|  |
| --- |
| BAN CƠ YẾU CHÍNH PHỦ  **HỌC VIỆN KỸ THUẬT MẬT MÃ**  ¯¯¯¯¯¯¯¯¯¯¯¯¯¯¯¯ |
| ĐỀ CƯƠNG 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** |

# Mở đầu

## Tính cấp thiết của đề tài

Bất động sản là một trong những lĩnh vực quan trọng của nền kinh tế, đặc biệt là trong các thành phố lớn. Tuy nhiên, quản lý và giao dịch bất động sản vẫn còn nhiều khó khăn và tranh chấp. Sử dụng công nghệ blockchain và Fungible token có thể giúp giải quyết một số vấn đề này, đồng thời tăng tính minh bạch và hiệu quả trong quản lý và giao dịch bất động sản.

Hiện nay, thị trường bất động sản đang phát triển mạnh mẽ trên toàn thế giới và đặc biệt là tại các quốc gia có nền kinh tế phát triển như Hoa Kỳ, Trung Quốc, Nhật Bản, Châu Âu. Tuy nhiên, việc quản lý và giao dịch bất động sản vẫn còn nhiều khó khăn và tranh chấp.

Corda là một nền tảng blockchain được thiết kế đặc biệt cho các ứng dụng kinh doanh. Nền tảng này có nhiều ưu điểm như tính riêng tư cao, khả năng mở rộng linh hoạt và hỗ trợ tích hợp với các hệ thống kinh doanh hiện có. Việc sử dụng Corda để triển khai ứng dụng quản lý kinh doanh bất động sản sử dụng Fungible token sẽ giúp tăng tính đáng tin cậy và hiệu quả của ứng dụng.

Một số công ty bất động sản lớn đã bắt đầu áp dụng công nghệ blockchain trong quản lý và giao dịch bất động sản, nhưng vẫn chưa có nhiều thông tin về việc sử dụng Fungible token trong các ứng dụng này.

Chính vì vậy việc xây dựng ứng dụng quản lý bất động sản sử dụng Fungible token trên Corda mang tính mới mẻ, phù hợp với nhu cầu thực tế hiện nay.

## Mục tiêu thực hiện đồ án

* Nghiên cứu công nghệ sổ cái phân tán và công nghệ DAG
* Nghiên cứu công nghệ DAG trên corda và Fungible Token
* Xây dựng ứng dụng quản lý bất động sản trên Corda

# Dự kiến các Chương, mục

1. Công nghệ sổ cái phân tán và DAG

Chương này sẽ giải thích khái niệm Cụ thể, chương này sẽ giải thích về nguyên lý hoạt động của DLT và các ứng dụng phổ biến của nó trong các lĩnh vực như tài chính, chuỗi cung ứng, bảo hiểm, chứng khoán và quản lý tài sản.

Chương cũng sẽ giải thích về mô hình DAG, một loại DLT khác nhau so với blockchain truyền thống. Chúng ta sẽ tìm hiểu về cách DAG hoạt động, cách nó khác biệt so với blockchain và các ứng dụng của nó. nguyên lý hoạt động của DLT

* 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.

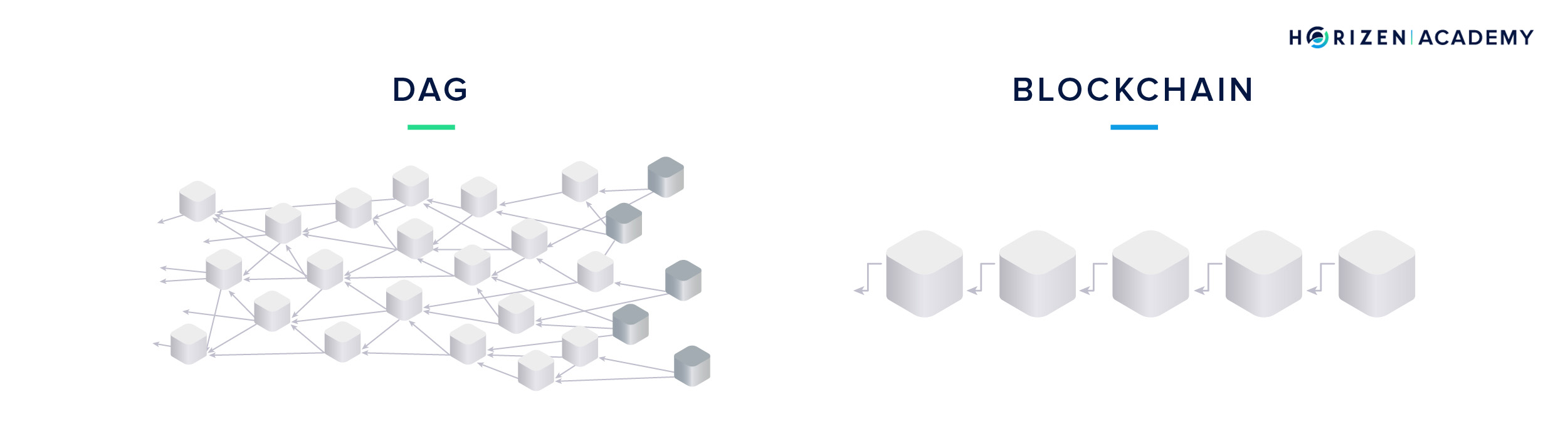
Cơ chế bảo mật có thể khác nhau tùy thuộc vào hệ thống DLT cụ thể và ứng dụng sử dụng nó. Mỗi hệ thống DLT có thể có các phương pháp và cơ chế bảo mật riêng, và việc bảo mật dữ liệu trong DLT là một lĩnh vực nghiên cứu và phát triển tiếp tục. Các cơ chế bảo mật này đóng vai trò quan trọng trong việc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

