Mục lục

1. Giới thiệu về công nghệ Blockchain

1.1 Blockchain là gì?

Blockchain là 1 cơ sở dữ liệu của những bản ghi phân tán phi tập trung của tất cả các giao dịch và sự kiện kỹ thuật số đã xảy ra và được chia sẻ giữa các bên tham gia. Mỗi giao dịch được xác minh bởi hầu hết các bên tham gia hệ thống. Khi 1 tập các giao dịch đạt tới 1 giới hạn nhất định nó sẽ tạo ra khối (Block), đây là nơi mỗi giao dịch trên 1 blockchain được xác thực và sau đó nó được lưu trữ vĩnh viễn. Chuỗi (Chain) của blockchain là 1 loạt các khối liên tiếp được kết nỗi với nhau, tạo nên sổ cái bất biến và minh bạch. Nó chứa từng bản ghi duy nhất của mỗi giao dịch.

Ví dụ: Bitcoin là tiền điện tử phổ biến nhất được phát triển dựa trên công nghệ blockchain.

1.2 Sự khác nhau giữa blockchain và cơ sở dữ liệu truyền thống?

Blockchain khác với cơ sở dữ liệu truyền thống ở 2 điểm: cách nó hoạt động và ai sẽ chịu trách nhiệm cho nó. Blockchain hoạt động độc lập khỏi công ty hoặc dưới sự giám sát của bên thứ 3 cho phép giao dịch không cần quyền hạn và không cần tin tưởng, với cơ sở dữ liệu truyền thống thì thường được sở hữu và vận hành bởi 1 thực thể duy nhất.

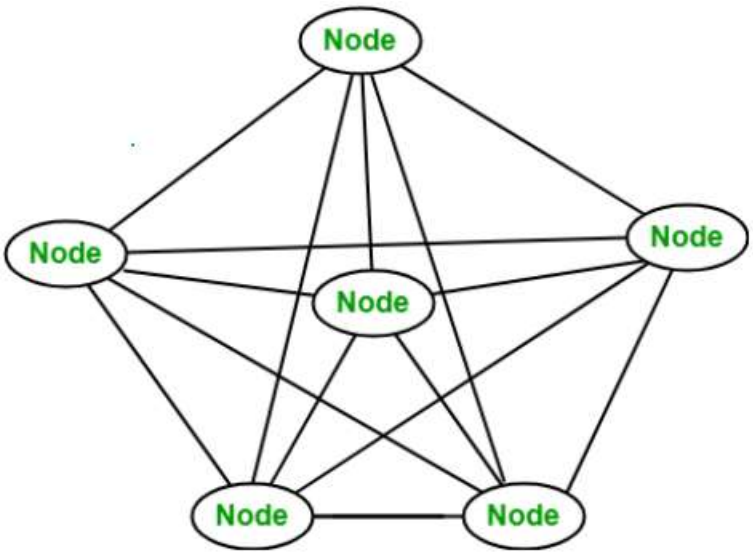
1.3 Thành phần cốt lõi của mạng Blockchain.

Thành phần cốt lõi của mạng blockchain thiết yếu cho khả năng hoạt động và chức năng của nó. Mỗi thành phần đóng 1 vai trò quan trọng trong việc duy trì tính nhất quán bảo mật và hiệu quả của mạng. Dưới đây là những thành phần cốt lõi của mạng blockchain.

1.3.1 Node

Một Node là 1 máy tính kết nối đến mạng blockchain . Node kết nối với blockchain bằng cách sử dụng phần mềm client. Client hỗ trợ trong việc xác thực và lan truyền giao dịch lên mạng blockchain. Khi 1 máy tính kết nối đến mạng Blockchain, 1 bản sao của dữ liệu blockchain được tải xuống vào trong hệ thống và node đồng bộ nó với khối (block) dữ liệu mới nhất trên blockchain (mỗi node lưu trữ 1 bản sao toàn bộ blockchain hoặc 1 phần của nó). Các Node kết nỗi đến mạng Blockchain hỗ trợ trong việc thực thi giao dịch sẽ nhận được phần thưởng gọi là thợ đào (miner).
Phân loại node:

1. Full Nodes: nó duy trì 1 bản sao đầy đủ của tất cả các giao dịch. Nó có khản năng xác thực, chấp nhận và từ chối giao dịch.
2. Partial Nodes: nó chỉ chứa các giá trị băm (hash value) của giao dịch. Toàn bộ giao dịch được truy cập thông qua giá trị băm này.
3. **Mining Nodes: là những máy tính xác thực giao dịch và thêm chúng vào blockchain thông qua** quá trình đào (mining)



1.3.2 Giao dịch (transaction)

Giao dịch là đơn vị dữ liệu cơ bản trong blockchain, đại diện cho việc trao đổi thông tin hoặc giá trị. Một giao dịch được tạo và xác minh bởi nodes trong mạng và sau đó lưu trữ vào blockchain.

1.3.3 Sổ cái (ledger)

Bản thân Blockchain là 1 sổ cái phân tán để lưu trữ toàn bộ giao dịch an toàn và bất biến. Sổ cái bao gồm các khối. Mỗi khối chứa 1 tập các giao dịch, dấu thời gian, mã băm của khối trước đó, merkel tree…

Các loại sổ cái:

1. Public ledger: nó mở và minh bạch, bất kỳ ai trên mạng cũng có thể đọc và ghi nó
2. Sổ cái phân tán (distributed ledger): tất cả các node có 1 bản sao cục bộ của cơ sở dữ liệu, 1 nhóm các nút cùng với nhau thực hiện xác minh giao dịch
3. Sổ cái phi tập trung (decentralized ledger): không có 1 node hay nhóm các node nào có quyền điều kiển trung tâm, mỗi nút tham gia đều phải thực hiện công việc như xác thực, duy trì tính nhất quán…

1.3.4 Thuật toán đồng thuận (consensus Algorithm)

Là 1 thuật toán cho phép người tham gia mạng tham gia vào quá trình xác minh giao dịch và duy trì tính nhất quán trên sổ cái.

1.3.5 Mật mã học

Là 1 phần rất quan trọng cho việc đảm bảo giao dịch, dữ liệu nhất quán và duy trì sự riêng tư trong mạng blockchain.

1. Hàm băm (hash function): tạo ra 1 đầu ra cố định duy nhất cho bất kỳ đầu vào nào, điều này đảm bảo rằng bất kỳ sự thay đổi nhỏ nào trong đầu vào sẽ tạo ra mã băm (hash) khác nhau đầu ra ngăn chặn giả mạo
2. Chữ ký số (digital signature): sử dụng cho việc xác minh tính xác thực giao dịch. Nó được tạo bằng cách sử dụng Private key của người gửi và dùng Public key của người gửi để xác minh từ đó đảm bảo tính nhất quán và nguồn gốc của giao dịch.
3. Public và Private key: Mỗi người dùng đều có cặp public, private key. Public key có thể chia sẻ cho mọi người nhưng private phải được bảo mật.

1.3.6 Hợp đồng thông minh

Là hợp đồng tự thực thi với những điều khoản được viết trực tiếp vào trong code, và chạy trên mạng blockchain.

1. Tự động thực thi mà không yêu cầu bên thứ 3 giúp giảm chi phí, tăng tính hiệu quả giảm lỗi do con người gây ra
2. Thực thi khi các điều kiện được thỏa mãn

1.3.7 Tokens

Là những tài sản kỹ thuật số được tạo trên blockchain có thể đại diện cho nhiều tiện ích, quyền lợi và tài sản khác nhau.

Ví dụ:

1. Utility tokens: cung cấp cho người dùng khản năng truy cập vào sản phẩm hoặc dịch vụ trong 1 hệ sinh thái Blockchain cụ thể (Ethereum's Ether)
2. **Security Tokens:** đại diện cho quyền sở hữu tài sản thực tế, chẳng hạn chư cổ phiếu…
3. Stablecoin

1.4 Phi tập trung là gì?

Phi tập trung được biết đến như là sự phân bổ chức năng giữa nhiều đơn vị. Đó là một hệ thống kết nối, nơi không có thực thể nào có toàn quyền kiểm soát. Đây là một kiến trúc trong đó khối lượng công việc, bao gồm cả phần cứng và phần mềm, được phân phối giữa nhiều trạm làm việc.
Lợi ích:

- Không có cơ quan kiểm soát ở trung tâm: mỗi người dùng đều có quyền ra quyết định của họ
- Khản năn mở rộng lớn: có thể thêm nhiều máy tính vào mạng mà không cần lo lắng
- Người dùng có thể chia sẻ ý kiến và dữ liệu của họ 1 cách tự do và ít kiểm soát

Vấn đề: vấn đề mà hệ thống phi tập trung là không nhất quán, 1 số thực thể có hại có thể gây ảnh hưởng mà làm mất dữ liệu

Ví dụ về 1 hệ thống phi tập trung:

- WWW có tính phi tập trung cao, hàng triệu người dùng có thể kết nối với nhau và không người dùng nào có quyền hoàn toàn với nó.

