng thuận cho phép sao chép, chi sẻ và đồng bộ hóa dữ liệu kỹ thuật số giữa nhiều trang web, quốc gia hay tổ chức mà không cần một trung tâm quản trị như cở sở dữ liệu tập trung. DLT đôi khi sẽ được diễn tả bằng thuật ngữ thay thế RJT (Replicated Journal Technology).

Để triển khai công nghệ số cái phân tán cần có một mạng ngang hàng (Peer to Peer) cùng với các thuật toán đồng thuận để đảm bảo việc chia sẻ dữ liệu giữa các nút mạng.

Một ví dụ đáng chú ý về công nghệ sổ cái phân tán là Bitcoin (sử dụng blockchain công khai) và Etherium (sử dụng blockchain công khai và cơ chế hợp đồng thông minh). Tuy nhiên, công nghệ sổ cái phân tán không chỉ giới hạn trong lĩnh vực tiền điện tử mà có thể áp dụng rộng rãi trong các ngành công nghiệp khác.

* + 1. Các tính năng chính
       1. Phân tán

Phân tán là một trong những đặc điểm quan trọng nhất của sổ cái phân tán. Nó đề cập tới việc lưu trữ và quản lý dữ liệu trên nhiều nút (nodes) trong mạng lưới thay vì chỉ lưu trữ trên một trung tâm quản trị duy nhất.

Trong DLT dữ liệu được sao chép và lưu trữ trên nhiều nút khác nhau (nodes) trong mạng lưới. Mỗi nút sẽ giữ một bản sao đầy đủ của thông tin và được liên kết với nhau để tạo ra một mạng lưới phân tán. Các khía cạnh cụ thể về tính phân tán trong công nghệ sổ cái phân tán (DLT)

* + - 1. Đồng thuận

Đồng thuận (consensus) là một quá trình quan trọng trong Distributed Ledger Techology (DLT). Quá trình đồng thuận đề cập đến sự thống nhất giữa các nút trong mạng lưới về trạng thái và lịch sử của sổ cái.

Dữ liệu trong DLT sẽ được đồng thuận trước các nút trong mạng lưới. Các nút phải đạt được thỏa thuận về tính toàn vẹn và nhất quán của dữ liệu trước khi chấp nhận vào lưu trữ thông tin mới vào hệ thống sổ cái. Điều này đảm bảo tính nhất quán và đồng bộ hóa dữ liệu trong sổ cái phân tán.

Để đạt được quá trình đồng thuận trong hệ thống Distributed Ledger Technology (DLT), các thuật toán đồng thuận được sử dụng. Mỗi thuật toán có hiệu quả khác nhau đối với việc duy trì sổ cái (ledger) của hệ thống.Ví dụ thực tế trong Solana blockchain, Thuật toán Proof of History (POH) đóng vai trò quan trọng trong việc xây dựng Solana thành một nền tảng Blockchain nổi tiếng với tốc độ nhanh, khả năng mở rộng mạnh mẽ và khả năng giao dịch vượt trội.

Các phương pháp đồng thuận khác nhau có ưu điểm và hạn chế riêng, sự lựu chọn phụ thuộc vào yêu cầu và tính của từng hệ thống DLT cụ thể. Mục tiêu chung của tất cả các giao thức đồng thuận là đạt được sự nhất quán và đồng bộ hóa dữ liệu giữa các nút trong mạng lưới.

* + - 1. Bất biến

Một tính chất quan trọng khác trong DLT là tính bất biến (immutability). Tính chất này đảm bảo rằng thông tin đã được ghi vào sổ cái không thể thay đổi hay bị xóa sau khi đã được xác nhận và kết nối với các khối trước đó.

Dữ liệu đã được ghi vào sổ cái không thể bị thay đổi hoặc chỉnh sửa một cách trái phép. Điều này tạo ra một sự tin cậy cao và khả năng kiểm tra lại lịch sử giao dịch. Nó giúp ngăn chặn các cuộc tấn công và thay đổi trái phép trong hệ thống, đồng thời cung cấp sự đáng tin cậy khi xem xét lịch sử giao dịch và thông tin trong DLT.

Tính chất bất biến trong DLT được đạt được thông qua sự kết hợp nhiều yếu tố khác nhau:

* Mã hóa băm (Hashing): Mỗi khối dữ liệu trong DLT được mã hóa bằng một hàm băm (hash function) để tạo ra một giá trị duy nhất, gọi là hash. Hash của mỗi khối chứa thông tin về khối đó cùng với hash của khối trước đó. Bất kỳ sự thay đổi nào trong dữ liệu của khối đều sẽ làm thay đổi hash của khối đó, từ đó phá vỡ tính bất biến.
* Chuỗi khối (Blockchain): Dữ liệu trong DLT được tổ chức thành chuỗi các khối, trong đó mỗi khối chứa hash của khối trước đó. Việc liên kết các khối thông qua hash tạo ra một chuỗi liên kết, nếu có sự thay đổi ở bất kỳ khối nào, toàn bộ các khối liên quan sẽ bị ảnh hưởng. Điều này làm cho việc thay đổi dữ liệu trong DLT trở nên khó khăn và dễ bị phát hiện.
* Thuật toán đồng thuận: DLT sử dụng các thuật toán đồng thuận như Proof of Work (PoW), Proof of Stake (PoS), Practical Byzantine Fault Tolerance (PBFT), và nhiều thuật toán khác để đạt được sự đồng thuận giữa các thành viên trong mạng. Nhờ đó, các thành viên trong mạng phải đồng ý với các thay đổi trong sổ cái trước khi chúng được chấp nhận và kết nối với sổ cái chung. Điều này đảm bảo tính bất biến của dữ liệu trong DLT.
  + - 1. Tính nhất quán

Nhất quán (consistency) trong công nghệ phân tán (DLT - Distributed Ledger Technology) đề cập đến tính đồng nhất của dữ liệu trên một mạng phân tán. Điều này đảm bảo rằng tất cả các thành viên trong mạng có quyền truy cập vào một bản sao giống nhau của dữ liệu và thấy các phiên bản dữ liệu này như nhau.

Dữ liệu trong DLT được cập nhật và đồng bộ hóa trên tất cả các nút trong mạng lưới. Mỗi nút có phiên bản đầy đủ và nhất quán của sổ cái, đảm bảo rằng mọi thay đổi được lan truyền và phản ánh đúng trên toàn bộ mạng lưới. Tính nhất quán là một yếu tố quan trọng trong DLT để đảm bảo rằng tất cả các thành viên trong mạng đồng thuận với trạng thái và lịch sử giao dịch của hệ thống. Nó đóng vai trò quan trọng trong việc xây dựng niềm tin và đảm bảo rằng dữ liệu không thể bị thay đổi một cách trái phép.

DLT được sử dụng trong các hệ thống blockchain như Bitcoin và Ethereum để đảm bảo tính nhất quán của giao dịch và trạng thái của hệ thống. Có một số cách để đạt được tính nhất quán trong DLT:

* Cơ chế đồng thuận (Consensus): DLT sử dụng cơ chế đồng thuận để đảm bảo rằng tất cả các thành viên trong mạng đồng ý với trạng thái mới của hệ thống. Các cơ chế đồng thuận như Proof of Work (PoW) hoặc Proof of Stake (PoS) được sử dụng để đảm bảo rằng các thành viên phải chứng minh rằng họ đã thực hiện công việc hoặc góp vốn để đạt được sự nhất quán.
* Mạng phân tán (Distributed network): Dữ liệu và trạng thái hệ thống được sao chép và lưu trữ trên nhiều nút (nodes) trong mạng. Các nút này cần phải đồng bộ và cập nhật thông tin với nhau để đảm bảo tính nhất quán. Khi có sự thay đổi trong dữ liệu hoặc trạng thái, mạng phân tán sẽ sử dụng cơ chế đồng thuận để đạt được sự thống nhất trong mạng.
* Mã hóa và chữ ký số (Encryption and digital signatures): Dữ liệu trong DLT thường được mã hóa và chữ ký số để bảo mật và xác thực tính nhất quán. Mã hóa đảm bảo rằng dữ liệu không thể bị thay đổi mà không được phát hiện, trong khi chữ ký số đảm bảo rằng người dùng có thể xác minh tính toàn vẹn của dữ liệu.
  + - 1. Trao đổi trực tiếp

Trong nhiều giao dịch truyền thống, các bên thường phải dựa vào các bên trung gian như ngân hàng, sàn giao dịch, hoặc các tổ chức tài chính khác để xác nhận và thực hiện giao dịch. Điều này có thể tạo ra các rào cản, phức tạp và tốn thời gian, đồng thời cũng tăng chi phí giao dịch.

Khác với truyền thống DLT cho phép trao đổi trực tiếp giữa các bên mà không cần sự can thiệp của bên trung gian. Hệ thống DLT được xây dựng trên một mạng phân tán, trong đó mỗi nút trong mạng (thành viên) giữ một bản sao của dữ liệu và trạng thái hệ thống. Khi hai bên muốn thực hiện một giao dịch, họ có thể trao đổi trực tiếp thông qua mạng DLT mà không cần thông qua bên thứ ba. Điều này giảm thiểu sự phụ thuộc vào các bên trung gian và tăng tính hiệu quả và tốc độ trong quá trình giao dịch. Sự trao đổi trực tiếp trong DLT mang lại một số lợi ích quan trọng:

* Loại bỏ bên trung gian: Với DLT, không cần có bên thứ ba để xác nhận và thực hiện giao dịch. Các bên có thể trực tiếp giao tiếp và thỏa thuận với nhau mà không cần phải tin tưởng vào một bên trung gian. Điều này giảm bớt sự phụ thuộc và chi phí liên quan đến các bên trung gian.
* Tăng tính hiệu quả: Quá trình giao dịch trực tiếp giữa các bên trong DLT thường nhanh chóng và hiệu quả hơn. Các bên có thể thực hiện giao dịch mà không cần phải chờ đợi xác nhận từ bên thứ ba hoặc chờ đợi các quy trình xử lý phức tạp. Điều này giúp giảm thiểu thời gian và công sức liên quan đến giao dịch.
* Tăng tính minh bạch và tin cậy: Dữ liệu giao dịch và trạng thái hệ thống trong DLT được lưu trữ trên một mạng phân tán, nơi mỗi thành viên có quyền truy cập vào các phiên bản dữ liệu này. Điều này tạo ra tính minh bạch và tin cậy cao, vì mọi thành viên trong mạng có thể kiểm tra và xác minh giao dịch và trạng thái hệ thống.
* Giảm rủi ro và gian lận: Sự trao đổi trực tiếp trong DLT giúp giảm thiểu rủi ro và gian lận. Vì các giao dịch được ghi chép và chia sẻ trên toàn mạng, việc thay đổi dữ liệu một cách trái phép trở nên khó khăn. Điều này tăng tính bảo mật và sự tin cậy của hệ thống.

Lợi ích của việc trao đổi trực tiếp thông qua DLT là thế, nhưng DLT (Distributed Ledger Technology) chủ yếu là một công nghệ ghi chép phân tán và không trực tiếp liên quan đến việc trao đổi trực tiếp giữa các bên. Mặc dù DLT có thể hỗ trợ việc trao đổi tài sản và dữ liệu trong một mạng phân tán, việc trao đổi trực tiếp hay gián tiếp giữa các bên phụ thuộc vào ứng dụng cụ thể và lớp giao tiếp được xây dựng trên nền tảng DLT.

* + - 1. Tính bảo mật

Bảo mật là một yếu tố quan trọng trong DLT (Distributed Ledger Technology) để đảm bảo tính toàn vẹn và an toàn của dữ liệu. Dữ liệu trong DLT được bảo mật sử dụng mã hóa và cơ chế xác thực. Các giao dịch và thông tin được bảo vệ,chỉ những người có quyền truy cập được ủy quyền mới có thể tham gia vào mạng lưới và thực hiện các hoạt động. Một số cơ chế bảo mật phổ biến trong DLT hiện nay:

* Mã hóa (Encryption): Dữ liệu trong DLT thường được mã hóa để bảo vệ nó khỏi truy cập trái phép. Kỹ thuật mã hóa sử dụng các thuật toán mật mã để chuyển đổi dữ liệu thành dạng không đọc được (ciphertext) trừ khi có khóa mã hóa đúng để giải mã nó. Mã hóa đảm bảo rằng chỉ những người có khóa mã hóa chính xác mới có thể đọc và hiểu nội dung dữ liệu.
* Cơ chế xác thực (Authentication): DLT sử dụng cơ chế xác thực để đảm bảo rằng chỉ những người được ủy quyền mới có thể tham gia vào mạng lưới và thực hiện các hoạt động. Thông qua việc sử dụng các phương pháp xác thực như chứng chỉ số, chữ ký số, hoặc các cơ chế xác thực dựa trên khóa công khai, DLT đảm bảo rằng mỗi thành viên trong mạng lưới được xác định và có quyền truy cập tương ứng.
* Hệ thống quyền riêng tư (Privacy): Trong một số trường hợp, DLT có thể hỗ trợ quyền riêng tư bằng cách giới hạn quyền truy cập vào dữ liệu. Một số giao thức DLT cho phép chỉ có các bên được ủy quyền mới có thể truy cập và xem dữ liệu cụ thể. Cơ chế như mã hóa dữ liệu hoặc sử dụng các cơ chế quyền riêng tư như ZK-SNARKs (Zero-Knowledge Succinct Non-Interactive Argument of Knowledge) có thể được áp dụng để bảo vệ quyền riêng tư của người dùng.
* Cơ chế đồng thuận (Consensus Mechanism): Cơ chế đồng thuận trong DLT không chỉ đảm bảo tính nhất quán của dữ liệu mà còn đóng vai trò quan trọng trong bảo mật. Các cơ chế đồng thuận như Proof of Work (PoW), Proof of Stake (PoS), Practical Byzantine Fault Tolerance (PBFT) và các biến thể khác đảm bảo rằng các thành viên trong mạng lưới đồng thuận về trạng thái hệ thống và xác nhận các giao dịch một cách an toàn và tin cậy.
* Kiểm tra hợp lệ (Validity Checks): Dữ liệu và giao dịch trong DLT thường phải trải qua các kiểm tra hợp lệ để đảm bảo tính toàn vẹn và đáng tin cậy. Các quy tắc và ràng buộc được thiết lập để kiểm tra tính hợp lệ của dữ liệu, ví dụ như kiểm tra chữ ký số, xác minh nguồn gốc giao dịch và đảm bảo rằng nó tuân thủ các quy tắc đã được đặt ra.

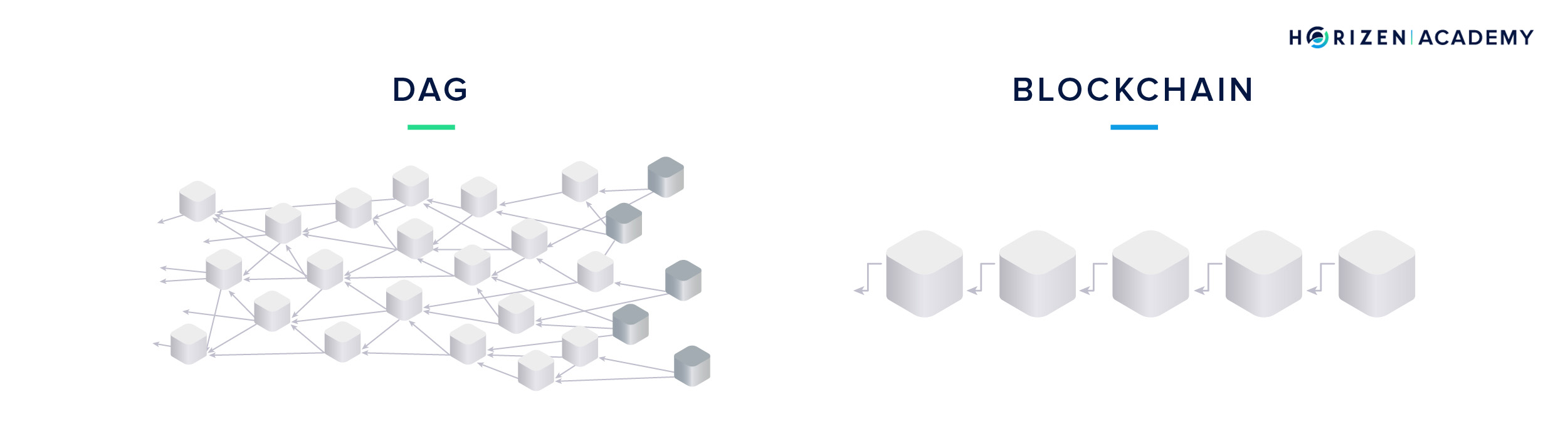
Cơ chế bảo mật có thể khác nhau tùy thuộc vào hệ thống DLT cụ thể và ứng dụng sử dụng nó. Mỗi hệ thống DLT có thể có các phương pháp và cơ chế bảo mật riêng, và việc bảo mật dữ liệu trong DLT là một lĩnh vực nghiên cứu và phát triển tiếp tục. Các cơ chế bảo mật này đóng vai trò quan trọng trong việc xây dựng một mạng lưới DLT an toàn và đáng tin cậy.

