BLOCKCHAIN CƠ BẢN

LỐI VÀO CHO NGƯỜI MỚI BẮT
ĐẦU TÌM HIỂU VỀ BLOCKCHAIN

NHÓM TÁC GIẢ :

1. **TS. Đỗ Ngọc Minh**
2. **TS. Nguyễn Đức Dư**
3. **TS. Hoàng Văn Thông**
4. **ThS Trịnh Văn Chung**
5. **ThS Nguyễn Văn Hiệu**

BIÊN TẬP :

ThS. Nguyễn Anh Tiến

MỤC LỤC

MỞ ĐẦU 1
CHƯƠNG 1: CÁC KIẾN THỨC CƠ SỞ 4
1.1. MÃ HÓA 4
1.1.1. Lịch sử mã hóa 4
1.1.2. Khái niệm mã hóa và giải mã 9
1.1.3. Mã hóa cổ điển 10
1.1.4. Mã hóa đối xứng 13
1.1.5. Mã hóa bất đối xứng 16
1.2. HÀM BĂM 18
1.2.1. Khái niệm và vai trò của hàm băm trong bảo mật 18
1.2.2. Các hàm băm phổ biến 21
1.2.3. Một số ứng dụng của hàm băm 25
1.3. CHỮ KÝ SỐ 28
1.3.1. Khái niệm chữ ký số 28
1.3.2. Vai trò của chữ ký số 28
1.3.3. Các thành phần của chữ ký số 28
1.3.4. Nguyên lý hoạt động của chữ ký số 30
1.3.5. Ứng dụng chữ ký số 31
1.3.6. Lợi ích và hạn chế của chữ ký số 33
1.4. HỆ PHI TẬP TRUNG 35
1.4.1. Khái niệm hệ phi tập trung 35
1.4.2. Đặc điểm của hệ phi tập trung 35
1.4.3. Cấu trúc và mô hình của hệ phi tập trung 35
1.4.4. Ưu điểm của cấu trúc phi tập trung và hệ phi tập trung 37
1.4.5. Ứng dụng của hệ phi tập trung 38
1.5. HỆ PHÂN TÁN 40
1.5.1. Khái niệm hệ phân tán 40
1.5.2. Đặc điểm của hệ phân tán 41
1.5.3. Các mô hình hệ phân tán 41

1.5.4. Tính chất của hệ phân tán 43
1.5.5. Quản lý đồng bộ và tính toàn vẹn 44
1.5.6. Ứng dụng của hệ phân tán 46
1.6 MẠNG NGANG HÀNG 48
1.6.1. Khái niệm mạng ngang hàng 48
1.6.2. Đặc điểm của mạng ngang hàng 49
1.6.3. Các loại mạng ngang hàng 49
1.6.4. Cơ chế hoạt động của mạng P2P 49
1.6.5. Công nghệ và giao thức trong mạng ngang hàng 50
1.6.6. Ứng dụng của mạng ngang hàng 50
CHƯƠNG 2: CÁC KHÁI NIỆM CỦA BLOCKCHAIN 53
2.1. KHÁI NIỆM 53
2.1.1. Khái niệm 53
2.1.2. Một số đặc điểm quan trọng của blockchain 54
2.1.3. Các thành phần cơ bản của blockchain 55
2.1.4. Quy trình hoạt động của blockchain 56
2.2. LỊCH SỬ RA ĐỜI CỦA BLOCKCHAIN 57
2.2.1. Sơ lược về lịch sử công nghệ blockchain 57
2.2.2. Quá trình hình thành và phát triển của công nghệ blockchain 59
2.3. CÁC LOẠI MẠNG BLOCKCHAIN 61
2.3.1. Blockchain công khai 62
2.3.2. Blockchain riêng tư 62
2.3.3. Blockchain lai 63
2.3.4. Blockchain liên kết 64
2.4. TIỀN MÃ HÓA VÀ TOKENOMICS 65
2.4.1. Tiền mã hóa 65
2.4.2. Tokenomics 69
2.5. NFT 76
2.5.1. Khái niệm 76
2.5.2. Đặc điểm 77
2.5.3. Ứng dụng 78
2.5.4. Thách thức và cơ hội 80

2.6. VÍ VÀ ĐỊA CHỈ....85
2.6.1 Ví (wallet)....85
2.6.2. Địa chỉ....94
2.7. SỔ CÁI (LEDGER)....100
2.7.1. Khái niệm....100
2.7.2. Đặc điểm của Sổ Cái trong Blockchain?....100
2.7.3. Nguyên lý hoạt động của Sổ Cái trong Blockchain?....101
2.8. CÁC LĨNH VỰC ỨNG DỤNG BLOCKCHAIN....101
2.8.1. Tài chính và ngân hàng....101
2.8.2. Quản lý chuỗi cung ứng (Supply Chain Management)....102
2.8.3. Quản trị và hợp đồng thông minh....103
2.8.4. Sở hữu và sưu tầm tài sản Kỹ thuật số (NFT)....104
2.8.5. Ứng dụng trong Y tế....104
2.8.6. Bầu cử và Quản lý chính phủ....106
2.8.7. Bảo mật và quyền sở hữu dữ liệu....107
CHƯƠNG 3: MỘT SỐ NỀN TẢNG BLOCKCHAIN....112
3.1. Thế hệ đầu tiên: Bitcoin – Blockchain đầu tiên....112
3.1.1. Giới thiệu về Bitcoin....112
3.1.2. Nguyên lý hoạt động và cơ chế giao dịch của Bitcoin....114
3.1.3. Khóa, địa chỉ và ví....119
3.1.4. Mạng lưới Bitcoin....123
3.1.5. Ý nghĩa và tác động của Bitcoin....126
3.2. Ethereum: Hợp đồng thông minh và DApps....127
3.2.1 Ethereum....127
3.2.2. Hợp đồng thông minh (Smart Contract)....132
3.2.3. Các ứng dụng phi tập trung (DApps)....137
3.3. Thế hệ thứ ba: Cardano – Xây dựng từ nghiên cứu học thuật....140
3.3.1. Giới thiệu về Cardano....140
3.3.2. Nguyên lý hoạt động và cơ chế giao dịch của Cardano....144
3.3.3 Mô hình EUTxO của Blockchain Cardano....150
3.3.4. Khóa, địa chỉ của Blockchain cardano....153
3.3.5. Hợp đồng thông minh trên Cardano....158

3.3.6 Quản trị On-Chain trên Cardano 162
3.4 Tóm tắt chương và So sánh các thế hệ Blockchain 164
CHƯƠNG 4: CÁC THUẬT TOÁN ĐỒNG THUẬN BLOCKCHAIN 169
4.1. THUẬT TOÁN ĐỒNG THUẬN 169
4.1.1. Khái niệm 169
4.1.2. Cơ chế hoạt động của thuật toán đồng thuận 169
4.1.3. Các yêu cầu của một thuật toán đồng thuận Blockchain 170
4.2. HỆ THỐNG CHỊU LỖI BYZANTINE (BFT) 171
4.3. THUẬT TOÁN BẰNG CHỨNG CÔNG VIỆC 173
4.3.1. Lịch sử phát triển của thuật toán bằng chứng công việc 173
4.3.2. Cơ chế hoạt động của PoW 174
4.3.3. Cơ chế đồng thuận trong mạng Bitcoin 175
4.3.4. Ưu nhược điểm của thuật toán đồng thuận PoW 183
4.4. THUẬT TOÁN BẰNG CHỨNG CỔ PHẦN (POS) 184
4.4.1. Lịch sử phát triển của thuật toán bằng chứng cổ phần 185
4.4.2. Cơ chế hoạt động của PoS 186
4.4.3. Cơ chế đồng thuận của mạng Cardano 189
4.4.4. Ưu nhược điểm của của PoS 193
4.5. CÁC BIẾN THỂ CỦA THUẬT TOÁN BẰNG CHỨNG CỔ PHẦN 195
4.5.1. Thuật toán Bằng chứng ủy cổ phần được ủy quyền (DPoS) 195
4.5.2. Thuật toán Bằng chứng trọng số (PoWeight) 196
4.5.3 Một số thuật toán khác. 198
CHƯƠNG 5: THÁCH THỨC VÀ XU HƯỚNG MỚI 204
5.1. Các thách thức của Blockchain 204
5.1.1. Thách thức về mặt kỹ thuật 204
5.1.2. Thách thức về quản trị và khả năng tương tác 209
5.1.3. Thách thức về pháp lý và tuân thủ 211
5.1.4. Thách thức về xã hội và chấp nhận 214
5.2. Blockchain 3.0: Các Đột Phá Mới trong Công Nghệ Blockchain 215

MỞ ĐẦU

Đã 17 năm trôi qua kể từ khi một người có bút danh **Satoshi Nakamoto** công bố bài báo về một hệ thống chuyển tiền ngang hàng có tiêu đề *"Bitcoin: A Peer-to-Peer Electronic Cash System"*. Bài báo này không chỉ đưa ra khái niệm về **Bitcoin** – một loại tiền mã hóa (cryptocurrency) phi tập trung, có khả năng xử lý vấn đề lặp chi, một trong những nguyên nhân góp phần cho khủng hoảng kinh tế toàn cầu thời kỳ đó, mà còn khai sinh một công nghệ mang tính cách mạng: **Blockchain**.

Công nghệ Blockchain sau đó đã liên tục trải qua những nâng cấp và cải tiến: từ Blockchain của những ngày đầu với mục tiêu hỗ trợ giao dịch tài chính (Blockchain 1.0), đến Blockchain có khả năng thực thi hợp đồng thông minh (Blockchain 2.0), và gần đây là các nền tảng Blockchain hiệu năng cao, chi phí thấp, có khả năng mở rộng và đảm bảo các yếu tố bảo vệ môi trường (Blockchain 3.0).

Tạp chí Forbes đã bắt đầu vinh danh các công ty ứng dụng Blockchain từ năm 2018, khi họ đưa ra danh sách "The Blockchain 50", một danh sách các công ty hàng đầu đang tích cực áp dụng công nghệ Blockchain vào hoạt động của mình. Điều này đã đánh dấu một cột mốc quan trọng trong sự phát triển của Blockchain, khi công nghệ này không còn là khái niệm chỉ dành riêng cho các dự án tiền mã hóa mà đã bắt đầu mở rộng ra nhiều ngành nghề và lĩnh vực khác nhau.

Ngày nay, **Blockchain** đã và đang trở thành một trụ cột quan trọng trong **Cuộc cách mạng công nghiệp lần thứ 4**, song hành cùng các công nghệ cốt lõi như **Trí tuệ nhân tạo (AI)**, **Dữ liệu lớn (Big Data)**, **Internet vạn vật (IoT)**, và **Mạng 5G**. Những tiến bộ của Blockchain đã và đang góp phần thúc đẩy một thế giới số minh bạch, công bằng và thuận tiện hơn, với tiềm năng tạo ra những thay đổi sâu sắc trong mọi khía cạnh của cuộc sống.

Vai trò và tầm quan trọng của Blockchain một lần nữa được khẳng định khi chính phủ Việt Nam gần đây ban hành Quyết định số **1236/QĐ-TTg ngày 22/10/2024**, công bố Chiến lược quốc gia về ứng dụng và phát triển công nghệ Blockchain đến năm 2025, với định hướng đến năm 2030. Tầm nhìn đến năm 2030, Việt Nam sẽ trở thành quốc gia thuộc nhóm dẫn đầu trong khu vực và có vị thế quốc tế trong nghiên cứu, triển khai, ứng dụng và khai thác công nghệ Blockchain.

Trong bối cảnh này, việc biên soạn và ra mắt "**Giáo trình Blockchain cơ bản**" cho sinh viên, đặc biệt là sinh viên khối ngành kỹ thuật, trong các trường Đại học tại Việt Nam, trở

nên cấp bách hơn bao giờ hết. Chúng tôi hy vọng qua giáo trình này, các bạn sinh viên sẽ không chỉ nắm vững các kiến thức cơ bản về công nghệ Blockchain mà còn hiểu rõ tầm quan trọng của nó trong việc thay đổi các ngành công nghiệp, từ tài chính, y tế, đến chuỗi cung ứng và nhiều lĩnh vực khác. Giáo trình này cũng trang bị cho các bạn những kỹ năng cần thiết để tham gia vào quá trình phát triển và ứng dụng Blockchain trong thực tế, từ việc thiết kế các hệ thống phi tập trung, phát triển hợp đồng thông minh cho đến tối ưu hóa hiệu suất của các nền tảng Blockchain hiện đại. Chúng tôi cũng hy vọng rằng các bạn sẽ có cái nhìn sâu sắc về những xu hướng phát triển của công nghệ Blockchain, từ đó có thể đóng góp tích cực vào việc thúc đẩy sự phát triển bền vững và ứng dụng rộng rãi của Blockchain trong tương lai.

Ngoài chương mở đầu, giáo trình được chia thành 5 chương, bao gồm:

Chương 1: Các kiến thức cơ sở

Chương này giúp người đọc nắm vững các khái niệm cơ bản về mã hóa, hàm băm, chữ ký số, hệ thống phi tập trung và phân tán, cũng như mạng ngang hàng (P2P) - những yếu tố cốt lõi xây dựng nền tảng của công nghệ Blockchain. Chương này do TS Nguyễn Đức Dư - Khoa CNTT, Trường Đại học Giao thông vận tải biên soạn.

Chương 2: Các khái niệm của Blockchain

Giới thiệu các khái niệm cơ bản về Blockchain, lịch sử ra đời của công nghệ này, các loại mạng Blockchain khác nhau, cũng như các ứng dụng quan trọng như tiền mã hóa, tokenomics và NFT. Chương này cũng làm rõ khái niệm về ví và địa chỉ trong Blockchain, đồng thời giới thiệu sổ cái phân tán và các lĩnh vực ứng dụng của công nghệ Blockchain. Chương này được biên soạn bởi ThS Trịnh Văn Chung - Khoa CNTT, Trường Đại học Nguyễn Trãi.

Chương 3: Một số nền tảng Blockchain

Chương này tập trung vào các nền tảng Blockchain phổ biến và quan trọng trong ngành, bao gồm Bitcoin - nền tảng Blockchain đầu tiên, Ethereum với hợp đồng thông minh và DApps, cũng như các nền tảng Blockchain thế hệ mới như Cardano. Bên cạnh đó, các nền tảng khác như BNB Chain, Polkadot và Avalanche cũng được đề cập và bổ sung các nền tảng mới đang nổi bật. Chương này được biên soạn bởi ThS Nguyễn Văn Hiệu.