1.5 Những phiên bản khác nhau của blockchain

1.5.1 Blockchain 1.0 (Cryptocurrency)

Được ứng dụng cho tiền điện tử, thực hiện các giao dịch mà không có bên thứ 3. Mục tiêu tạo ra 1 sổ cái minh bạch, phân tán, phi tập trung và bất biến và được duy trì bởi người tham gia mạng. Ví dụ: bitcoin

1.5.2 Blockchain 2.0 (Hợp đồng thông minh – Smart Contract)

Vì vấn đề tiêu tốn năng lượng và khản năng mở rộng kém của Blockchain 1.0. Blockchain 2.0 không bị giới hạn trong tiền điện tử (cryptocurrency) mà còn có "Hợp đồng thông minh".

Hợp đồng thông minh là 1 chương trình máy tính nằm trong chuỗi khối, có thể tự thực thi khi các điều kiện được định nghĩa trước đó được thỏa mãn.

1.5.3 Blockchain 3.0 (Ứng dụng phi tập trung – Dapp)

Phiên bản 3.0 giới thiệu về Ứng dụng phi tập trung (dapp). Nó cũng giống như các app thông thường, fontend tương tác với backend phi tập trung chạy trên mạng ngang hàng. Dapp hoàn toàn phi tập trung không có chủ sở hữu duy nhất giúp nó minh bạch bảo mật cao dữ liệu công khai và chống kiểm duyệt. Lợi ích không bảo giờ tắt, đảm bảo quyền riêng tư.

1.6 Phân loại Blockchain theo quyền truy cập

1.6.1 Blockchain không cần cấp quyền (Permisstionless Blockchain)

Là 1 loại mạng Blockchain cho phép bất kỳ ai tham gia mạng mà không cần quyền hay phê duyệt đặc biệt.

1. Mở: Bất kỳ ai cũng có thể tham gia mạng, xác thực giao dịch và đóng góp vào blockchain. Điều này làm tăng tính phi tập trung nơi không có 1 thực thể duy nhất nào kiểm soát mạng.

2. Phi tập trung: Blockchain không cần cấp quyền hoạt động trên mạng phi tập trung hỗ trợ phân phối quyền lực, giảm kiểm duyệt và thao túng bởi bất kỳ thực thể nào.

3. Thuật toán đồng bộ: Mạng blockchain này thường sử dụng thuật toán đồng bộ để xác thực giao dịch và bảo mật mạng.

4. Tính minh bạch: Tất cả giao dịch được xác minh và lưu trữ trên sổ cái công cộng, nơi bất kỳ ai cũng có thể xem lịch sử giao dịch và tăng tính toàn vẹn của dữ liệu.

5. Tính ẩn danh: trong khi giao dịch minh bạch, người tham gia vẫn thường ẩn danh dưới dạng bút danh. Người dùng thường được xác định dưới dạng public key thay vì thông tin cá nhân, tạo ra thêm 1 lớp bảo mật.

1.6.2 Blockchain được cấp quyền (permisstioned blockchain)

Là 1 loại mạng blockchain hạn chế truy cập và người tham gia chỉ 1 nhóm người dùng được ủy quyền. Không giống như Blockchain không được ủy quyền nơi mà bất kỳ ai cũng có thể tham gia và xác thực giao dịch, blockchain được ủy quyền yêu cầu người tham gia thực hiện 1 số quy tắc nhất định hoặc là nhận được quyền truy cập mạng.

1. Kiểm soát truy cập: Chỉ những người dùng được cấp quyền mới có thể tham gia mạng. Đảm bảo rằng các node được xác minh và kiểm soát. Từ đó cho phép kiểm soát tốt ai xác minh giao dịch và truy cập dữ liệu.
2. Quản trị tập trung: Thường được quản lý bởi 1 liên minh tổ chức hoặc là 1 cơ quan trung ương, cơ quan hoặc tổ chức đó sẽ quyết định về nguyên tắc và chính sách.
3. Tăng cường quyền riêng tư: giao dịch và dữ liệu thường riêng tư hơn vì thông tin nhạy cảm có thể được lưu trữ ngoài chuỗi và chỉ được chia sẻ với những bên được ủy quyền.
4. Tùy chỉnh giao thức: Tổ chức có thể tùy chỉnh giao thức đồng thuận và những giao thức khác để phù hợp với nhu cầu của họ.

1.7 Phân loại theo mô hình triển khai

1.7.1 Public Blockchain

Public Blockchain là gì?

Là 1 loại blockchain hoàn toàn mở và phi tập trung nơi bất kỳ ai cũng có thể tham gia vào mạng, cho phép người dùng đọc dữ liệu, gửi giao dịch và tham gia vào quá trình xác thực trên mạng.

Đặc điểm chính:

Phi tập trung: không dựa vào 1 cơ quan trung ương hoặc 1 thực thể duy nhất, thay vào đó chúng chạy trên mạng ngang hàng (P2P) nơi mà nhiều node xác minh và lưu trữ giao dịch

Minh bạch: Tất cả giao dịch hiển thị cho tất cả mọi người tham gia vào mạng để đảm bảo dữ liệu được xác minh và kiểm toán bởi bất kỳ ai.

Tính bất biến: Khi dữ liệu hay giao dịch được ghi vào mạng blockchain thì nó sẽ không bị sửa hay xóa cung cấp nơi lưu trữ dữ liệu an toàn và vĩnh viễn.

Trường hợp sử dụng:

1. Giao dịch tiên điện tử: Public Blockchain chủ yếu được sử dụng cho tiền điện tử cho phép chuyển tiền điện tử mà không cần bên trung gian

Ví dụ về 1 số tiền điện tử dựa trên public blockchain: bitcoin, etherium, solana

2. Tài chính phi tập trung(DeFi): Public blockchain cho phép thực hiện 1 loạt các dịch vụ tài chính như cho vay, …. Mà không cần đến ngân hàng truyền thống.
3. NFT: NFTs đại diện cho quyền sở hữu tài sản kỹ thuật số duy nhất trên mạng public blockchain. Etherium là nền tảng dẫn đầu cho việc khai thác và giao dịch NFT
4. Quản lý chuỗi cung ứng: Public Blockchain nâng cao khản năng minh bạch và tính có thể truy vết nguồn gốc trong chuỗi cung ứng, cho phép các bên liên quan biết nguồn gốc và phương thức vận chuyển…
5. Hệ thống voting: Tạo điều kiện cho quá trình voting minh bạch và bảo mật, giảm khản năng giả mạo, tăng lòng tin vào kết quả, người vote hoàn toàn có thể không để lộ thông tin(danh tính đc xác định qua public key)
6. Xác minh danh tính: Cho phép xác minh danh tính mà không cần bên thứ 3

Lợi ích:

1. Phi tập trung: Không có thực thể duy nhất hay 1 liên minh nào kiểm soát mạng, giảm nguy cơ bị kiểm soát hay mua bán dữ liệu. Trao quyền cho người dùng.
2. Minh bạch: Tất cả giao dịch và sự kiện kỹ thuật số được lưu trữ công khai trên blockchain, cho phép mọi người có thể xác minh và kiểm toán chúng. Nâng cao trách nhiệm và sự tin tưởng cho mỗi bên tham gia.
3. Tính bất biến: Khi dữ liệu được ghi vào blockchain thì nó sẽ không thể bị thay đổi hay xóa, đảm bảo dữ liệu được lưu trữ an toàn và vĩnh viễn.
4. Bảo mật: Public Blockchain sử dụng kỹ thuật mã hóa cao để bảo mật dữ liệu làm cho chúng khó bị giả mạo hay hack. Tính phi tập trung nâng cao khản năng chống lại tấn công
5. Khản năng tiếp cận : bất kỳ ai cũng có thể tham gia vào mạng ,đóng góp và phát triển mạng làm cho hệ sinh thái ngày càng phát triển.

