NFT

NFT là gì?

NFT, thường được gọi là Token không thể thay thế (Non-Fungible Token), là một loại tiền kỹ thuật số độc nhất, được bảo mật bằng công nghệ blockchain và không thể sao chép. Các Token thường được mã hóa bằng phần mềm tương tự như nhiều loại tiền điện tử khác. Mỗi Token không thể thay thế (NFT) đều có một mã định danh duy nhất và siêu dữ liệu(metadata). NFT thường được xem là tương tự như tiền điện tử, nhưng không giống như tiền điện tử, NFT không thể được trao đổi cho nhau và không thể thay thế được và NFT cung

cấp một chứng chỉ xác thực công khai hoặc bằng chứng sở hữu của bất kỳ tài sản kỹ thuật số nào.

Cách NFT hoạt động

- Công nghệ NFT: NFT được xây dựng trên nền tảng blockchain. Do cấu trúc độc đáo của chúng, mỗi NFT có thể được sử dụng cho nhiều ứng dụng khác nhau. NFT được xem là tối ưu để đại diện kỹ thuật số cho các tài sản vật lý như tác phẩm nghệ thuật và bất động sản, một nền tảng quản lý tài sản kỹ thuật số. Vì NFT được xây dựng trên blockchain, chúng có thể thu hẹp khoảng cách giữa nghệ sĩ và khán giả, loại bỏ trung gian và cũng có thể hoạt động như các nền tảng quản lý danh tính. NFT có tiềm năng loại bỏ các bên trung gian và tăng tốc giao dịch. Video và các đoạn highlight thể thao.Sự khác biệt duy nhất giữa NFT và việc mua hàng vật lý là NFT không thể được sử dụng trực tiếp; tuy nhiên, chúng đi kèm với một chứng chỉ sở hữu mà chủ sở hữu có thể trao đổi với nhau. Ngoài ra, dữ liệu duy nhất của NFT giúp việc xác minh quyền sở hữu trở nên đơn giản, cho phép chủ sở hữu lưu trữ hoặc sửa đổi thông tin, và thậm chí cho phép chữ ký kỹ thuật số trong siêu dữ liệu (metadata).

- Vai trò của hợp đồng thông minh trong NFT: Hợp đồng thông minh (Smart contracts) đóng một vai trò quan trọng trong NFT bằng cách tự động hóa việc thực hiện các giao dịch và xác định các quy tắc và điều kiện cho việc chuyển giao quyền sở hữu. Hợp đồng thông minh cho phép người sáng tạo tự động kiếm tiền bản quyền mỗi khi NFT của họ được bán lại trên thị trường. Chúng cũng đảm bảo tính minh bạch và loại bỏ sự cần thiết của các bên trung gian trong quá trình mua và bán

- Công nghệ NFT được xây dựng trên các nền tảng blockchain, trong đó Ethereum là lựa chọn phổ biến nhất nhờ vào chức năng hợp đồng thông minh của nó. Blockchain của Ethereum cho phép các nhà phát triển tạo và triển khai các ứng dụng phi tập trung (DApps) tương tác với NFT. Các tiêu chuẩn ERC-721 và ERC-1155 định nghĩa các thông số kỹ thuật cho NFT trên mạng Ethereum

Ứng dụng thực tế của NFT

NFT mở rộng ra ngoài nghệ thuật, chơi game và âm nhạc, tìm kiếm các ứng dụng trong các lĩnh vực thực tế khác nhau. NFT có thể được sử dụng để token hóa bất động sản, cho phép quyền sở hữu phân số và giao dịch tài sản hợp lý. NFT cũng có các trường hợp sử dụng tiềm năng trong xác minh nhận dạng, quản lý chuỗi cung ứng, hệ thống bán vé, v.v., cung cấp tính minh bạch, bảo mật và hiệu quả nâng cao.Nghệ thuật và đồ sưu tầm: NFT cho phép mua bán nghệ thuật kỹ thuật số và đồ sưu tầmGame: NFT đại diện cho các vật phẩm trong game, thúc đẩy quyền sở hữu, giao dịch và trải nghiệm chơi game độc đáo.Bán vé: NFT cung cấp vé an toàn và chống gian lận cho các sự kiện, mang lại các đặc quyền bổ sung và quyền truy cập vào nội dung độc quyền.Chuỗi cung ứng: NFT theo dõi quyền sở hữu và tính xác thực của hàng hóa vật lý, xác minh nguồn gốc hàng xa xỉ và đảm bảo an toàn thực phẩm.Tài chính phi tập trung (DeFi): NFT cũng có thể được sử dụng trong các ứng dụng DeFi, chẳng hạn như