Chương 4: Các thuật toán đồng thuận

Thuật toán đồng thuận là một phần không thể thiếu trong việc vận hành các mạng Blockchain. Chương này làm rõ vai trò của các thuật toán đồng thuận trong Blockchain, các khái niệm chính như BFT, PoW và PoS, và các thuật toán khác như DPoS/Ouroboros, PoH, PoA và PoC. Chương cũng sẽ phân tích ưu nhược điểm và các ứng dụng của từng thuật toán. Chương này do TS Hoàng Văn Thông - Khoa CNTT, Trường Đại học Giao thông vận tải biên soạn.

Chương 5: Thách thức và xu hướng mới

Cuối cùng, chương này sẽ đi sâu vào các thách thức hiện tại của Blockchain, bao gồm tính mở rộng, chi phí năng lượng và vấn đề bảo mật. Đồng thời, chương cũng trình bày về xu hướng mới trong Blockchain 3.0, như Blockchain xanh, Zero-Knowledge Proof (ZKP) và các giải pháp Layer 2 và Rollups. Chương cũng sẽ phân tích ưu nhược điểm và các ứng dụng của từng thuật toán. Nội dung chương này do TS Đỗ Ngọc Minh - Viện CNTT, Đại học Quốc gia Hà Nội biên soạn.

Mỗi chương sẽ đều kết thúc với phần câu hỏi và bài tập, giúp sinh viên củng cố kiến thức và rèn luyện khả năng giải quyết vấn đề trong lĩnh vực Blockchain.

Giáo trình được biên soạn với sự nỗ lực lớn nhằm cung cấp một cái nhìn toàn diện và dễ hiểu về công nghệ Blockchain, song chắc chắn sẽ không tránh khỏi thiếu sót. Chúng tôi xin được ghi nhận các ý kiến đóng góp từ quý thầy cô và các bạn sinh viên để có thể hoàn thiện hơn trong các lần tái bản sau. Mọi ý kiến xin gửi về địa chỉ email: uba@uba.edu.vn

CHƯƠNG 1: CÁC KIẾN THỨC CƠ SỞ

1.1. MÃ HÓA

1.1.1. Lịch sử mã hóa

Lịch sử mã hóa kéo dài hàng nghìn năm, với sự phát triển từ những hệ thống đơn giản đến các thuật toán phức tạp được sử dụng ngày nay. Mã hóa không chỉ là một công cụ bảo vệ thông tin mà còn là nền tảng của sự an toàn và bảo mật trong thế giới kỹ thuật số.

1.1.1.1. Thời kỳ cổ đại: Bắt đầu của mã hóa

Trong giai đoạn này, các hệ thống mã hóa đơn giản được tạo ra nhằm mục đích bảo mật thông tin trong các cuộc chiến và giao tiếp quân sự.

Mật mã Atbash (khoảng thế kỷ VI TCN): Sử dụng trong văn bản Hebrew cổ đại, Atbash là một dạng mã hóa hoán vị, trong đó chữ cái đầu tiên bị thay thế bởi chữ cái cuối cùng, chữ cái thứ hai bị thay thế bởi chữ cái áp chót, và tiếp tục như vậy.

Mật mã Polybius (thế kỷ II TCN): Phát minh bởi nhà triết học Hy Lạp Polybius, mật mã này sử dụng một bảng vuông 5x5 để chuyển các chữ cái thành các tọa độ số.

Mật mã Caesar (khoảng năm 58-50 TCN): Julius Caesar sử dụng phương pháp mã hóa thay thế đơn giản, được gọi là Mã Caesar, để mã hóa các thông điệp quân sự. Đây là dạng mã hóa dịch chuyển trong bảng chữ cái với số lần dịch chuyển cố định. Ví dụ, với dịch chuyển 3 vị trí, “A” trở thành “D”.

Mặc dù ra đời từ thời La Mã cổ đại, mã Caesar – một dạng mã hóa đơn giản bằng cách dịch chuyển các chữ cái trong bảng chữ cái – vẫn còn được sử dụng trong nhiều tình huống hiện đại. Dù không đủ mạnh để bảo mật dữ liệu trong thế giới số ngày nay, mã Caesar vẫn là một công cụ thú vị trong giáo dục, giải trí và lập trình.

Dưới đây là ba tình huống cụ thể thể hiện cách mã Caesar vẫn có chỗ đứng trong thực tiễn:

Tình huống 1: Trò chơi trong lớp học lập trình

Trong một tiết học Tin học, giáo viên đưa cho học sinh một thông điệp bí ẩn:
"Wklv lv d whvw phvvdjh"

Học sinh được yêu cầu suy luận và giải mã câu này bằng cách thử dịch chuyển các chữ cái trong bảng chữ cái.

Đáp án: Khi dịch lùi 3 chữ cái (Caesar -3), thông điệp trở thành:
"This is a test message"

Tình huống 2: Manh mối trong trò chơi Escape Room

Trong một trò chơi phòng thoát hiểm, nhóm người chơi tìm thấy một mảnh giấy ghi:
"Wklv lv wkh nhb wr wkh grru"

Họ đoán rằng đây là một thông điệp đã được mã hóa theo kiểu mã Caesar.

Đáp án: Dịch lùi 3 chữ cái, họ sẽ đọc được:
"This is the key to the door"
Thông điệp này giúp họ tìm được vị trí của chiếc chìa khóa và vượt qua thử thách.

Tình huống 3: Làm mờ thông điệp lỗi trên website

Một lập trình viên thiết kế trang web không muốn người dùng đọc được thông báo lỗi rõ ràng nếu xảy ra sự cố. Vì thế, thay vì viết:
"Invalid user token"
Anh ta sử dụng mã Caesar với dịch chuyển +5 để tạo ra:
"Nsafqni zjxjw ytspjs"

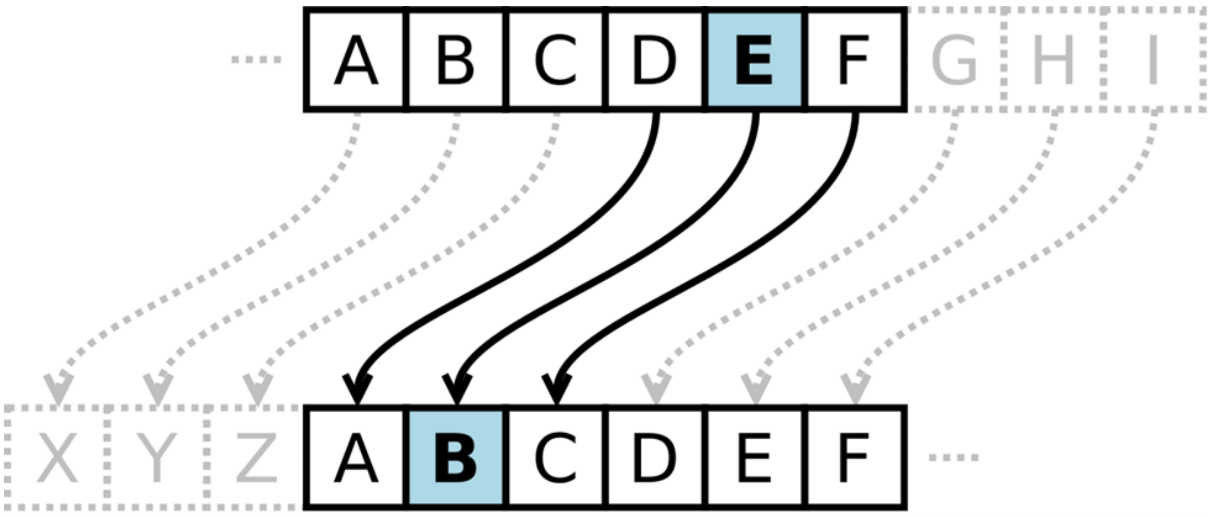
Đáp án: Khi dịch lùi 5 chữ cái, thông điệp gốc được khôi phục:
"Invalid user token"

Cách làm này không đủ mạnh để bảo mật, nhưng có thể ngăn người dùng tò mò đọc được nội dung dễ dàng.

Mã Caesar, tuy đơn giản và dễ phá, vẫn giữ được giá trị trong nhiều ngữ cảnh hiện đại – từ lớp học đến trò chơi giải trí. Những ứng dụng này giúp làm sống lại kiến thức lịch sử trong một thế giới kỹ thuật số, vừa mang tính giáo dục, vừa đầy thú vị.

Hình 1-1: Enigma – cỗ máy mã hóa huyền thoại của Phát xít Đức

Mật mã Caesar trong đó mỗi ký tự ở văn bản ban đầu sẽ được thay thế bằng một ký tự khác, có vị trí cách nó một khoảng xác định trong bảng chữ cái.



Hình 2: Thay thế ký tự trong mật mã Caesar

1.1.1.2. Thời Trung đại và Phục hưng: Phát triển mã hóa đa dạng

Trong thời kỳ này, mã hóa bắt đầu trở nên phức tạp hơn, với sự xuất hiện của các hệ thống mã hóa đa bảng và mã hóa cặp chữ.

Mật mã Vigenère (1553): Blaise de Vigenère, một nhà ngoại giao người Pháp, đã phát triển hệ thống mã hóa đa bảng. Mã hóa này sử dụng một từ khóa để điều chỉnh việc dịch chuyển ký tự trong thông điệp. Với phương pháp này, mỗi chữ cái trong văn bản gốc được mã hóa bằng một bảng dịch chuyển khác nhau, làm cho việc giải mã mà không có khóa trở nên rất khó khăn.

Mật mã Playfair (1854): Charles Wheatstone phát triển hệ thống mã hóa này, trong đó các cặp chữ cái trong văn bản gốc được mã hóa thay vì từng chữ cái đơn lẻ, điều này giúp gia tăng độ phức tạp và bảo mật cho thông tin.

Mật mã Morse (1837): một phương pháp được sử dụng trong viễn thông để mã hóa văn bản ký tự như trình tự chuẩn của hai khoảng thời gian tín hiệu khác nhau, được gọi là *dấu chấm (dots)* và *dấu gạch ngang (dash).*

1.1.1.3. Thế kỷ 20 và hai cuộc Chiến tranh Thế giới: Bước tiến vượt bậc trong mã hóa

Với sự phát triển của công nghệ và máy tính, mã hóa trở thành một yếu tố quan trọng trong chiến tranh và các hệ thống bảo mật quốc gia.

Mã hoá Enigma (1920s): Máy Enigma được Đức quốc xã sử dụng trong Chiến tranh Thế giới II để mã hóa thông tin quân sự. Mỗi thông điệp được mã hóa bằng cách sử dụng các rô-to xoay có thể thay đổi hàng triệu cấu hình khác nhau. Nhóm của Alan Turing tại Bletchley Park (Anh) đã phát triển các phương pháp giải mã thành công hệ thống mã hóa này, đóng góp to lớn vào kết quả của chiến tranh. Nhờ giải mã Enigma, quân đồng minh đã ngăn chặn được một cuộc tấn công bất ngờ của tàu ngầm Đức vào năm 1943, qua đó giúp rút ngắn chiến tranh khoảng 2 năm và cứu sống hàng triệu người.

Claude Shannon (1949): Nhà toán học người Mỹ Claude Shannon, trong nghiên cứu "A Mathematical Theory of Cryptography" đã đưa ra định nghĩa mã hóa theo các nguyên tắc toán học. Nghiên cứu của ông trở thành nền tảng cho lý thuyết mật mã hiện đại.

Mã hóa Huffman (1952) là một thuật toán mã hóa dùng để nén dữ liệu. Nó dựa trên bảng tần suất xuất hiện các ký tự cần mã hóa để xây dựng một bộ mã nhị phân là mã tiền tố cho các ký tự đó sao cho dung lượng (số bit) sau khi mã hóa là nhỏ nhất

1.1.1.4. Sự ra đời của máy tính và mật mã hiện đại (1970 - nay)

Với sự phát triển của máy tính, các hệ thống mã hóa ngày càng trở nên phức tạp và tinh vi, từ mã hóa đối xứng đến mã hóa bất đối xứng.

Mã hoá DES (1977): Data Encryption Standard (DES) được phát triển bởi IBM và được phê duyệt bởi NIST (Viện Tiêu chuẩn và Công nghệ Quốc gia Hoa Kỳ). Đây là tiêu chuẩn mã hóa đối xứng với khóa 56-bit, từng được coi là không thể phá vỡ. DES sử dụng khóa 56-bit, tạo ra 72,057,594,037,927,936 (2^56) khả năng khóa.

Mã hoá RSA (1977): Rivest, Shamir và Adleman phát triển thuật toán mã hóa bất đối xứng RSA, sử dụng khóa công khai và khóa riêng. Đây là nền tảng của mã hóa công khai và được sử dụng rộng rãi trong giao dịch bảo mật. RSA sử dụng các số nguyên tố rất lớn, lên đến hàng trăm bit. Hiện nay, khóa 2048-bit RSA được sử dụng phổ biến cho bảo mật cao.