* + 1. Phân loại công nghệ DLT

Công nghệ DLT (Distributed Ledger Technology) có thể được phân loại thành các loại chính dựa trên cơ chế đồng thuận (consensus mechanism) và cấu trúc mạng lưới (network structure). Dưới đây là một số phân loại phổ biến của công nghệ DLT:

* + - 1. Blockchain

Blockchain là một công nghệ DLT (Distributed Ledger Technology) phổ biến nhất và được sử dụng rộng rãi trong nhiều lĩnh vực. Nó cung cấp một cơ chế để ghi và xác nhận các giao dịch một cách an toàn và minh bạch trong một mạng lưới phân tán. Nó được xây dựng dựa trên cơ sở dữ liệu phân tán, trong đó thông tin được lưu trữ dưới dạng các khối (blocks) liên kết với nhau thành một chuỗi khối (blockchain). Mỗi khối chứa một tập hợp các giao dịch và một mã băm (hash) của khối trước đó, tạo thành một chuỗi không thể sửa đổi và không thể thay đổi lịch sử giao dịch.

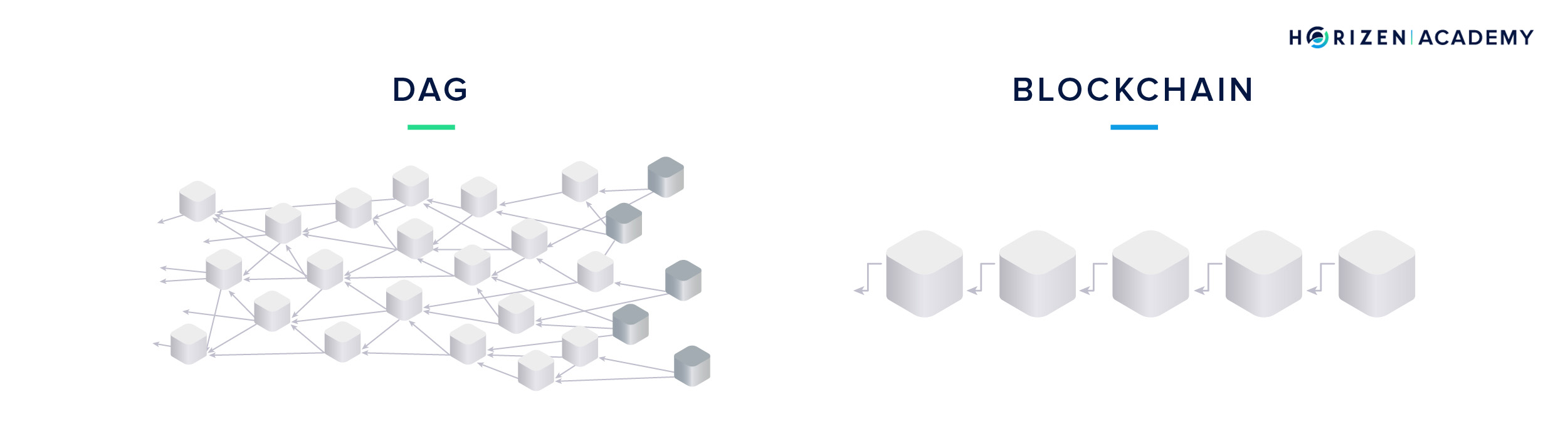
****

|  |  |
| --- | --- |
| **Ưu điểm** | **Nhược điểm** |
| Minh bạch: Blockchain cung cấp tính minh bạch cao vì mọi thành viên trong mạng lưới có thể xem và xác nhận các giao dịch. | Tốc độ giao dịch kém: Quá trình xác nhận và chứng thực giao dịch trên blockchain có thể mất thời gian và tốn năng lượng. Điều này có thể làm giảm tốc độ xử lý giao dịch so với các hệ thống truyền thống. |
| An toàn: Do dữ liệu được phân tán và mã hóa, blockchain có tính an toàn cao. Một giao dịch một khi đã được xác nhận trong blockchain, rất khó để thay đổi hay xóa bỏ nó. | Quyền riêng tư: Mặc dù blockchain đảm bảo tính minh bạch, việc bảo vệ quyền riêng tư của người dùng vẫn là một thách thức. Trong một số trường hợp, thông tin cá nhân có thể được hiển thị công khai trên blockchain. |
| Tính toàn vẹn: Blockchain sử dụng cơ chế mã băm (hashing) để liên kết các khối với nhau, tạo thành một chuỗi không thể thay đổi. Bất kỳ sự thay đổi nào trong một khối sẽ làm thay đổi mã băm và làm hỏng tính toàn vẹn của chuỗi. | Khả năng mở rộng: Khi blockchain mở rộng, kích thước của chuỗi cũng tăng lên, điều này có thể gây ra vấn đề về dung lượng lưu trữ và khả năng xử lý của mạng lưới. |
| Tính mở rộng: Blockchain có thể mở rộng bằng cách thêm các khối mới vào chuỗi, tạo ra một lịch sử giao dịch ngày càng lớn. Ngoài ra, có thể tạo ra các mạng lưới blockchain song song (sidechains) để tăng khả năng mở rộng. | Chi phí: Các giao dịch trên blockchain thường có một khoản phí liên quan đến việc chứng thực và xác nhận giao dịch. Trong một số trường hợp, chi phí này có thể cao đối với các giao dịch nhỏ. |
| Tự động hóa thông qua hợp đồng thông minh: Blockchain cung cấp khả năng thực thi các hợp đồng thông minh (smart contracts), là các chương trình tự động hóa mà không cần sự canthiết cửu của các bên trung gian. Hợp đồng thông minh được lưu trữ và thi hành trên blockchain, đảm bảo rằng các điều khoản và điều kiện của hợp đồng được tuân thủ một cách tự động và không thể thay đổi. |  |

Mặc dù có những hạn chế, Blockchain vẫn có tiềm năng để thay đổi nhiều lĩnh vực khác nhau, bao gồm tài chính, chuỗi cung ứng, bảo hiểm, quản lý tài sản và nhiều lĩnh vực khác. Sự phát triển và ứng dụng của công nghệ này tiếp tục được nghiên cứu và mở rộng để đáp ứng các yêu cầu và thách thức của thế giới kỹ thuật số ngày nay.

* + - 1. Directed Acyclic Graph (DAG)

DAG là một loại DLT khác, không sử dụng cấu trúc chuỗi khối như Blockchain. Thay vào đó, DAG sử dụng một cấu trúc mạng lưới hướng đồ thị (graph) không có chu trình. Các giao dịch trong DAG được liên kết với nhau thông qua các mối quan hệ không định hướng, tạo thành một mạng lưới phân tán. Các ví dụ nổi tiếng của DAG bao gồm IOTA và Nano.



DAG trong hệ thống phân tán là một cấu trúc dữ liệu được sử dụng để lưu trữ và quản lý thông tin trong một mạng lưới phân tán. Đây là một mô hình không có chu trình, trong đó các đối tượng (như giao dịch hoặc đơn vị dữ liệu) được biểu diễn dưới dạng các đỉnh và các mối quan hệ giữa chúng được biểu diễn bằng các cạnh có hướng.

Một số dự án nổi tiếng sử dụng mạng DAG trong hệ thống phân tán bao gồm IOTA và Nano. IOTA sử dụng mạng DAG để xây dựng một hệ thống Internet of Things (IoT) phân tán và an toàn. Nano, trước đây được gọi là RaiBlocks, sử dụng mạng DAG để tạo ra một loại tiền mã hóa phân tán với tốc độ giao dịch nhanh và không có phí giao dịch. Trên thực tế, DAG trong hệ thống phân tán đang được nghiên cứu và phát triển để áp dụng trong nhiều lĩnh vực khác nhau, từ các hệ thống thanh toán đến quản lý dữ liệu phân tán và nhiều ứng dụng khác.

* + - 1. Hashgraph

Hashgraph là một loại công nghệ sổ cái phân tán (DLT) có nền tảng trong việc xây dựng s ự đồng thuận. Mục tiêu chính của Hashgraph là đạt được đồng thuận phân tán trong mạng lưới một cách hiệu quả và tin cậy. Nó đặc trưng bởi cơ chế đồng thuận gọi là gossip protocol. Thuật toán đồng thuận của Hashgraph dựa trên một số nguyên tắc chính, bao gồm việc sử dụng dấu thời gian và việc truyền thông tin ngẫu nhiên giữa các thành viên trong mạng.

Dấu thời gian đồng thuận trong Hashgraph được gọi là "Gossip About Gossip" và cho phép các thành viên trong mạng truyền thông tin về các sự kiện mà họ biết cho các thành viên khác. Các sự kiện này được ghi lại trong một cấu trúc DAG (Directed Acyclic Graph), cho phép xác định thứ tự và quan hệ giữa các sự kiện.

Hashgraph sử dụng một thuật toán gọi là "Gossip Protocol" để truyền thông tin giữa các thành viên trong mạng. Thuật toán này cho phép thông tin được truyền ngẫu nhiên và phân tán trong mạng, đồng thời tính toán và so sánh thông tin từ các thành viên khác nhau để xác định thứ tự và đồng thuận về trạng thái hệ thống.

Nhờ vào cấu trúc DAG và thuật toán đồng thuận của mình, Hashgraph có thể đạt được tốc độ xử lý nhanh, khả năng mở rộng và bảo mật cao trong việc xây dựng và duy trì sổ cái phân tán. Hashgraph có khả năng xử lý giao dịch nhanh hơn so với Blockchain truyền thống và được cho là có khả năng mở rộng tốt hơn.

* + - 1. MultiChain

MultiChain là một DLT được phát triển dựa trên công nghệ Blockchain, nhưng với sự tập trung vào việc xây dựng các mạng lưới phân quyền (permissioned networks). MultiChain cho phép các tổ chức xây dựng và quản lý mạng lưới DLT của riêng mình, giới hạn quyền truy cập vào mạng và thực hiện các chính sách riêng.

* + - 1. Holochain

Holochain là một công nghệ phân tán (DLT - Distributed Ledger Technology) được phát triển bởi Holochain Foundation. Holochain khác với các hệ thống blockchain truyền thống bằng cách tập trung vào việc xây dựng các ứng dụng phân tán và hệ thống thanh toán, thay vì tạo ra một blockchain duy nhất để lưu trữ và xác nhận giao dịch. Mỗi ứng dụng của Holochain được xây dựng như một hệ thống phân tán độc lập, với chính sách và quy tắc riêng. Thay vì sử dụng một đồng tiền chung như Bitcoin hoặc Ethereum, Holochain cho phép các ứng dụng xây dựng các hệ thống thanh toán riêng, cho phép tạo ra các đơn vị giá trị tùy chỉnh.

Holochain cung cấp một mô hình lập trình dựa trên sự phân tách dữ liệu và tính toán. Thay vì đồng bộ dữ liệu trên toàn mạng, mỗi nút trong hệ thống Holochain chỉ lưu trữ dữ liệu liên quan đến chính nó. Khi có sự thay đổi, các nút lân cận sẽ truyền thông tin cập nhật cho nhau, giúp mỗi nút xây dựng và duy trì một phiên bản riêng của dữ liệu. Mô hình này cho phép Holochain mở rộng tốt hơn so với các hệ thống blockchain truyền thống. Vì mỗi ứng dụng hoạt động độc lập, không cần phải xử lý tất cả các giao dịch trên toàn mạng. Điều này tạo ra khả năng mở rộng ngang tốt hơn và giảm được sự phụ thuộc vào các nút mạng khác. Holochain cũng hướng đến việc cung cấp sự riêng tư cao hơn cho người dùng. Thay vì lưu trữ thông tin công khai trên toàn mạng, Holochain cho phép người dùng kiểm soát dữ liệu của họ và quyết định chia sẻ thông tin với ai.

* + 1. Ứng dụng DLT
  1. Directed Acyclic Graph (DAG)
     1. Giới thiệu

DAG (Directed Acyclic Graph) là một cấu trúc dữ liệu phi tuyến tính, trong đó các đỉnh (nodes) được liên kết với nhau theo hướng đi từ một đỉnh đến các đỉnh khác mà không tạo thành chu trình. DAG được sử dụng trong nhiều lĩnh vực khác nhau, như lý thuyết đồ thị, khoa học máy tính và cả trong lĩnh vực tiền điện tử.

Trong lĩnh vực Distributed Ledger Technology (DLT) hay Blockchain, DAG được sử dụng như một mô hình cho hệ thống ghi chép phi truyền thống, thay thế cho cấu trúc blockchain truyền thống. Các hệ thống ghi chép phi truyền thống dựa trên DAG, các giao dịch không được nhóm lại thành các khối, mà được liên kết trực tiếp với các giao dịch khác trong DAG. Điều này cho phép các giao dịch được xử lý song song và có thể xác minh một cách nhanh chóng. Trong DAG-based DLT, các giao dịch không được gom nhóm thành các khối, mà được xác minh và liên kết trực tiếp với các giao dịch khác trong DAG.

DAG (Directed Acyclic Graph) được sử dụng trong DLT (Distributed Ledger Technology) là một cấu trúc dữ liệu được sử dụng như một phương thức thay thế cho blockchain truyền thống.

* + 1. Cấu Trúc DAG

DAG là một cấu trúc dữ liệu dạng đồ thị hướng không chu trình, trong đó các đỉnh biểu diễn các đối tượng và các cạnh biểu diễn mối quan hệ giữa chúng.

Ảnh có chứa vòng tròn, ảnh chụp màn hình, hàng, biểu đồ

Mô tả được tạo tự động

Cấu trúc DAG gồm các thành phần sau:

* Đỉnh (Vertex): Mỗi đỉnh trong DAG đại diện cho một đối tượng hoặc sự kiện cần mô hình hóa. Ví dụ, trong một DAG biểu diễn quá trình xử lý công việc, mỗi đỉnh có thể đại diện cho một bước xử lý cụ thể.
* Cạnh (Edge): Các cạnh trong DAG biểu diễn mối quan hệ hướng dẫn giữa các đỉnh. Cạnh thường được hướng từ một đỉnh gốc đến một đỉnh đích để thể hiện sự thứ tự hoặc phụ thuộc giữa các đối tượng hoặc sự kiện. Các cạnh này thể hiện quyết định về thứ tự thực hiện hoặc sự phụ thuộc logic.
* Đường dẫn (Direction): DAG yêu cầu rằng các cạnh phải có hướng, tức là chúng chỉ trỏ từ một đỉnh đến một đỉnh khác. Điều này đảm bảo rằng không có chu trình trong đồ thị, điều quan trọng để giữ cho DAG duyệt và tính toán hiệu quả.