cho vay và đi vay. Điều này có thể cho phép mọi người thế chấp NFT của họ để nhận khoản vay hoặc kiếm lãi từ việc nắm giữ NFT của họ.Danh tính Web3: NFT cho phép tạo ra danh tính phi tập trung, trao quyền kiểm soát dữ liệu cá nhân cho cá nhân và tạo điều kiện thuận lợi cho việc xác minh danh tính trực tuyến.

Siêu dữ liệu(metadata) của NFT

Siêu dữ liệu của NFT được sử dụng trong blockchain để cung cấp thông tin bổ sung hoặc dữ liệu về 1 tài sản, hữu ích khi thực hiện giao dịch với tài sản đó. Một vài vấn đề đã được nêu ra bao gồm:
- Tính minh bạch mà blockchain cung cấp, có bao nhiêu blockchain có thể được sử dụng đồng thời
- Cách các token dược giao dịch giữa các blockchain khác nhau
Hai vấn đề này liên quan đến nhau vì dữ liệu có thể được lấy từ một chuỗi, chuyển sang chuỗi khác qua các kênh mã hóa, sau đó được chuyển đổi khi chuỗi đích chấp nhận nó. Siêu dữ liệu NFT này có thể được lưu trữ trên blockchain nơi token tồn tại và được sử dụng như một nguồn xác thực (source of truth) về tài sản, đồng thời cung cấp thêm thông tin hữu ích khác

Metadata NFT được sử dụng như thế nào?

Siêu dữ liệu(metadata) NFT có thể được sử dụng cho nhiều thứ bao gồm
+ Cung cấp nguồn xác thực
+ Cung cấp thông tin bổ sung về tài sản(ảnh, mô tả, chi phí...)
+ Cho phép lưu trữ dữ liệu phi tập trung
+ Giúp đỡ khi thực hiện các giao dịch giữa chuỗi hoặc hồ sơ được lưu trữ ngoài chuỗi (trên các máy chủ tập trung như IPFS hoặc các trường hợp sử dụng khác).

Cách metadata NFT hoạt động?

Blockchain là một công nghệ rất an toàn để lưu trữ tài sản kỹ thuật số và thực hiện giao dịch. NFT là một dạng tài sản số có thể được mua bán, trao đổi giữa các người dùng mà không cần trung gian như ngân hàng hay chính phủ.
NFT metadata là dữ liệu giúp xác định và mô tả NFT, bao gồm các thông tin như hợp đồng thông minh, hình ảnh, tên, mô tả, và các thuộc tính khác. Metadata này giúp người dùng kiểm tra trạng thái của NFT hoặc chuyển nó sang tài khoản khác.
Thông tin NFT metadata thường được lưu trên mạng blockchain để đảm bảo tính minh bạch và bảo mật. Để hoạt động tốt, nó cần có cơ chế đồng thuận giúp duy trì sự an toàn cho hệ thống.

Cách Metadata được lưu trữ

Cách lưu trữ metadata của NFT phụ thuộc vào blockchain mà nó đang sử dụng.
Mỗi blockchain có cơ chế đồng thuận khác nhau, ảnh hưởng đến cách dữ liệu được lưu trữ. Trên sổ cái phân tán (distributed ledger), metadata có thể được lưu theo nhiều cách, tùy vào loại blockchain (công khai hay riêng tư) và cách nó được thiết kế.