Nếu như mã Caesar là đại diện cho thời kỳ đầu của mật mã học – đơn giản, dễ hiểu, phù hợp cho giáo dục hoặc giải trí. RSA là một cột mốc quan trọng trong mật mã học hiện đại – có nền tảng toán học vững chắc, khó phá mã, và được ứng dụng rộng rãi trong công nghệ bảo mật. Mã Caesar giống như ổ khóa đồ chơi, trong khi RSA là két sắt điện tử cấp ngân hàng

So sánh mức độ phức tạp toán học		
Tiêu chí	**Mã Caesar (Cổ điển)**	**Mã RSA (Hiện đại)**
Nguyên lý	Dịch chuyển các chữ cái theo một số cố định (ví dụ: +3)	Dựa trên lý thuyết số, đặc biệt là bài toán phân tích số nguyên lớn thành thừa số nguyên tố
Tính toán	Cộng/trừ số nguyên đơn giản	Phép toán mũ và modulo với các số rất lớn
Độ dài khóa	Chỉ có 25 khóa có thể (dịch từ 1 đến 25)	Có thể có khóa dài hàng trăm hoặc hàng ngàn bit (1024, 2048, 4096 bit...)
Độ phức tạp giải mã	Dễ đoán hoặc thử hết (brute force) trong vài giây	Cực kỳ khó giải mã nếu không có khóa riêng – mất hàng triệu năm để bẻ bằng brute force

Bảng 1: So sánh mức độ phức tạp toán học của mã hóa RSA và mã hóa Caesar

Mức độ bảo mật (Security Strength)		
Tiêu chí	**Mã Caesar**	**Mã RSA**
Khả năng bị phá mã	Rất dễ – chỉ mất vài giây thử từng trường hợp	Hầu như không thể nếu khóa đủ dài và được quản lý tốt
Tính bảo mật hiện đại	Không còn được dùng trong bảo mật thực tế	Là nền tảng cho các hệ thống bảo mật hiện đại như HTTPS, chữ ký số
Tấn công phổ biến	Phân tích tần suất, thử tất cả dịch chuyển	Tấn công số học phức tạp (nhưng chưa khả thi với khóa đủ lớn)

Bảng 1-2: So sánh mức độ bảo mật của mã hóa RSA và mã hóa Caesar

Ứng dụng thực tế (Real-World Applications)		
Tiêu chí	**Mã Caesar**	**Mã RSA**
Ứng dụng hiện nay	Dùng trong trò chơi giải đố, giáo dục, mô phỏng đơn giản	Dùng trong ngân hàng, giao dịch điện tử, bảo vệ dữ liệu cá nhân
Tính khả thi thực tế	Chỉ mang tính minh họa	Rất thực tế và được sử dụng rộng rãi toàn cầu
Mã hóa đối xứng / bất đối xứng	Mã hóa đối xứng (khóa mã và khóa giải giống nhau)	Mã hóa bất đối xứng (khóa công khai và khóa riêng biệt)

Bảng 1-3: So sánh ứng dụng thực tế

Mã hoá AES (2001): Advanced Encryption Standard (AES) được phát triển để thay thế DES. AES sử dụng các kích thước khóa 128, 192, và 256-bit. Đây là một trong những phương pháp mã hóa nhanh, an toàn và hiệu quả nhất hiện nay.AES 256-bit có 2^256 khả năng khóa, tương đương với một con số gần như không thể bẻ khóa bằng các phương tiện tính toán hiện đại.

1.1.1.5. Sự phát triển của mật mã lượng tử và blockchain (Thế kỷ 21)

Mã hóa không chỉ phát triển trong không gian kỹ thuật số truyền thống mà còn mở rộng sang các lĩnh vực mới như máy tính lượng tử và công nghệ blockchain.

Shor's Algorithm (1994): Peter Shor phát triển một thuật toán lượng tử có thể phân tích các số nguyên tố rất nhanh, đe dọa tính bảo mật của các hệ thống mã hóa dựa trên RSA[1] và ECC. Một máy tính lượng tử sử dụng thuật toán Shor có thể bẻ khóa RSA 2048-bit chỉ trong vài giờ, trong khi các siêu máy tính hiện nay phải mất hàng triệu năm.

Blockchain và Bitcoin (2009): Bitcoin và blockchain sử dụng các khái niệm mã hóa tiên tiến, bao gồm các hàm băm mật mã và chữ ký số để bảo mật các giao dịch. Đây là một trong những ứng dụng lớn nhất của mật mã trong hệ thống tài chính. Hàm băm SHA-256, được sử dụng trong blockchain Bitcoin, tạo ra 2^256 kết quả khả dĩ.

1.1.2. Khái niệm mã hóa và giải mã

Mã hóa là quá trình chuyển đổi thông tin từ dạng dễ đọc (plaintext) sang dạng không thể đọc được nếu không có công cụ hoặc khóa giải mã (ciphertext). Mục tiêu của mã hóa là bảo vệ thông tin quan trọng, đảm bảo rằng chỉ những người có quyền truy cập mới có thể đọc và hiểu được thông tin.

Giải mã là quá trình ngược lại, tức là chuyển đổi thông tin từ dạng mã hóa (ciphertext) về lại dạng nguyên bản (plaintext). Quá trình này chỉ có thể được thực hiện nếu biết chính xác khóa giải mã hoặc thuật toán tương ứng.

Mã hóa dựa vào hai thành phần cơ bản:

Thuật toán mã hóa (Cipher): Đây là phương thức hoặc tập hợp các quy tắc dùng để chuyển đổi từ bản rõ sang bản mã. Một số thuật toán phổ biến bao gồm AES, RSA, và DES.

Khóa mã hóa (Key): Đây là giá trị đặc biệt mà cả quá trình mã hóa và giải mã dựa vào. Nếu không có khóa này, quá trình giải mã không thể thực hiện.

Có 2 loại mã hóa là mã hóa đối xứng và mã hóa bất đối xứng:

Mã hóa đối xứng (Symmetric Encryption): Cả mã hóa và giải mã sử dụng cùng một khóa bí mật. Thuật toán này nhanh hơn nhưng yêu cầu phải bảo mật khóa khi chia sẻ với người nhận (ví dụ: AES, DES).

Mã hóa bất đối xứng (Asymmetric Encryption): Sử dụng một cặp khóa, bao gồm khóa công khai để mã hóa và khóa riêng tư để giải mã. Phương pháp này an toàn hơn nhưng chậm hơn (ví dụ: RSA, ECC).

Mã hóa có nhiều ứng dụng trong thực tế:

Bảo mật thông tin cá nhân và tài chính: Mã hóa được sử dụng rộng rãi trong các giao dịch ngân hàng và thương mại điện tử để bảo vệ dữ liệu thẻ tín dụng và thông tin cá nhân.

Bảo mật email và tin nhắn: Công nghệ mã hóa như PGP (Pretty Good Privacy) được sử dụng để bảo vệ nội dung email khỏi việc bị đọc trộm.

Mạng riêng ảo (VPN): Sử dụng mã hóa để bảo vệ các kết nối mạng khỏi tin tặc hoặc các gián điệp mạng.

[1] RSA, ECC: xxxx

1.1.3. Mã hóa cổ điển

Mã hóa cổ điển (Classical Cryptography) là lĩnh vực mã hóa xuất hiện trước khi máy tính ra đời. Các kỹ thuật mã hóa này dựa trên sự thay thế hoặc hoán vị ký tự và chủ yếu phục vụ cho các mục đích quân sự, chính trị, và ngoại giao. Phần này trình bày các kiến thức quan trọng về mã hóa cổ điển, bao gồm những phương pháp nổi tiếng và các khái niệm cơ bản.

1.1.3.1 Mã hóa thay thế (Substitution Cipher)

Mã hóa thay thế là kỹ thuật mã hóa cổ điển trong đó mỗi ký tự trong văn bản gốc (plaintext) được thay thế bằng một ký tự khác. Các loại mã hóa thay thế phổ biến bao gồm:

Mã Caesar (Caesar Cipher): Một trong những phương pháp mã hóa lâu đời nhất, được Julius Caesar sử dụng để mã hóa các thông điệp quân sự. Mã Caesar là một loại mã hóa thay thế trong đó mỗi ký tự trong văn bản gốc được dịch chuyển một số vị trí cố định trong bảng chữ cái.

Nếu p là ký tự gốc và k là số vị trí dịch chuyển, thì ký tự mã hóa c được tính theo công thức: $c = (p+k) \bmod 26$. Để giải mã: $p = (c-k) \bmod 26$.

Ví dụ: Với dịch chuyển 3, chữ "A" trở thành "D", "B" trở thành "E", và tiếp tục như vậy.

Mật mã Atbash (Atbash Cipher): Đây là một dạng mã hóa thay thế ngược, trong đó chữ cái đầu tiên của bảng chữ cái bị thay thế bởi chữ cái cuối cùng, chữ cái thứ hai bị thay thế bởi chữ cái áp chót, và tiếp tục như vậy.

Ví dụ: "A" sẽ trở thành "Z", "B" sẽ trở thành "Y", và "C" sẽ trở thành "X".

Mật mã đa bảng (Polyalphabetic Cipher): Mã hóa này sử dụng nhiều bảng thay thế khác nhau để mã hóa các ký tự ở các vị trí khác nhau. Mỗi ký tự trong văn bản gốc được mã hóa theo một bảng khác nhau, do đó việc bẻ khóa trở nên khó khăn hơn.

1.1.3.2 Mã hóa hoán vị (Transposition Cipher)

Mã hóa hoán vị thay đổi thứ tự của các ký tự trong văn bản gốc thay vì thay thế chúng bằng các ký tự khác. Kỹ thuật này thường được sử dụng kết hợp với mã hóa thay thế để tăng độ phức tạp.

Mã hóa Scytale: Scytale là một phương pháp mã hóa của người Spartan, sử dụng một cây gậy (scytale) để viết các thông điệp trên một dải giấy quấn quanh cây gậy. Khi giấy được tháo ra, văn bản trở thành không thể đọc được trừ khi nó được quấn lại trên một cây gậy có cùng đường kính.

Mã hóa cột (Columnar Transposition): Trong mã hóa cột, văn bản gốc được viết thành các hàng của một bảng với số cột xác định trước. Sau đó, các ký tự được đọc theo thứ tự từ trên xuống dưới qua các cột thay vì từ trái sang phải.

Ví dụ: Văn bản gốc “HELLOWORLD” với khoá là HACK

Dữ liệu được biểu diễn theo bảng 4 cột theo độ dài của HACK

H	A	C	K

H	E	L	L
O	W	O	R
L	D		

Sắp xếp các cột lại theo bảng chữ cái của khoá ta được

A	C	H	K
E	L	H	L
W	O	O	R
D		L	

Bây giờ ta lấy dữ liệu theo từng cột được kết quả mã hoá "EWDLOHOLLR"

1.1.3.3 Mã hóa Vigenère (Vigenère Cipher)

Đây là một dạng mã hóa đa bảng, sử dụng một từ khóa để quyết định cách mã hóa từng ký tự trong văn bản gốc. Mỗi chữ cái trong từ khóa được sử dụng để xác định bảng dịch chuyển cho các ký tự tương ứng trong văn bản gốc. Điều này làm cho mã hóa Vigenère trở nên khó bẻ khóa hơn nhiều so với mã hóa thay thế đơn giản.

Nếu ký tự thứ i trong văn bản gốc là p_i và ký tự thứ i trong từ khóa là k_i, thì ký tự mã hóa c_i được tính như sau: $c_i = (p_i + k_i) \bmod 26$. Để giải mã: $p_i = (c_i - k_i) \bmod 26$

Ví dụ: Với văn bản gốc "ATTACKATDAWN" với khóa "LEMON":

Plaintext: A T T A C K A T D A W N

Key: L E M O N L E M O N L E

Ciphertext: L X F O P V E F R N H R

1.1.3.4. Mã hóa Playfair (Playfair Cipher)

Phát minh bởi Charles Wheatstone năm 1854, mã hóa Playfair là một hệ thống mã hóa cặp ký tự. Mỗi cặp chữ cái được mã hóa dựa trên một bảng vuông 5x5 chứa các chữ cái trong bảng chữ cái (loại bỏ chữ Q hoặc I/J được dùng chung).

Quy tắc mã hóa: Với một cặp chữ cái:

Nếu hai chữ cái nằm trên cùng một hàng, thay thế mỗi chữ bằng chữ bên phải nó.

Nếu hai chữ cái nằm trên cùng một cột, thay thế mỗi chữ bằng chữ bên dưới nó.

Nếu hai chữ cái tạo thành một hình chữ nhật, thay thế mỗi chữ bằng chữ nằm cùng hàng ở góc còn lại của hình chữ nhật đó.

Ví dụ:

Bảng mã hóa Playfair (không chứa "Q"):

P L A Y F

I/J B C D E

G H K M N

O R S T U

V W X Y Z

Mã hoá cặp “HI” nằm khác hàng khác cột nên ta lấy theo góc hình chữ nhật cùng hàng “H” thay thế bằng “G” còn “I” thay thế bằng “B”

Mã hoá cặp “SC” nằm cùng cột nên lấy ký tự dịch xuống 1 hàng “S” thành “X” còn “C” thành “K”.

Mã hoá cặp “EB” nằm cùng hàng nên lấy dịch sang phải 1 hàng “E” thành “I/J” còn “B“thành “C”.

1.1.3.5 Mã hóa Hill (Hill Cipher)

Mã hóa Hill được phát minh bởi Lester Hill vào năm 1929, sử dụng toán học tuyến tính và đại số ma trận để mã hóa các khối ký tự. Phương pháp này sử dụng ma trận vuông để mã hóa các ký tự trong văn bản gốc.

Công thức: Cho một khối ký tự có n ký tự, mã hóa Hill sử dụng một ma trận n×n khóa để thực hiện phép nhân ma trận với khối văn bản gốc. Mỗi chữ cái được chuyển thành một số từ 0 đến 25 (A=0, B=1, C=2, D=3, E=4, F=5, G=6, H = 7 ... … Z=25), sau đó áp dụng phép nhân ma trận để tính toán văn bản mã hóa.

Giải mã được thực hiện bằng cách nhân với ma trận nghịch đảo của ma trận khóa.

Ví dụ: Với văn bản gốc "HOME" và ma trận khóa 2x2 là:

$$(3\ 3\ 2\ 5)$$

Mã hóa Hill sẽ chuyển "HOME" thành chuỗi số “HO” (7, 14) và “ME” (10, 4) nhân modulo 26 với ma trận khóa và sau đó chuyển kết quả thành văn bản mã hóa

Với “HO” xét $(3\ 3\ 2\ 5) * (7\ 14) = (63\quad 84)\ mod\ 26 = (11\ \ 6)$ tương ứng là “LG”

Với “ME” xét $(3\ 3\ 2\ 5) * (10\ 4) = (42\ 40)\ mod\ 26 = (16\ \ 14)$ tương ứng là “QO”

Vậy “HOME” sẽ mã hoá thành “LGQO”.

1.1.3.6. Mã hóa Affine (Affine Cipher)

Đây là dạng mã hóa thay thế dựa trên phép biến đổi affine trong toán học. Mỗi ký tự trong văn bản gốc được mã hóa bằng một hàm tuyến tính với dạng: c=(a·p+b) mod 26.

Trong đó: p là vị trí của ký tự trong bảng chữ cái, a và b là các tham số của hàm tuyến tính (với a phải nguyên tố cùng nhau với 26) c là ký tự mã hóa.