Điều đặc biệt DAG không thể chứa chu trình (acyclic), nó có nghĩa là không có đường đi từ một đỉnh trở lại chính nó thông qua một chuỗi các cạnh. Điều này khác với đồ thị thông thường, trong đó có thể tồn tại chu trình.

* + 1. Cách thức hoạt động

Trong DLT, Các đỉnh trong đồ thị biểu diễn các đối tượng, chẳng hạn như giao dịch hoặc thông tin liên quan đến tài sản. Các cạnh trong đồ thị biểu diễn mối quan hệ giữa các đối tượng. Mỗi đỉnh chứa thông tin về một giao dịch hoặc một sự kiện quan trọng trong hệ thống. Đối với mỗi đỉnh, nó có thể liên kết với một hoặc nhiều đỉnh khác, đại diện cho các giao dịch hoặc sự kiện trước đó mà nó phụ thuộc vào. Điều này tạo ra một mạng lưới của các đỉnh được kết nối với nhau thông qua các cạnh, tạo thành cấu trúc DAG. Các giao dịch mới được xác nhận bằng cách thực hiện xác thực và ghi lại các giao dịch trước đó trong DAG. Các giao dịch mới có thể liên kết với nhiều giao dịch trước đó mà không cần chờ đợi cho một khối mới được thêm vào như trong blockchain truyền thống. Điều này cho phép mạng xử lý tốt hơn và mở rộng hơn.

Cấu trúc DAG có những ưu điểm hơn so với blockchain truyền thống, bao gồm khả năng mở rộng tốt hơn, tốc độ giao dịch nhanh hơn và giảm độ trễ. Tuy nhiên, nó cũng đối mặt với một số thách thức, như việc sắp xếp giao dịch và bảo mật.

Việc sắp xếp các giao dịch trong cấu trúc DAG là một yếu tố quan trọng để đảm bảo tính toàn vẹn của dữ liệu và xác định thứ tự chính xác của các giao dịch trong hệ thống. Điều này đòi hỏi một thuật toán đặc biệt để thực hiện quá trình này. Một trong những thuật toán phổ biến được sử dụng để sắp xếp các giao dịch trong DAG-DLT là thuật toán GHOST (Greedy Heaviest Observed Subtree). Thuật toán này tập trung vào việc chọn một nhánh con có trọng số lớn nhất trong DAG để xác định thứ tự của các giao dịch. Nó giúp xác định thứ tự chính xác của các giao dịch trong DAG bằng cách chọn nhánh con có trọng số lớn nhất, đảm bảo rằng các giao dịch quan trọng và có trọng số cao nhất được xác nhận trước. Điều này giúp bảo đảm tính toàn vẹn của dữ liệu và đồng thời cải thiện hiệu suất của hệ thống.

Hoạt động của DAG trong DLT có nhiều khía cạnh khác nhau nhưng có thể tổng kết qua những khía cạnh sau:

Giao dịch và liên kết: Trong một hệ thống DLT dựa trên DAG, mỗi giao dịch mới được thêm vào DAG thông qua việc liên kết với các giao dịch đã được xác minh trước đó. Thay vì gom nhóm các giao dịch vào khối như trong blockchain, giao dịch trong DAG có thể kết nối với nhiều giao dịch khác, tạo thành một mạng lưới các giao dịch liên quan.

* Xác minh các giao dịch: Khi một giao dịch mới được thêm vào DAG, nó phải được xác minh bởi các thành viên khác trong mạng. Điều này thường đòi hỏi người gửi giao dịch phải tham gia vào việc xác minh một số giao dịch khác. Quá trình xác minh này giúp đảm bảo tính nhất quán và độ tin cậy của hệ thống.
* Xử lý đan luồng: DAG cho phép xử lý các giao dịch song song, nghĩa là nhiều giao dịch có thể được xác minh và xử lý cùng một lúc. Điều này giúp tăng tốc độ giao dịch và khả năng mở rộng của hệ thống.
* Xử lý xung đột: Vì DAG không có khái niệm chuỗi khối như blockchain, các giao dịch có thể xảy ra cùng lúc và xung đột với nhau. Để giải quyết vấn đề này, các hệ thống DLT dựa trên DAG thường sử dụng các thuật toán đặc biệt để giải quyết xung đột và đảm bảo tính nhất quán của dữ liệu.
  + 1. Ứng dụng DAG

DAG có rất nhiều ứng dụng trong việc xử lý dữ liệu, khai phá dữ liệu, học máy – trí tuệ nhân tạo hay thậm chí là lập lịch. Có thể đúc kết một số ứng dụng của DAG như sau:

* DAG được sử dụng trong các thuật toán quyết định để biểu diễn quy trình ra quyết định. Ví dụ, trong thuật toán tìm kiếm A\* (A-star), DAG được sử dụng để biểu diễn không gian trạng thái và các quyết định di chuyển từ trạng thái này sang trạng thái khác.
* Trong lĩnh vực phân tích mạng xã hội, DAG thường được sử dụng để mô hình hóa quan hệ kết nối giữa các thành viên trong mạng. Điều này có thể giúp phân tích sự lan truyền thông tin, phân nhóm, tìm kiếm cộng đồng, hay xác định vai trò của các thành viên trong mạng xã hội.
* DAG được sử dụng trong các hệ thống xử lý dữ liệu phân tán như Apache Hadoop hoặc Apache Spark để biểu diễn luồng công việc (workflow) và quan hệ phụ thuộc giữa các tác vụ.
* DAG được sử dụng để biểu diễn sự phụ thuộc giữa các thành phần trong hệ thống phần mềm, như biểu đồ gọi hàm trong ngôn ngữ lập trình. Điều này giúp xác định thứ tự thực hiện các tác vụ và quản lý luồng điều khiển của chương trình.
  + 1. So sánh DAG và mô hình DLT khác
    2. Một số nền tảng DAG

Apache Airflow: Đây là một hệ thống quản lý công việc phân tán mã nguồn mở được xây dựng trên cơ sở của DAG. Airflow cho phép bạn định nghĩa, lên lịch và thực thi các công việc trong một luồng công việc phức tạp. Nó cung cấp giao diện người dùng dễ sử dụng và tích hợp với nhiều công cụ khác nhau.

Apache Spark: Đây là một hệ thống tính toán phân tán mã nguồn mở được sử dụng rộng rãi trong xử lý dữ liệu lớn. Spark hỗ trợ DAG để biểu diễn và thực thi các tác vụ xử lý dữ liệu phức tạp. Nó cung cấp một API dễ sử dụng và hỗ trợ xử lý dữ liệu theo thời gian thực, xử lý đồng thời và xử lý dữ liệu trong bộ nhớ.

TensorFlow: Đây là một thư viện mã nguồn mở phổ biến trong lĩnh vực học máy và trí tuệ nhân tạo. TensorFlow sử dụng DAG để biểu diễn mô hình học máy và quá trình huấn luyện. Các phép tính trong mô hình được biểu diễn dưới dạng các nút trong DAG, trong đó các nút đại diện cho các phép tính và các cạnh đại diện cho quan hệ phụ thuộc giữa chúng.

Dask: Dask là một thư viện tính toán phân tán mã nguồn mở và cung cấp một API tương tự với NumPy và Pandas. Dask sử dụng DAG để biểu diễn và thực thi các phép tính phân tán. Nó cho phép xử lý dữ liệu lớn vượt qua khả năng của một máy tính đơn lẻ bằng cách phân chia công việc thành các tác vụ nhỏ hơn và thực thi song song trên nhiều máy tính.

Luigi: Luigi là một hệ thống quản lý công việc phân tán mã nguồn mở được phát triển bởi Spotify. Nó cho phép xây dựng các luồng công việc phức tạp bằng cách sử dụng DAG. Luigi cung cấp một DSL (Domain-specific Language) để định nghĩa các công việc và quyết định thứ tự thực hiện chúng dựa trên các quan hệ phụ thuộc.

* 1. CryptoToken
     1. Khái niệm CryptoToken

CryptoToken là một thuật ngữ được sử dụng trong lĩnh vực blockchain và tiền điện tử để chỉ một loại tài sản kỹ thuật số được tạo ra và quản lý trên một nền tảng blockchain. CryptoToken đại diện cho quyền sở hữu, quyền truy cập hoặc giá trị của một tài sản thực, như tiền tệ, chứng khoán, bất động sản, nghệ thuật kỹ thuật số hoặc các tài sản kỹ thuật số khác.

CryptoToken được xây dựng và quản lý thông qua sử dụng các hợp đồng thông minh (smart contracts) trên blockchain, cho phép tự động hóa việc phát hành, giao dịch và quản lý tài sản. Qua các hợp đồng thông minh, các quy tắc và điều kiện cho việc giao dịch và sử dụng CryptoToken có thể được xác định, bao gồm việc áp dụng phí giao dịch, quyền truy cập và xác thực. CryptoToken có thể được chia nhỏ thành đơn vị nhỏ hơn, cho phép giao dịch một phần nhỏ của tài sản. Ngoài ra, nó có thể được phân loại thành các loại khác nhau như utility tokens, security tokens và stablecoins, mỗi loại có mục đích và tính chất riêng.

Sự phát triển của CryptoToken đã mở ra nhiều ứng dụng tiềm năng, bao gồm việc gọi vốn thông qua Initial Coin Offerings (ICO) và Security Token Offerings (STO), tạo ra các hệ thống tiền tệ kỹ thuật số mới, tham gia vào thị trường DeFi (Decentralized Finance) và thực hiện việc tokenization của các tài sản truyền thống.

* + 1. Đặc trưng thiết kế

Trước khi tìm hiểu về các đặc trưng thiết kế của một CryptoToken, hãy hiểu rằng CryptoToken là một khái niệm tổng quát dùng để đề cập đến các loại tài sản kỹ thuật số phát hành trên các nền tảng blockchain. Các CryptoToken có thể đại diện cho các tài sản, quyền sở hữu, dịch vụ hoặc thậm chí các quyền lợi trong một mạng lưới blockchain.

Đặc trưng thiết kế của một CryptoToken là những yếu tố quan trọng mà dự án hoặc giao thức blockchain xác định để xây dựng và quản lý Token đó. Các đặc trưng này định nghĩa cách mà Token được phát hành, giao dịch và quản lý, cũng như quyền lợi, tính năng và tính bảo mật của Token đó. Các đặc trưng này bao gồm tiêu chuẩn token, hợp đồng thông minh, phân phối và phát hành, quyền sở hữu và quyền điều khiển, giao dịch và thanh toán, tính tương thích và tương tác. Bằng cách hiểu những đặc trưng này, chúng ta sẽ có cái nhìn tổng quan về cách mà các dự án và giao thức xây dựng và quản lý CryptoToken trên các nền tảng blockchain khác nhau.

* Tiêu chuẩn token: Một CryptoToken thường được xác định bởi một tiêu chuẩn cụ thể, chẳng hạn như ERC-20 trên Ethereum, BEP-20 trên Binance Smart Chain hoặc SPL Token trên Solana. Tiêu chuẩn này định nghĩa các quy tắc và giao thức cho việc phát hành và quản lý CryptoToken, bao gồm các phương thức chính như chuyển đổi, chuyển nhượng và xem số dư.
* Hợp đồng thông minh (smart contracts): CryptoToken thường được tạo và quản lý thông qua sử dụng hợp đồng thông minh. Hợp đồng thông minh là các đoạn mã tự thực thi chứa các quy tắc và điều kiện xác định việc phát hành, giao dịch và quản lý CryptoToken. Điều này cho phép tự động hóa các quy trình và loại bỏ sự phụ thuộc vào bên thứ ba.
* Phân phối và phát hành: CryptoToken có thể được phân phối và phát hành theo các phương thức khác nhau. Một số phương thức phổ biến bao gồm ICO (Initial Coin Offering), STO (Security Token Offering), airdrop (phát token miễn phí) và mining (khai thác). Quy tắc và điều kiện của phân phối và phát hành được xác định trong hợp đồng thông minh.
* Quyền sở hữu và quyền điều khiển: CryptoToken cho phép người sở hữu sở hữu và kiểm soát các quyền liên quan đến tài sản hoặc dịch vụ mà nó đại diện. Quyền sở hữu và quyền điều khiển có thể bao gồm quyền bỏ phiếu, quyền tham gia vào quyết định cộng đồng, quyền nhận lợi tức hoặc quyền truy cập vào các tính năng và dịch vụ.
* Giao dịch và thanh toán: CryptoToken cho phép người dùng thực hiện giao dịch và thanh toán trên nền tảng blockchain. Việc giao dịch và thanh toán có thể được thực hiện trực tiếp giữa các bên mà không cần sự can thiệp của bên thứ ba trung gian. CryptoToken cũng có thể có tính năng bảo mật và ẩn danh để bảo vệ sự riêng tư của người dùng.
* Tính tương thích và tương tác: CryptoToken có thể tương thích và tương tác với các ứng dụng và dịch vụ khác trên cùng một nền tảng blockchain. Điều này mở ra khả năng tích hợp và sử dụng trong các hệ thống DeFi (Decentralized Finance), NFT (Non-Fungible Token), các nền tảng trao đổi và các ứng dụng phụ thuộc vào blockchain.

Ngoài ra đặc trưng thiết kế của một CryptoToken cụ thể có thể khác nhau tùy thuộc vào mục đích và yêu cầu của dự án hoặc giao thức blockchain cụ thể mà nó được xây dựng trên.

* + 1. Phân loại CryptoToken

Việc phân loại CryptoToken sẽ dựa trên nhiều tiêu chí khác nhau, bao gồm mục đích sử dụng, quyền sở hữu, cơ chế phát hành và quản lý, cấu trúc kỹ thuật, và nền tảng blockchain mà chúng được phát triển trên. Dưới đây là một số phân loại phổ biến của CryptoToken:

* Currency Tokens: Đây là loại Token được sử dụng như một đơn vị tiền tệ trong một hệ thống kinh tế số hoặc mạng lưới blockchain cụ thể. Ví dụ phổ biến nhất là Bitcoin (BTC), Ethereum (ETH) và Ripple (XRP). Token tiền tệ thường được sử dụng để thực hiện các giao dịch, chuyển tiền và lưu trữ giá trị.
* Security Tokens: Đây là loại Token đại diện cho quyền sở hữu hoặc giá trị tài sản truyền thống, chẳng hạn như cổ phiếu, trái phiếu hoặc quỹ đầu tư. Token bảo mật thường tuân thủ các quy định về chứng khoán và có thể đòi hỏi tuân thủ các quy định pháp lý nghiêm ngặt.
* Utility Tokens: Đây là loại Token được sử dụng để truy cập và sử dụng các dịch vụ hoặc ứng dụng trên một nền tảng blockchain cụ thể. Token tiện ích thường cung cấp các quyền lợi, ưu đãi hoặc tiện ích nhất định cho người sở hữu Token đó. Ví dụ điển hình là Token được phát hành trong các dự án ICO (Initial Coin Offering).
* Non-Fungible Tokens - NFTs: Đây là loại Token độc nhất, không thể thay đổi và đại diện cho một đối tượng duy nhất hoặc một tác phẩm nghệ thuật số độc nhất. NFTs đã tạo ra sự đột phá trong lĩnh vực nghệ thuật số và cho phép việc giao dịch, sở hữu và đảm bảo tính xác thực của các tác phẩm nghệ thuật số.
* Non-Financial Application Tokens: Đây là loại Token được sử dụng trong các ứng dụng phi tài chính như trò chơi điện tử, giáo dục, dịch vụ xã hội, hợp đồng thông minh và nhiều lĩnh vực khác. Token này thường được tạo ra để thúc đẩy sự tương tác và tiếp thị trong các cộng đồng người dùng.
  + 1. Cryptotoken Standards

Các Cryptotoken Standards được xây dựng dựa trên sự thống nhất và sự đồng thuận của cộng đồng người dùng, các nhà phát triển và các bên liên quan trong lĩnh vực blockchain. Tiêu chuẩn này được tạo ra để đảm bảo tính tương thích, tương tác và tiêu chuẩn hóa trong việc phát triển và quản lý Cryptotoken trên các nền tảng blockchain khác nhau. Cryptotoken Standards thường được đề xuất, thảo luận và phát triển thông qua các quy trình công khai và cộng đồng. Các quy trình này có thể bao gồm các giai đoạn như đề xuất tiêu chuẩn, đánh giá, phản hồi và sửa đổi. Các bên liên quan có thể đóng góp ý kiến, đưa ra đề xuất và thảo luận với nhau để đạt được sự đồng thuận về các tiêu chuẩn cụ thể.