Giới hạn và thử thách

1. Khản năng mở rộng: vì số lượng người dùng và giao dịch tăng làm cho tốc độ giao dịch giảm xuống độ trễ tăng lên. Điều này cản trở nó xử lý khối lượng giao dịch lớn 1 cách hiệu quả.
   Ví dụ: Bitcoin giới hạn giao dịch thấp (7 giao dịch / s) và giới hạn kích thước khối 1 MB khiến nó bị hạn chế khi nhu cầu cao, phí giao dịch đắt đỏ (năm 2017 bitcoin bùng nổ với phi giao dịch trung bình lên tới 50$/giao dịch
2. Tiêu tốn năng lượng: Thuật toán đồng bộ Proof of Work cần khản năng tính toán mạnh mẽ dẫn đến khản năng tiêu thụ năng lượng lớn ảnh hưởng môi trường và sự bền vững của hệ thống.
3. Mối quan tâm về quyền riêng tư: Mặc dù minh bạch là 1 thế mạnh nhưng có cũng có rủi ro về quyền riêng tư, Tất cả giao dịch hiển thị trên blockchain có nguy cơ lộ ra những thông tin nhạy cảm
   Ví dụ mọi giao dịch đều có địa chỉ ví của người gửi và người nhận, mặc dù không để lộ thông tin cá nhân nhưng nó vẫn sẽ bị các tổ chức theo dõi hoạt động của ví.
4. Không tuân thủ quy định: dễ dàng truy cập và tính phi tập trung tạo ra thách thức trong tuân thủ quy định pháp lý.
   Ví dụ: Chợ đen Silk Road hoatj động năm 2011 – 2013 chủ yếu dùng bitcoin để thực hiện mua bán ma túy , vũ khí , tài liệu giả mạo…
5. Có khản năng bị tấn công: nếu 1 thực thể chiếm quyền điều kiển trên 50% node thì có thể ảnh hưởng đến mạng, gây bất lợi cho mạng

1.7.2 Private Blockchain

Private blockchain, còn được biết đến là permisstioned blockchain, là 1 sổ cái phân tán trong đó 1 công ty hoặc là 1 tổ chức kiểm soát ai có thể truy cập vào mạng và tham gia vào quá trình đồng thuận.

Đặc điểm chính:

1. Quyền truy cập (permissioned): Private blockchain chỉ có thể truy cập bởi những người tham gia được ủy quyền.
2. Quản trị tập trung: Không giống như public blockchain, private blockchain thường được quản lý bởi 1 tổ chức hoặc công ty quản lý mạng. Từ đó thành lập quy tắc, quản lý quyền thay đổ giao thức, xem thông tin người tham gia….
3. Quyền riêng tư về dữ liệu: cho phép quyền riêng tư về dữ liệu cao vì những thông tin nhạy cảm sẽ không thể truy cập bởi những người dùng không được ủy quyền. Chỉ những thành viên được chấp nhận có thể xem bản ghi hoặc giao dịch làm cho chúng phù hợp với doanh nghiệp xử lý những dữ liệu bảo mật.
4. Tốc độ giao dịch nhanh hơn: với chỉ 1 số ít người tham gia vào trong quá trình đồng thuận, private blockchain có thể xử lý giao dịch nhanh hơn public blockchain. Điều này hiệu quả cho những tổ chức yêu cầu xác minh giao dịch nhanh chóng.
5. Giao thức tùy chinh: tổ chức có thể điều chỉnh các tính năng, cơ chế đồng thuận, giao thức của blockchain để phù hợp hơn với nhu cầu
6. Giảm yêu cầu về năng lượng: rất nhiều private blockchain sử dụng ít năng lượng hơn public blockchain. Giảm sử dụng năng lượng từ đó cũng giảm chi phí.
7. Minh bạch có chọn lọc: Private blockchain duy trìn 1 cấp độ minh bạch gọi là chọn lọc. Người tham gia có thể chia sẻ những thông tin cụ thể với các bên liên quan bên ngoài mà vẫn giữ được những thông tin bảo mật quan trọng bên trong
8. Khản năng tương tác: Private blockchain có thể được thiết kế để tương tác với hệ thống đã tồn tại và mạng dễ dàng hơn public blockchain, tạo điều kiện tích hợp những cơ sở hạ tầng có sẵn và cải thiện hiệu quả tổng thể.

Trường hợp sử dụng:

1. Ứng dụng cho doanh nghiệp: Tính năng đặc thù của private blockchain cung cấp phương thức cho việc lưu trữ hồ sơ và quản lý dữ liệu cho Doanh nghiệp đến doanh nghiệp(B2B), doanh nghiệp đến người tiêu dùng.(B2C).
2. Quản lý chuỗi cung ứng: Bằng cách cung cấp sự minh bạch, trách nhiệm và bảo mật của dữ liệu trong quá trình di chuyển sản phẩm từ nhà sản xuất đến người dùng.
3. Tài chính và ngân hàng
4. Chăm sóc sức khỏe: cho phép chia sẻ hồ sơ bệnh nhân an toàn giữa những nhà chăm sóc sức khỏe được ủy quyền. Điều này nâng cao tính toàn vẹn của dữ liệu, tạo điều kiện chăm sóc bệnh nhân tốt hơn và đảm bảo tuân thủ quy định trong khi vẫn duy trì được sự riêng tư của bệnh nhân.

Lợi ích:

1. Bảo mật được nâng cao: Bởi vì tính bất biến, thông tin không thể bị thay thế do đó chống làm giả. Blockchain sử dụng danh tính để xác nhận thành viên và quyền truy cập, thông thường chỉ cho những tổ chức đã xác nhận tham gia.
2. Cải thiện hiệu suất: Vì số lượng nodes ít hơn nên xác thực khối nhanh hơn. Loại blockchain này có thông lượng và giảm độ trễ.

3. Khản năng mở rộng: Vì mạng không lưu trữ hàng triệu node nên nó có khản năng thực hiện các thay đổi và tính năng từ đó tăng khản năng mở rộng.
4. Thông lượng cao: Vì số lượng người dùng bị giới hạn nên thông lượng cao. Có lợi thế trong tốc độ giao dịch.
5. Tăng cường niềm tin: Vì mạng private blockchain không ẩn danh nên tăng cường niềm tin. Phù hợp cho các ứng dụng nơi doanh nghiệp có thể chia sẻ thông tin trong khi có thể giữ lại được những thông tin quan trọng.
6. Tiết kiệm năng lượng: vì số lượng người dùng bị giới hạn nên khản năng tiêu thụ năng lượng ít, là 1 lựa chọn phù hợp cho doanh nghiệp cho việc tiết kiệm năng lượng và vật liệu.
7. Tiết kiệm chi phí: private blockchain có thể hoạt động trên những cơ sở hạ tầng đã tồn tại, không tốn chi phí cho việc xây dựng 1 cái mới.
8. Tính linh hoạt: Có thể dễ dàng điều chỉ tính năng và thành phần thích hợp cho nhu cầu của doanh nghiệp.
9. Kiểm soát: Private blockchain được cung cấp bởi doanh nghiệp nên nó có thể dễ dàng kiểm soát dữ liệu và mạng. Có thể kiểm soát ai truy cập mạng và đặt ra quy tắc.
10. Khản năng hợp tác: có thể thiết kế tạo sự hợp tác giữa các doanh nghiệp tạo ra khản năng chia sẻ lớn hơn an toàn hơn, rõ ràng hơn.