Mã hóa cổ điển là nền tảng quan trọng của lĩnh vực mật mã. Mặc dù các phương pháp này hiện nay không đủ an toàn trước những công nghệ giải mã hiện đại, nhưng chúng vẫn có

giá trị lịch sử lớn. Các hệ thống mã hóa cổ điển là bước đệm để phát triển các kỹ thuật mã hóa phức tạp hơn, như mã hóa đối xứng và bất đối xứng, được sử dụng trong thế giới kỹ thuật số ngày nay.

1.1.4. Mã hóa đối xứng

Mã hóa đối xứng (Symmetric Encryption) là một trong những phương pháp mã hóa cơ bản và lâu đời nhất, trong đó cùng một khóa bí mật được sử dụng để mã hóa và giải mã dữ liệu. Khóa này phải được giữ bí mật giữa hai bên giao tiếp để bảo đảm an toàn. Mã hóa đối xứng thường được sử dụng cho việc truyền tải dữ liệu nhanh chóng do tốc độ cao của các thuật toán. Đặc điểm chính của mã hóa đối xứng:

Sử dụng một khóa bí mật chung: Cả hai bên (người gửi và người nhận) phải chia sẻ chung một khóa bí mật.

Tốc độ cao: Các thuật toán mã hóa đối xứng thường nhanh hơn các thuật toán mã hóa bất đối xứng.

Vấn đề phân phối khóa: Việc bảo mật và phân phối khóa giữa các bên là một thách thức lớn trong mã hóa đối xứng.

Mã hóa đối xứng thường được sử dụng trong các hệ thống cần tốc độ cao và khối lượng dữ liệu lớn, chẳng hạn như mã hóa dữ liệu đĩa, giao thức bảo mật mạng (VPN, SSL/TLS).

1.1.4.1. Một số mật mã đối xứng

a. Data Encryption Standard (DES)

DES được phát triển bởi IBM vào những năm 1970 và được NIST (Viện Tiêu chuẩn và Công nghệ Quốc gia Hoa Kỳ) phê duyệt làm tiêu chuẩn mã hóa vào năm 1977. DES sử dụng khóa 56-bit (thực tế khóa là 64-bit, nhưng 8 bits được sử dụng để kiểm tra tính toàn vẹn). DES là một khối mã hóa (block cipher) với kích thước khối 64-bit, sử dụng thuật toán mã hóa khối với chuỗi các phép biến đổi (Feistel network). Với sự gia tăng sức mạnh tính toán, khóa 56-bit của DES trở nên không an toàn. DES đã bị tấn công thành công nhiều lần thông qua các cuộc tấn công vét cạn (brute force).

Ví dụ: Giả sử bạn muốn mã hóa thông điệp "HELLO", DES sẽ chia văn bản thành các khối 64-bit và mã hóa từng khối bằng khóa 56-bit.

b. Triple DES (3DES)

Triple DES được phát triển để tăng cường độ bảo mật của DES bằng cách áp dụng thuật toán DES ba lần với hai hoặc ba khóa khác nhau. 3DES sử dụng khóa khóa 112-bit (sử dụng hai khóa) hoặc 168-bit (sử dụng ba khóa). 3DES mã hóa dữ liệu bằng cách sử dụng ba lần DES: mã hóa, giải mã, và mã hóa lần nữa (Encrypt-Decrypt-Encrypt). Mặc dù 3DES cải thiện bảo mật, nhưng nó vẫn bị coi là chậm và có độ dài khóa ngắn so với các thuật toán hiện đại.

Ví dụ: Thay vì mã hóa "HELLO" một lần với DES, 3DES sẽ thực hiện ba lần mã hóa với các khóa khác nhau để tăng cường tính an toàn.

c. Advanced Encryption Standard (AES)

AES được phát triển vào cuối những năm 1990 để thay thế DES và 3DES, và được phê chuẩn bởi NIST vào năm 2001 sau một cuộc thi toàn cầu tìm kiếm một thuật toán mã hóa an toàn và hiệu quả. Thuật toán này hỗ trợ ba độ dài khóa: 128-bit, 192-bit, và 256-bit. AES là thuật toán mã hóa khối với kích thước khối cố định 128-bit, sử dụng mạng biến đổi thay thế (Substitution-Permutation Network). AES có ưu điểm an toàn, nhanh chóng và được sử dụng rộng rãi trong các ứng dụng bảo mật hiện đại như SSL/TLS, WPA2 (Wi-Fi), và mã hóa dữ liệu đĩa.

Ví dụ: Mã hóa văn bản "HELLO WORLD" bằng AES với khóa 128-bit: Chia văn bản thành các khối: AES yêu cầu đầu vào là các khối 128-bit, vì vậy văn bản "HELLO WORLD" sẽ được chuyển đổi thành các khối nhị phân, sau đó được chia thành các khối phù hợp (bao gồm cả việc thêm padding nếu cần).

AES sẽ sử dụng khóa 128-bit để mã hóa từng khối, trải qua 10 vòng biến đổi bao gồm các bước thay thế byte (SubBytes), hoán vị hàng (ShiftRows), trộn cột (MixColumns), và thêm khóa (AddRoundKey).

Kết quả: Kết quả là một chuỗi dữ liệu nhị phân được mã hóa mà chỉ có thể giải mã bằng khóa bí mật 128-bit ban đầu.

d. Blowfish

Blowfish được Bruce Schneier phát triển vào năm 1993 như một sự thay thế miễn phí cho DES. Khóa của thuật toán này có thể thay đổi từ 32-bit đến 448-bit, cho phép tính linh hoạt về độ bảo mật. Blowfish là mã hóa khối với kích thước khối 64-bit, sử dụng mạng Feistel với 16 vòng lặp. Blowfish rất nhanh trong các hệ thống 32-bit, có thể thay đổi độ dài khóa, và được sử dụng rộng rãi trong các ứng dụng như bảo mật mật khẩu.

Ví dụ: Bạn có thể sử dụng khóa 128-bit để mã hóa "HELLO" thành khối 64-bit.

e. Twofish

Twofish được phát triển bởi các nhà thiết kế của Blowfish như một phiên bản nâng cao vào năm 1998 và là một trong những ứng viên cuối cùng của cuộc thi AES. Twofish hỗ trợ các khóa 128-bit, 192-bit, và 256-bit. Twofish là mã hóa khối với kích thước khối 128-bit, có cấu trúc Feistel với 16 vòng lặp. Nó cũng sử dụng các phép toán XOR, hoán vị, và các phép biến đổi trên các byte dữ liệu. Twofish có độ linh hoạt và bảo mật cao, được thiết kế cho tốc độ và an toàn trên cả phần cứng và phần mềm.

Ví dụ: Khi mã hóa chuỗi "HELLO" bằng khóa 256-bit trong Twofish, thông điệp sẽ được chia thành các khối 128-bit và mã hóa qua 16 vòng biến đổi.

f. RC4 (Rivest Cipher 4)

RC4 là một mã hóa dòng (stream cipher) do Ron Rivest phát triển vào năm 1987. Thay vì mã hóa khối, nó mã hóa từng byte dữ liệu một cách tuần tự. Thuật toán RC4 hỗ trợ các khóa từ 40-bit đến 2048-bit. RC4 tạo ra một dòng khóa ngẫu nhiên (keystream) và XOR nó với từng byte trong văn bản gốc để tạo ra văn bản mã hóa. Mặc dù RC4 rất nhanh và được sử dụng rộng rãi (trong SSL, WEP), nhưng nó đã bị phát hiện có nhiều lỗ hổng bảo mật, dẫn đến việc nó bị thay thế trong nhiều ứng dụng.

Ví dụ: Nếu mã hóa chuỗi "HELLO" bằng RC4, mỗi ký tự sẽ được XOR với một byte của dòng khóa để tạo ra văn bản mã hóa.

g. Serpent

Serpent được phát triển vào năm 1998 bởi Anderson, Biham, và Knudsen như một ứng viên cho AES. Thuật toán Serpent hỗ trợ các khóa 128-bit, 192-bit, và 256-bit. Serpent sử dụng một cấu trúc mạng hoán vị thay thế với 32 vòng biến đổi, với mục tiêu ưu tiên tính an toàn hơn là tốc độ. Serpent được thiết kế để chống lại tất cả các cuộc tấn công đã biết vào thời điểm phát triển và được coi là an toàn hơn AES, mặc dù chậm hơn.

Ví dụ: Khi mã hóa "HELLO" bằng khóa 128-bit trong Serpent, thông điệp sẽ được chia thành khối 128-bit và trải qua 32 vòng biến đổi.

1.1.4.2. Chế độ hoạt động của mã hóa khối (Block Cipher Modes of Operation)

Các thuật toán mã hóa khối như DES, AES, và Blowfish hoạt động trên các khối dữ liệu có kích thước cố định (ví dụ: AES mã hóa các khối 128-bit). Tuy nhiên, dữ liệu thực tế thường không chia đều thành các khối có kích thước cố định. Để giải quyết vấn đề này và xử lý các khối dữ liệu có độ dài thay đổi, cũng như tăng cường tính bảo mật, các chế độ hoạt động (modes of operation) đã được phát triển. Các chế độ hoạt động phổ biến của mã hóa khối được trình bày dưới đây:

ECB (Electronic Codebook): Trong chế độ ECB, mỗi khối dữ liệu sẽ được mã hóa độc lập. Nếu có hai khối giống nhau trong văn bản gốc, chúng sẽ được mã hóa thành hai khối giống nhau trong văn bản mã hóa.

ECB đơn giản và nhanh chóng do mỗi khối có thể được mã hóa song song. Tuy nhiên ECB không bảo mật khi dữ liệu có các mẫu lặp lại, vì các khối giống nhau sẽ tạo ra văn bản mã hóa giống nhau, làm lộ cấu trúc dữ liệu. Ví dụ, hình ảnh mã hóa bằng ECB vẫn giữ lại các mẫu của hình ảnh ban đầu.

ECB hiếm khi được sử dụng trong các hệ thống bảo mật hiện đại do những lỗ hổng bảo mật của nó.

Ví dụ: Khi mã hóa một file hình ảnh có các vùng màu giống nhau, ECB sẽ tạo ra các khối mã hóa giống nhau cho các vùng này, làm lộ mẫu hình ảnh.

CBC (Cipher Block Chaining): Mỗi khối dữ liệu sẽ được XOR với khối mã hóa trước đó trước khi được mã hóa. Khối đầu tiên được XOR với một giá trị khởi tạo ngẫu nhiên gọi là Initialization Vector (IV).

CBC giải quyết vấn đề lặp lại của ECB bằng cách đảm bảo rằng các khối giống nhau sẽ tạo ra các khối mã hóa khác nhau, miễn là IV khác nhau. Nó cũng tạo ra tính ngẫu nhiên ngay cả khi văn bản gốc có các mẫu lặp lại. CBC không hỗ trợ mã hóa song song, vì mỗi khối phụ thuộc vào khối trước đó. Điều này khiến CBC chậm hơn khi xử lý nhiều dữ liệu cùng lúc.

CBC được sử dụng rộng rãi trong các giao thức bảo mật như SSL/TLS và IPsec.

Ví dụ: Khi mã hóa chuỗi "HELLO WORLD" bằng CBC, mỗi khối sẽ được XOR với khối mã hóa trước đó, tạo ra các khối mã hóa khác nhau ngay cả khi chuỗi gốc có các phần giống nhau.

CFB (Cipher Feedback): CFB là một chế độ mã hóa dòng (stream mode) dựa trên mã hóa khối. Thay vì mã hóa toàn bộ khối, CFB mã hóa một phần dữ liệu theo từng đoạn (ví dụ: 8-bit hoặc 64-bit), sau đó XOR đoạn này với văn bản gốc để tạo thành văn bản mã hóa.

CFB cho phép mã hóa và giải mã các đoạn dữ liệu có kích thước thay đổi, do đó phù hợp cho truyền thông dữ liệu liên tục (streaming). Tuy vậy, giống như CBC, CFB không hỗ trợ mã hóa song song.

CFB thường được sử dụng cho mã hóa dòng dữ liệu trong mạng truyền tải và liên lạc thời gian thực.

Ví dụ: Khi mã hóa chuỗi ký tự bằng CFB, hệ thống sẽ xử lý từng đoạn nhỏ của dữ liệu và XOR với văn bản mã hóa trước đó.

OFB (Output Feedback): OFB cũng là chế độ mã hóa dòng, nhưng thay vì sử dụng đầu ra của khối trước đó, nó tạo ra một chuỗi khóa ngẫu nhiên từ mã hóa của IV. Chuỗi khóa này sẽ được XOR với từng đoạn dữ liệu của văn bản gốc để tạo ra văn bản mã hóa.

OFB cho phép xử lý song song và bảo vệ dữ liệu khỏi lỗi truyền tải, vì lỗi trong một khối không ảnh hưởng đến các khối sau. Nhưng OFB yêu cầu IV được giữ bí mật và không được sử dụng lại, vì việc sử dụng lại IV có thể dẫn đến lỗ hổng bảo mật.

OFB phù hợp cho các ứng dụng yêu cầu bảo vệ mạnh mẽ trước lỗi truyền thông, như mã hóa liên lạc vệ tinh.

Ví dụ: Khi mã hóa chuỗi dữ liệu bằng OFB, mỗi khối sẽ được XOR với một phần của chuỗi khóa ngẫu nhiên để tạo ra văn bản mã hóa.

CTR (Counter Mode): Trong CTR, mỗi khối sẽ được XOR với đầu ra của một bộ đếm (counter) đã được mã hóa bằng thuật toán mã hóa khối. Bộ đếm tăng dần theo mỗi khối, tạo ra một chuỗi khóa duy nhất cho mỗi khối.

CTR cho phép mã hóa và giải mã song song, làm tăng hiệu suất đáng kể, đặc biệt là trên phần cứng đa lõi. Nó cũng không yêu cầu padding, giúp đơn giản hóa mã hóa các dữ liệu có độ dài thay đổi. Giống như OFB, CTR có nhược điểm là yêu cầu giá trị bộ đếm không được tái sử dụng, nếu không sẽ tạo ra lỗ hổng bảo mật.

CTR được sử dụng rộng rãi trong các giao thức bảo mật như IPsec và các ứng dụng mã hóa dữ liệu lớn.

Ví dụ: Khi mã hóa một file lớn bằng CTR, bộ đếm sẽ được mã hóa để tạo ra các giá trị khác nhau cho mỗi khối và XOR với văn bản gốc.