Ngoài ra, các Cryptotoken Standards cũng có thể dựa trên các tiêu chuẩn chung trong lĩnh vực kỹ thuật và phát triển phần mềm, chẳng hạn như JSON (JavaScript Object Notation) để định dạng dữ liệu, các chuẩn mã hóa và chữ ký số, cơ chế giao tiếp mạng như giao thức HTTP và TCP/IP, và các ngôn ngữ lập trình như Solidity (dành cho Ethereum) hoặc Rust (dành cho Solana).

Các tiêu chuẩn Cryptotoken thường được xây dựng và duy trì bởi các tổ chức và cộng đồng chuyên về blockchain và phát triển phần mềm. Các ví dụ điển hình bao gồm Ethereum Foundation cho tiêu chuẩn ERC và Binance Chain và Solana Foundation cho tiêu chuẩn BEP và SPL. Quá trình đề xuất, phát triển và thảo luận tiêu chuẩn là một quá trình mở và liên đới, với sự tham gia của cộng đồng người dùng và các bên liên quan khác nhau để đảm bảo tính tương thích và sự phát triển bền vững của hệ sinh thái Cryptotoken.

Ví dụ về một số tiêu chuẩn phổ biến cho Cryptotoken:

* ERC-20 (Ethereum Request for Comments 20): Đây là một tiêu chuẩn phổ biến cho Cryptotoken trên nền tảng Ethereum. ERC-20 xác định một giao diện chuẩn cho việc phát hành, chuyển giao và quản lý Cryptotoken trên blockchain Ethereum. Nó bao gồm các phương thức cơ bản như chuyển tiền, kiểm tra số dư và thông báo sự chuyển đổi.
* ERC-721 (Ethereum Request for Comments 721): Đây là một tiêu chuẩn dành cho Non-Fungible Tokens (NFTs) trên Ethereum. ERC-721 cho phép tạo ra các Cryptotoken không thể thay đổi và đại diện cho các đối tượng độc nhất, chẳng hạn như tác phẩm nghệ thuật, trò chơi điện tử hoặc tài sản kỹ thuật số khác. Nó cung cấp các phương thức để xác định sự độc nhất và quản lý quyền sở hữu của các đối tượng trong hệ thống.
* BEP-20 (Binance Smart Chain Token Standard 20): Đây là một tiêu chuẩn tương tự ERC-20 nhưng được sử dụng trên mạng lưới Binance Smart Chain (BSC). BEP-20 cho phép phát hành và quản lý Cryptotoken trên BSC và đảm bảo tính tương thích với các ví và dApps (ứng dụng phi tài chính) trên Binance Smart Chain.
* TRC-20 (TRON Token Standard 20): Đây là tiêu chuẩn cho Cryptotoken trên mạng lưới TRON. TRC-20 tương tự như ERC-20 và BEP-20, nó xác định giao diện chuẩn cho việc phát hành, chuyển giao và quản lý Cryptotoken trên TRON. Điều này cho phép tích hợp và tương tác giữa các ứng dụng và dịch vụ trên TRON.
* SPL (Solana Program Library): Đây là một tiêu chuẩn cho Cryptotoken trên nền tảng blockchain Solana. SPL cung cấp một tập hợp các tiêu chuẩn phát hành Token và quản lý Token trên Solana, bao gồm SPL Token, SPL Token Swap và SPL Token Registry. Điều này giúp đảm bảo tương thích và tương tác giữa các ứng dụng và giao thức trên mạng lưới Solana.
  + 1. Blockchain Tokenzation
    2. Ứng dụng CryptoToken

Cryptotoken là một thành phần quan trọng trong hệ sinh thái blockchain và tiền điện tử, và nó có nhiều ứng dụng đa dạng. Từ việc được sử dụng như một hình thức tiền tệ kỹ thuật số cho đến việc tạo ra các tài sản số không thể thay đổi và cung cấp dịch vụ tài chính phi trung gian, Cryptotoken đã thay đổi cách chúng ta tương tác với tài sản và giao dịch tài chính.

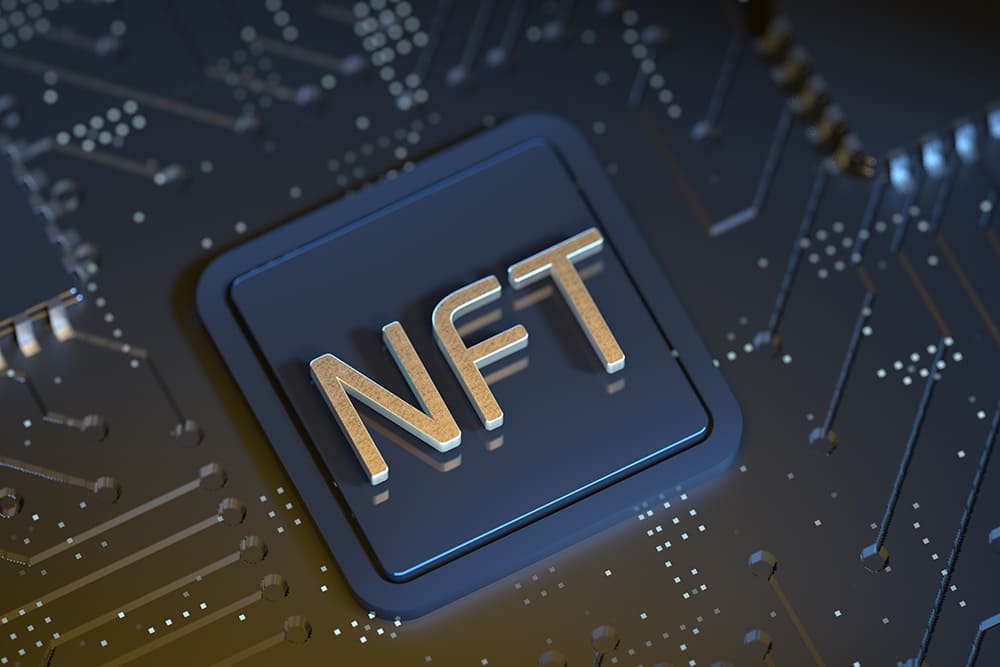
Tiền điện tử: Một trong những ứng dụng quan trọng của Cryptotoken là tiền điện tử. Đồng tiền điện tử như Bitcoin, Ethereum và nhiều đồng tiền khác đã trở thành một phương tiện thanh toán trực tuyến phổ biến, cho phép người dùng thực hiện các giao dịch an toàn và nhanh chóng trên toàn cầu mà không cần thông qua ngân hàng trung gian.

ICOs (Initial Coin Offerings): Cryptotoken cũng đóng vai trò quan trọng trong việc huy động vốn thông qua ICOs (Initial Coin Offerings). Các dự án mới có thể phát hành Cryptotoken riêng của họ và bán chúng cho nhà đầu tư để tài trợ cho sự phát triển dự án. Điều này cung cấp một cách tiềm năng để tài trợ dự án độc lập và đẩy mạnh sự đổi mới trong lĩnh vực công nghệ.

Ảnh có chứa hộp, màu vàng

Mô tả được tạo tự động

NFTs (Non-Fungible Tokens): Một ứng dụng khác của Cryptotoken là trong lĩnh vực NFTs (Non-Fungible Tokens). NFTs đại diện cho các tài sản số không thể thay đổi như tác phẩm nghệ thuật, video, âm nhạc và đồ trang sức. Việc sử dụng Cryptotoken cho NFT cho phép xác định rõ ràng và giao dịch các tài sản số độc nhất, tạo ra một thị trường phát triển nhanh chóng và sự quan tâm của nghệ sĩ, người chơi game và các nhà đầu tư.



DeFi (Decentralized Finance): Cryptotoken cũng đóng vai trò quan trọng trong DeFi (Decentralized Finance). DeFi là một lĩnh vực trong blockchain tập trung vào cung cấp các dịch vụ tài chính truyền thống mà không cần sự trung gian trung tâm. Cryptotoken được sử dụng trong DeFi để thực hiện các hoạt động như cho vay, vay mượn, tạo thanh khoản và giao dịch tài sản. Điều này mở ra cơ hội tiềm năng để mọi người có thể tiếp cận các dịch vụ tài chính một cách dễ dàng và linh hoạt hơn.

Tokenization tài sản truyền thống: Cryptotoken cũng cho phép tokenization của các tài sản truyền thống như bất động sản, cổ phiếu và quyền sở hữu. Việc tokenization cho phép chia nhỏ và giao dịch tài sản một cách linh hoạt, tăng cường tính thanh khoản và tiện lợi trong việc quản lý và chuyển đổi tài sản.

Ngoài ra còn nhiều ứng dụng thực tiễn khác, nhưng ứng dụng của Cryptotoken phụ thuộc vào nhiều yếu tố quan trọng như công nghệ blockchain, chuẩn Cryptotoken, quy định pháp lý, chấp nhận và sử dụng của người dùng và sự phát triển công nghệ. Sự hợp nhất của các yếuHiện tại, tôi không có thông tin về ứng dụng cụ thể có tên "CryptoToken". Có thể đó là một ứng dụng cụ thể do một công ty hoặc dự án tạo ra. Nếu bạn có thông tin cụ thể hơn về CryptoToken mà bạn muốn tìm hiểu, vui lòng cung cấp thêm thông tin để tôi có thể giúp bạn một cách tốt nhất.

* + 1. So sánh CryptoToken và Cryptocurrency
  1. Ứng dụng tài chính phi tập trung (DeFi)
     1. Ứng dụng phi tập trung Dapp

Ứng dụng phi tập trung (Decentralized Applications - DApps) đã trở thành một lĩnh vực nổi bật trong lĩnh vực công nghệ và tài chính trong những năm gần đây. DApps là những ứng dụng được xây dựng trên nền tảng blockchain hoặc các công nghệ phi tập trung khác, mà không có một cơ quan trung gian duy nhất kiểm soát và quản lý dữ liệu. Thay vào đó, các hoạt động của DApps được thực hiện thông qua các giao thức và hợp đồng thông minh.

Với sự phát triển nhanh chóng của công nghệ blockchain, DApps đã mang lại những lợi ích đáng kể cho người dùng và các lĩnh vực khác nhau. Trước hết, tính phi tập trung của DApps đã làm thay đổi cách chúng ta tưởng tượng về việc xây dựng và vận hành ứng dụng. Không còn tồn tại một cơ sở dữ liệu tập trung duy nhất, mà dữ liệu và hoạt động của DApps được phân tán trên nhiều nút mạng, tạo ra một môi trường an toàn và khó bị tấn công. Điều này mang lại sự tin cậy và đáng tin cậy hơn cho người dùng, giảm bớt rủi ro và sự phụ thuộc vào các bên trung gian.

Một ưu điểm quan trọng khác của DApps là tính toàn vẹn và bảo mật dữ liệu. Các giao thức và hợp đồng thông minh được sử dụng trong DApps được xác minh và mã hóa, đảm bảo tính toàn vẹn và bảo mật dữ liệu. Mỗi giao dịch và hoạt động trong DApps được ghi lại trên blockchain, không thể thay đổi hay gian lận. Điều này tạo ra một môi trường công bằng và minh bạch, nâng cao sự tin tưởng và sự hợp tác giữa các bên tham gia.

Một khía cạnh quan trọng khác của DApps là quyền sở hữu tài sản. Thông qua việc sử dụng các chuẩn token phi tập trung, người dùng có quyền sở hữu và giao dịch các tài sản kỹ thuật số như tiền điện tử, token hay tài sản số một cách trực tiếp và an toàn. Điều này loại bỏ sự phụ thuộc vào các bên trung gian và tạo ra một mô hình kinh tế mới, trong đó người dùng có toàn quyền kiểm soát và sở hữu tài sản của mình.

Ứng dụng phi tập trung DApps không chỉ mang lại những lợi ích kỹ thuật và an toàn, mà còn mở ra những cơ hội và tiềm năng trong nhiều lĩnh vực khác nhau. Ví dụ, trong lĩnh vực tài chính, DApps đã thay đổi cách chúng ta giao dịch, cho phép trao đổi tiền điện tử và tài sản kỹ thuật số một cách trực tiếp và an toàn hơn. Trong lĩnh vực trò chơi, DApps đã tạo ra những trải nghiệm mới và độc đáo, nơi người dùng có thể sở hữu và giao dịch các tài sản trong trò chơi một cách rõ ràng và công bằng. Trong lĩnh vực bất động sản, DApps có thể cung cấp các nền tảng phi tập trung cho việc mua bán và giao dịch bất động sản, đảm bảo tính toàn vẹn và minh bạch trong quá trình giao dịch.

Dưới đây là một số ví dụ về ứng dụng phi tập trung (DApps):

* DeFi (Decentralized Finance): DApps trong lĩnh vực tài chính phi tập trung cho phép người dùng thực hiện các giao dịch tài chính mà không cần tới trung gian truyền thống như ngân hàng. Ví dụ như Uniswap, Compound và Aave là những DApps DeFi phổ biến.
* NFT (Non-Fungible Tokens): DApps trong lĩnh vực NFT cho phép người dùng tạo, mua, bán và giao dịch các tài sản phi tập trung không thể thay thế. Ví dụ như CryptoKitties và Decentraland là những DApps NFT nổi tiếng.
* Trò chơi phi tập trung: Có nhiều DApps cho phép người dùng tham gia vào trò chơi phi tập trung, nơi các tài sản trong trò chơi được giao dịch và quản lý bằng công nghệ blockchain. Ví dụ như Axie Infinity và CryptoPunks là những DApps trò chơi phi tập trung phổ biến. DApps cũng là một thách thức không nhỏ.
  + 1. Khái niệm DeFi

DeFi, viết tắt của "Decentralized Finance" (Tài chính phi tập trung), là một thuật ngữ được sử dụng để chỉ một hệ sinh thái tài chính phi tập trung được xây dựng trên nền tảng blockchain và các công nghệ phi tập trung khác. DeFi nhằm mục tiêu tạo ra các dịch vụ tài chính truy cập mở, minh bạch và không cần đến các bên trung gian truyền thống như ngân hàng hay quỹ đầu tư. DeFi sử dụng các hợp đồng thông minh (smart contracts) để thực hiện và quản lý các giao dịch tài chính. Các giao dịch này được ghi lại trên blockchain, đảm bảo tính toàn vẹn và bảo mật dữ liệu. DeFi cung cấp các dịch vụ tài chính như vay mượn, giao dịch, cho thuê tài sản, thanh khoản và phân phối thu nhập một cách phi tập trung.

Một trong những ứng dụng nổi bật của DeFi là các nền tảng vay mượn phi tập trung (decentralized lending platforms). Nhờ vào sự kết hợp của blockchain và hợp đồng thông minh, người dùng có thể vay và cho vay tiền điện tử mà không cần thông qua các ngân hàng truyền thống. Điều này mang lại tính linh hoạt và tiện lợi cho người dùng, đồng thời giảm bớt các rào cản và chi phí liên quan đến vay mượn truyền thống.