Thử thách:

1. Thiếu sự tin tưởng: Người dùng bên ngoài phải tin tưởng vào mạng và không có quyền xác minh. Bên được tin tưởng có trách nhiệm thông báo những giao dịch mới cho phần còn lại của mạng.
2. Tính tập trung: Bởi vì sự hiện diện và kiểm soát mạng của doanh nghiệp nên nó có tính tập trung và có khản năng những cá nhân không đáng tin cậy kiểm soát mạng.
3. **Tính toàn vẹn: cần sự** toàn vẹn để có được sự tin cậy từ người dùng.
4. **Kiểm soát:** có thể dễ dàng bị hack do sự quản lý tập trung của mạng và từ đó hacker có thể thao tác dữ liệu.
5. **Giá trị** của mạng thấp do số lượng người tham gia ít.
6. Vấn đề tương tác: private blockchain có vấn đề tương tác với các blockchain khác như public blockchain, do khác biệt về quyền truy cập, giao thức và quy tắc xác thực.
7. Chi phí: private blockchain có thể tiết kiệm chi phí trong 1 số trường hợp. Nhưng họ phải đầu tư cho phần cứng, mềm và duy trì hoạt động của mạng.
8. **Thiếu sự minh bạch:** Vì chỉ có 1 số lượng người tham gia nhất định có quyền truy cập dẫn đến khó khăn cho việc minh bạch cho các bên liên quan.

1.7.3 Hybrid Blockchain

Là 1 loại blockchain kết hợp yếu tố của public và private blockchain. Nó được thiết kế để giảm thiểu nhược điểm của 2 blockchain nhưng mà vẫn tận dụng được lợi ích tối đa của nó.

- Cơ sở dữ liệu Hybrid chứa cả mục công khai và riêng tư
- Tương tự như public blockchain, nơi mà bất kỳ ai cũng có thể tham gia vào mạng, public nodes hoạt động tương tự như những hệ thống đó. Private Node chịu trách nhiệm về việc xác thực và xác minh giao dịch và được quản lý bởi 1 tổ chức hoặc cá nhân.
- Sử dụng private node có thể xử lý giao dịch nhanh hơn với mức độ bảo mật và riêng tư cao hơn. Public node mạng lại tính phi tập trung và minh bạch, làm cho 1 nhóm hoặc 1 cá nhân có thể kiểm soát hoàn toàn mạng.
- Trong Hybrid các thành viên có thể quyết định ai có thể tham gia mạng và giao dịch nào được công bố.

Cách Hybrid blockchain hoạt động?

Hybrid blockchain có 2 giao diện: private blockchain với sổ cái riêng của nó và public blockchain cho việc xác minh dữ liệu giữa những sổ cái của private blockchain.

- Khi người dùng nhận đc quyền truy cập vào hybrid blockchain, người dùng có thể tham gia đầy đủ vào các hoạt động của blockchain
- Người dùng có thể **giao dịch, xem dữ liệu** và **thêm giao dịch mới**, nhưng **không thể chỉnh sửa giao dịch đã xác nhận**. Danh tính người dùng được giữ bí mật khỏi người tham gia khác, danh tính chỉ đc tiết lộ cho bên thực hiện giao dịch

Ví dụ: Một công ty muốn giao dịch với một công ty khác. Giao dịch được xử lý bởi private blockchain (bản ghi kỹ thuật số được tạo ra và xác minh bởi private blockchain). Sau khi giao dịch được xác nhận, private blockchain thông báo cho public blockchain rằng có một giao dịch đã xảy ra. Một khối mới sẽ được tạo trên public blockchain, nhưng chỉ chứa thông tin tối thiểu cần thiết để xác nhận giao dịch mà không tiết lộ chi tiết. Người ngoài có thể thấy rằng một giao dịch đã diễn ra nhưng không thể biết nội dung cụ thể hoặc ai đã thực hiện giao dịch

Lợi ích

1. Bảo mật dữ liệu: Cung cấp bảo mật dữ liệu chặt chẽ và linh hoạt hơn private blockchain. Cho phép người dùng giữ hoạt động riêng tư mà không lo lắng bất kỳ ai khác có thể truy cập chúng.
2. Chi phí giao dịch: chi phí giao dịch thấp hơn vì chỉ có 1 vài node tham gia vào quá trình xác nhận.
3. Hệ sinh thái đóng: duy trì tính ẩn danh nhưng vẫn có thể kết nối với bên ngoài, do đó không thể bị tấn công 51% vì nó là 1 môi trường đóng.
4. Xử lý giao dịch minh bạch: Cung cấp tính minh bạch nhưng không mất đi riêng tư của người dùng. Trong khi private không công khai dữ liệu để bảo vệ giao dịch giữa cá nhân và tổ chức, hybrid cho phép công khai 1 số dữ liệu nhưng mà vẫn có thể giữ lại được thông tin nhạy cảm.

1.7.4 Consortium Blockchain

Là Blockchain được quản lý và chạy bởi 1 nhóm các tổ chức. Là 1 permissioned blockchain nên người dùng phải được ủy quyền trước khi họ tham gia vào mạng.

- Việc duy trì mạng và xác minh giao dịch được chia cho các nhóm hoặc các tổ chức tham gia.
- Thường được các tổ chức cần làm việc với nhau trên 1 nền tảng mà vẫn có thể giữ được dữ liệu và giao dịch của họ.
- Cần bằng giữa phi tập trung và kiểm soát

Cách hoạt động?

Blockchain consortium là một loại blockchain mà trong đó các tổ chức hoặc nhóm chọn lọc điều hành các nút và xác minh giao dịch thay mặt cho mạng lưới. Nó kết hợp đặc điểm của blockchain công khai và riêng tư, cung cấp khả năng mở rộng và bảo mật, nhưng chỉ có một số thành viên đáng tin cậy tham gia, giúp giảm tải cho mạng. Mạng này có thể sử dụng các cơ chế đồng thuận như bỏ phiếu hoặc proof-of-stake (PoS), trong đó các thành viên có cổ phần trong mạng chịu trách nhiệm phê duyệt giao dịch. Blockchain consortium chỉ có thể truy cập bởi các thành viên được chọn và rất phù hợp cho các tổ chức cần hợp tác trên nền tảng chung nhưng vẫn giữ quyền kiểm soát.

Lợi ích:

1. Hiệu quả hơn: vì số lượng node trong mạng bị giới hạn chỉ trong 1 nhóm người tham gia đáng tin cậy nên nó hiệu quả hơn public blockchain. Do đó dẫn đến việc xác minh giao dịch nhanh hơn và rẻ hơn
2. Nâng cao bảo mật: bởi vì 1 nhóm thành viên đáng tin cậy kiểm soát, nên nó khó cho việc thành phần khác nguy hại đến mạng.
3. Chi phí được chia sẻ: ít chi phí hơn trong việc xây dựng và kiểm soát bởi vì chi phí được phân chia cho các thành viên điều hành của mạng.
4. Dữ liệu riêng tư hơn: Bởi vì 1 nhóm các thành viên uy tín có thể truy cập mạng nên nó phù hợp cho việc quản lý và trao đổi dữ liệu quan trọng hơn.
5. Kiểm soát hơn:
6. **Khả n**ăng mở rông: do có ít số lượng người tham gia nên xử lý giao dịch có thể tăng mà không ảnh hưởng đến hiệu suất của mạng.
7. **Tương tác**: có khản năng tương tác với các mạng blockchain khác hoặc hệ thống truyền thống

Thử thách:

1. **Khó** nâng cấp: nâng cấp khó khăn, phải có sự đồng ý người dùng mạng
2. Là 1 loại blockchain mới chưa được hoàn thiện
3. Mất nhiều công sức xây dựng
4. Hạn chế tính phi tập trung: phải dựa vào 1 nhóm thành viên quản lý mạng
5. Cung đột lợi ích giữa các bên quản lý mạng
6. Minh bạch hạn chế
7. Khó quản trị cho lợi ích các bên

1.8 Tính năng của Blockchain

1.8.1 Tính bất biến

Tính bất biến nghĩa là Blockchain là mạng không thể thay đổi được và vĩnh viễn. Công nghệ blockchain hoạt động thông qua 1 tập hợp các Nodes để đạt được 1 sự đồng thuận chung. Khi 1 giao dịch được ghi vào blockchain thì nó không thể bị thay thế hay bị xóa. Nó làm cho blockchain có tính bất biến và sổ cái không thể bị giả mạo từ đó cung cấp bảo mật và tính xác thực cao.

- Mỗi Node trong mạng có 1 bản sao của sổ cái phân tán(chain of blocks). Để thêm 1 giao dịch, mỗi node kiểm tra tính xác thực của giao dịch và nếu phần lớn nodes nghĩ rằng giao dịch đó là hợp lệ thì nó được thêm vào mạng, điều này có nghĩa rằng không có sự chấp nhận của phần lớn node thì không ai có thể thêm bất kỳ khối giao dịch nào vào sổ cái.
- Bất kỳ bản ghi hợp lệ nào cũng không thể chỉnh sửa, thay đổi hay xóa nó khi nó đã được thêm vào blockchain.