Trong các blockchain công khai, metadata thường được lưu trữ bằng Merkle Tree Root, còn gọi là cây băm (hash tree).
- Merkle Tree là một cấu trúc dữ liệu dạng cây nhị phân không cân bằng.
- Mỗi nút trong cây chứa giá trị băm của các nút con bên dưới nó.
- Nút gốc (root node) là kết quả của việc băm toàn bộ các nút lá (leaf nodes).
- Mỗi nút con chứa giá trị băm của nút cha, tạo thành một chuỗi liên kết chặt chẽ.
Khi dữ liệu được lưu trên blockchain, nó phải được ký bởi khóa riêng (private key) của chủ sở hữu. Khóa riêng này giúp đảm bảo chỉ chủ sở hữu mới có thể đọc hoặc xác nhận dữ liệu của mình trong sổ cái phân tán.

Ứng dụng

NFT metadata có thể được sử dụng trong nhiều trường hợp khác nhau để làm cho việc sử dụng NFT trở nên hữu ích và hiệu quả hơn. Dưới đây là một số ứng dụng cơ bản:
- Ghi lại thông tin bổ sung cho token: NFT metadata có thể chứa thông tin như mã số sê-ri hoặc hóa đơn, giúp xác minh NFT là duy nhất và dễ dàng nhận diện khi giao dịch.
Ví dụ: Khi bạn mua một NFT, metadata có thể ghi lại ngày mua, giá trị, hoặc các chi tiết khác giống như một biên lai điện tử.
- Cung cấp thêm thông tin về tài sản
Metadata có thể chứa các thông tin về NFT như giá trị hiện tại, hình ảnh liên quan, hoặc vị trí của tài sản (nếu có).
Ví dụ: Một NFT về đất đai có thể chứa thông tin về vị trí, diện tích, hoặc lịch sử giao dịch của khu đất đó.
- Lưu trữ dữ liệu ngoài blockchain
Một số dữ liệu của NFT có thể không được lưu trực tiếp trên blockchain mà lưu trữ trên các máy chủ tập trung (như các máy chủ web bình thường).
Điều này có thể hữu ích khi các máy tính hoặc thiết bị có băng thông hoặc dung lượng lưu trữ hạn chế.
Mặc dù dữ liệu này được lưu ngoài blockchain, khi cần, nó vẫn có thể được truy cập qua kênh mã hóa để đảm bảo an toàn và bảo mật.

NFT có an toàn không?

NFT rất khó bị hack nhờ vào blockchain, nhưng mối nguy hiểm lớn nhất là khóa riêng của bạn. Nếu khóa bị mất, bị đánh cắp, hoặc lưu trữ không an toàn, NFT của bạn cũng có thể bị mất. Câu "not your keys, not your coin" cũng áp dụng cho NFT.
+ Mua từ người bán uy tín: Kiểm tra thông tin và đánh giá của người sáng tạo hoặc người bán.
+ Kiểm tra metadata: Đảm bảo thông tin về NFT, như người sáng tạo và mô tả, là chính xác.
+ Lưu trữ trong ví bảo mật: Không lưu NFT trong ví không đáng tin cậy hoặc ví nóng.
+ Cẩn thận với liên kết: Tránh nhấp vào liên kết từ nguồn không quen thuộc để tránh phishing.
+ Cập nhật phần mềm: Giữ phần mềm ví và thiết bị luôn được cập nhật để bảo vệ an toàn.

Lợi ích

Xác minh nguồn gốc: NFTs cung cấp một bản ghi minh bạch và không thể thay đổi về quyền sở hữu, đảm bảo tính xác thực và nguồn gốc của tài sản số.
Tiếp cận dễ dàng hơn: NFTs giúp thị trường nghệ thuật và sưu tầm trở nên dân chủ hóa, mang đến cơ hội cho các nhà sáng tạo và nhà sưu tập trên toàn thế giới.
Nguồn thu nhập mới: NFTs mang đến cơ hội kiếm tiền cho các nhà sáng tạo thông qua việc bán trực tiếp, tiền bản quyền và đấu giá.
Quyền sở hữu nâng cao: NFTs cung cấp quyền kiểm soát và sở hữu lớn hơn cho người dùng, cho phép họ chuyển nhượng, bán hoặc cấp phép NFT theo mong muốn.
Sự khan hiếm: Sự hạn chế về số lượng NFT có thể làm tăng giá trị của chúng, đặc biệt là những NFT liên kết với các nghệ sĩ hoặc thương hiệu nổi tiếng.
Có thể lập trình: NFTs có thể được lập trình để bao gồm các tính năng như tiền bản quyền hoặc điều khoản cấp phép, giúp chúng trở nên linh hoạt và có thể được sử dụng cho nhiều mục đích khác nhau.