Ngoài ra, DeFi còn cung cấp các dịch vụ giao dịch phi tập trung (decentralized exchanges - DEXs), cho phép người dùng trao đổi các loại tiền điện tử và tài sản kỹ thuật số một cách trực tiếp, không cần thông qua sàn giao dịch trung gian. Điều này tạo ra sự minh bạch và tính toàn vẹn trong quá trình giao dịch, đồng thời giảm thiểu rủi ro liên quan đến việc trao đổi tài sản. Mô hình DeFi cũng cho phép người dùng kiếm lợi từ việc nhắm mục tiêu phân phối thu nhập (yield farming) thông qua việc cung cấp vốn hoặc tham gia vào các quy trình thanh khoản trên các nền tảng DeFi. Người dùng có thể nhận được lợi suất hoặc các token phần thưởng trong quá trình này.

Tuy DeFi mang lại những lợi ích về tính minh bạch, tiện lợi và truy cập mở, nhưng cũng đối mặt với một số thách thức như khả năng mở rộng của blockchain, rủi ro bảo mật và quản lý rủi ro tài chính. Dẫu vậy, với sự phát triển của công nghệ blockchain và sự quan tâm ngày càng tăng về DeFi, có thể dự đoán rằng DeFi sẽ tiếp tục phát triển và tạo ra những thay đổi quan trọng trong lĩnh vực tài chính truyền thống.

* + 1. Nguyên lý hoạt động của các ứng dụng Defi

Nguyên lý hoạt động của DeFi dựa trên sự kết hợp giữa blockchain, hợp đồng thông minh và giao thức phi tập trung để tạo ra một môi trường tài chính phi tập trung và cung cấp các dịch vụ tài chính truy cập mở. Trong DeFi, các giao dịch và hoạt động tài chính được thực hiện trực tiếp giữa các bên, không cần sự can thiệp của bất kỳ tổ chức trung gian nào. Điều này đòi hỏi sự tin tưởng vào công nghệ blockchain, nền tảng được xây dựng trên nguyên tắc phi tập trung và công khai. Blockchain ghi lại mọi giao dịch và hoạt động trên một hệ thống phân tán, cho phép mọi người xem xét và xác minh thông tin.

Hợp đồng thông minh chính là "nền tảng" của DeFi. Được viết bằng ngôn ngữ lập trình, hợp đồng thông minh là các chương trình tự thực thi các quy tắc và điều khoản của giao dịch. Chúng giúp tự động hóa các quy trình và loại bỏ sự phụ thuộc vào bên thứ ba. Bằng cách thiết lập các điều kiện và hành động, hợp đồng thông minh đảm bảo tính trung thực và minh bạch trong các giao dịch.

DeFi cũng cho phép token hóa các tài sản truyền thống như tiền tệ, chứng khoán và hàng hóa. Nhờ đó, các tài sản này có thể được biểu diễn dưới dạng các token trên blockchain. Việc token hóa tài sản tạo ra tính linh hoạt và khả năng giao dịch dễ dàng, mở ra cơ hội mới cho việc quản lý và tạo lập giá trị.

Giao thức tài chính phi tập trung là cốt lõi của DeFi. Các giao thức này được xây dựng trên blockchain và cung cấp các dịch vụ như vay mượn, lưu trữ, thanh toán và giao dịch tài sản. Với sự kết hợp giữa hợp đồng thông minh và giao thức phi tập trung, DeFi tạo ra một môi trường tài chính mở và minh bạch, nơi mọi người có thể tham gia vào các hoạt động tài chính mà không cần phụ thuộc vào các tổ chức truyền thống.

Cuối cùng, DeFi tạo ra một môi trường thanh khoản và lưu thông tài sản mới. Người dùng có thể gửi tiền vào các hợp đồng thông minh để kiếm lãi, thực hiện vay mượn, cho vay và thực hiện các giao dịch trao đổi giữa các loại token khác nhau. Điều này tăng cường tính thanh khoản của các tài sản và mở ra cơ hội đầu tư và tạo ra giá trị mới.

* + 1. Các tính chất của DeFi
       1. Phi tập trung

Tính phi tập trung là một trong những đặc điểm quan trọng của DeFi (Decentralized Finance), đó là một hệ thống tài chính hoạt động trên nền tảng phi tập trung, không cần sự can thiệp của bên thứ ba truyền thống như ngân hàng trung tâm. Trong DeFi, các giao dịch và hoạt động tài chính diễn ra trên blockchain, một cơ sở dữ liệu phân tán được lưu trữ trên nhiều nút mạng. Thay vì dựa vào một cơ quan tài chính trung gian, DeFi sử dụng các hợp đồng thông minh (smart contracts) để thực hiện và xác minh các giao dịch. Nhờ đó, mọi người có thể tham gia vào DeFi mà không cần phải dựa vào sự cho phép hay xác nhận từ bên thứ ba.

Tính phi tập trung của DeFi mang lại nhiều lợi ích quan trọng. Đầu tiên, nó tạo ra sự công bằng và minh bạch, vì tất cả các giao dịch và thông tin đều được lưu trữ trên blockchain và có thể được xem và kiểm tra bởi bất kỳ ai. Không có bên trung gian duy nhất kiểm soát hệ thống, điều này giúp ngăn chặn sự thiên vị và gian lận.

Thứ hai, tính phi tập trung trong DeFi mang lại sự tự chủ cho người dùng. Mọi người có khả năng kiểm soát hoàn toàn tài sản của mình thông qua việc sở hữu khóa riêng tư. Điều này đồng nghĩa với việc người dùng không cần phải ủy thác tài sản cho bên thứ ba, nhưng vẫn có thể tham gia vào các hoạt động tài chính và tận hưởng các lợi ích của nó.

Cuối cùng, tính phi tập trung trong DeFi mang lại sự linh hoạt và khả năng mở rộng. Vì hệ thống không phụ thuộc vào một trung tâm duy nhất, nó có khả năng chịu tải cao và có thể mở rộng để đáp ứng nhu cầu ngày càng tăng của người dùng mà không gặp các rào cản truy cập hay hạn chế từ phía các bên thứ ba.

* + - 1. Tự do tham gia

Tính tự do tham gia đề cập tới việc bất kỳ ai cũng có thể tham gia và tận dụng các dịch vụ và ứng dụng DeFi mà không cần phải xin phép hoặc được chấp thuận từ bất kỳ ai khác. Trong một môi trường DeFi không cần sự cho phép, không có rào cản truy cập hay hạn chế đối với người dùng. Bất kỳ ai có thể truy cập vào các dịch vụ DeFi, tạo ví tiền điện tử, gửi và nhận tiền, tham gia vào việc cho vay hoặc vay mượn, và thực hiện các giao dịch tài chính khác mà không cần phải xin phép từ bất kỳ ai khác. Điều này khác biệt hoàn toàn so với mô hình truyền thống, trong đó người dùng phải tuân thủ các quy tắc và quy định của các tổ chức tài chính trung gian, và thường phải xin phép hoặc chịu sự kiểm duyệt từ bên thứ ba để có thể sử dụng các dịch vụ tài chính. Nó giúp tăng tính công bằng và minh bạch trong hệ thống tài chính. Mọi người có quyền truy cập vào DeFi và sử dụng các dịch vụ một cách tự do, không bị giới hạn bởi địa điểm, tài chính hay hệ thống trung gian.

Tính tự do cho phép cung cấp sự tự chủ cho người dùng. Mọi người có khả năng kiểm soát tài sản của mình và tự quyết định các giao dịch tài chính mà không cần chờ đợi hay phụ thuộc vào sự cho phép từ bất kỳ ai khác. Ngoài ra, nó cho phép tạo ra một môi trường sáng tạo và phát triển độc lập. Bất kỳ ai cũng có thể tạo ra và triển khai các smart contract và ứng dụng mới trên nền tảng DeFi mà không cần phải xin phép từ bất kỳ ai. Điều này tạo điều kiện cho sự đa dạng và sự tiến bộ trong việc phát triển các dịch vụ và sản phẩm DeFi.

Ví dụ, nếu bạn muốn trao đổi ETH (Ethereum) sang DAI (stablecoin được gắn kết với đồng USD), bạn có thể truy cập vào giao thức Uniswap thông qua một ví tiền điện tử tương thích và thực hiện giao dịch trực tiếp. Bạn không cần phải xin phép từ bất kỳ ai và không cần tài khoản trên sàn giao dịch trung gian. Mọi người có thể trao đổi tiền điện tử của họ một cách tự do và nhanh chóng trên Uniswap (một giao thức giao dịch trao đổi tiền điện tử phi tập trung (decentralized exchange, DEX) được xây dựng trên blockchain Ethereum).

* + - 1. An toàn dựa trên mã nguồn

Tính “An toàn dựa trên mã nguồn” chỉ ra rằng việc một hệ thống có thể hoạt động mà không đòi hỏi người dùng phải tin tưởng hoặc phụ thuộc vào bất kỳ bên thứ ba nào để đảm bảo tính an toàn và đáng tin cậy.

Trong một hệ thống DeFi, các giao dịch và hoạt động được thực hiện thông qua các quy tắc và logic được thiết lập trước mà không cần phải dựa vào lòng tin của bất kỳ ai. Điều này được đảm bảo bởi sự sử dụng các hợp đồng thông minh (smart contracts) trong các mạng blockchain. Smart contract là các chương trình chạy tự động, đáng tin cậy và không thể thay đổi sau khi được triển khai, và chúng thực hiện các giao dịch mà không cần sự can thiệp của bên thứ ba. Một ví dụ cụ thể về tính Trustless là giao thức giao dịch Uniswap đã được đề cập ở trên. Trong Uniswap, các giao dịch xảy ra một cách tự động thông qua các smart contract. Người dùng không cần phải tin tưởng vào sàn giao dịch hoặc bất kỳ ai khác để thực hiện giao dịch mua bán. Thay vào đó, các giao dịch được thực hiện trên blockchain Ethereum thông qua mã logic được viết trước trong smart contract của Uniswap.

Vì tính chất không thể thay đổi của smart contract, mọi giao dịch trên Uniswap được thực hiện theo các quy tắc đã được xác định trước mà không thể bị thay đổi bởi ai đó. Điều này đảm bảo rằng các giao dịch không bị gian lận hoặc gian lận và không cần phải đặt niềm tin vào sàn giao dịch hay bất kỳ bên thứ ba nào khác. Tính chất này trong DeFi đóng vai trò quan trọng trong việc tạo ra một môi trường an toàn và đáng tin cậy. Người dùng có thể thực hiện các giao dịch và tham gia vào các hoạt động tài chính mà không cần phải tin tưởng hoặc phụ thuộc vào bất kỳ ai khác. Các quy tắc và logic được thiết lập trước trong smart contract đảm bảo tính toàn vẹn và đáng tin cậy của các giao dịch và hoạt động trong hệ thống.

* + - 1. Tính minh bạch

Tính minh bạch trong DeFi đảm bảo rằng thông tin và hoạt động trong hệ thống đều được công khai và dễ dàng kiểm tra. Nó đóng vai trò quan trọng trong việc xây dựng lòng tin và đáng tin cậy trong cộng đồng người dùng. Trong một hệ thống minh bạch, thông tin về giao dịch, tài sản, thanh khoản và các hoạt động khác được công khai và truy cập công khai. Điều này cho phép mọi người kiểm tra và xác minh thông tin một cách độc lập, đảm bảo rằng không có hoạt động lừa đảo hoặc gian lận xảy ra và mọi giao dịch đều được thực hiện một cách minh bạch và công bằng.

Một ví dụ về tính minh bạch trong DeFi là sử dụng blockchain công khai. Blockchain là một hệ thống phân tán và không thể thay đổi, trong đó các giao dịch được ghi lại và được công khai cho mọi người xem. Bất kỳ ai đều có thể xem thông tin về các giao dịch, số dư tài khoản và các hoạt động khác trên blockchain. Các hợp đồng thông minh (smart contracts) cũng đóng vai trò quan trọng trong tính minh bạch. Các smart contract là các chương trình chạy tự động và không thể thay đổi, và tất cả các điều khoản và điều kiện của giao dịch được xác định trước trong mã logic của smart contract. Mọi người có thể xem và kiểm tra smart contract để đảm bảo rằng không có điều kiện ẩn hay lươn lẹo trong giao dịch.

Ngoài ra, trong một hệ thống DeFi minh bạch, thông tin về tài sản và thanh khoản cũng phải được công khai. Ví dụ, trong một giao thức giao dịch trao đổi tiền điện tử phi tập trung, thông tin về các cặp giao dịch, tỷ giá và khối lượng giao dịch phải được cung cấp công khai để mọi người có thể kiểm tra và xác minh.

Tính minh bạch trong DeFi không chỉ tạo ra niềm tin và lòng tin cậy trong cộng đồng người dùng, mà còn cho phép người dùng tham gia vào các hoạt động tài chính một cách thông minh và cân nhắc. Mọi người có thể kiểm tra và xem thông tin một cách độc lập, đảm bảo rằng họ đang tham gia vào một môi trường minh bạch và công bằng.

* + - 1. Không cần ủy thác

Tính Không cần ủy thác (Self-Custody) trong lĩnh vực Tài chính phi tập trung (DeFi) đề cập đến khả năng và quyền tự quản lý và bảo vệ tài sản tiền điện tử của người dùng mà không cần phải dựa vào bên thứ ba. Trong DeFi, tính Không cần ủy thác là một yếu tố quan trọng để đạt được tính phi tập trung và tăng cường an ninh và quyền riêng tư cho người dùng.

DeFi là một hệ sinh thái tài chính xây dựng trên nền tảng blockchain, cho phép người dùng tham gia vào các hoạt động tài chính mà không cần dựa vào các bên trung gian truyền thống như ngân hàng hay sàn giao dịch trung tâm. Tính Không cần ủy thác là một trong những nguyên tắc cốt lõi của DeFi, đảm bảo rằng người dùng có quyền kiểm soát tài sản của mình và không cần tin tưởng vào các bên thứ ba. Người dùng có thể sử dụng ví tiền điện tử cá nhân để tự quản lý tài sản của mình. Ví tiền điện tử cá nhân có thể là một ứng dụng phần mềm hoặc phần cứng, cho phép người dùng lưu trữ và kiểm soát các khóa riêng tư của mình. Khóa riêng tư là mật khẩu mã hóa được sử dụng để xác thực và điều khiển quyền sở hữu tài sản tiền điện tử. Khi sử dụng tính Không cần ủy thác trong DeFi, người dùng có thể tham gia vào các hoạt động như cho vay, vay mượn, giao dịch, và tham gia vào các quỹ hoặc nền tảng tài chính phi tập trung mà không cần chuyển giao tài sản của họ cho bên thứ ba. Thay vào đó, họ giữ quyền kiểm soát đầy đủ và an toàn của tài sản.

Tính Không cần ủy thác trong DeFi mang lại nhiều lợi ích cho người dùng. Nó cung cấp tính riêng tư và an ninh, người dùng không cần tiết lộ thông tin cá nhân hoặc tin tưởng vào các bên thứ ba để lưu trữ hoặc quản lý tài sản của mình. Thay vào đó, họ giữ quyền kiểm soát đầy đủ và an toàn của tài sản. Tính Không cần ủy thác trong DeFi cung cấp tính linh hoạt. Người dùng có thể truy cập và quản lý tài sản của mình bất cứ khi nào và ở bất kỳ đâu mà không cần phụ thuộc vào các bên trung gian. Điều này giúp tiết kiệm thời gian và phí tổn liên quan đến việc tham gia vào các hoạt động tài chính.

Tuy nhiên, tính Không cần ủy thác trong DeFi yêu cầu người dùng chịu trách nhiệm bảo vệ và sao lưu đúng cách các khóa riêng tư của mình. Nếu khóa riêng tư bị mất hoặc bị đánh cắp, người dùng có thể mất hoàn toàn quyền kiểm soát và truy cậpvào tài sản của họ. Do đó, người dùng cần chú ý đến việc bảo mật và sao lưu khóa riêng tư của mình để tránh mất mát tài sản.