1.8.2 Phân tán

Tất cả mọi người tham gia mạng có 1 bản sao của sổ cái để minh bạch hoàn toàn. Một sổ cái công cộng sẽ cung cấp đầy đủ thông tin về tất cả người tham gia trên mạng và giao dịch.

Sổ cái phân tán là 1 trong những tính năng quan trọng của blockchain bởi vì

- Trong sổ cái phân tán theo dõi sự thay đổi của sổ cái rất dễ dàng vì sự lan truyền thay đổi thực sự nhanh trong sổ cái phân tán.
- Mỗi node trong mạng blockchain phải duy trì 1 bản sao của sổ cái và tham gia vào quá trình xác thực.

- Nếu 1 người dùng muốn tạo ra 1 khối mới thì các người tham gia còn lại phải xác minh các giao dịch trong khối (block) đó. Để cho mỗi khối được thêm vào mạng blockchain thì nó phải được chấp nhận bởi hầu hết phần lớn các node trong mạng.

1.8.3 Phi tập Trung

Công nghệ blockchain là 1 hệ thống phi tập trung, là không có sự tồn tại của cơ quan trung tâm kiểm soát mạng. Thay vào đó thì mạng được cấu thành từ 1 tập hơn số lượng lớn node hoạt động và làm việc với nhau để xác thực và xác minh giao dịch. Mỗi node trong mạng blockchain sẽ có bản sao của sổ cái.

Các Thuộc tính của Phi tập trung tạo lợi thế cho mạng blockchain:

- Vì không có sự phụ thuộc vào tính toán của con người nên nó được tổ chức đầy đủ và khản năng chịu lỗi cao.
- Mạng blockchain ít bị lỗi do tính phân tán của mạng.
- Không có bên thứ 3 liên quan do đó giảm chi phí và không rủi ro trong hệ thống.
- Dễ dàng theo dõi sự thay đổi.
- Người dùng tự kiểm soát các thuộc tính và tự quản lý và duy thì tài sản của họ.

1.8.4 Bảo mật

Tất cả các bản ghi trong blockchain được mã hóa. Sử dụng mã hóa để thêm 1 lớp an toàn cho toàn bộ quá trình trong mạng(vì không có bên thứ 3 không có nghĩa là không có ai có thể them sử xóa dữ liệu trên mạng). Mỗi thông tin được băm mật mã có nghĩa là mỗi mảnh thông tin dữ liệu có 1 định danh duy nhất trên mạng. Tất cả khối đều chứa 1 mã băm duy nhất của nó và phụ thuộc vào mã băm của khối trước đó (trừ khối đầu tiên – genesis block). Vì thuộc tính này nên các khối được kết nối logic với nhau và bất kỳ sự thay dổi nào sẽ ảnh hưởng đến băm của block phụ thuộc vào nó, do đó thay đổi là không thể.

1.8.5 Đồng thuận

Mỗi blockchain đều có cơ chế đồng thuận để hỗ trợ mạng trong việc đưa ra quyết định nhanh chóng và không thiên vị. Đồng thuận là 1 thuật toán cho nhóm các node trên mạng đi đến 1 quyết định chung 1 cách nhanh chóng từ đó cải thiện hiệu suất của hệ thống. Các node không cần tin tưởng lẫn nhau nhưng họ có thể tin tưởng thuật toán. Mỗi mạng blockchain phải có 1 thuật toán đồng thuận nếu không thì nó không có giá trị.

1.8.6 Sự nhất trí

Tất cả mọi người tham gia mạng phải xác thực cho bản ghi trước khi được thêm vào blockchain. Khi khối mới muốn được thêm vào mạng phải có sự đồng ý của hầu hết mọi thành viên trong mạng, mọi sự thay đổi đều cần phải có sự đồng thuận, từ đó việc 1 node không thể dễ dàng thêm, sửa xóa thông tin trên mạng.

1.8.7 Thanh toán nhanh hơn

Hệ thống ngân hàng thường mất nhiều thời gian xử lý giao dịch, dễ dàng gian lận và dễ bị hack. Ngược lại blockchain thanh toán nhanh hơn, minh bạch và bảo mật hơn.

1.8.8 Tính minh bạch và Hợp đồng thông minh

Blockchain có sổ cái phân tán, bất kỳ ai cũng có thể truy cập và xem xét các giao dịch hoặc các hoạt động kỹ thuật số tạo nên tính minh bạch cao, chống giả mạo.

Hợp đồng thông minh là hợp đồng được nhúng vào mã code, cho phép tạo ra và thực thi khi các điều kiện nhất định được thỏa mãn.

1.9 Nhược điểm của blockchain

Khả năng mở rộng: Đây là một trong những hạn chế lớn nhất của blockchain, vì nó không thể mở rộng do kích thước khối cố định để lưu trữ thông tin. Kích thước khối chỉ 1 MB, nên mỗi khối chỉ có thể chứa một số ít giao dịch.

Chưa trưởng thành: Blockchain là một công nghệ còn khá mới, vì vậy nhiều người chưa có đủ niềm tin vào nó và chưa sẵn sàng đầu tư. Dù một số ứng dụng blockchain đang phát triển mạnh trong nhiều ngành công nghiệp, nhưng vẫn cần thêm thời gian để đạt được sự công nhận rộng rãi hơn.

Tiêu tốn năng lượng: Quá trình xác minh giao dịch tiêu thụ rất nhiều năng lượng. Theo một cuộc khảo sát, đến năm 2018, công nghệ blockchain đã tiêu thụ khoảng 0,3% lượng điện trên toàn cầu chỉ để xác minh giao dịch.

Tốn thời gian: Để thêm một khối mới vào chuỗi, các thợ đào cần tính toán giá trị nonce nhiều lần, khiến quá trình này tốn nhiều thời gian. Blockchain cần được cải thiện tốc độ để có thể ứng dụng rộng rãi trong công nghiệp.

Thủ tục pháp lý: Ở một số quốc gia, ứng dụng của blockchain bị cấm, chẳng hạn như tiền mã hóa (cryptocurrency), do những vấn đề về môi trường hoặc chính sách quản lý. Vì vậy, blockchain chưa được khuyến khích sử dụng trong lĩnh vực thương mại.

Lưu trữ dữ liệu: Cơ sở dữ liệu blockchain được lưu trên tất cả các nút trong mạng, dẫn đến vấn đề về dung lượng lưu trữ. Khi số lượng giao dịch tăng lên, yêu cầu lưu trữ cũng tăng theo.

Quy định pháp lý: Blockchain gặp nhiều thách thức từ các tổ chức tài chính. Để công nghệ này được áp dụng rộng rãi hơn, cần có những điều chỉnh phù hợp với quy định và chính sách hiện hành.

2. Mật mã và hàm băm

Trong blockchain có 2 khái niệm chính là mật mã và hàm băm.

- Mật mã được sử dụng để mã hóa tin nhắn và giao dịch trong mạng P2P. Từ đó đảm bảo an ninh cho người tham gia, giao dịch.
- Băm được sử dụng để bảo mật thông tin khối và các khối liên kết trong mạng blockchain.

2.1 Mật mã trong Blockchain

Mật mã là phương pháp bảo mật dữ liệu khỏi truy cập trái phép. Trong Blockchain, mật mã được sử dụng để bảo mật các giao dịch giữa 2 nút.

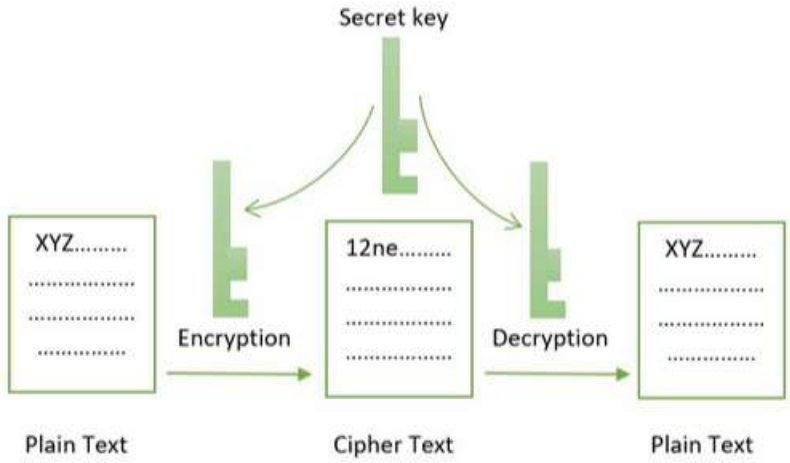
Vai trò của mật mã trong Blockchain

Blockchain được phát triển với nhiều khái niệm mật mã khác nhau. Sự phát triển của công nghệ mật mã đã thúc đẩy những hạn chế cho sự phát triển hơn nữa của blockchain.