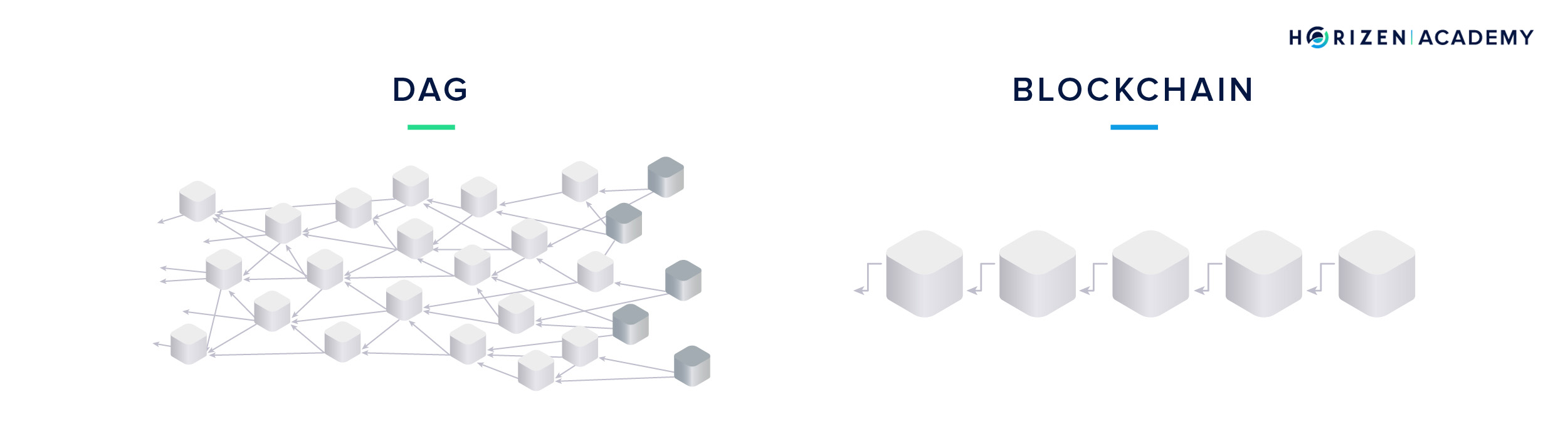


|  |  |
| --- | --- |
| Ưu điểm | Nhược điểm |
| Minh bạch: Blockchain cung cấp tính minh bạch cao vì mọi thành viên trong mạng lưới có thể xem và xác nhận các giao dịch. | Tốc độ giao dịch kém: Quá trình xác nhận và chứng thực giao dịch trên blockchain có thể mất thời gian và tốn năng lượng. Điều này 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
     2. Cấu Trúc DAG
     3. Cách thức hoạt động
     4. Ứng dụng DAG
     5. So sánh DAG và mô hình DLT khác
     6. Một số nền tảng DAG
  2. 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
  3. 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
  4. Kết luận Chương 1

1. Công nghệ DLT trên Corda

Chương này trình bày về nền tảng Corda một nền tảng được phát triển bởi R3, được thiết kế để hỗ trợ xây dựng các ứng dụng Blockchain cho các tổ chức và ngành tài chính – ngân hàng.

* 1. Tổng quan về corda
     1. Lịch sử phát triển
     2. Giới thiệu Corda
     3. Công nghệ liên quan
     4. Đặc trưng của Corda
     5. Ứng dụng của Corda
     6. Lợi ích khi sử dụng Corda
  2. Dữ liệu Corda
     1. Danh tính và địa chỉ Corda
     2. Sổ cái Corda
     3. States (Trạng thái)
     4. Mô hình ghi chép thông tin UTXO
     5. Tính riêng tư trong Corda
     6. Lưu trữ trong Corda
  3. Mạng Corda
     1. Kiến trúc mạng Corda
     2. Các nodes (nút) mạng Corda
     3. Notary Services (dịch vụ công chứng)
     4. Consensus (đồng thuận)
  4. Ứng dụng trên Corda
     1. Khái niệm và kiến trúc ứng dụng Corda
     2. SmartContract trong corda
     3. Một số lĩnh vực ứng dụng
  5. 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
  6. Kết luận Chương 2

1. Xây dựng ứng dụng quản lý bất động sản trên Corda

Chương này sẽ trình bày về quá trình triển khai ứng dụng quản lý kinh doanh bất động sản sử dụng Fungible token trên mạng blockchain Corda. Bao gồm môi trường triển khai như cấu hình phần cứng phần mềm,

* 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)* |
|  |  |  |