* + - 1. Các tính chất khác
    1. Phân loại các ứng dụng DeFi
    2. So sánh DeFi và CeFi

CeFi (Centralized Finance) là mô hình tài chính truyền thống, trong đó các hoạt động tài chính được thực hiện và quản lý bởi các tổ chức tài chính tập trung như ngân hàng, sàn giao dịch truyền thống và các tổ chức tài chính truyền thống khác. CeFi đặt trung tâm quyền kiểm soát và quản lý vào các tổ chức tài chính này, và người dùng phải tin tưởng và phụ thuộc vào chúng để sử dụng các dịch vụ tài chính. Dưới đây là so sánh về các khía cạnh khác nhau giữa DeFi(Decentralized Finance) và CeFi(Centralized Finance):

|  |  |  |
| --- | --- | --- |
| **Yếu tố** | **DeFi(Decentralized Finance)** | **CeFi(Centralized Finance)** |
| Kiểm soát | Phi tập trung, không có bên thứ ba | Tập trung, quản lý bởi tổ chức tài chính |
| Quyền riêng tư | Người dùng giữ quyền kiểm soát dữ liệu | Dữ liệu được lưu trữ và quản lý bởi tổ chức tài chính |
| Tính minh bạch | Công khai, các giao dịch được ghi lại công khai trên blockchain | C ó thể không công khai, dữ liệu được kiểm soát bởi tổ chức tài chính |
| Quyền truy cập và tự do | Mở cửa cho mọi người tham gi a, không cần phê duyệt | Có thể yêu cầu phê duyệt hoặc hạn chế quyền truy cập |
| Tốc độ giao dịch | Tùy thuộc vào mạng lưới blockchain, có thể chậm hơn | Thường nhanh hơn do hệ thống tập trung |
| Phí giao dịch | Có thể thấp hơn do loại bỏ bên thứ ba trung gian | Thường có phí giao dịch được thu bởi tổ chức tài chính |
| Rủi ro | Nguy cơ hệ thống thông tin không an toàn, rủi ro thông minh | Rủi ro liên quan đến tổ chức tài chính và môi trường tập trung |

Mặc dù CeFi có những ưu điểm như tiện lợi và tốc độ, nhưng nó cũng có nhược điểm liên quan đến quyền riêng tư, tính minh bạch và sự phụ thuộc vào các tổ chức tài chính trung gian.

* 1. Kết luận Chương 1

1. Công nghệ DLT trên Corda
   1. Tổng quan về corda
      1. Lịch sử phát triển

Corda là một nền tảng được phát triển bởi R3, đây là một công ty công nghệ tài chính có trụ sở ở Luân Đôn – Anh. Corda R3 đã trải qua một hành trình phát triển đáng chú ý trong lĩnh vực công nghệ blockchain. Từ những bước đầu tiên với việc thành lập một hợp tác quy mô lớn giữa các ngân hàng và tổ chức tài chính hàng đầu, Corda đã nhanh chóng trở thành một trong những nền tảng blockchain hàng đầu trong lĩnh vực kinh doanh và tài chính. Có thể tóm tắt lịch sử phát triển của Corda qua các giai đoạn sau:

* Tháng 9 năm 2015: R3 công bố việc thành lập một hợp tác giữa các ngân hàng hàng đầu thế giới với mục tiêu nghiên cứu và phát triển công nghệ blockchain dành riêng cho ngành tài chính. Ban đầu được gọi là "R3CEV" với sự tham gia của 9 công ty tài chính: Barclays, BBVA, Commonwealth Bank of Australia, Credit Suisse, Goldman Sachs, JP Morgan, Royal Bank of Scotland, State Street và UBS.
* Ngày 29 tháng 9 năm 2015: có thêm 13 công ty tài chính tham gia: Bank of America, BNY Mellon, Citi, Commerzbank, Deutsche Bank, HSBC, Tập đoàn tài chính Mitsubishi UFJ, Morgan Stanley, Ngân hàng Quốc gia Úc, Ngân hàng Hoàng gia Canada, Skandinaviska Enskilda Banken, Société Générale và Ngân hàng Toronto-Dominion.
* Tháng 4 năm 2016: R3 công bố Corda lần đầu tiên tại một hội nghị về blockchain. Corda được mô tả là một nền tảng blockchain phân tán, tập trung vào việc xây dựng và quản lý các hợp đồng thông minh giữa các bên tin cậy.
* Tháng 11 năm 2016: R3 đưa Corda vào chương trình mã nguồn mở và chính thức công bố mã nguồn của nền tảng. Điều này cho phép cộng đồng phát triển và đóng góp vào Corda.
* Năm 2017: R3 tiếp tục phát triển Corda và tăng cường các đối tác và khách hàng. Họ tiến hành các dự án thử nghiệm và ứng dụng Corda trong các trường hợp sử dụng thực tế, đặc biệt là trong lĩnh vực tài chính và ngân hàng.
* Năm 2018: R3 công bố phiên bản Corda Enterprise, mở rộng tính năng và khả năng của Corda để phục vụ các doanh nghiệp lớn hơn. Corda Enterprise cung cấp tính năng bảo mật và quản lý mở rộng, giúp đáp ứng yêu cầu của các tổ chức tài chính và doanh nghiệp.
* Năm 2019 đến nay: R3 liên tục phát triển với những dự án thực tế trên toàn thế giới. Corda được sử dụng trong các lĩnh vực như giao dịch tài chính, bảo hiểm, chuỗi cung ứng và nhiều lĩnh vực khác.
  + 1. Giới thiệu Corda

Corda là một nền tảng mã nguồn mở nhằm giảm thiểu các rào cản trong giao dịch thương mại. Nó được xây dựng dựa trên công nghệ Sổ cái phân tán (DLT) hoặc còn được biết đến là công nghệ blockchain. Corda là một blockchain cấp phép, có nghĩa là nó hoạt động trong một môi trường được kiểm soát và phê duyệt bởi các tổ chức tham gia vào giao dịch.



Một trong những ứng dụng điển hình của Corda là xây dựng các nền tảng KYC (Know Your Customer) nhằm xác minh danh tính và thông tin khách hàng, hàng hóa hoặc đối tác. Corda cung cấp một cơ chế an toàn và tin cậy để quản lý và chia sẻ thông tin nhằm đảm bảo tuân thủ các quy định về KYC và bảo vệ quyền riêng tư của các bên tham gia.

Hiện nay, Corda đang được nghiên cứu và triển khai rộng rãi trong các lĩnh vực như bảo hiểm, ngân hàng, tổ chức tín dụng, sản xuất và thương mại. Nền tảng này cung cấp các giải pháp công nghệ cho các nghiệp vụ chứng thực số, giúp tăng cường tính hiệu quả, minh bạch và bảo mật trong các hoạt động kinh doanh của các tổ chức này. Với sự tập trung vào quyền riêng tư và sự tin cậy, Corda cho phép các bên tham gia xác định và kiểm soát dữ liệu của mình trong các giao dịch và hợp đồng thông minh. Điều này đặc biệt quan trọng trong các lĩnh vực như tài chính, bảo hiểm và chuỗi cung ứng, nơi quyền riêng tư và bảo mật dữ liệu là yếu tố quan trọng.

Ngoài ra corda cũng hướng đến việc ghi chép và sao lưu các tiện ích trong hệ sinh thái. Điều này có nghĩa là toàn bộ hồ sơ và thỏa thuận đều được quản lý và mã hóa để đáp ứng các yêu cầu về tính hợp pháp và bảo mật.

Để đảm bảo sự đón nhận và sự phát triển rộng rãi trong cộng đồng tài chính, Corda đề cao tính mở và cung cấp các tính năng hoạt động trong một cơ chế mở. Điều này khuyến khích sự tương tác, phát triển ứng dụng và tích hợp với các hệ thống khác, đồng thời đảm bảo tính linh hoạt và khả năng mở rộng của nền tảng.

* + 1. Công nghệ liên quan

Sổ cái phân tán - Distributed Ledger Technology (DLT): Corda được xây dựng dựa trên công nghệ DLT, còn được gọi là công nghệ sổ cái phân tán. DLT là một hệ thống phân tán cho phép các bên tham gia đồng thuận về trạng thái và lịch sử giao dịch mà không cần sự tin cậy vào một bên thứ ba trung gian.

Blockchain: Corda sử dụng một số khái niệm và công nghệ từ blockchain. Tuy nhiên, Corda không phải là một blockchain công cộng truyền thống. Thay vào đó, nó là một blockchain cấp phép (permissioned blockchain) với các tính năng và thiết kế được tối ưu hóa cho các ứng dụng doanh nghiệp.

Hợp đồng thông minh - Smart Contracts: Corda hỗ trợ triển khai và thực thi các hợp đồng thông minh (smart contracts). Smart contracts là các đoạn mã chứa các quy tắc và điều kiện tự động hóa các giao dịch và hành động dựa trên các sự kiện được xác định trước. Corda cho phép viết và thực thi smart contracts một cách an toàn và riêng tư.

Mật mã: Corda sử dụng các thuật toán mật mã mạnh mẽ để đảm bảo tính bảo mật và xác thực trong quá trình giao dịch. Các thuật toán mật mã bao gồm mã hóa khóa công khai (public-key cryptography), chữ ký số (digital signatures) và các phép nhân ma trận (matrix multiplication) để bảo vệ dữ liệu và xác minh danh tính.

Cơ chế đồng thuận: Corda không sử dụng một cơ chế đồng thuận (consensus mechanism) trung gian để đạt được sự đồng thuận giữa các bên trong mạng. Thay vào đó, Corda cho phép các bên tham gia đạt được đồng thuận trực tiếp với nhau thông qua các giao thức và quy trình yêu cầu.

* + 1. Đặc trưng của Corda
    2. Ứng dụng của Corda

Corda được thiết kế hướng tới nhiều lĩnh vực khác nhau của doanh nghiệp có thể kể đến:

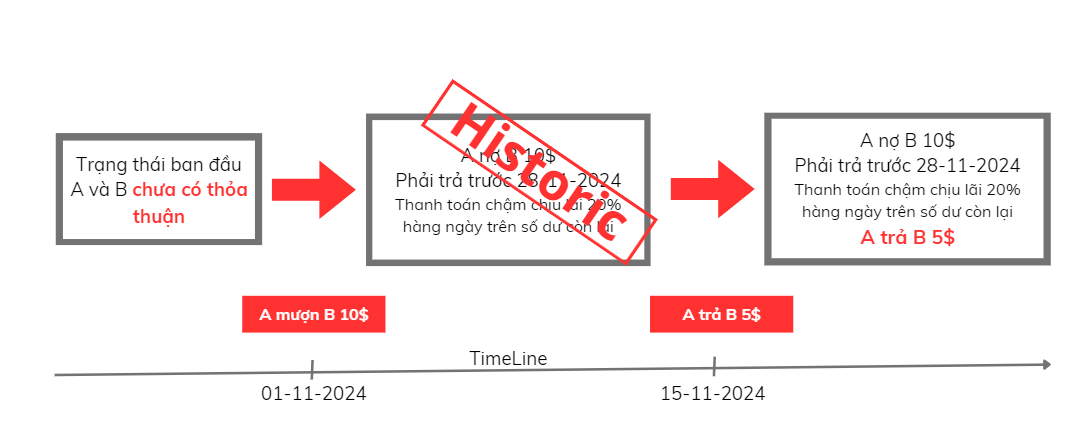
* Ngành bảo hiểm: Corda có thể được sử dụng để tạo ra các nền tảng bảo hiểm phân tán, cho phép các bên tham gia chia sẻ thông tin về hợp đồng bảo hiểm, tình trạng tổn thất và thanh toán một cách an toàn và minh bạch. Nó cũng giúp tăng cường quy trình xác thực và quản lý rủi ro trong ngành bảo hiểm.
* Ngành tài chính: Corda có thể được áp dụng trong các giao dịch tài chính như thanh toán quốc tế, giao dịch chứng khoán, vay mượn và giao dịch hợp đồng tương lai. Nó giúp cải thiện tính hiệu quả và tốc độ trong việc xác minh và xử lý giao dịch tài chính, đồng thời giảm thiểu rủi ro và chi phí giao dịch.
* Chuỗi cung ứng: Corda có thể tạo ra các nền tảng chuỗi cung ứng phân tán, giúp quản lý thông tin về nguồn gốc, vận chuyển, lưu trữ và xác minh hàng hóa. Nó cung cấp tính nhất quán và minh bạch cho toàn bộ quy trình chuỗi cung ứng, từ nhà cung cấp đến người tiêu dùng cuối cùng.
* Ngành công nghiệp sản xuất: Corda có thể được sử dụng để theo dõi quá trình sản xuất và quản lý thông tin về các thành phần, linh kiện và lịch sử sản xuất. Nó giúp tăng cường tính minh bạch, đáng tin cậy và tuân thủ các quy định trong ngành công nghiệp sản xuất.
* Thương mại quốc tế: Corda có thể áp dụng trong các giao dịch thương mại quốc tế, giúp xác minh và xử lý các hợp đồng, thanh toán và thông tin về hàng hóa. Nó cung cấp tính bảo mật và tin cậy cho các giao dịch quốc tế và giúp giảm thiểu sự kiểm soát trung gian và thời gian giao dịch.
  + 1. Lợi ích khi sử dụng Corda

Sử dụng Corda trong môi trường doanh nghiệp có thể mang lại nhiều lợi ích quan trọng các nền tảng sử dụng nó. Dưới đây là một số lợi ích chính khi sử dụng Corda:

* Quyền riêng tư và bảo mật: Corda được thiết kế với sự tập trung vào quyền riêng tư và bảo mật dữ liệu. Thông tin chỉ được chia sẻ giữa các bên tham gia cụ thể trong mạng, đảm bảo tính riêng tư và ngăn chặn truy cập trái phép.
* Hiệu suất cao: Corda được tối ưu hóa để đạt hiệu suất cao trong việc xử lý giao dịch. Thay vì phải xác minh mọi giao dịch trên toàn mạng, Corda chỉ yêu cầu các bên liên quan xác minh các giao dịch của mình. Điều này giúp giảm độ trễ và tăng hiệu suất trong mạng Corda.
* Smart contracts linh hoạt: Corda hỗ trợ việc triển khai và thực thi smart contracts trong các giao dịch. Điều này giúp tự động hóa các quy trình và giảm thiểu sự phụ thuộc vào các bên trung gian. Smart contracts trong Corda cũng có khả năng tương tác với các hệ thống và ứng dụng khác, tạo ra tích hợp linh hoạt.
* Tích hợp dễ dàng: Corda được thiết kế để dễ dàng tích hợp với các hệ thống và ứng dụng hiện có trong doanh nghiệp. Nó cung cấp các tiêu chuẩn và cơ chế để trao đổi dữ liệu và thông tin một cách linh hoạt và tiện lợi, giúp tận dụng tối đa các hệ thống có sẵn và giảm thiểu công sức tích hợp.
* Quản lý rủi ro tốt: Corda cung cấp các công cụ và cơ chế để quản lý rủi ro trong quá trình giao dịch và cũng giúp đảm bảo tuân thủ các quy định và quy trình trong ngành công nghiệp cụ thể. Việc sử dụng Corda giúp giảm thiểu sai sót, xác thực dễ dàng và tạo ra bằng chứng số về các giao dịch.
* Khả năng mở rộng cao: Corda khuyến khích sự phát triển và mở rộng thông qua cơ chế mở và tài liệu chi tiết. Nó hỗ trợ việc xây dựng ứng dụng đa dạng và tương tác với các mạng Corda khác nhau, mở ra khả năng mở rộng và tích hợp với nhiều hệ thống và doanh nghiệp khác nhau.
  1. Dữ liệu Corda
     1. Danh tính và địa chỉ Corda
     2. Sổ cái Corda
     3. States (Trạng thái)

Trong Corda, trạng thái (state) của một hợp đồng, giao dịch hoặc tài sản được lưu trữ và duy trì trong sổ cái của các node trong mạng. Mỗi trạng thái đại diện cho một trạng thái cụ thể của hợp đồng hoặc tài sản tại một thời điểm nhất định và không thể thay đổi trực tiếp (immutable). Khi một trạng thái mới được tạo ra, nó sẽ được thêm vào sổ cái và trở thành một phần của chuỗi các trạng thái (state sequences). Mỗi trạng thái đều được đánh dấu với một chỉ mục duy nhất để phân biệt và truy xuất.