1.1.5. Mã hóa bất đối xứng

Mã hóa bất đối xứng (Asymmetric Encryption), còn được gọi là mã hóa khóa công khai, là một hệ thống mã hóa sử dụng hai khóa khác nhau nhưng liên kết với nhau: một khóa công khai (public key) và một khóa bí mật (private key). Khóa công khai được sử dụng để mã hóa

dữ liệu và khóa bí mật dùng để giải mã dữ liệu. Điều đặc biệt là dữ liệu được mã hóa bằng khóa công khai chỉ có thể được giải mã bằng khóa bí mật tương ứng và ngược lại.

Khóa công khai: Được chia sẻ rộng rãi và dùng để mã hóa dữ liệu.

Khóa bí mật: Được giữ bí mật và dùng để giải mã dữ liệu.

Một số thuật toán mã hóa bất đối xứng điển hình

a. RSA (Rivest-Shamir-Adleman)

RSA dựa trên độ khó của việc phân tích một số lớn thành các thừa số nguyên tố. Khóa công khai và khóa bí mật được tạo dựa trên các cặp số nguyên tố lớn.

Đây là thuật toán phổ biến và đã được sử dụng rộng rãi trong các hệ thống như SSL/TLS, email bảo mật (PGP), và chữ ký số. Nhưng RSA yêu cầu độ dài khóa lớn để đảm bảo an toàn, gây tốn tài nguyên tính toán.

Ví dụ: Trong một phiên giao dịch bảo mật trên web, khóa công khai RSA của máy chủ được sử dụng để mã hóa dữ liệu truyền giữa máy chủ và trình duyệt.

b. DSA (Digital Signature Algorithm)

DSA được thiết kế riêng để tạo và xác minh chữ ký số. DSA không trực tiếp mã hóa dữ liệu, mà chỉ tạo chữ ký số để xác thực tính toàn vẹn và nguồn gốc của thông tin.

Ưu điểm của DSA là tối ưu hóa cho việc ký và xác minh chữ ký số. Nhược điểm của nó là không thể sử dụng để mã hóa dữ liệu.

Ví dụ: DSA thường được sử dụng trong các hệ thống như GPG để xác thực email và tài liệu.

c. ECC (Elliptic Curve Cryptography)

ECC dựa trên các tính chất toán học của đường cong elliptic để tạo khóa công khai và khóa bí mật. ECC cung cấp mức độ bảo mật tương tự như RSA với kích thước khóa nhỏ hơn nhiều.

ECC có hiệu suất tốt hơn RSA, đặc biệt trên các thiết bị có tài nguyên hạn chế (ví dụ: điện thoại di động, IoT). Tuy nhiên cần phải chọn đúng các tham số đường cong elliptic để đảm bảo tính bảo mật.

Ví dụ: ECC được sử dụng trong các giao thức bảo mật hiện đại như HTTPS, VPN và blockchain (ví dụ: Bitcoin sử dụng ECC để quản lý các khóa ví).

d. ElGamal

ElGamal là một thuật toán mã hóa dựa trên độ khó của bài toán logarithm rời rạc. Nó cung cấp cả tính năng mã hóa dữ liệu và tạo chữ ký số.

ElGamal có ưu điểm là bảo mật tốt với các khóa lớn, có khả năng chống lại nhiều loại tấn công nhưng kích thước văn bản mã hóa lớn hơn so với RSA và ECC.

Ví dụ: ElGamal thường được sử dụng trong các hệ thống yêu cầu mã hóa và chữ ký số đồng thời.

e. Paillier

Paillier là một thuật toán mã hóa đồng cấu (homomorphic encryption), cho phép thực hiện các phép toán trên văn bản mã hóa mà không cần giải mã nó.

Paillier có thể áp dụng cho các hệ thống yêu cầu tính toán bảo mật trên dữ liệu mã hóa, như các dịch vụ lưu trữ đám mây. Tuy vậy, nó có hiệu suất kém hơn so với các thuật toán khác trong các ứng dụng thông thường.

Ví dụ: Paillier thường được sử dụng trong các ứng dụng yêu cầu tính toán trên dữ liệu bí mật mà không cần giải mã, như xử lý dữ liệu tài chính.

Một vài ví dụ thực tiễn

Giao thức SSL/TLS: Trong một phiên SSL/TLS, mã hóa bất đối xứng (thường là RSA hoặc ECC) được sử dụng để trao đổi khóa đối xứng ban đầu. Sau đó, mã hóa đối xứng (thường là AES) được sử dụng để mã hóa các dữ liệu tiếp theo nhằm tối ưu hóa hiệu suất.

Chữ ký số trong email (PGP/GPG): Người gửi sử dụng khóa bí mật của mình để tạo chữ ký số, và người nhận sử dụng khóa công khai của người gửi để xác minh rằng email chưa bị thay đổi và đúng là từ người gửi.

Blockchain: Trong blockchain như Bitcoin, ECC được sử dụng để quản lý khóa ví. Người dùng tạo địa chỉ ví công khai để nhận tiền, và chỉ họ với khóa bí mật tương ứng mới có thể chi tiêu số tiền đó.

1.2. HÀM BĂM

1.2.1. Khái niệm và vai trò của hàm băm trong bảo mật

Hàm băm (hash function) là một hàm toán học có khả năng chuyển đổi dữ liệu đầu vào có kích thước bất kỳ (ví dụ: văn bản, tệp tin, số liệu) thành một chuỗi ký tự có độ dài cố định, gọi là giá trị băm (hash value) hoặc băm (hash). Giá trị này đại diện duy nhất cho dữ liệu ban đầu và thay đổi hoàn toàn nếu chỉ một chút thông tin trong dữ liệu đầu vào bị thay đổi.

Hàm băm có một số đặc tính chủ yếu

Xác định (Deterministic): Cùng một đầu vào luôn cho ra cùng một giá trị băm.

Kích thước cố định: Dù đầu vào có độ dài bất kỳ, đầu ra của hàm băm luôn có kích thước cố định.

Tính nhanh chóng: Hàm băm phải tính toán giá trị băm nhanh chóng ngay cả với lượng dữ liệu lớn.

Kháng va chạm (Collision-resistant): Rất khó hoặc không thể tìm được hai dữ liệu khác nhau có cùng giá trị băm.

Một chiều (One-way): Rất khó hoặc không thể tái tạo dữ liệu gốc từ giá trị băm.

Tính lan truyền (Avalanche Effect): Một thay đổi nhỏ trong dữ liệu đầu vào sẽ gây ra sự thay đổi đáng kể trong giá trị băm.

Vai trò của hàm băm trong bảo mật

Hàm băm đóng vai trò quan trọng trong nhiều lĩnh vực của bảo mật thông tin, giúp đảm bảo tính toàn vẹn và bảo vệ dữ liệu khỏi các cuộc tấn công. Dưới đây là một số vai trò nổi bật:

Đảm bảo tính toàn vẹn của dữ liệu: Hàm băm được sử dụng để kiểm tra tính toàn vẹn của dữ liệu, đảm bảo rằng dữ liệu không bị thay đổi trong quá trình truyền tải hoặc lưu trữ. Ví dụ, khi tải một tệp tin từ internet, một giá trị băm của tệp (thường là SHA-256 hoặc MD5) được cung cấp để người dùng có thể so sánh giá trị băm của tệp tải về với giá trị băm đã được công bố. Nếu các giá trị này khớp nhau, điều đó chứng tỏ tệp không bị thay đổi.

Chữ ký số (Digital Signatures): Trong quá trình tạo chữ ký số, hàm băm được sử dụng để tạo ra một giá trị đại diện duy nhất cho tài liệu hoặc thông điệp. Sau đó, giá trị băm này sẽ được mã hóa bằng khóa bí mật của người gửi để tạo chữ ký số. Người nhận sử dụng khóa công khai của người gửi để kiểm tra chữ ký và đối chiếu giá trị băm với tài liệu ban đầu để xác thực tính toàn vẹn và nguồn gốc.

Mật mã hóa mật khẩu: Trong các hệ thống đăng nhập, thay vì lưu trữ mật khẩu gốc của người dùng, hệ thống thường lưu trữ giá trị băm của mật khẩu. Khi người dùng nhập mật khẩu, hệ thống sẽ băm mật khẩu đó và so sánh giá trị băm với giá trị đã lưu. Điều này giúp bảo vệ mật khẩu khỏi việc bị lộ khi dữ liệu bị tấn công. Các kỹ thuật như salting (thêm một chuỗi ngẫu nhiên vào mật khẩu trước khi băm) giúp tăng cường bảo mật, làm cho việc tấn công từ điển hoặc tấn công Rainbow Table (bảng băm sẵn) trở nên khó khăn hơn.

Blockchain: Trong các hệ thống blockchain như Bitcoin, hàm băm được sử dụng để liên kết các khối (blocks) với nhau và đảm bảo tính toàn vẹn của chuỗi. Mỗi khối chứa một giá trị băm của khối trước đó, làm cho việc thay đổi dữ liệu trong một khối yêu cầu phải thay đổi tất cả các khối sau nó, điều này gần như là không thể. Quá trình khai thác (mining) trong blockchain cũng dựa trên việc tìm ra giá trị băm phù hợp với các yêu cầu nhất định, thông qua các phép tính toán rất phức tạp.

Xác thực dữ liệu trong giao thức truyền thông

Hàm băm được sử dụng trong các giao thức bảo mật như SSL/TLS, IPsec, HMAC (Hashed Message Authentication Code) để đảm bảo rằng các thông điệp không bị thay đổi trong quá trình truyền và để xác thực tính xác thực của các bên tham gia.

HMAC là một kỹ thuật kết hợp giữa khóa bí mật và hàm băm, giúp bảo vệ dữ liệu khỏi tấn công sửa đổi.

Phát hiện virus và malware: Các phần mềm phát hiện virus thường sử dụng hàm băm để so sánh tệp tin với các mẫu virus đã biết. Nếu giá trị băm của một tệp khớp với giá trị băm của một mẫu virus, phần mềm sẽ cảnh báo về sự tồn tại của malware trong hệ thống.

Trong cuộc sống, dấu vân tay là duy nhất đối với mỗi người – không ai có dấu vân tay giống hệt bạn. Dù bạn thay đổi kiểu tóc, quần áo hay thậm chí tên, dấu vân tay của bạn vẫn giữ nguyên, giúp xác định danh tính một cách chính xác.

Tương tự như vậy, trong thế giới số, hàm băm (hash function) tạo ra một chuỗi ký tự duy nhất (gọi là "giá trị băm" hoặc hash value) cho nội dung của một tập tin. Dù tập tin đó có tên gì, nếu

nội dung không thay đổi, “dấu vân tay” này vẫn như cũ. Nhưng chỉ cần một thay đổi nhỏ, ví dụ sửa một chữ cái trong file, giá trị băm sẽ thay đổi hoàn toàn.

Tình huống thực tế: Bạn truy cập trang web chính thức để tải phần mềm diệt virus. Ở trang tải về, bạn thấy dòng chữ thế này:

SHA-256 checksum:
a7c4d8f90b3f83a6a9e84c11d44fcb14d5a21e40ac7a82758a05edc98f6e8b9d

Bạn thắc mắc: “Tại sao họ lại đưa ra cái chuỗi dài ngoằng này?”

Giải thích:

- Chuỗi đó chính là giá trị hàm băm (giống như “dấu vân tay”) của tập tin cài đặt mà bạn sắp tải về.
- Khi bạn tải xong, bạn dùng một công cụ kiểm tra hash (có sẵn trên máy tính hoặc dùng phần mềm như HashCalc, QuickHash...).
- Máy tính tạo ra giá trị hash của tập tin bạn vừa tải và so sánh với chuỗi trên trang web.

Nếu hai chuỗi khớp nhau, bạn biết chắc chắn:

- Tập tin chưa bị thay đổi.
- Không ai can thiệp giữa đường (ví dụ: hacker chèn mã độc).
- Giống như xác minh "đây đúng là tập tin gốc", nhờ "vân tay số" trùng khớp.

Nếu không khớp, bạn biết tập tin đã bị sửa đổi hoặc không an toàn để cài.

Ví dụ thực tế: Google dùng hàm băm để bảo vệ mật khẩu người dùng

Tình huống: Bạn tạo tài khoản Gmail và đặt mật khẩu là “IlovePizza123!”

Nhiều người nghĩ rằng Google sẽ lưu trực tiếp mật khẩu này trong cơ sở dữ liệu. Nhưng KHÔNG! Việc làm như vậy sẽ cực kỳ nguy hiểm nếu bị rò rỉ dữ liệu. Thực tế Google làm gì?

Google (và hầu hết các công ty lớn như Facebook, Twitter...) sẽ không bao giờ lưu mật khẩu thật của bạn. Thay vào đó, họ làm như sau:

Quá trình lưu mật khẩu bằng hàm băm:

1. Khi bạn đăng ký, hệ thống sẽ băm mật khẩu của bạn bằng một thuật toán như SHA-256 hoặc bcrypt.

   - Ví dụ:

IlovePizza123! → a94a8fe5ccb19ba61c4c0873d391e987982fbbd3

2. Họ chỉ lưu chuỗi băm đó trong cơ sở dữ liệu, chứ không lưu mật khẩu gốc.
3. Khi bạn đăng nhập sau này:

   - Bạn nhập lại IlovePizza123!
   - Hệ thống lại băm mật khẩu bạn vừa nhập.

- Nếu kết quả băm trùng khớp với giá trị đã lưu, bạn được cho phép đăng nhập.

Vì sao an toàn?

Không thể đảo ngược: Không ai (kể cả hacker) có thể từ chuỗi băm mà suy ra mật khẩu gốc.

Ngay cả Google cũng không biết mật khẩu của bạn – họ chỉ có "dấu vân tay mật khẩu".

Bảo vệ tốt hơn khi có rò rỉ dữ liệu: Nếu hacker lấy được cơ sở dữ liệu, họ chỉ thấy hàng loạt chuỗi mã hóa – không thể biết bạn dùng mật khẩu gì, trừ khi đoán đúng và thử băm lại.

Hàm băm giúp bảo vệ thông tin cực kỳ quan trọng như mật khẩu của bạn, biến chúng thành những "dấu vân tay số" mà không ai có thể đảo ngược được. Các công ty như Google dùng kỹ thuật này như một tiêu chuẩn bắt buộc trong bảo mật hiện đại.

