|  |
| --- |
| 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.

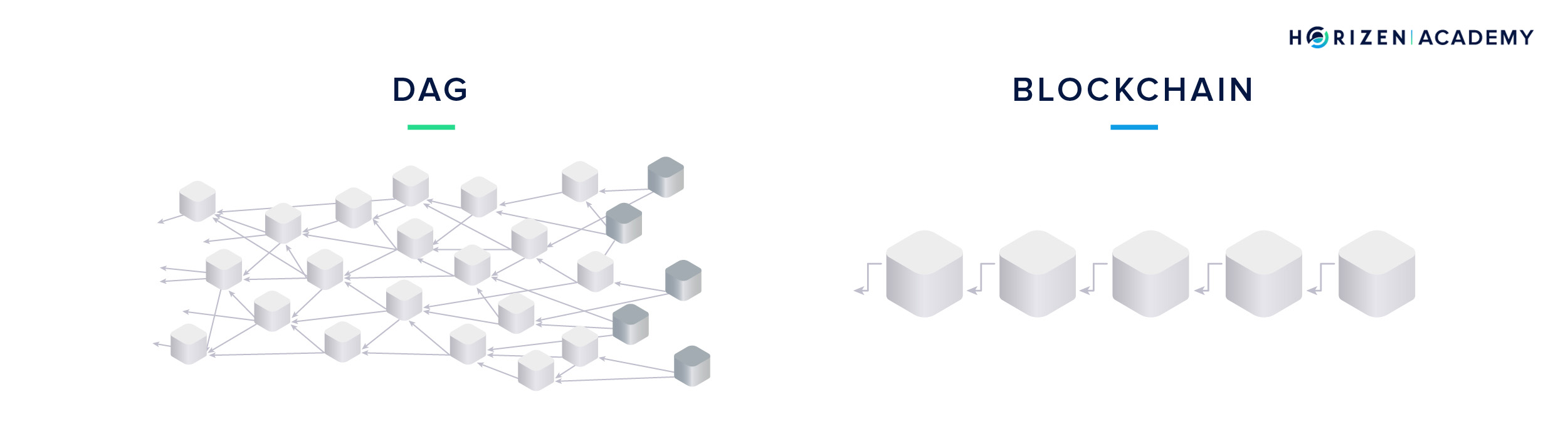
Cơ chế bảo mật có thể khác nhau tùy thuộc vào hệ thống DLT cụ thể và ứng dụng sử dụng nó. Mỗi hệ thống DLT có thể có các phương pháp và cơ chế bảo mật riêng, và việc bảo mật dữ liệu trong DLT là một lĩnh vực nghiên cứu và phát triển tiếp tục. Các cơ chế bảo mật này đóng vai trò quan trọng trong việc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