Các trạng thái cũ được đánh dấu là "Historic" để chỉ ra rằng chúng đã trải qua quá trình chuyển đổi và không thể thay đổi. Ví dụ về trạng thái trong Corda cho trường hợp Alice đang nợ Bob 10$ sẽ được biểu diễn dưới dạng một trạng thái mới trong sổ cái, và sau đó trở thành một phần của chuỗi các trạng thái. Các trạng thái cũ trước đó sẽ được đánh dấu là **Historic** để theo dõi và lưu trữ lịch sử chuyển đổi trạng thái của hợp đồng nợ.



Mỗi node có một thành phần tên là **Vault** lư trữ tất cả các trạng thái liên quan đến nodes đó. Việc lưu trữ các trạng thái cũ trong sổ cái giúp tạo ra một lịch sử đầy đủ về các chuyển đổi và thay đổi trạng thái trong hệ thống. Điều này cho phép các bên tham gia trong mạng Corda có thể xem lại và kiểm tra lịch sử giao dịch, đảm bảo tính toàn vẹn và tin cậy của dữ liệu. Ngoài ra, sổ cái cũng cung cấp khả năng tra cứu và khảo sát các trạng thái trước đó, giúp phục hồi thông tin hoặc phân tích quá trình chuyển đổi.

Ảnh có chứa văn bản, biểu đồ, Phông chữ, hàng

Mô tả được tạo tự động

* + 1. Mô hình ghi chép thông tin UTXO

Corda được thiết kế với mục tiêu rõ ràng là tránh tối đa các vấn đề về khả năng mở rộng và quyền riêng tư phát sinh từ việc sử dụng phương pháp phát sóng toàn cầu và mô hình dữ liệu “global computer” (máy tính toàn cầu). Trong một hệ thống đồng thuận, việc tất cả các bộ xử lý của một giao dịch đạt được cùng một kết luận về tác động của nó là rất quan trọng. Trong những tình huống mà hai giao dịch có thể tác động lên cùng một tập dữ liệu, điều này có nghĩa là hai giao dịch phải được xử lý theo cùng một thứ tự bởi tất cả các nút. Nếu điều này không xảy ra, thì có thể tạo ra các tình huống trong đó các nút xử lý các giao dịch theo các thứ tự khác nhau và đạt đến những kết luận khác nhau về trạng thái của hệ thống. Vì lý do này, các hệ thống sử dụng chuỗi khối hoạt động "đơn luồng", có nghĩa là tất cả các giao dịch được sắp xếp liên quan đến nhau và áp dụng theo “**chuỗi**”.

Trong Corda, chúng ta giả định rằng dữ liệu đang được xử lý đại diện cho các thỏa thuận tài chính giữa các bên có thể xác định được và các tổ chức này sẽ áp dụng hệ thống chỉ khi một số lượng đáng kể các thỏa thuận như vậy có thể được quản lý bởi nền tảng. Vì vậy, hệ thống phải hỗ trợ việc thực hiện song song trong mức tối đa có thể, đồng thời đảm bảo sắp xếp giao dịch đúng khi hai giao dịch cố gắng tác động lên cùng một phần chia sẻ dữ liệu.

Để đạt được điều này, chúng ta phải giảm thiểu số lượng các bên cần nhận và xử lý các bản sao của bất kỳ giao dịch cụ thể nào và giảm thiểu mức độ hai giao dịch cố gắng biến đổi (hoặc thay thế) bất kỳ phần chia sẻ dữ liệu nào. Một giải pháp đã được áp dụng, các giao dịch chỉ được gửi cho các bên liên quan trực tiếp đến giao dịch đó. Điều này giảm thiểu số lượng các bên cần nhận và xử lý các bản sao của giao dịch và cung cấp quyền riêng tư cho các bên tham gia. Thay vì sử dụng mô hình phát sóng toàn cầu, Corda sử dụng mô hình truyền tin nhắn điểm-đến-điểm (point-to-point), nơi các bên chỉ nhận được thông tin cần thiết.

Điều quan trọng trong Corda là quyết định về đơn vị dữ liệu chia sẻ nhỏ nhất trong hệ thống. Quyết định này cũng ảnh hưởng sâu sắc đến quyền riêng tư: càng xác định tệ hơn các đơn vị dữ liệu chia sẻ, càng có nhiều bên liên quan có lợi ích trong việc đảm bảo tính chính xác của nó và phải xử lý và quan sát bất kỳ cập nhật nào đối với nó. Điều này trở nên rõ nhất khi chúng ta xem xét hai mô hình để biểu diễn số dư tiền mặt và thanh toán. Một mô hình tài khoản đơn giản cho tiền mặt sẽ xác định một cấu trúc dữ liệu chứa danh sách số dư tại một ngân hàng cụ thể cho mỗi chủ tài khoản. Mọi chủ sở hữu số dư sẽ cần một bản sao của cấu trúc này và do đó phải xử lý và xác nhận mọi giao dịch thanh toán, trong quá trình đó họ sẽ biết về các giao dịch và số dư của tất cả mọi người khác. Tất cả các thanh toán trên tập hợp tài khoản đó sẽ phải được xử lý tuần tự trên nền tảng, giới hạn tối đa khả năng xử lý.

Mô hình "UTXO" (unspent transaction outputs) sẽ xác định một cấu trúc dữ liệu đại diện cho một yêu cầu gửi đến ngân hàng. Người dùng tài khoản có thể nắm giữ nhiều yêu cầu như vậy, tổng số của chúng sẽ tiết lộ số dư của họ tại ngân hàng đó. Tuy nhiên, người dùng tài khoản chỉ cần tiết lộ cho người nhận thanh toán những yêu cầu đã sử dụng trong quá trình thực hiện thanh toán cho người nhận đó. Điều này cũng có nghĩa là người thanh toán có thể thực hiện nhiều thanh toán song song.

Có ví dụ sau, gồm 2 quá trình:

1. A và B giao dịch tài sản mức giá trị 2$
2. A cho C vai 3$



Giải thích A có 10$ muốn chuyển cho B 2$ đầu vào của giao dịch sẽ là “A có 10$”, đầu ra của giao dịch “A có 9$” và “B có 2$” khi giao dịch hoàn tất đầu vào (input) sẽ được đánh dấu **historic (\*)** – không thể sử dụng làm đầu vào cho các giao dịch khác.

1. Ưu điểm

* Các mục nhập sổ cái bất biến mang lại những lợi ích thông thường mà cách tiếp cận mang tính chức năng hơn mang lại: thật dễ dàng thực hiện phân tích trên ảnh chụp nhanh tĩnh của dữ liệu và lý do về nội dung, ngay cả khi nó thay đổi.
* Bởi vì không có tài khoản nên rất dễ dàng áp dụng các giao dịch song song, ngay cả đối với lưu lượng truy cập cao, giả sử các mục nhập đủ chi tiết.
* Không thể sắp xếp sai thứ tự các giao dịch do phụ thuộc vào hàm băm để xác định các trạng thái trước đó. Không cần số thứ tự hoặc những thứ khác khó cung cấp trong một hệ thống phân tán đầy đủ.
* Giải quyết xung đột tập trung vào vấn đề chi tiêu gấp đôi (double spends), đặt ra những yêu cầu cực kỳ tối thiểu đối với các thuật toán đồng thuận (vì biến mà bạn đang cố gắng đạt được sự đồng thuận là một tập hợp các boolean).
* Hợp đồng thông minh chỉ đơn giản là các hàm boolean và không trực tiếp thay đổi trạng thái. Do đó, không có vấn đề gì về tham nhũng nhà nước do những thứ như tái nhập bất ngờ, như trường hợp trong cuộc tấn công DAO mà Ethereum chứng kiến ​​hồi đầu năm.

1. Nhược điểm

* Việc biểu thị số lượng bằng cách sử dụng các mục không thay đổi trong mô hình UTXO có thể gây ra những vấn đề và tiềm ẩn rủi ro về quyền riêng tư. Ví dụ: Bạn có được $1000 và muốn gửi đi $100 cho một người khác. Để làm điều này trong mô hình UTXO, bạn sẽ sử dụng UTXO đầu vào trị giá $1000 và tạo ra hai UTXO mới: một UTXO trị giá $100 cho người nhận và một UTXO trị giá $900 làm tiền thừa trả lại cho bản thân. Quá trình này được gọi là tiền thừa hoặc tiền lẻ (change) và là một phần không thể tránh được trong mô hình UTXO. Thông qua phân tích các đầu vào và đầu ra của giao dịch, một người quan sát có thể suy ra thông tin nhạy cảm như số tiền mà bạn nhận được và số tiền thừa mà bạn nhận lại. Điều này có thể tiết lộ thông tin cá nhân và ảnh hưởng đến quyền riêng tư của bạn trong một mạng lưới công khai.
* Bởi vì người dùng cần phải suy nghĩ về số dư và báo cáo, nên bạn phải xếp lớp này lên trên sổ cái cơ bản: bạn phải tính toán số dư của người dùng thay vì chỉ đọc nó từ cơ sở dữ liệu. Do đó, tính toán số dư là một tính năng cốt lõi của ứng dụng “ví” rất quan trọng đối với Bitcoin. Ở Corda, ví tương đương được gọi là vault, nhưng nó thực hiện các nhiệm vụ tương tự.
* Kinh nghiệm từ những người đã phát triển ví cho Bitcoin và các hệ thống khác là chúng có thể là những đoạn mã phức tạp, mặc dù yếu tố góp phần đáng kể vào sự phức tạp của ví là việc xử lý việc thiếu tính hữu hạn (tức là khả năng tổ chức lại chuỗi).
* Mặc dù các giao dịch có thể được áp dụng song song nhưng việc tạo cho chúng song song sẽ khó hơn do cần phải thực thi nghiêm ngặt một thứ tự tổng thể. Đối với việc tạo song song, nếu người dùng là một luồng thì điều này thật dễ dàng, nhưng trong một tình huống phức tạp hơn khi bạn muốn nhiều giao dịch đồng thời, điều này có thể gây ra một hạn chế - trong trường hợp xấu nhất khi bạn có một đầu ra duy nhất đại diện cho tất cả giá trị của bạn, bạn buộc phải tuần tự hóa việc tạo mọi giao dịch (theo thứ tự).
  + 1. Tính riêng tư trong Corda

Mạng Corda được thiết kế với tính riêng tư cao và hướng tới các ứng dụng doanh nghiệp và tài chính. Dưới đây là những yếu tố quan trọng trong tính riêng tư của mạng Corda:

* Mạng Corda private: Corda không phải là một mạng công khai mà là một mạng riêng tư. Điều này có nghĩa là chỉ có các bên được ủy quyền nhất định mới được phép tham gia vào mạng và tham gia vào các giao dịch và hợp đồng thông minh.
* Quyền truy cập kiểm soát: Corda cho phép các bên tham gia kiểm soát quyền truy cập vào dữ liệu của mình. Mỗi bên có khả năng xác định rõ ràng quyền truy cập cho từng phần dữ liệu hoặc trạng thái. Điều này đảm bảo rằng chỉ có những bên được cho phép mới có thể truy cập và xem dữ liệu nhạy cảm.
* Mã hóa dữ liệu: Corda hỗ trợ mã hóa dữ liệu để đảm bảo tính riêng tư. Các bên tham gia có thể mã hóa thông tin nhạy cảm trong giao dịch hoặc trạng thái trước khi chúng được chia sẻ. Điều này đảm bảo rằng dữ liệu chỉ có thể được giải mã bởi các bên được ủy quyền.
* Quy tắc nhất quán: Corda cho phép thiết lập các quy tắc tuân thủ và ràng buộc để kiểm soát việc chia sẻ dữ liệu. Các bên tham gia có thể định nghĩa các quy tắc riêng để đảm bảo tính riêng tư và tuân thủ quy định pháp luật và quyền riêng tư.
* Tích hợp danh tính: Mạng Corda có thể tích hợp với các hệ thống quản lý danh tính (identity management systems) để xác định và xác minh danh tính của các bên tham gia. Điều này giúp đảm bảo rằng chỉ có các bên được xác thực mới có thể tham gia vào mạng và thực hiện các hoạt động giao dịch.
  + 1. Lưu trữ trong Corda

Trong Corda, lưu trữ được quản lý và tổ chức một cách phân tán và bảo mật. Corda sử dụng mô hình lưu trữ trạng thái (state storage) để lưu trữ các trạng thái của các đối tượng trong mạng.nCác trạng thái (states) trong Corda đại diện cho các đối tượng như tài sản, hợp đồng, thông tin giao dịch và thông tin kinh doanh khác. Mỗi trạng thái được lưu trữ dưới dạng một phiên bản không thay đổi (immutable) và có thể được truy cập và truy vấn bởi các bên có quyền truy cập tương ứng.

Corda hỗ trợ lưu trữ trạng thái bằng cách sử dụng cơ sở dữ liệu SQL như MySQL, PostgreSQL hoặc Oracle. Mỗi node trong mạng Corda có một cơ sở dữ liệu local để lưu trữ và quản lý các trạng thái của nó. Các cơ sở dữ liệu này được cấu hình để đảm bảo tính riêng tư và bảo mật của dữ liệu.

Ngoài việc lưu trữ trạng thái trong cơ sở dữ liệu SQL, Corda cũng hỗ trợ lưu trữ trạng thái bằng các công nghệ lưu trữ phân tán như Apache Cassandra hoặc H2. Điều này cho phép lưu trữ dữ liệu phân tán trên nhiều nút trong mạng Corda, đảm bảo tính sẵn sàng cao và khả năng mở rộng.

Một tính năng quan trọng khác của lưu trữ trong Corda là khả năng quản lý lịch sử trạng thái (state history). Corda lưu trữ lịch sử các phiên bản trạng thái để cho phép kiểm tra và xác minh tất cả các thay đổi trạng thái từng xảy ra trong quá trình giao dịch. Điều này đảm bảo tính minh bạch và tra cứu thông tin về các hoạt động kinh doanh trên mạng Corda. Tổ chức lưu trữ trong Corda đảm bảo tính riêng tư, bảo mật và sẵn sàng cao của dữ liệu, đồng thời cung cấp khả năng tương tác và truy xuất thông tin kinh doanh trong mạng Corda.

* 1. Mạng Corda
     1. Kiến trúc mạng Corda
     2. Các nodes (nút) mạng Corda
        1. Tổng quát

Một node (hay nút) trong Corda là một thực thể trong mạng Corda thường đại diện cho một bên trong mạng doanh nghiệp (Một bên có thể là một tổ chức, một công ty, hoặc một thực thể cá nhân). Mỗi bên vận hành nút chứa CorDapps mà bên đó sử dụng để tương tác với các đối tác khác trên mạng. Mỗi bên trong mạng Corda thường có một hoặc nhiều nút Corda để tham gia vào các hoạt động kinh doanh và giao dịch. Các nút Corda có thể chạy trên các máy chủ riêng biệt hoặc trong môi trường đám mây, và chúng được cấu hình để tham gia vào mạng Corda và giao tiếp với các nút khác. Corda node là môi trường chạy máy ảo Java (Java Virtual Machine run-time), mỗi node trong mạng đều có cho mình một định danh riêng.

Các thành phần trong kiến trúc của một Corda Node:

* Persistence layer: làm nhiệm vụ lưu trữ dữ liệu. Nó gồm 2 thành phần chính là Vault dùng để lưu trữ trạng thái của số cái và Storage service nơi lưu trữ các giao dịch
* Network interface thực hiện việc tương tác với các nodes khác trong mạng.
* RPC interface có chức năng tương tác với các thành phần khác trong node.
* Service Hub là nơi trung gian để tương tác với các services trong mạng (oracles, notary)
  + 1. Notary Services (dịch vụ công chứng)
       1. Tổng quát

Notary Services (dịch vụ công chứng) Công chứng viên là một dịch vụ độc đáo trong nền tảng Corda, được thiết kế để đảm bảo tính toàn vẹn và tính nhất quán của các giao dịch trong mạng lưới Corda. Vai trò chính của công chứng viên là ngăn chặn việc chi tiêu gấp đôi (**double spending**) bằng cách kiểm tra và đảm bảo rằng mỗi giao dịch chỉ chứa các trạng thái đầu vào duy nhất chưa được sử dụng.