Hàm băm (hash function) là một công cụ quan trọng trong bảo mật dữ liệu hiện đại, giúp tạo ra một "dấu vân tay số" duy nhất cho mỗi chuỗi thông tin. Ví dụ, khi ta nhập chuỗi văn bản **"BLOCKCHAIN CƠ BẢN"** vào hàm băm SHA-256, kết quả nhận được là một chuỗi mã hóa dài:

9137aac32069619247f358fb5b436da546fd5195b5dc76fe8e2c122a4cd8b9bb

Chuỗi này hoàn toàn đại diện cho nội dung ban đầu và **không thể suy ngược** để lấy lại chuỗi gốc. Điều đặc biệt là, chỉ cần thay đổi một phần nhỏ trong văn bản – chẳng hạn như chuyển từ "CƠ BẢN" sang "cơ bản" trong cụm **"BLOCKCHAIN cơ bản",** hàm băm sẽ cho ra một kết quả hoàn toàn khác:

1b6435469a5b209a1815fa335461666c12802188d4b2c8ebb46e14db915d8a39

Điều này cho thấy tính nhạy cảm với thay đổi của hàm băm: **chỉ một khác biệt nhỏ cũng tạo ra "dấu vân tay số" mới hoàn toàn**. Chính đặc điểm này khiến hàm băm rất hữu ích trong việc xác minh tính toàn vẹn dữ liệu – chẳng hạn như khi tải phần mềm hoặc kiểm tra mật khẩu – vì bất kỳ thay đổi nào cũng dễ dàng bị phát hiện.

1.2.2. Các hàm băm phổ biến

Hàm băm là một thành phần quan trọng trong các hệ thống bảo mật và mật mã học. Nó giúp bảo vệ tính toàn vẹn của dữ liệu, xác thực và bảo mật trong nhiều ứng dụng. Phần này trình bày chi tiết hơn về các hàm băm phổ biến

MD5 (Message Digest Algorithm 5)

Thuật toán MD5 do Ronald Rivest phát triển năm 1991 là phiên bản kế tiếp của MD4, với mục tiêu cải thiện tính bảo mật và hiệu suất. Trước khi bị lỗ hổng bảo mật phát hiện, MD5 được sử dụng rộng rãi trong việc xác minh tính toàn vẹn của dữ liệu.

Ý tưởng của MD5 được thiết kế để chuyển đổi đầu vào có độ dài bất kỳ thành một giá trị băm cố định 128-bit. MD5 sử dụng một quá trình bao gồm 4 vòng lặp xử lý dữ liệu qua một loạt các phép toán bổ sung và dịch chuyển bit.

Thuật toán MD5 chia thông tin đầu vào thành các khối 512-bit, sau đó thực hiện một loạt các phép toán khối XOR, phép toán bổ sung, và dịch chuyển để tạo ra giá trị băm cuối cùng. Quy trình này bao gồm một số vòng lặp với các phép toán bí mật.

Ví dụ: Chuỗi "hello" có mã băm MD5: 5d41402abc4b2a76b9719d911017c592

MD5 có tốc độ tính toán nhanh chóng và dễ dàng triển khai và sử dụng trong nhiều ứng dụng.

Nhược điểm của MD5 là dễ bị tấn công va chạm, nơi hai thông điệp khác nhau có thể cho cùng một giá trị băm. Điều này làm giảm tính an toàn của nó. Một nhược điểm nữa là do các lỗ hổng bảo mật, MD5 không còn an toàn cho các ứng dụng bảo mật như xác thực mật khẩu hay chữ ký số.

MD 5 thường được áp dụng:

+ Kiểm tra tính toàn vẹn của tệp tin: MD5 được sử dụng để xác nhận rằng tệp tin không bị thay đổi khi truyền qua internet.

+ Mã hóa mật khẩu: Trước đây, MD5 được sử dụng để băm mật khẩu trong các hệ thống, nhưng hiện nay đã bị thay thế bởi các thuật toán mạnh mẽ hơn.

SHA-1 (Secure Hash Algorithm 1)

Thuật toán SHA-1 phát triển bởi NSA (Cơ quan An ninh Quốc gia Hoa Kỳ) năm 1993. Thuật toán SHA-1 được sử dụng rộng rãi trong nhiều ứng dụng bảo mật, bao gồm chứng chỉ SSL/TLS, nhưng các nghiên cứu cho thấy SHA-1 không còn an toàn.

Ý tưởng của SHA-1 là tạo ra một giá trị băm 160-bit từ đầu vào có độ dài bất kỳ. Quá trình băm bao gồm các phép toán XOR, phép dịch chuyển bit và bổ sung trong các vòng lặp để tạo ra giá trị băm.

Thuật toán SHA-1 sử dụng 5 khối dữ liệu 32-bit trong 80 vòng lặp. Mỗi vòng lặp áp dụng một phép toán XOR, phép toán bổ sung, và một phép toán logic.

Ví dụ: Chuỗi "hello" băm SHA-1: 2ef7bde608ce5404e97d5f042f95f89f1c232871

SHA-1 là được sử dụng rộng rãi trong các giao thức bảo mật và xác thực số. Đảm bảo tính toàn vẹn của thông tin trong các ứng dụng như chữ ký số và chứng chỉ SSL.

Tuy vậy, SHA-1 có một số nhược điểm:

+ Khả năng va chạm: Từ năm 2005, các nhà nghiên cứu đã chỉ ra rằng SHA-1 dễ bị tấn công va chạm.

+ Khuyến cáo ngừng sử dụng: NIST đã khuyến cáo không sử dụng SHA-1 cho các ứng dụng bảo mật vì tính dễ bị tấn công của nó.

Áp dụng:

+ Chữ ký số và chứng chỉ SSL/TLS: SHA-1 được sử dụng trong quá trình tạo chữ ký số cho các chứng chỉ SSL.

+ Xác thực thông điệp: Trước khi bị thay thế, SHA-1 được sử dụng để xác thực tính toàn vẹn của thông điệp trong giao thức bảo mật.

SHA-2 (Secure Hash Algorithm 2)

Thuật toán SHA-2 phát triển bởi NSA năm 2001 là phiên bản cải tiến của SHA-1, được thiết kế để khắc phục các lỗ hổng của SHA-1.

Ý tưởng của SHA-2 là một họ các hàm băm bao gồm các phiên bản SHA-224, SHA-256, SHA-384, và SHA-512, mỗi phiên bản có độ dài băm khác nhau. Quá trình băm trong SHA-2 sử dụng các phép toán bổ sung, XOR và dịch chuyển để tạo ra giá trị băm an toàn.

Thuật toán SHA-2 áp dụng một loạt các phép toán logic mạnh mẽ hơn SHA-1, với độ dài băm thay đổi tùy thuộc vào phiên bản được sử dụng.

Ví dụ: Chuỗi: "hello" có mã băm SHA-256 là

2cf24dba5fb0a30e26e83b2ac5b9e29e1b169e7e9e1c8e4e58c96d9e2b9bda94

SHA-2 an toàn hơn SHA-1 và MD5, được khuyến nghị cho các ứng dụng bảo mật hiện đại như blockchain, SSL/TLS. Tính bảo mật cao, kháng lại các cuộc tấn công va chạm.

Tốc độ SHA-2 có thể chậm hơn MD5 và SHA-1, nhưng đổi lại nó mang lại tính bảo mật cao hơn.

Áp dụng:

+ Blockchain: SHA-256 được sử dụng trong các blockchain như Bitcoin để bảo mật các giao dịch.

+ Chữ ký số: SHA-2 được sử dụng trong các chứng chỉ SSL/TLS và chữ ký số để đảm bảo tính toàn vẹn và xác thực của dữ liệu.

SHA-3 (Secure Hash Algorithm 3)

Thuật toán SHA-3 được phát triển bởi NIST năm 2015 để thay thế SHA-2 trong trường hợp SHA-2 bị phá vỡ trong tương lai. Thuật toán SHA-3 sử dụng một cấu trúc khác với SHA-2 (Keccak), mang lại tính an toàn cao hơn.

Ý tưởng của SHA-3 sử dụng một cấu trúc khác biệt hoàn toàn gọi là Keccak, một cấu trúc dựa trên phương pháp sponge, khác với các phương pháp dựa trên Merkle–Damgård của SHA-1 và SHA-2.

Thuật toán của Keccak chia thông tin thành các khối và sử dụng các phép toán cộng, XOR, và dịch chuyển bit để tạo ra giá trị băm.

Ví dụ: Chuỗi: "hello" có mã băm SHA-3-256 là
b94d27b9934d3e08a52e52d7da7dabfad3a9c404b85e347506f906420dce2086

Ưu điểm của SHA-3 là có tính an toàn cao, không có lỗi va chạm được phát hiện. Cấu trúc Keccak mạnh mẽ hơn SHA-2 trong việc bảo vệ chống lại các tấn công tiềm ẩn.

Mặc dù mạnh mẽ nhưng SHA-3 chưa được áp dụng rộng rãi như SHA-2.

Áp dụng:

+ Ứng dụng bảo mật cao: SHA-3 có thể được sử dụng trong các ứng dụng bảo mật yêu cầu độ an toàn cực kỳ cao.

+ Blockchain tương lai: Có thể sử dụng SHA-3 thay thế SHA-2 trong các hệ thống blockchain trong tương lai.

BLAKE2

Thuật toán BLAKE2 được phát triển bởi các nhà nghiên cứu Jean-Philippe Aumasson, Samuel Neves, Zooko Wilcox-O'Hearn năm 2012. Sự phát triển: BLAKE2 được thiết kế như một phiên bản thay thế cho MD5 và SHA-2, với hiệu suất cao và bảo mật tốt hơn.

BLAKE2 là một hàm băm nhanh và an toàn, có thể thay thế MD5 và SHA-2 trong nhiều ứng dụng cần tốc độ cao và tính bảo mật.

BLAKE2 sử dụng một cấu trúc Merkle tree và có hiệu suất rất cao khi so với SHA-2.

Ví dụ: Chuỗi "hello" băm BLAKE2b-256: f1d2d2f924e986ac86fdf7b2a5a7f52d

Ưu điểm: Tốc độ nhanh chóng, hiệu suất cao, Bảo mật mạnh mẽ và dễ triển khai.

Nhược điểm: Chưa phổ biến rộng rãi như SHA-2, mặc dù nó mạnh mẽ và nhanh.

Áp dụng:

+ Hệ thống tệp tin: BLAKE2 được sử dụng trong nhiều hệ thống tệp tin và ứng dụng cần tính toán băm nhanh.

+ Phần mềm bảo mật: BLAKE2 được sử dụng trong các phần mềm bảo mật và xác minh dữ liệu.

VRF (Verifiable Random Function)

Hàm băm VRF (Verifiable Random Function) là một hàm băm có tính xác minh, cho phép người tạo ra giá trị ngẫu nhiên không chỉ tính toán nó mà còn cung cấp bằng chứng để người khác có thể xác minh rằng giá trị đó được tạo ra đúng cách, mà không cần tiết lộ khóa bí mật của người tạo. VRF là một thành phần quan trọng trong nhiều hệ thống mật mã, đặc biệt là trong các ứng dụng yêu cầu tính ngẫu nhiên có thể xác minh và bảo mật.

VRF được giới thiệu lần đầu tiên vào cuối những năm 1990 bởi các nhà nghiên cứu như Micali, Rabin và Vadhan, những người đã phát triển các khái niệm về các hàm ngẫu nhiên có thể xác minh trong mật mã. Ban đầu, VRF được phát triển với mục đích tạo ra các giá trị ngẫu nhiên có thể xác minh trong môi trường mật mã phân tán và các hệ thống blockchain. Nó đã trở thành một khái niệm phổ biến trong các ứng dụng hiện đại, đặc biệt là với sự xuất hiện của công nghệ blockchain và các giao thức đồng thuận mới.

VRF hoạt động dựa trên nguyên lý của các hệ thống mã hóa khóa công khai, kết hợp với các hàm băm mật mã. Các bước cơ bản của một VRF bao gồm:

- Bước 1: Tạo cặp khóa
    - Một người dùng tạo ra một cặp khóa bí mật (private key) và khóa công khai (public key). Khóa bí mật được dùng để tính toán giá trị ngẫu nhiên và khóa công khai sẽ được sử dụng để xác minh.
- Bước 2: Tính toán giá trị ngẫu nhiên
    - Người dùng sử dụng khóa bí mật và thông điệp đầu vào (input) để tạo ra một giá trị ngẫu nhiên cùng với bằng chứng mật mã liên quan (proof).

- Bước 3: Xác minh giá trị ngẫu nhiên
    - Người xác minh sử dụng khóa công khai của người tạo ra giá trị, thông điệp đầu vào và bằng chứng mật mã để kiểm tra xem giá trị ngẫu nhiên có thực sự được tạo ra từ thông điệp đầu vào với khóa bí mật tương ứng hay không.

VRF có nhiều ứng dụng quan trọng trong các hệ thống yêu cầu tính ngẫu nhiên có thể xác minh và bảo mật:

- Blockchain và hệ thống đồng thuận: VRF được sử dụng trong nhiều giao thức đồng thuận của blockchain, ví dụ như Algorand. Ở đây, VRF giúp chọn ngẫu nhiên các nhà xác thực khối (validators) trong mạng lưới mà không cần tiết lộ quá trình lựa chọn cho đến khi quá trình hoàn tất. Điều này giúp tăng cường tính bảo mật, ngăn chặn các cuộc tấn công từ bên ngoài nhằm vào các nhà xác thực.
- Quản lý danh tính: VRF có thể được sử dụng để tạo ra các mã nhận dạng (ID) ngẫu nhiên cho các hệ thống quản lý danh tính mà không cần tiết lộ toàn bộ thông tin về người dùng. Điều này bảo vệ quyền riêng tư của người dùng trong các hệ thống yêu cầu bảo mật cao.
- Bầu cử trực tuyến và bỏ phiếu bảo mật: VRF đảm bảo rằng các phiếu bầu hoặc lựa chọn trong một cuộc bầu cử có thể được xác minh mà không tiết lộ chi tiết nhạy cảm, giúp duy trì sự minh bạch và an toàn cho quy trình bầu cử.
- IoT và các hệ thống phân tán: Trong các hệ thống IoT và phân tán, VRF được sử dụng để tạo ra các giá trị ngẫu nhiên an toàn và có thể xác minh trong việc phân phối tài nguyên hoặc quyết định ngẫu nhiên, giúp cải thiện bảo mật và hiệu quả

Mỗi hàm băm có những đặc điểm riêng biệt và phù hợp với các nhu cầu khác nhau. MD5 và SHA-1 đã dần lỗi thời do các lỗ hổng bảo mật, trong khi SHA-2 và SHA-3 đang là các lựa chọn chính trong các ứng dụng bảo mật hiện đại. BLAKE2 là một lựa chọn mới mạnh mẽ với hiệu suất nhanh chóng. Hàm băm ED25519 và hàm băm VRF là các hàm băm được sử dụng trong nền tảng Blockchain Cardano.