Thách thức

Rủi ro gian lận: Do sự mới mẻ của NFTs, có một rủi ro về các giao dịch gian lận và các yêu cầu sở hữu bị trình bày sai.
Rủi ro biến động: Giá của NFTs có thể dao động đáng kể, gây ra rủi ro đầu tư với khả năng thiệt hại.
Rủi ro tác động môi trường: Bản chất tiêu tốn năng lượng của công nghệ blockchain được sử dụng trong NFTs góp phần vào các mối lo ngại về môi trường.
Cân nhắc trong tương lai: Chuẩn hóa, quy định, bảo mật và khả năng mở rộng là những khía cạnh quan trọng cần được giải quyết để phát triển và ổn định thị trường NFT trong tương lai

Ví Blockchain là gì?

Ví Blockchain là một ứng dụng phần mềm hoặc thiết bị phần cứng cho phép người dùng tương tác với mạng lưới blockchain. Nó cho phép người dùng gửi, nhận và lưu trữ tài sản kỹ thuật số một cách an toàn. Mỗi ví blockchain chứa một cặp khóa: một khóa công khai (public key) và một khóa riêng tư (private key).

- Khóa Công khai (Public Key): Giống như số tài khoản ngân hàng của bạn, khóa công khai được sử dụng để tạo địa chỉ ví mà người khác có thể dùng để gửi tiền điện tử cho bạn. Bạn có thể chia sẻ địa chỉ này một cách công khai mà không ảnh hưởng đến bảo mật của ví.
- Khóa Riêng tư (Private Key): Đây là khía cạnh quan trọng nhất của ví blockchain. Khóa riêng tư giống như mật khẩu hoặc mã PIN cho tài khoản ngân hàng của bạn. Nó cấp quyền truy cập và

kiểm soát hoàn toàn đối với số tiền điện tử được liên kết với địa chỉ ví tương ứng. Việc giữ khóa riêng tư an toàn và bí mật là cực kỳ quan trọng. Nếu ai đó có được khóa riêng tư của bạn, họ có thể truy cập và đánh cắp tiền của bạn.

Ví Blockchain hoạt động như thế nào?

Khi ai đó gửi tiền điện tử cho bạn, họ thực chất đang gửi chúng đến địa chỉ công khai của bạn trên blockchain. Giao dịch này được ghi lại trên sổ cái công khai của blockchain. Tiền không thực sự di chuyển vào ví của bạn; thay vào đó, ví của bạn giữ khóa riêng tư cho phép bạn "mở khóa" số tiền đó tại địa chỉ của bạn trên blockchain và chứng minh quyền sở hữu.

Khi bạn muốn gửi tiền điện tử, bạn sử dụng khóa riêng tư của mình để ký (ủy quyền) giao dịch. Chữ ký số này chứng minh rằng bạn là chủ sở hữu hợp pháp của số tiền và cho phép giao dịch được xác thực bởi mạng lưới blockchain.

Các loại Ví Blockchain:

Có nhiều loại ví blockchain khác nhau, mỗi loại có mức độ bảo mật và tiện lợi riêng:

Ví Phần mềm (Software Wallets):

- Ví Máy tính để bàn (Desktop Wallets): Được cài đặt trên máy tính cá nhân. Cung cấp mức độ bảo mật tốt nếu máy tính được bảo vệ đúng cách.
- Ví Di động (Mobile Wallets): Ứng dụng trên điện thoại thông minh. Tiện lợi cho việc sử dụng hàng ngày và giao dịch khi di chuyển. Thường có tính năng quét mã QR.
- Ví Web/Trực tuyến (Web/Online Wallets): Truy cập thông qua trình duyệt web. Tiện lợi nhưng thường kém an toàn nhất vì khóa riêng tư có thể được quản lý bởi bên thứ ba hoặc lưu trữ trực tuyến.