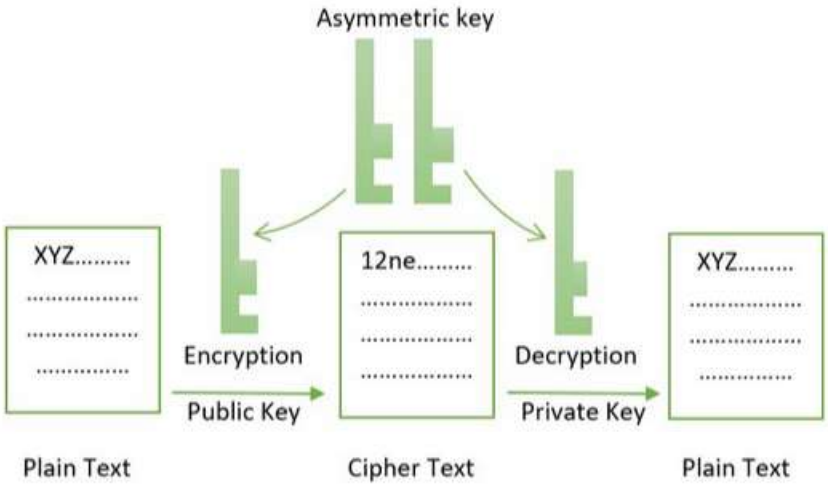
- Trong Blockchain, mật mã chủ yếu được sử dụng để bảo vệ quyền riêng tư của người dùng thông tin và đảm bảo tính nhất quán của giao dịch và dữ liệu.
- Các công nghệ cốt lõi của mật mã bao gồm:
    - Mã hóa đối xứng
    - Mã hóa bất đối xứng: sử dụng chữ ký số cho mục đích xác minh, mọi giao dịch được ghi vào khối đều được người gửi bằng chữ ký số và đảm bảo dữ liệu không bị hỏng, duy trì tính toàn vẹn và bảo mật.

Các lại mật mã

1. Mã hóa khóa đối xứng



2. Mã hóa khóa bất đối xứng



Ví

Là 1 phần mềm đặc biệt hoặc thiết bị phần cứng đặc biệt để lưu trữ thông tin giao dịch và thông tin cá nhân của người dùng. Nó không chứa tiền tệ thực tế. Ví được sử dụng để lưu trữ khóa riêng và lưu trữ số dư giao dịch. Nó cũng là công cụ giao tiếp nhằm thực hiện giao dịch với người khác. (Dữ liệu hoặc tiền tệ được lưu trữ trong các khối của blockchain).

Chữ ký số (Digital Signature)

Là bằng chứng mà người dùng cung cấp cho người nhận và nút khác trong mạng để chứng minh rằng đó là 1 nút hợp pháp trong mạng để thực hiện giao dịch.

Ví dụ: Khi thực hiện giao dịch hoặc sự kiện kỹ thuật số trong mạng, trước tiên người dùng phải tạo 1 chữ ký số duy nhất bằng cách kết hợp dữ liệu giao dịch với khóa riêng của người dùng bằng 1 thuật toán đặc biệt. Quá trình này đảm bảo tính xác thực của nút và tính toàn vẹn dữ liệu.

Lợi ích

- Mã hóa: đảm bảo giao dịch trên mạng khỏi việc tiết lộ và truy cập thông tin trái phép.
- Tính bất biến: giúp các khối liên kết an toàn với các khối khác, đồng thời đảm bảo độ tin cập của dữ liệu được lưu trữ trong blockchain và không có kẻ tấn công nào có thể lấy được chữ ký hợp lệ cho các truy vấn.
- Bảo mật: Ghi lại giao dịch dễ dàng hơn bằng các mã hóa dữ liệu và truy cập dữ liệu bằng khóa public và private.
- Khản năng mở rộng: giao dịch kh thể đảo ngược cho phép ghi các giao dịch không giới hạn 1 cách an toàn.
- Ngăn chặn tin tặc: chữ ký số ngăn chặn tin tặc thay đổi và nếu thay đổi chữ ký số sẽ không hợp lệ.

Nhược điểm:

- Thông tin khó truy cập: thông tin được mã hóa mạnh và được ký số có thể khó truy cập ngay cả đối với người dùng hợp pháp.
- Không có biện pháp bảo vệ chống lại các lỗ hổng: mật mã không bảo vệ chống lại các lỗ hổng và mỗi đe dọa phát sinh từ thiết kế kém của các giao thức, quy trình và hệ thống. Cần khắc phục bằng thiết kế phù hợp cơ sở hạ tầng phòng thủ.
- Độ trễ lớn

2.2 Hàm băm

Là 1 hàm toán học lấy một chuỗi đầu vào có độ dài bất kỳ và chuyển đổi nó thành 1 chuỗi đầu ra có độ dài cố định. Đầu ra có độ dài cố định được gọi là giá trị băm (hash value).

Sử dụng hàm băm trong Blockchain

Cây Merkle: Phương pháp này sử dụng hàm băm để đảm bảo không thể tìm thấy 2 cây Merkle có cùng giá trị băm gốc. Phương pháp này giúp bảo vệ tính toàn vẹn của tiêu đề khối bằng các lưu trữ giá trị băm gốc trong tiêu đề khối và do đó bảo vệ tính toàn vẹn của các giao dịch.

Chuỗi khối: mỗi tiêu đề khối trong blockchain chứa hàm băm của tiêu đề khối trước đó. Điều này đảm bảo rằng không thể thay đổi 1 khối duy nhất trong blockchain mà không bị phát hiện. Vì việc sửa đổi 1 khối đòi hỏi phải tạo ra các phiên bản mới của mọi khối tiếp theo, do đó làm tăng độ khó.

3. Thuật toán đồng thuận (Consensus Algorithm) trong Blockchain

Bởi vì không có cơ quan trung ương nào xác thực và xác minh các giao dịch nhưng mỗi giao dịch trong blockchain vẫn được đảm bảo về bảo mật và xác minh rõ ràng. Điều này là nhờ thuật toán đồng thuận (Consensus Algorithm) phần cốt lõi của bất kỳ mạng Blockchain nào.

Một thuật toán đồng thuận là 1 tập hợp các thủ tục mà thông qua đó các Node của mạng Blockchain (phần lớn các thuật toán đồng thuận yêu cầu trên 50% hoặc 2/3 các Node để đảm bảo bảo mật và ổn định) đi đến đồng ý chung về trạng thái hiện tại của chuỗi block (chain of blockchain) và sổ cái phân tán (distributed ledger) , thông qua đó đạt được tính tin cậy trong việc giao tiếp trong mạng Blockchain giữa những Node không xác định đảm bảo tính riêng tư và bảo mật cho người dùng.

Mục tiêu của thuật toán đồng thuận: tạo ra sự hợp tác và các quyền giống nhau giữa các nút trong quán trình đồng thuận để đi đến sự đồng ý chung cho toàn mạng

Hãy thảo luận về 1 số thuật toán đồng thuận phổ biến**:**

- Proof of Work (PoW): Thuật toán dựa trên 1 thợ đào (Miner) tính toán nhanh nhất và cho ra kết quả hợp lệ sẽ thực hiện việc tạo khối tiếp theo. Ý tưởng của thuật toán là giải quyết 1 bài toán phức tạp cần nhiều năng lượng tính toán do đó thợ đào (Miner) thực hiện nhanh nhất, chính xác sẽ được chọn khối block của họ vào chuỗi khối (chain of blocks). Ví dụ Bitcoin sử dụng Proof of Work nhằm thực hiện cơ chế đồng thuận của mình.
- Proof of Stake
- Proof of Burn
- Delegated Proof of Stake
- Practical Byzantine Fault Tolerance (PBT)

3.1 Proof of Work Trong blockchain

Thuật toán dùng để xác minh giao dịch và tạo 1 khối mới trong Blockchain. Nguyên tắc của thuật toán là tìm kiếm giải pháp khó nhưng dễ dàng xác minh.