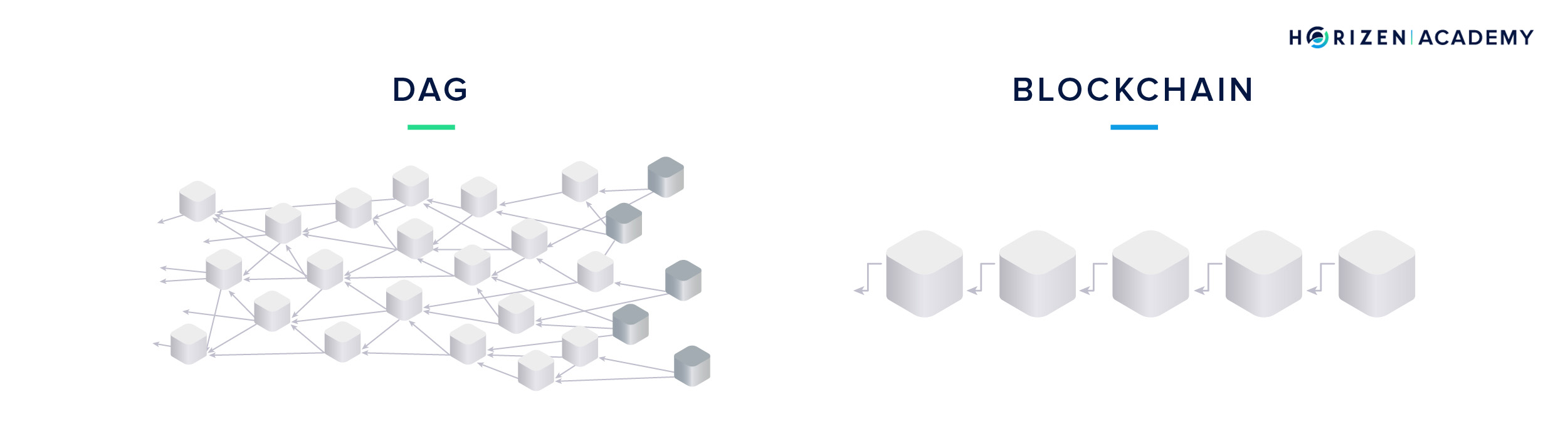


|  |  |
| --- | --- |
| Ưu điểm | Nhược điểm |
| Minh bạch: Blockchain cung cấp tính minh bạch cao vì mọi thành viên trong mạng lưới có thể xem và xác nhận các giao dịch. | Tốc độ giao dịch kém: Quá trình xác nhận và chứng thực giao dịch trên blockchain có thể mất thời gian và tốn năng lượng. Điều này 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
     2. Đặc trưng thiết kế
     3. Phân loại CryptoToken
     4. Cryptotoken Standards
     5. Blockchain Tokenzation
     6. Ứng dụng CryptoToken
     7. So sánh CryptoToken và Cryptocurrency
  2. Ứng dụng tài chính phi tập trung (DeFi)
     1. Ứng dụng phi tập trung DApp
     2. Khái niệm DeFi
     3. Nguyên lý hoạt động của các ứng dụng Defi
     4. Tính chất của DeFi
     5. Phân loại các ứng dụng Defi
  3. 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. 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.

Ví dụ về trạng thái trong Corda cho trường hợp Alice đang nợ Bob 100$ 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.

* + 1. Mô hình ghi chép thông tin UTXO

Mô hình UTXO (Unspent Transaction Output) là một phương thức quản lý tài sản trong các blockchain như Bitcoin. Trong mô hình UTXO, mỗi giao dịch tạo ra một hoặc nhiều UTXO, đại diện cho số tiền hoặc tài sản được gửi tới địa chỉ người nhận. Các UTXO đại diện cho các đầu ra giao dịch chưa được sử dụng, tức là chưa được tiêu thụ hoặc chi tiêu. Mỗi UTXO có một số lượng tiền hoặc tài sản cụ thể và địa chỉ người sở hữu. Khi một giao dịch mới được tạo, nó sẽ tiêu thụ một hoặc nhiều UTXO cũ để tạo ra các UTXO mới, đại diện cho số tiền hoặc tài sản được chuyển đi và được gửi tới các địa chỉ người nhận.

Mô hình UTXO cho phép xác định rõ ràng quyền sở hữu và nguồn gốc của tài sản trên mạng lưới blockchain. Bằng cách theo dõi và xác nhận các UTXO chưa được sử dụng, người dùng có thể kiểm tra xem một số tiền hoặc tài sản đã được chi tiêu hay chưa. Điều này đảm bảo tính toàn vẹn và tin cậy của lịch sử giao dịch trên blockchain.

Giống như mô hình UTXO cho các giao dịch giống như Bitcoin, Output của giao dịch này sẽ là Input cho giao dịch kế tiếp. Trong mô hình Corda, mỗi giao dịch chứa trạng thái (state) mới được tạo ra hoặc thay đổi từ trạng thái hiện có. Tuy nhiên đầu ra chỉ chứa thông tin về trạng thái mới và các bên tham gia liên quan.

**Ví dụ:** khi Alice muốn chuyển 1$ cho Bob, giao dịch sẽ có đầu vào (input) là trạng thái hiện tại của Alice có 10$. Đầu ra (output) của giao dịch sẽ bao gồm trạng thái mới cho Alice có 9$ và trạng thái mới cho Bob có 1$.

Sau khi giao dịch hoàn tất, trạng thái đầu vào (input) của giao dịch sẽ được đánh dấu là "Historic" để chỉ ra rằng nó đã được tiêu thụ và không thể sử dụng lại làm đầu vào cho các giao dịch tiếp theo. Điều này đảm bảo tính toàn vẹn của lịch sử giao dịch và ngăn cản việc chi tiêu hai lần của cùng một đầu ra.

* + 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
  1. Mạng Corda
     1. Kiến trúc mạng Corda
     2. Các nodes (nút) mạng Corda
     3. Notary Services (dịch vụ công chứng)
     4. Consensus (đồng thuận)
  2. Ứng dụng trên Corda
     1. Khái niệm và kiến trúc ứng dụng Corda
     2. SmartContract trong corda
     3. Một số lĩnh vực ứng dụng
  3. 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
  4. 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)* |
|  |  |  |  |