Ví Phần cứng (Hardware Wallets):

- Đây là các thiết bị vật lý (thường giống USB) được thiết kế đặc biệt để lưu trữ khóa riêng tư ngoại tuyến (offline), còn gọi là "lưu trữ lạnh" (cold storage).
- Chúng được coi là một trong những lựa chọn an toàn nhất vì khóa riêng tư không bao giờ rời khỏi thiết bị, ngay cả khi kết nối với máy tính bị nhiễm phần mềm độc hại. Các giao dịch được ký bên trong thiết bị.

Ví Giấy (Paper Wallets):

- Là một bản in vật lý của khóa công khai và khóa riêng tư của bạn (thường dưới dạng mã QR).

    - Đây là một dạng lưu trữ lạnh vì các khóa hoàn toàn ngoại tuyến. Tuy nhiên, chúng dễ bị tổn thương do hư hỏng vật lý (cháy, nước), mất mát hoặc bị đánh cắp vật lý.

Tầm quan trọng của Ví Blockchain:

- Bảo mật: Cung cấp một cách an toàn để quản lý tài sản kỹ thuật số nếu được sử dụng đúng cách (đặc biệt là ví phần cứng).
- Quyền kiểm soát: Người dùng có toàn quyền kiểm soát khóa riêng tư và do đó, kiểm soát hoàn toàn tiền của họ (trừ khi sử dụng ví lưu ký - custodial wallet nơi bên thứ ba giữ khóa).
- Khả năng tiếp cận: Cho phép người dùng dễ dàng gửi và nhận tiền điện tử trên toàn cầu.
- Minh bạch: Các giao dịch được ghi lại công khai trên blockchain (mặc dù danh tính người dùng thường là bút danh).

Các Biện pháp Bảo mật cho Ví Blockchain:

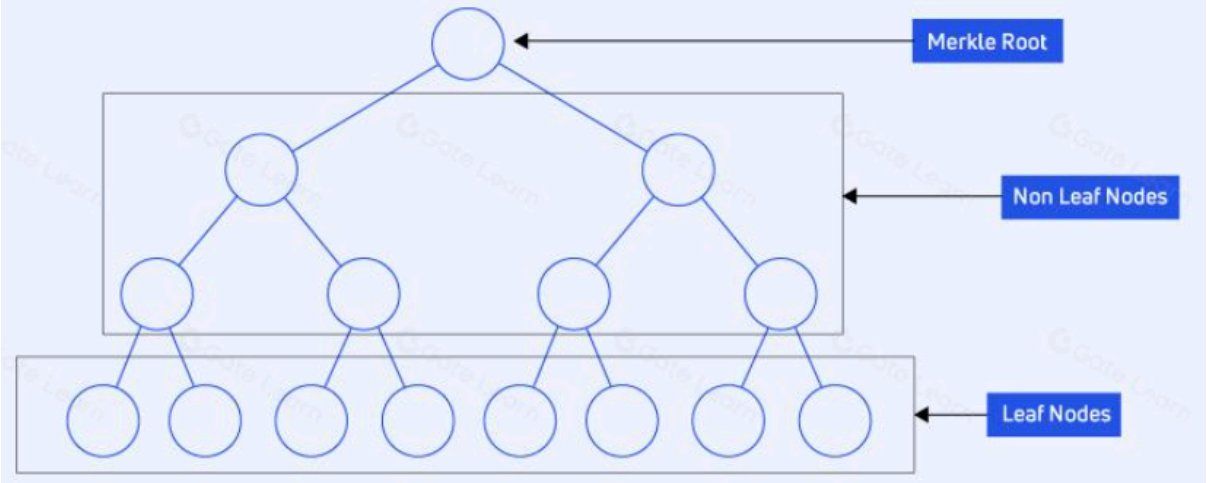
- Giữ bí mật Khóa Riêng tư: Không bao giờ chia sẻ khóa riêng tư hoặc cụm từ khôi phục (seed phrase) của bạn với bất kỳ ai.
- Sử dụng Mật khẩu Mạnh: Bảo vệ ví phần mềm của bạn bằng mật khẩu mạnh và duy nhất.
- Kích hoạt Xác thực Hai yếu tố (2FA): Thêm một lớp bảo mật bổ sung nếu ví hỗ trợ.
- Sao lưu Ví của Bạn: Hầu hết các ví đều cung cấp một cụm từ khôi phục (thường là 12 hoặc 24 từ). Hãy viết nó ra và cất giữ ở nhiều nơi an toàn, ngoại tuyến. Cụm từ này có thể khôi phục ví của bạn nếu thiết bị bị mất hoặc hỏng.
- Cẩn thận với Lừa đảo Trực tuyến (Phishing): Cảnh giác với các trang web, email hoặc ứng dụng giả mạo cố gắng đánh cắp thông tin đăng nhập hoặc khóa riêng tư của bạn.
- Cập nhật Phần mềm: Giữ cho phần mềm ví và hệ điều hành của bạn được cập nhật để vá các lỗ hổng bảo mật.