Mục đích của thuật toán là nhận được sử đồng thuận của tất cả các nút trong 1 môi trường mức độ tin tưởng lẫn nhau thấp.

- Tất cả các giao dịch trong khối mới sẽ được xác minh và mỗi khối mới sẽ được thêm vào Blockchain
- Các Thợ đào (Miners – những chiếc máy tính mạnh mẽ) giải 1 vấn đề toán học phức tạp sẽ thêm khối vào mạng

3.1.1 Cách PoW hoạt động

Khai thác (mining): quá trình khai thác liên quan đến việc giải quyết 1 vấn đề toán học phức tạp để tạo ra 1 khối mới (new block). Các node trong mạng blockchain tham gia vào quá trình đào là thợ đào (miner). Lợi ích của việc khai thác là các thợ đào sẽ nhận được 1 khoản phí như là 1 phần thưởng.

Vấn đề về tiêu tốn thời gian và năng lượng

- Quá trình xác minh giao dịch, tổ chức nó theo thứ tự thời gian và thông báo khối mới được đào cho toàn bộ mạng không mất nhiều thời gian và năng lượng
- Phần tiêu tốn năng lượng là giải quyết 1 vấn đề toán học khó tìm 1 hash hợp lệ để kết nối khối mới với khối cuối cùng của blockchain. Sau khi thợ đào tìm được giải pháp thì phải quảng bá nó đến toàn bộ mạng cùng lúc. Do đó theo thời gian thì các bài toán sẽ càng phức tạp hơn và khó giải quyết hơn gây ra độ trễ trên mạng và phí giao dịch cao.

Phần thưởng khai thác:

- Trong bitcoin, khai thác 1 khối trong mạng mang lại cho thợ đào chiến thắng 1 số lượng coin xác định và số lượng bitcoin chiến thắng giảm theo chu kỳ 4 năm
- Với số lượng thợ đào tăng thời gian khai thác giảm đi và duy trì 1 khai thác 1 khối trong vòng 10 phút để đảm bảo sự ổn định của coin (Lưu ý chỉ tồn tại tối đa 21 triệu bitcoin).

3.1.2 Proof of Work trong Bitcoin 

Vấn đề toán học trong việc khai thác block có thể được trừu tượng hóa như sau: “Với dữ liệu A đã cho tìm x sao cho băm của x khi thêm vào A là 1 số nhỏ hơn B”.

Những thợ đào gom những giao dịch vào trong 1 khối và cố gắng khai thác nó. Để khai thác cần giải quyết 1 vấn đề toán học phức tạp và thợ đào phải chứng minh rằng đã tìm ra được giải pháp ho vấn đề và khối được đào phải hợp lệ.

Câu trả lời cho bài toán phải là 1 số nhỏ hơn target hash(1 giá trị do mạng bitcoin quy định và có thể thay đổi theo thời gian dựa vào độ khó khai thác).

Thợ đào tiếp tục kiểm tra những giá trị duy nhất khác nhau (được biết đến là nonce) cho đến khi tìm được 1 giá trị hợp lệ

Thợ đào đã giải quyết được vấn đề nhận được tiền thưởng và thêm 1 khối vào blockchain bằng cách quảng bá khối đã khai thác đến mạng blockchain.

Thuật toán mật mã phổ biến trong PoW: SHA-256 (là 1 phần của bitcoin), Scrypt, SHA-3, …

Ví dụ về việc khai thác khối trong bitcoin

- Xem xét khối (block) ở hình bên dưới với phần tiêu đề bao gồm băm của khối trước đó và 1 số ngẫu nhiên thay đổi để thợ đào (miners) thử tạo ra băm của khối (tiêu đề bao gồm nhiều trường nữa như merkel tree, phiên bản.. nhưng không đề cập trong hình ảnh này, chỉ tập trung vào phần quan trọng).

- Các thợ đào sẽ thử các giá trị nonce khác nhau để tính toán ra new hash (là kết quả băm của khối bao gồm tiêu đề và các transaction) thông qua SHA-256 và kết quả nhỏ hơn hoặc bằng target hash thì được xem là hợp lệ.
- Sau khi block hợp lệ miner nhận được phần thưởng và nó sẽ được quảng bá lên mạng bitcoin đến các node để các thợ đào khác dùng nó cho giá trị băm của khối trước đó.

3.1.3 Những vấn đề của PoW

Tấn công 51%: nếu như có 1 thực thể kiểm soát hơn 50% nodes mạng thì thực thể đó có thể giành quyền kiểm soát mạng và làm hỏng blockchain.

Tốn thời gian:các thợ đào cần phải thử nhiều giá trị nonce khác nhau để giải được bài toán ➔ tốn thời gian

Tốn tài nguyên và ảnh hưởng đến môi trường: Thợ đào phải tiêu tốn số lượng lớn năng lượng tính toán để giải quyết bài toán khó và gây ảnh hưởng đến môi trường.

Có độ trễ lớn trong giao dịch: việc xác minh giao dịch mất nhiều thời gian (10 -60 phút) vì nó cần thời gian để thợ đào khai thác giao dịch và đưa vào blockchain.

3.2 Proof of Stake trong blockchain

Là 1 thuật toán mục tiêu là đạt được đồng thuận phân tán trong blockchain

Những blockchains sử dụng PoS là Ethereum, Peercoin, Nxt.

3.2.1 Proof of Stake là gì?

Một cổ phần (Stake) là giá trị và tiền mà chúng ta đặt cược vào 1 kết quả nhất định.

Những nodes trên mạng Blockchain đặt cược 1 số lượng tiền điện tử của mình để tham gia vào quá trình xác thực 1 khối mới và nhận được phí từ đó. Thuật toán sẽ lựa chọn 1 Node (là 1 trong số các node được tham gia vào quá trình xác thực) để xác thực khối mới.

Các tiêu chí mà thuật toán sử dụng để lựa chọn node xác thực nhằm tạo ra sự công bằng

- Số lượng tiền điện tử (coin) mà người đó đặt
- Lựa chọn dựa trên tuổi đồng coin (coin age based selection), nếu các node đặt cược lâu hơn thì sẽ có cơ hội trở thành node xác thực hơn, giống như đợi càng lâu cơ hội sẽ cao hơn vậy.
- Lựa chọn khối ngẫu nhiên (Random Block Selection), nút nào là sự kết hợp tốt nhất giữa 2 yếu tố là node có hash thực hiện trước đó thấp nhất và đặt cược cao nhất.

3.2.2 Quá trình thực thi phổ biến dựa trên PoS

1. Người dùng tạo ra giao dịch. Thuật toán PoS (Proof of Stake) đặt tất cả giao dịch vào memory pool

2. Tất cả các node cạnh tranh với nhau để trở thành node xác thực cho khối tiếp theo bằng cách đặt cược (cổ phần – stake). Cổ phần này sẽ được kết hợp với các yếu tố khác như 'coin-age' và 'random block selection' để chọn ra node xác thực.

3. Node xác thực sẽ xác minh tất cả giao dịch và tạo ra block. Cổ phần mà node đặt cược vẫn được giữ lại và phần thưởng chưa được cấp. Trừ khi phần lớn khối trên mạng blockchain xem nó là hợp lệ.

4. Nếu khối mới được chấp nhận bởi các nodes thì node xác thực sẽ nhận lại cổ phần đã đặt cược và phần thưởng của nó. Nếu thuật toán dùng cơ chế 'coin-age' để lựu chọn node xác thực thì coin-age của node xác thực hiện tại trở về 0, điều này đảm bảo cho node có mức ưu tiên thấp cho việc chọn node xác thực cho giao dịch tiếp theo để tạo nên sự công bằng trong mạng blockchain.

5. Nếu khối mới không được xác minh bởi nút khác trên mạng blockchain thì node xác thực sẽ **mất cổ phần (stake)** và bị đánh dấu là 'tệ' bởi thuật toán và quay lại thực hiện bước 1 để tạo khối mới.