1.2.3. Một số ứng dụng của hàm băm

Hàm băm có nhiều ứng dụng trong bảo mật và các hệ thống thông tin, đặc biệt là trong việc đảm bảo tính toàn vẹn của dữ liệu, bảo vệ mật khẩu, và hỗ trợ các giao dịch an toàn. Dưới đây là một số ứng dụng phổ biến của hàm băm:

1.2.3.1. Kiểm tra tính toàn vẹn của phần mềm và tệp tin (Software and File Integrity Checking)

Hàm băm được sử dụng rộng rãi để kiểm tra tính toàn vẹn của phần mềm hoặc tệp tin tải về từ internet, nhằm đảm bảo rằng tệp không bị thay đổi hoặc bị tấn công.

- Tải phần mềm từ website: Các trang web cung cấp phần mềm hoặc tệp tin (như ISO hệ điều hành, phần mềm, tài liệu) thường công bố giá trị băm (MD5, SHA-1 hoặc SHA-256) của tệp. Người dùng có thể tải về phần mềm và tính toán lại giá trị băm của tệp sau khi tải xuống, nếu giá trị băm trùng khớp, tệp không bị thay đổi.

- Phần mềm bảo mật: Các công cụ như Tripwire kiểm tra sự thay đổi của các tệp trong hệ thống và cảnh báo người dùng khi có sự thay đổi không mong muốn. Những thay đổi này có thể là kết quả của phần mềm độc hại hoặc thao tác bất hợp pháp.

1.2.3.2. Hệ thống quản lý mật khẩu (Password Management Systems)

Hàm băm giúp bảo vệ mật khẩu của người dùng trong hệ thống đăng nhập. Khi người dùng tạo mật khẩu, hệ thống không lưu trữ mật khẩu gốc mà lưu trữ giá trị băm của mật khẩu đó. Khi người dùng đăng nhập, hệ thống sẽ băm mật khẩu và so sánh với giá trị băm đã lưu trữ.

Để làm tăng tính bảo mật, khi băm mật khẩu, các hệ thống thêm một chuỗi ngẫu nhiên (salt) vào mật khẩu trước khi tính toán giá trị băm, giúp ngăn chặn các cuộc tấn công từ điển (dictionary attacks) và tấn công vết dầu (rainbow table attacks). Ví dụ: bcrypt và Argon2 sử dụng salt để bảo vệ mật khẩu người dùng.

1.2.3.3. Blockchain và Tiền mã hóa (Cryptocurrency and Blockchain)

Hàm băm là thành phần thiết yếu trong các hệ thống blockchain như Bitcoin, Ethereum, giúp bảo vệ tính toàn vẹn của dữ liệu giao dịch và tạo ra các khối (block) trong chuỗi. Mỗi khối chứa giá trị băm của khối trước đó và giao dịch mới, tạo thành một chuỗi không thể thay đổi.

- Bitcoin: SHA-256 được sử dụng trong việc bảo vệ giao dịch và các khối trong blockchain Bitcoin. Mỗi khối trong chuỗi chứa giá trị băm của khối trước đó, giúp tạo ra một chuỗi liên kết mà không thể thay đổi.

- Ethereum: Ethereum sử dụng SHA-3 để băm các giao dịch và khối trong mạng blockchain của mình.

- Cardano chủ yếu sử dụng Ed25519, Blake2b, VRF, SHA-3 để bảo vệ hệ thống, đồng thời nghiên cứu áp dụng Mithril và ZKPs để tăng cường bảo mật và quyền riêng tư.

1.2.3.4. Chữ ký số (Digital Signatures)

Hàm băm là một phần quan trọng trong chữ ký số, giúp xác thực tính toàn vẹn của dữ liệu và xác minh danh tính người ký. Quy trình tạo chữ ký số bao gồm băm dữ liệu và mã hóa giá trị băm bằng khóa riêng của người ký.

- Chứng chỉ SSL/TLS: Hàm băm như SHA-256 được sử dụng để băm dữ liệu chứng chỉ số trong quy trình tạo và kiểm tra chữ ký số, giúp đảm bảo tính toàn vẹn và xác thực nguồn gốc của các chứng chỉ SSL/TLS.

- Chữ ký điện tử: Các tổ chức, ngân hàng, và dịch vụ điện tử sử dụng chữ ký số để ký hợp đồng, tài liệu, hoặc giao dịch trực tuyến. Ví dụ, chữ ký số trong giao dịch ngân hàng điện tử giúp xác nhận tính hợp pháp của giao dịch.

1.2.3.5. Kiểm tra tính toàn vẹn của cơ sở dữ liệu (Database Integrity Checking)

Trong các hệ thống quản lý cơ sở dữ liệu (DBMS), hàm băm có thể được sử dụng để kiểm tra sự thay đổi của các bản ghi trong cơ sở dữ liệu. Điều này giúp xác định xem có sự truy cập trái phép hoặc thay đổi dữ liệu không mong muốn trong cơ sở dữ liệu hay không.

- Phát hiện gian lận trong giao dịch ngân hàng: Các ngân hàng có thể sử dụng hàm băm để theo dõi các giao dịch tài chính và kiểm tra tính toàn vẹn của dữ liệu.

- Kiểm soát thay đổi: Các công cụ quản lý cơ sở dữ liệu có thể sử dụng hàm băm để xác thực rằng không có sự thay đổi trái phép trong các bản ghi quan trọng của cơ sở dữ liệu.

1.2.3.6. Xác thực thông điệp (Message Authentication)

Hàm băm kết hợp với một khóa bí mật có thể tạo ra mã xác thực thông điệp (MAC) để đảm bảo tính toàn vẹn và xác thực của thông điệp trong các giao dịch điện tử hoặc giao tiếp qua mạng.

- HMAC (Hash-based Message Authentication Code): HMAC sử dụng một hàm băm (như SHA-256) kết hợp với một khóa bí mật để tạo ra mã xác thực cho thông điệp. Điều này giúp bảo vệ các thông điệp khỏi việc bị thay đổi trong quá trình truyền tải. HMAC được sử dụng trong các giao thức bảo mật như SSL/TLS, IPsec và SSH.

- API và Web Services: Trong các giao dịch API hoặc giao tiếp giữa các máy chủ, HMAC được sử dụng để bảo vệ tính toàn vẹn của dữ liệu và ngăn chặn các cuộc tấn công man-in-the-middle.

1.2.3.7. Quản lý dữ liệu và phân tán (Distributed File Systems)

Hàm băm giúp đảm bảo tính toàn vẹn của dữ liệu trong các hệ thống lưu trữ phân tán như IPFS (InterPlanetary File System) và Ceph. Các tệp trong các hệ thống này thường được băm và lưu trữ với giá trị băm làm chỉ mục, giúp xác thực dữ liệu và tìm kiếm nhanh chóng.

- IPFS: Dữ liệu trong IPFS được chia thành các khối, mỗi khối được gán với một giá trị băm duy nhất. Điều này giúp đảm bảo tính toàn vẹn của tệp tin khi lưu trữ và chia sẻ trên mạng phân tán.

- Ceph: Hệ thống lưu trữ phân tán Ceph sử dụng hàm băm để theo dõi và kiểm tra tính toàn vẹn của các tệp trong hệ thống.

1.2.3.8. Xác thực mạng và giao thức an toàn (Network Authentication and Secure Protocols)

Hàm băm là thành phần quan trọng trong việc xác thực các giao thức an toàn như SSL/TLS và IPsec. Chúng giúp bảo vệ dữ liệu khỏi bị thay đổi và đảm bảo tính xác thực của các giao dịch.

- SSL/TLS: Các giao thức bảo mật web như SSL/TLS sử dụng hàm băm để xác thực dữ liệu trong quá trình kết nối giữa máy khách và máy chủ. SHA-256 là một trong các hàm băm phổ biến trong SSL/TLS.

+ IPsec: Trong các mạng riêng ảo (VPN), IPsec sử dụng HMAC để bảo vệ tính toàn vẹn và xác thực của các gói dữ liệu trong khi truyền tải qua mạng.

1.2.3.9. Phát hiện gian lận và chống tấn công (Fraud Detection and Anti-Attack)

Hàm băm có thể giúp phát hiện các hành vi gian lận và các cuộc tấn công trong các hệ thống bảo mật. Ví dụ, trong các hệ thống giao dịch tài chính, hàm băm có thể được sử dụng để kiểm tra các giao dịch nhằm phát hiện các hoạt động bất thường.

- Hệ thống thanh toán trực tuyến: Hệ thống có thể sử dụng hàm băm để kiểm tra các giao dịch bất hợp pháp hoặc gian lận trong các giao dịch tài chính.

- Phát hiện tấn công từ chối dịch vụ (DDoS): Các công cụ bảo mật có thể sử dụng hàm băm để theo dõi các mô hình truy cập và phát hiện các cuộc tấn công từ chối dịch vụ (DDoS) hoặc các cuộc tấn công mạng khác.

Hàm băm có một loạt ứng dụng trong các lĩnh vực bảo mật và công nghệ thông tin hiện đại, từ bảo vệ dữ liệu cá nhân, xác thực thông điệp, đến bảo mật trong các giao dịch blockchain và hệ thống mạng. Việc hiểu rõ và ứng dụng đúng các hàm băm trong từng ngữ cảnh là yếu tố quan trọng để đảm bảo an toàn và tính toàn vẹn của hệ thống.

1.3. CHỮ KÝ SỐ

1.3.1. Khái niệm chữ ký số

Chữ ký số (Digital Signature) là một công nghệ bảo mật dùng để xác thực và bảo vệ tính toàn vẹn của thông tin trong môi trường điện tử. Nó giống như một chữ ký viết tay, nhưng được sử dụng trong các giao dịch và tài liệu điện tử. Chữ ký số giúp đảm bảo rằng thông điệp hoặc tài liệu không bị thay đổi sau khi ký và xác nhận rằng người ký là chính chủ thể mà họ tuyên bố.

Chữ ký số không chỉ giúp xác thực danh tính của người gửi mà còn chứng minh rằng dữ liệu không bị sửa đổi sau khi chữ ký được tạo ra. Để thực hiện ký số, sử dụng các thuật toán mật mã, đặc biệt là mã hóa bất đối xứng, bao gồm khóa công khai và khóa riêng.

1.3.2. Vai trò của chữ ký số

Chữ ký số dùng cho các văn bản số, cho biết toàn bộ văn bản đã được ký bởi người ký. Và người khác có thể xác minh điều này. Chữ ký số tương tự như chữ ký thông thường, đảm bảo nội dung tài liệu là đáng tin cậy, chính xác, không hề thay đổi trên đường truyền và cho biết người tạo ra tài liệu là ai.

Tuy nhiên, chữ ký số khác chữ ký thường, vì nó tuỳ thuộc vào văn bản. Chữ ký số sẽ thay đổi theo văn bản còn chữ ký thường thì không hề thay đổi.

Chữ ký số được sử dụng để cung cấp chứng thực chủ sở hữu, tính toàn vẹn dữ liệu và chống chối bỏ nguồn gốc trong rất nhiều các lĩnh vực.

1.3.3. Các thành phần của chữ ký số

Chữ ký số (Digital Signature) bao gồm các thành phần chính sau, giúp xác thực danh tính của người ký và bảo vệ tính toàn vẹn của thông điệp. Các thành phần này được tạo ra và sử dụng trong quá trình ký và kiểm tra chữ ký số:

1.3.3.1. Thông điệp hoặc tài liệu (Message/Document)

Đây là thông điệp hoặc tài liệu mà người ký muốn bảo vệ và xác thực.

Thông điệp là nội dung mà người ký muốn truyền đạt. Chữ ký số đảm bảo rằng thông điệp này không bị thay đổi sau khi ký và xác nhận danh tính của người ký.

Tính toàn vẹn của thông điệp được bảo vệ nhờ vào việc sử dụng hàm băm và mã hóa giá trị băm.

1.3.3.2. Khóa riêng (Private Key)

Khóa riêng là một phần của cặp khóa bất đối xứng, chỉ thuộc về người ký và được sử dụng để mã hóa giá trị băm của thông điệp.

Khóa riêng giúp người ký tạo ra chữ ký số bằng cách mã hóa giá trị băm của thông điệp. Khóa này được bảo vệ nghiêm ngặt và không được chia sẻ với bất kỳ ai.

Khóa riêng phải được giữ bí mật tuyệt đối. Nếu bị lộ, kẻ tấn công có thể giả mạo chữ ký số của người ký.

1.3.3.3. Khóa công khai (Public Key)

Khóa công khai là phần còn lại của cặp khóa bất đối xứng và được chia sẻ công khai với tất cả người nhận.

Khóa công khai dùng để giải mã chữ ký số mà người nhận nhận được. Bằng cách sử dụng khóa công khai, người nhận có thể kiểm tra xem chữ ký số có hợp lệ hay không và liệu thông điệp có bị thay đổi không.

Khóa công khai có thể được phát tán rộng rãi, miễn là khóa riêng vẫn được bảo vệ an toàn.

1.3.3.4. Giá trị băm (Hash Value)

Giá trị băm là kết quả của quá trình sử dụng hàm băm (ví dụ: SHA-256) trên thông điệp hoặc tài liệu. Đây chính là đại diện số học của thông điệp, được mã hóa để tạo ra chữ ký số.

Giá trị băm là đại diện số học của thông điệp, giúp giảm thiểu kích thước của dữ liệu và tăng tốc quá trình ký. Nó cũng đảm bảo rằng bất kỳ thay đổi nhỏ nào trong thông điệp sẽ dẫn đến sự thay đổi đáng kể trong giá trị băm.

Giá trị băm không thể đảo ngược và không thể bị giả mạo. Điều này giúp đảm bảo tính toàn vẹn của thông điệp trong quá trình truyền tải.

1.3.3.5. Hàm băm (Hash Function)

Hàm băm là một thuật toán mã hóa một chiều được sử dụng để chuyển đổi thông điệp thành giá trị băm có độ dài cố định. Thuật toán dùng để tạo giá trị băm của thông điệp, bảo vệ tính toàn vẹn của nó

Hàm băm đảm bảo tính toàn vẹn của thông điệp. Nếu thông điệp bị thay đổi, giá trị băm sẽ thay đổi và người nhận sẽ nhận ra sự thay đổi này khi kiểm tra chữ ký số.