Ngoài việc ngăn chặn double spending, Notary Services cũng hoạt động như một cơ quan đóng dấu thời gian. Mỗi giao dịch trong Corda có một khoảng thời gian nhất định và chỉ có thể được công chứng trong khoảng thời gian đó. Điều này giúp xác định thời điểm chính xác mà giao dịch được tạo ra và không thể bị thay đổi sau đó.

Dịch vụ công chứng được hình thành bởi một hoặc nhiều công chứng viên cùng nhau tạo thành một cụm công chứng (notary cluster). Mỗi cụm công chứng có thể có một cấu hình riêng đặt ra các quy tắc và chính sách cho việc công chứng giao dịch. Khi một giao dịch được tạo ra, nó sẽ được gửi đến cụm công chứng tương ứng để được công chứng. Trước khi cung cấp chữ ký cho giao dịch, cụm công chứng sẽ xác minh rằng trạng thái đầu vào của giao dịch không bị xung đột với các giao dịch trước đó đã được công chứng. Điều này đảm bảo rằng giao dịch mới không sử dụng trạng thái đã được sử dụng trong giao dịch trước đó, đồng thời duy trì tính nhất quán của dữ liệu trong mạng lưới Corda.

Khi xác định được rằng tất cả các trạng thái đầu vào của một giao dịch được tìm thấy là duy nhất và không bị trùng lặp, cụm công chứng viên sẽ ký giao dịch đó. Việc ký giao dịch này đảm bảo rằng giao dịch được công chứng và có thể được thêm vào sổ cái chung (ledger) của Corda. Tuy nhiên, nếu bất kỳ trạng thái đầu vào nào trong giao dịch giống hệt với trạng thái đã gặp trong một giao dịch trước đó, cụm công chứng viên sẽ từ chối giao dịch và gắn cờ rằng nỗ lực chi tiêu gấp đôi (double spending) đã xảy ra. Điều này đảm bảo rằng không có hai giao dịch trong mạng lưới Corda sử dụng cùng một trạng thái đầu vào, ngăn chặn việc chi tiêu gấp đôi và đảm bảo tính nhất quán của dữ liệu.

Mỗi trạng thái (states) chỉ có một cụm công chứng (notary cluster) được chỉ định, vì vậy cụm sẽ chỉ công chứng một giao dịch nếu đó là cụm công chứng được chỉ định của tất cả các trạng thái đầu vào của giao dịch. Một mạng Corda có thể có nhiều cụm công chứng, mỗi cụm chạy một thuật toán đồng thuận (consensus algorithm) khác nhau. Việc sử dụng nhiều cụm công chứng với các thuật toán khác nhau cho phép mạng tùy chỉnh và tuỳ biến quy trình công chứng tùy theo yêu cầu và nhu cầu cụ thể của từng phần tử trong mạng. Dịch vụ công chứng chạy một giao thức công chứng, quy định thuật toán đồng thuận và thực hiện xác thực bổ sung. Tuy nhiên trong Corda 5.0, chỉ hỗ trợ giao thức công chứng không xác thực, thực hiện các kiểm tra bổ sung tối thiểu ngoài xác thực chi tiêu kép và khung thời gian.

* + - 1. Phân loại

Corda có 2 loại công chứng:

1. Single-node (dich vụ công chứng đơn):

Đây là dịch vụ công chứng đơn giản chỉ lưu trữ các yêu cầu công chứng trong cơ sở dữ liệu của nút (node). Nó dễ cấu hình và có thể được sử dụng cho việc kiểm thử hoặc các mạng không yêu cầu tính sẵn có cao. Để nút Corda thông thường cung cấp dịch vụ công chứng chỉ cần thiết lập **notary** các giá trị cấu hình phù hợp như được chỉ định trong tệp cấu hình nút. Để client có thể sử dụng dịch vụ công chứng, notary.serviceLegalName phải được thêm vào các tham số mạng (network parameters). tuy nhiên Nếu đang sử dụng network bootstrapper dịch vụ công chứng sẽ được tự động thêm vào các tham số mạng.

1. Highly available (dịch vụ công chứng có tính sẵn sàng cao):

Đây là một dịch vụ công chứng được nhóm hóa do một bên duy nhất điều hành, có khả năng chịu được lỗi cao. Dịch vụ này được xây dựng để đảm bảo tính sẵn sàng cao và khảng năng hoặt động liên tục. Hai triển khai của Highly available là JPA và MySQL (không còn được dùng). Các dịch vụ công chứng JPA và MySQL có tính sẵn sàng cao được tạo thành bởi hai thàng phần:

* Công chứng viên: là một tập hợp các nút Corda được định cấu hình ở chế độ công chứng có tính sẵn sàng cao (HA). Mỗi nút trong tập hợp này có một danh tính pháp lý riêng biệt, nhưng chia sẻ cùng một danh tính công chứng duy nhất. Các nút công chứng viên này được cấu hình để hoạt động cùng nhau ở chế độ sẵn sàng cao, có khả năng chịu lỗi và đảm bảo tính sẵn sàng và tin cậy của dịch vụ công chứng.
* Cơ sở dữ liệu trạng thái công chứng: là một cơ sở dữ liệu logic duy nhất, được cấu hình để có tính sẵn sàng cao. Tất cả các nhân viên công chứng (notary worker) kết nối đến cơ sở dữ liệu này để lưu trữ và truy vấn trạng thái công chứng. MySQL là một trong những cơ sở dữ liệu phổ biến được sử dụng trong Corda để triển khai cơ sở dữ liệu trạng thái công chứng có tính sẵn sàng cao.

Để hình dung quá trình thiết lập như hình sau: Các nút thông thường sẽ ở tầng cao nhất và có màu vàng, các nút đóng vai trò là nút công chứng sẽ có màu đỏ, cuối cùng các nút cơ sở dữ liệu và bản sao cơ sở dữ liệu trạng thái hoạt động sẽ có màu xanh.

Ảnh có chứa văn bản, ảnh chụp màn hình, biểu đồ

Mô tả được tạo tự động

* + - 1. Bảo mật

Giao thức công chứng không xác thực trong Corda duy trì mức độ riêng tư bằng cách chỉ tiết lộ thông tin cần thiết để thực hiện xác thực giao dịch, trong khi giữ được tính bảo mật của các chi tiết khác. Dưới đây là một tóm tắt về các thành phần cụ thể trong giao dịch được tiết lộ:

|  |  |
| --- | --- |
| Thành phần | Mức độ bảo mật |
| Trạng thái đầu vào | Hiển thị ID giao dịch và vị trí đầu ra. Không tiết lộ loại tráng thái, nội dung. |
| Trạng thái đầu ra | Hiển thị tổng số trạng thái đầu ra mục đích cho giao thức theo dõi các trạng thái chưa được sử dụng. |
| Lệnh (Commands) | Không hiển thị |
| Tệp đính kèm(Attachments) | Không hiển thị |
| Cửa sổ thời gian (Time window) | Hiển thị đầu đủ |
| Danh tính công chứng (Notary identity) | Hiển thị đầy đủ |
| Chữ ký (Signatures) | Không hiển thị |
| Dữ liệu giao dịch (Transaction metadata) | Hiển thị đầy đủ |

* + - 1. Quy trình

Trong Corda R3 Notary Services được thực hiện qua nhiều quy trình khác nhau tuy nhiên có thể tổng quát thành bốn quy trình sau:

* Gửi yêu cầu công chứng: Khi một bên tham gia mạng Corda muốn công chứng một giao dịch, họ sẽ gửi yêu cầu công chứng đến dịch vụ công chứng. Yêu cầu này chứa thông tin về giao dịch cần công chứng, bao gồm các trạng thái đầu vào và đầu ra của giao dịch.
* Xác thực và xác minh: Dịch vụ công chứng (Notary Services) sẽ tiếp nhận yêu cầu và tiến hành xác thực và xác minh tính hợp lệ của giao dịch. Quá trình này bao gồm kiểm tra các trạng thái đầu vào của giao dịch, xác định tính hợp lệ của các chữ ký số và các quy tắc kinh doanh liên quan.
* Xác nhận và ký giao dịch: Nếu dịch vụ công chứng xác nhận rằng giao dịch là hợp lệ, nó sẽ thực hiện việc ký giao dịch bằng cách thêm chữ ký số của mình vào giao dịch. Chữ ký số này chứng minh rằng dịch vụ công chứng đã công nhận và xác nhận tính hợp lệ của giao dịch.
* Phân phối kết quả: Sau khi ký giao dịch, dịch vụ công chứng sẽ phân phối kết quả công chứng cho các bên liên quan. Kết quả này bao gồm thông tin về việc công chứng thành công hay không thành công của giao dịch.
  1. Ứng dụng trên Corda
     1. Khái niệm và kiến trúc ứng dụng Corda
     2. SmartContract trong corda
        1. Tổng quan

Hợp đồng thông minh số hóa các thỏa thuận bằng cách biến chúng thành mã thực thi tự động nếu các điều khoản hợp đồng được đáp ứng. Những người tham gia không cần phải tin tưởng lẫn nhau để tuân thủ các điều khoản trong hợp đồng vì các điều khoản này được thực thi theo quy tắc. Không cần thực thi từ bên ngoài và hợp đồng luôn được giải thích theo cùng một cách. Hợp đồng thông minh chi phối sự phát triển của các quốc gia tăng ca. Mã hợp đồng được sao chép trên các nút ảo trong mạng ứng dụng. Các thành viên mạng lưới phải đạt được sự đồng thuận rằng các điều khoản của thỏa thuận đã được đáp ứng trước khi họ thực hiện hợp đồng.

Tương tự Ethereum, Hyperledger hay Solana trong Corda cũng có smart contract. Tuy nhiên Smart contract trong Corda được thiết kế để tương thích với các quy trình kinh doanh hiện có và các yêu cầu pháp lý.

Trong Corda, smart contract được viết bằng ngôn ngữ lập trình như Kotlin và Java. Corda khác biệt ở chỗ nó tập trung vào ngôn ngữ pháp lý, quy trình kinh doanh, cách giải quyết các thỏa thuận tranh chấp và mối quan tâm cụ thể của các doanh nghiệp. Trong các nền tảng blockchain nêu trên Code là luật (Code is Law) thì Corda hướng tới triết lý Luật là luật (Law is Law).

Ví dụ về giao dịch tiền mặt, smart contract trong Corda có thể được viết để kiểm tra các điều kiện nhất định, chẳng hạn như tổng giá trị của input phải bằng tổng giá trị của output. Nếu giao dịch không thỏa mãn các điều kiện đã định, smart contract có thể từ chối (reject) giao dịch đó.

Ảnh có chứa văn bản, ảnh chụp màn hình, biểu đồ, Phông chữ

Mô tả được tạo tự động

Điều này cho phép Corda tạo ra các smart contract linh hoạt và tuân thủ các quy tắc kinh doanh và pháp lý hiện có. Các doanh nghiệp có thể sử dụng smart contract trong Corda để tự động hóa các quy trình kinh doanh và đảm bảo tính chính xác và tuân thủ pháp lý trong các giao dịch của họ.

* + - 1. Thành phần cấu tạo

Xét trên phiên bản mới nhất của Corda là 5.0 CDSE các thành phần chính cấu tạo lên hợp đồng thông minh trong Corda bao gồm:

* Ngôn ngữ lập trình: hiện tại Corda hỗ trợ việc viết smart contract bầng hai ngôn ngữ lập trình là Java và Kotlin. Ngôn ngữ lập trình cho phép lập trình viên xác định các quy tắc và điều kiện mà hợp đồng cần tuân thủ.
* States (Trạng thái): Trạng thái trong corda đại diện cho các thông tin quan trọng và dữ liệu liên quan đến hợp đồng. Mỗi trạng thái đại diện cho một phien bản cụ thể của hợp đồng và có thể thay đổi theo thời gian.
* Contracts (Hợp đồng): Hợp đồng trong Corda là một thành phần quan trọng xác định các quy tắc và điều kiện mà hợp đồng cần tuân thủ. Nó định nghĩa các quyền, nghĩa vụ và luật pháp áp dụng cho các bên trong hợp đồng. Hợp đồng trong Corda thường được viết dưới dạng mã lập trình và có thể chứa các điều kiện logic phức tạp.
* Transactions (Giao dịch): Giao dịch trong Corda đại diện cho các hoạt động và sự thay đổi trạng thái của hợp đồng. Các giao dịch có thể được khởi tạo bởi các bên tham gia và được thực thi tự động bởi hợp đồng thông minh. Giao dịch có thể chứa các thông tin và dữ liệu liên quan đến hợp đồng và có thể kích hoạt các hành động hoặc sự thay đổi trạng thái trong hợp đồng.
* Flows (Luồng): Luồng trong Corda định nghĩa các quy trình và quy trình kinh doanh mà hợp đồng cần tuân thủ. Nó mô tả các bước và tương tác giữa các bên trong quá trình thực hiện hợp đồng. Luồng có thể xác định các bước kiểm tra, xác minh và xử lý giao dịch, và cũng có thể gửi thông điệp và tương tác với các bên tham gia khác.

Để có một cái nhìn tổng quan nhìn hình ảnh dưới đây:

Ảnh có chứa văn bản, ảnh chụp màn hình, biểu đồ, phần mềm

Mô tả được tạo tự động

* + 1. Một số lĩnh vực ứng dụng
  1. Token trong Corda
     1. Khái niệm
     2. Phân loại token trong Corda
     3. Biểu diễn Fungible token
     4. Biểu diễn NonFungible token
     5. Token SDK
  2. Kết luận Chương 2

1. Xây dựng ứng dụng quản lý bất động sản trên Corda
   1. Giới thiệu tổng quan về ứng dụng
      1. Mô tả mục đích và tính năng của ứng dụng quản lý bất động sản trên Corda.
      2. Giới thiệu về các công nghệ và các thành phần trong mạng lưới Corda được sử dụng trong ứng dụng.
      3. Các lợi ích và ưu điểm của việc sử dụng Corda để phát triển ứng dụng quản lý bất động sản.
   2. Phân tích thiết kế ứng dụng
      1. Yêu cầu chức năng và phi chức năng
      2. Sơ đồ Use case
      3. Sơ đồ lớp
   3. Triển khai và vận hành ứng dụng
      1. Cài đặt và triển khai các nodes và các dịch vụ trong mạng lưới Corda.
      2. Định nghĩa các smart contract và các flow để xử lý các giao dịch.
      3. Kiểm thử và chạy thử ứng dụng.
   4. Kết luận Chương 3

# Tài liệu tham khảo

[] R3, Corda training: https://training.corda.net/

[2] R3, Corda token: https://docs.r3.com/en/platform/corda/4.8/enterprise/cordapps/token-sdk-introduction.html

[] Topdev, Blockchain: https://topdev.vn/blog/blockchain-la-gi/

[] AWS, Công nghệ Blockchain là gì?: https://aws.amazon.com/vi/what-is/blockchain/?aws-products-all.sort-by=item.additionalFields.productNameLowercase&aws-products-all.sort-order=asc

|  |  |  |  |
| --- | --- | --- | --- |
|  |  |  | *Hà Nội, ngày .... tháng .... năm 2023* |
| **XÁC NHẬN CỦA NGƯỜI HƯỚNG DẪN CHÍNH**  *(Ký, ghi rõ họ tên)* |  |  | **SINH VIÊN THỰC HIỆN**  *(Ký, ghi rõ họ tên)* |
|  |  |  |  |