3.3.3 Tính năng

Không thể tấn công thông qua 'Tấn công 51%'. Trước tiên hãy phân biệt giữa 'Tấn công 51% của Poof of work' và 'Tấn công 51% của Proof of Stake' ở PoW kẻ tấn công cố gắng sở hữu 51% Node trong mạng hoặc lớn hơn gây ảnh hưởng đến mạng nhưng ở PoS kẻ tấn công sẽ phải sở hữu 51% tổng số tiền điện tử của nó(coins) hoặc lớn hơn để gây ảnh hưởng đến mạng điều nay là không khả thi vì 1 số tiền điện tử (crytocurrency) không có giới hạn số lượng coin như Bitcoin mà nếu có thì thực hiện tấn công còn gây tốn kém và không có nhiều lợi ích và nếu mà còn xác thực sai giao dịch sẽ mất cổ phần (stake) và không nhận được phần thưởng.

Phí giao dịch là phần thưởng cho thợ đào, Mỗi giao dịch sẽ tính 1 số lượng phí nhất định, chi phí này sẽ tích lũy và đưa cho thực thể khai thác khối mới

3.2.4 Ưu điểm của PoS

Tiết kiệm năng lượng, vì tất cả các node (miners) không tranh nhau tính toán để đưa khối mới vào chuỗi tạo nên việc tiết kiệm năng lượng

Bảo mật: không thể tấn công 51% để kiểm soát mạng

Tính phi tập trung: ở trong các hệ thống PoW vì cần đến tính toán mạnh mẽ nên 1 nhóm các thợ đào hoặc 1 tổ chức hợp lại với nhau để thực hiện việc khai thác dẫn đến tính phi tập trung. PoS thì ngược lại số tiền thưởng sẽ tỉ lệ thuận với số cổ phần đặt ra tạo ra tính phi tập trung.

3.2.5 Những điểm yếu trong PoS

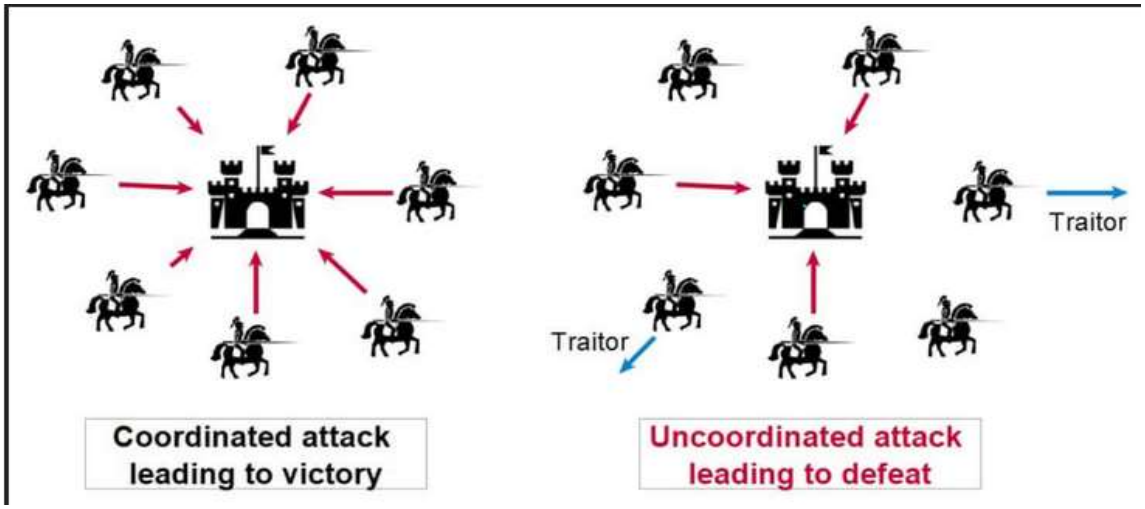
Những Node xác thực có số lượng cổ phần lớn, nếu như 1 nhóm các ứng viên cho node xác thực tập hợp lại với nhau và sở hữu 1 phần lớn coin thì sẽ có cơ hội trở thành node xác thực lớn và vì tỉ lệ thuận giữa coin đặt cược và phần thưởng nên node xác thực sẽ nhận được 1 khoản phí lớn dẫn đến sự tập trung hơn trên mạng theo thời gian.

Là 1 công nghệ mới cần nghiên cứu và phát triển thêm và làm cho nó khả thi trên mạng với nhữnggiao dịch tiền tệ thực tế.

Vấn đề "Nothing at Stake" xảy ra khi các validator trong hệ thống **Proof of Stake** có thể xác thực trên nhiều blockchain phân tách mà không gặp phải thiệt hại gì, dẫn đến việc mạng lưới không thể đạt được sự đồng thuận và trở nên không ổn định.

3.3 Vấn đề của các tướng Byzantine trong blockchain

3.3.1 Vấn đề của các tướng Byzantine là gì?



Năm 1982, vấn đề của các tướng Byzantine được giới thiệu bởi Leslie Lamport, Robert Shostak và Marshall Pease. Nó có 1 kết quả không thể xảy ra có nghĩa rằng giải pháp cho vấn đề này không được tìm thấy và cho chúng ta hiểu được tầm quan trong của **Blockchain. Vấn đề mô tả về việc các bên phi tập trung khó để đưa ra được sự đồng thuận chung mà không có bất kỳ bên trung gian đáng tin cậy nào.**

- Quân đội Byzantine được chia thành nhiều nhóm nhỏ và mỗi nhóm có 1 tướng quan dẫn đầu
- Các tướng quân trao đổi với nhau qua người đưa tin và lên 1 kế hoạch hành động chung để hợp tác tấn công từ mọi hướng để đạt được thành công.
- Nếu có kẻ phản bội hoặc người đưa tin bị chặn bắt và thay đổi tin nhắn.
- Để đạt được kết quả sử dụng chỉ huy trung thành để đi đến sự đồng thuận mà không có kẻ mạo danh làm giả kế hoạch của họ.

3.3.2 Tiền và vấn đề của các tướng quân Byzantine

Sự ra đời của hệ thông tập trung nơi các thực thể được tin cậy quản lý tiền nhưng lại kiểm soát dữ liệu. Không giải quyết được vấn đề của các tướng quân Byzantine cái mà yêu cầu sự tin tưởng.

Bitcoin tạo ra sự phi tập trung, blockchain đảm bảo tính xác minh chống giả mạo không cần bên thứ 3.

3.3.3 Cách Bitcoin giải quyết vấn đề ?

Vấn đề của các tướng liên quan đến sự trung thành phải đạt được sự đồng thuận dù có kẻ phản bội. Bitcoin giải quyết nó bằng blockchain, 1 số cái phân tán công khai ghi lại mọi giao dịch, giao dịch không cần bên thứ 3, dựa vào PoW block thêm vào được đảm bảo chống giả mạo tạo ra tính nhất quán và chính xác, tính bất biến tạo ra bằng chứng có thể chứng minh, tất cả các node đồng thuận về trạng thái của blockchain khi có node nào đó phát tán thông tin sai lệch các node sẽ từ chối tạo ra sự tin tưởng mà không cần bên thứ 3.

4 Kiến trúc Blockchain

Lưu trữ và quản lý dữ liệu

1. Tiêu đề (Header): Nó được sử dụng để xác định 1 khối cụ thể trong chuỗi. Một tiêu đề khối được băm bởi thợ đào (miner) bằng cách thay đổi giá trị nonce
2. Giá trị băm của khối trước đó (previous block hash): nó được sử dụng để kết nối khối thứ n + 1 với khối thứ n bằng giá trị băm (hash). Hay chính xác hơn là nó tham chiếu đến giá trị băm của khối trước đó trong chuỗi.
3. Dấu thời gian(timestamp): Ghi lại thời điểm một khối được tạo, giúp xác thực dữ liệu và sắp xếp thứ tự giao dịch.
4. Nonce: Là số chỉ được sử dụng một lần. Thợ đào liên tục thay đổi nonce để tạo ra giá trị băm mới và so sánh với giá trị băm mục tiêu (target hash). Nếu giá trị băm nhỏ hơn hoặc bằng mục tiêu, khối được xác nhận.
5. Merkle tree: Là một cấu trúc dữ liệu lưu trữ tất cả giao dịch trong một khối bằng cách tạo dấu vân tay kỹ thuật số. Nó giúp xác minh một giao dịch có nằm trong khối hay không.