Merkle Tree

Merkle tree là gì?

Một cây Merkle hay còn được biết đến là cây hash, là cấu trúc dữ liệu nền tảng cho công nghệ blockchain, đảm bảo xác minh giao dịch hiệu quả và an toàn, nó tổ chức các hash của các giao dịch trong 1 cấu trúc giống cây phân cấp nơi mà mỗi nút lá (leaf node) đại diện cho 1 mã băm mật mã của 1 dữ liệu giao dịch riêng lẻ và mỗi node không phải lá chứa mã băm của node con của nó.

Cấu trúc và thành phần



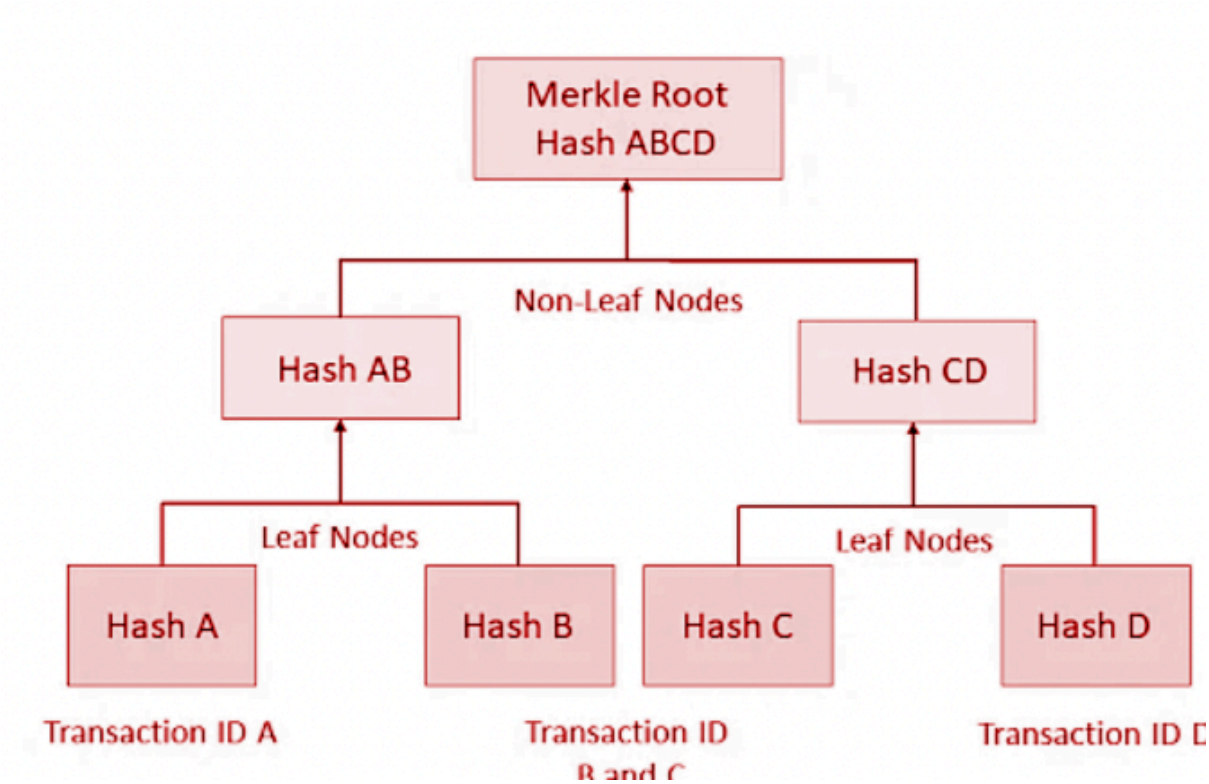
1. Leaf Node
   Mỗi giao dịch trong 1 khối có giá trị băm của riêng nó. Giá trị băm này được lưu trữ ở leaf node
2. Non Leaf Node
   Là node nằm ở giữa leaf node và root, chứa giá trị băm được tính toàn bằng việc kết hợp và băm các node con của nó
3. Merkle Root
   Là root của merkle tree, và chứa 1 giá trị băm đại diện cho tất cả giao dịch trong 1 khối và nó được lưu trữ trong Block header
   Một sự thay đổi trong bất kỳ dữ liệu nào sẽ dẫn đến sự thay đổi trong merkle root,
   đảm bảo không có dữ liệu nào trên mạng bị thay thế

Cách Merkle tree hoạt động?

Một merkle tree tổng hợp tất cả giao dịch trong 1 khối và tạo 1 dấu vân tay ký thuật số duy nhất cho tất cả các hoạt động, cho phép người dùng kiểm tra liệu 1 giao dịch có tồn tại trong 1 khối nào đó không.
Merkle được tạo ra bằng cách liên tục băm từng cặp node cho đến khi chỉ còn lại 1 giá trị băm duy nhất được biết đến là Merkle root
Được thiết kế từ dưới lên với giá trị băm của từng giao dịch làm nền tảng

Ví dụ:
Nếu 1 khối có 4 giao dịch (A, B, C, D) và H là 1 hàm băm.

1. Giá trị băm của từng giao dịch: H(A), H(B), H(C), H(D)
2. Ghép đôi và băm: H(AB) = H(H(A) + H(B)), H(CD) = H(H(C) + H(D))
3. H (ABCD) = H(H(AB) + H(CD))



Ứng dụng trong blockchain

1. Xác minh giao dịch 1 cách hiệu quả
   Thay vì tải toàn bộ blockchain để xác minh giao dịch, chỉ cần Block header và merkle path được yêu cầu. Điều này giảm chi phí tính toán và lưu trữ.
2. Toàn vẹn dữ liệu: merkle root thay đổi nếu có sự thay đổi trong các giao dịch và dễ dàng xác định giả mạo
3. Lưu trữ dữ liệu nhỏ gọn: merkle sử dụng không gian đĩa nhỏ khi so sánh các cấu trúc dữ liệu khác, cho phép xử lý tập dữ liệu lớn
4. Giao dịch thông tin nhanh: Bản chất nhỏ gọn của Root Merkle cho phép xác minh và chuyển nhanh hơn trên các mạng ngang hàng2.

Lợi ích

Hiệu suất xác thực: Xác minh nhanh tính toàn vẹn của dữ liệu mà không tiêu tốn nhiều tài nguyên xử lý.

Phát hiện giả mạo: Bất kỳ thay đổi nào đối với dữ liệu giao dịch đều làm thay đổi Merkle root, đảm bảo hồ sơ không thể bị giả mạo.

Giảm băng thông sử dụng: Các node có thể xác thực giao dịch mà không cần tải xuống toàn bộ blockchain.

Mekle Path trong Merkle Tree

loading…

Ethereum - Hợp đồng thông minh(smart contract) và ứng dụng phi tập trung(DAPP)