Các hàm băm phổ biến như SHA-256, SHA-3 có tính chất mạnh mẽ như không có va chạm (collision-resistant) và một chiều (one-way function), giúp bảo vệ thông tin khỏi bị giả mạo.

1.3.3.6. Chữ ký số (Digital Signature)

Chữ ký số là kết quả của việc mã hóa giá trị băm của thông điệp bằng khóa riêng của người ký. Dùng để xác nhận tính hợp lệ của thông điệp

Chữ ký số đảm bảo tính xác thực của người ký và bảo vệ tính toàn vẹn của thông điệp. Chữ ký này sẽ được gửi kèm với thông điệp để người nhận có thể kiểm tra tính hợp lệ.

Chữ ký số không thể giả mạo, vì chỉ có khóa riêng của người ký mới có thể tạo ra chữ ký số. Nếu thông điệp bị thay đổi, chữ ký số sẽ không còn hợp lệ.

Chữ ký số là một công cụ mạnh mẽ trong việc xác thực và bảo vệ thông tin trong môi trường điện tử, giúp đảm bảo tính toàn vẹn của dữ liệu và xác minh danh tính của người ký. Các thành phần của chữ ký số, bao gồm khóa riêng, khóa công khai, giá trị băm, và hàm băm, cùng nhau tạo ra một hệ thống bảo mật mạnh mẽ cho các giao dịch và tài liệu điện tử.

1.3.4. Nguyên lý hoạt động của chữ ký số

Chữ ký số (Digital Signature) hoạt động dựa trên nguyên lý của mã hóa bất đối xứng (asymmetric cryptography) và hàm băm. Quá trình này có mục đích chính là xác thực danh tính của người ký và đảm bảo rằng nội dung của tài liệu hoặc thông điệp không bị thay đổi sau khi ký.

Quy trình chữ ký số gồm hai bước chính: tạo chữ ký số và kiểm tra chữ ký số. Dưới đây là mô tả chi tiết về nguyên lý hoạt động của nó:

1.3.4.1. Tạo chữ ký số

Quá trình tạo chữ ký số của người ký có thể được mô tả qua các bước sau và được mô tả ở hình 1:

Bước 1: Tạo giá trị băm của thông điệp

Người gửi (hoặc người ký) sẽ tính toán giá trị băm của thông điệp hoặc tài liệu cần ký (ví dụ: một hợp đồng điện tử). Để tính toán giá trị băm, người ký sẽ sử dụng một hàm băm (ví dụ: SHA-256). Giá trị băm này là một chuỗi số và ký tự có độ dài cố định, đại diện cho nội dung của thông điệp.

Bước 2: Mã hóa giá trị băm bằng khóa riêng

Sau khi tính toán giá trị băm, người ký sẽ sử dụng khóa riêng của mình (private key) để mã hóa giá trị băm này. Quá trình mã hóa này tạo ra chữ ký số. Chữ ký số này sẽ được đính kèm cùng với thông điệp gửi đến người nhận. Chỉ người sở hữu khóa riêng mới có thể mã hóa và tạo ra chữ ký số, đảm bảo rằng chữ ký này là duy nhất và không thể giả mạo.

Bước 3: Gửi thông điệp và chữ ký số

Người ký sẽ gửi cả thông điệp và chữ ký số đến người nhận. Lúc này, người nhận sẽ có thể sử dụng chữ ký số và thông điệp để xác minh tính hợp lệ của thông điệp và người ký.

1.3.4.2. Kiểm tra chữ ký số

Khi người nhận nhận được thông điệp và chữ ký số, họ sẽ thực hiện các bước sau để kiểm tra tính hợp lệ của chữ ký:

Bước 1: Tạo giá trị băm của thông điệp nhận được

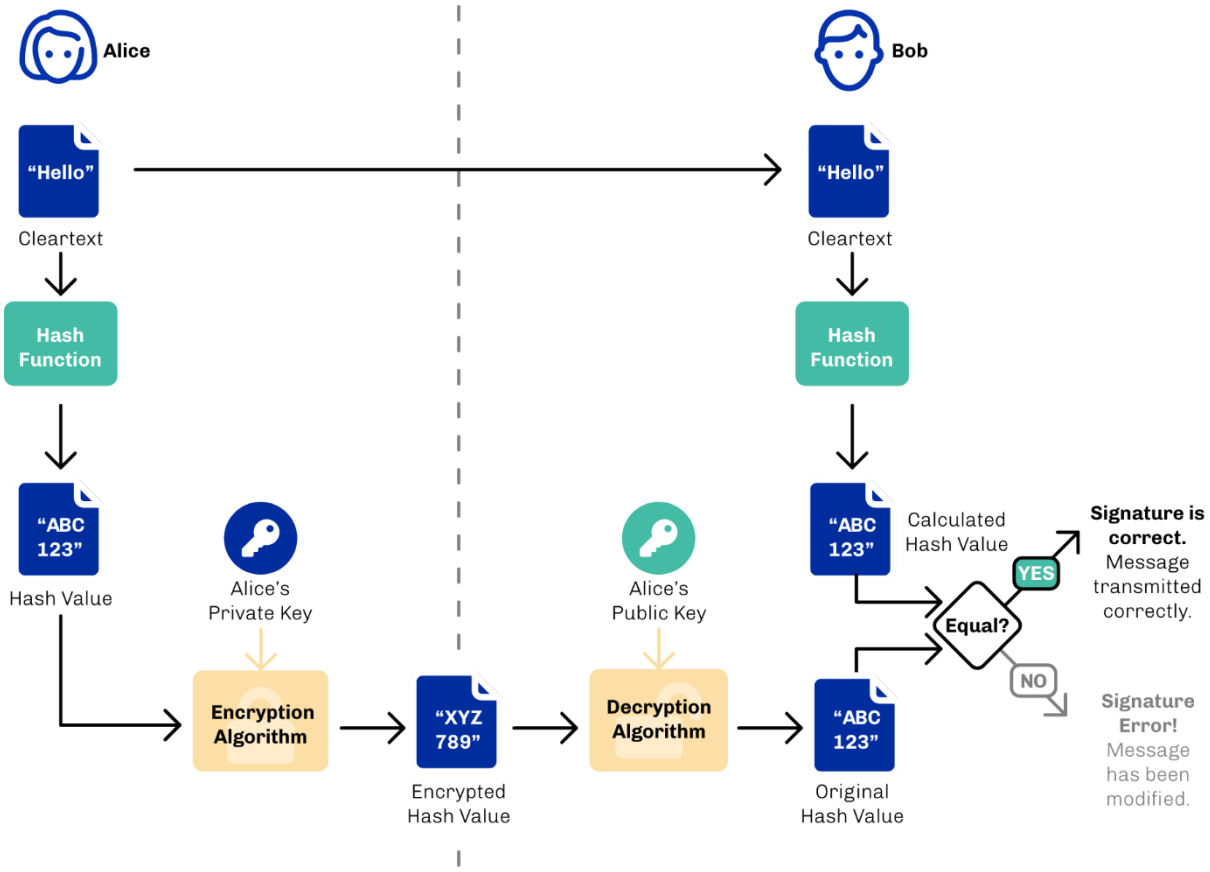
Người nhận sẽ tính toán lại giá trị băm của thông điệp hoặc tài liệu mà họ nhận được bằng cách sử dụng cùng một hàm băm mà người ký đã sử dụng (ví dụ: SHA-256). Điều này tạo ra một giá trị băm mới của thông điệp.

Bước 2: Giải mã chữ ký số bằng khóa công khai

Người nhận sẽ sử dụng khóa công khai của người ký (public key) để giải mã chữ ký số mà họ nhận được. Việc giải mã sẽ trả lại giá trị băm gốc mà người ký đã mã hóa.

Bước 3: So sánh giá trị băm

Người nhận sẽ so sánh giá trị băm mà họ tính toán được (từ thông điệp) với giá trị băm mà họ thu được từ việc giải mã chữ ký số. Nếu hai giá trị băm này khớp nhau, điều đó có nghĩa là thông điệp không bị thay đổi và chữ ký là hợp lệ. Nếu không khớp, nghĩa là thông điệp đã bị thay đổi hoặc chữ ký không hợp lệ.



Hình 1-1: Sơ đồ minh họa quy trình chữ ký số

1.3.5. Ứng dụng chữ ký số

Chữ ký số có nhiều ứng dụng trong các lĩnh vực khác nhau, nhờ tính năng xác thực, bảo mật và đảm bảo tính toàn vẹn của dữ liệu. Dưới đây là các ứng dụng quan trọng của chữ ký số:

1.3.5.1. Giao dịch điện tử và thương mại điện tử

Chữ ký số được sử dụng để ký các hợp đồng điện tử, hóa đơn điện tử, và các tài liệu liên quan đến giao dịch kinh doanh. Nó đảm bảo rằng người gửi và người nhận đều có thể xác minh danh tính của nhau và nội dung không bị thay đổi sau khi ký.

Ví dụ: Trong các hệ thống thương mại điện tử, doanh nghiệp và khách hàng sử dụng chữ ký số để ký hợp đồng mua bán, thanh toán và các thỏa thuận pháp lý khác.

1.3.5.2. Chính phủ điện tử

Chữ ký số là một thành phần quan trọng trong việc triển khai chính phủ điện tử, giúp xác thực danh tính công dân và các cơ quan chính phủ trong các giao dịch trực tuyến.

Ví dụ: Công dân có thể nộp thuế, đăng ký dịch vụ công, hoặc ký các tài liệu hành chính trực tuyến mà không cần phải đến các cơ quan chính phủ.

1.3.5.3. Hóa đơn điện tử (e-Invoice)

Chữ ký số được sử dụng để ký và xác thực tính hợp lệ của hóa đơn điện tử, đảm bảo rằng hóa đơn được gửi đi không thể bị sửa đổi và bên nhận có thể tin tưởng vào tính xác thực của hóa đơn.

Ví dụ: Trong các hệ thống kế toán, doanh nghiệp ký hóa đơn điện tử bằng chữ ký số để gửi đến khách hàng và cơ quan thuế.

1.3.5.4. Bảo mật email và tin nhắn

Chữ ký số giúp bảo mật các email và tin nhắn quan trọng bằng cách đảm bảo rằng nội dung không bị thay đổi và danh tính người gửi được xác thực.

Ví dụ: Trong giao tiếp nội bộ của doanh nghiệp, chữ ký số đảm bảo tính bảo mật và toàn vẹn của thông tin nhạy cảm được truyền qua email.

1.3.5.5. Chứng khoán và giao dịch tài chính

Chữ ký số được sử dụng trong các giao dịch chứng khoán và tài chính để xác thực danh tính của các bên tham gia và đảm bảo rằng các tài liệu tài chính được ký là chính xác và không thể bị thay đổi.

Ví dụ: Các giao dịch mua bán cổ phiếu trực tuyến thường yêu cầu chữ ký số để đảm bảo tính an toàn và hợp pháp của giao dịch.

1.3.5.6. Ngân hàng trực tuyến

Trong ngân hàng trực tuyến, chữ ký số giúp xác thực các giao dịch tài chính, chẳng hạn như chuyển khoản, vay vốn, và mở tài khoản. Điều này giúp giảm thiểu rủi ro gian lận và bảo vệ quyền lợi của khách hàng.

Ví dụ: Khi khách hàng thực hiện giao dịch lớn hoặc ký hợp đồng vay tiền trực tuyến, họ có thể sử dụng chữ ký số để xác nhận.

1.3.5.7. Ký hợp đồng từ xa

Chữ ký số cho phép các bên ký kết hợp đồng từ xa mà không cần gặp mặt trực tiếp. Điều này giúp tiết kiệm thời gian và chi phí trong quá trình ký kết hợp đồng.

Ví dụ: Trong các công ty đa quốc gia, các đối tác ở các quốc gia khác nhau có thể sử dụng chữ ký số để ký kết hợp đồng mà không cần gặp trực tiếp.

1.3.5.8. Xác thực phần mềm

Các nhà phát triển phần mềm sử dụng chữ ký số để ký các ứng dụng, nhằm xác nhận rằng phần mềm đó là đáng tin cậy và không bị thay đổi kể từ khi phát hành.

Ví dụ: Khi tải xuống một ứng dụng từ nhà phát triển đáng tin cậy, chữ ký số trên phần mềm giúp người dùng xác nhận rằng nó không bị chỉnh sửa hoặc chèn mã độc.

1.3.5.9. Blockchain và tiền mã hóa

Chữ ký số là một phần không thể thiếu trong các giao dịch blockchain và tiền mã hóa, giúp xác thực quyền sở hữu và tính toàn vẹn của các giao dịch.

Ví dụ: Trong hệ thống blockchain của Bitcoin và Ethereum, chữ ký số giúp xác nhận rằng một giao dịch được thực hiện bởi chủ sở hữu thực sự của địa chỉ ví tiền mã hóa.

1.3.5.10. Y tế điện tử

Trong lĩnh vực y tế, chữ ký số giúp xác thực hồ sơ bệnh nhân và các tài liệu y khoa điện tử, đảm bảo tính bảo mật và toàn vẹn của thông tin y tế.

Ví dụ: Bác sĩ có thể sử dụng chữ ký số để ký kết hồ sơ khám bệnh và đơn thuốc điện tử, giúp bệnh nhân dễ dàng lưu trữ và quản lý hồ sơ y tế trực tuyến.

1.3.6. Lợi ích và hạn chế của chữ ký số

Chữ ký số mang lại nhiều lợi ích trong việc bảo mật và xác thực giao dịch trực tuyến, đặc biệt trong các lĩnh vực thương mại điện tử, chính phủ điện tử và tài chính. Tuy nhiên, việc triển khai chữ ký số cũng gặp phải một số hạn chế liên quan đến chi phí, tính phức tạp, và các vấn đề pháp lý. Việc sử dụng chữ ký số hiệu quả đòi hỏi phải cân nhắc kỹ lưỡng giữa các lợi ích và hạn chế này.

1.3.6.1. Lợi ích của chữ ký số

a. Tính bảo mật cao

Chữ ký số sử dụng mã hóa bất đối xứng, đảm bảo tính bảo mật cao nhờ việc tách biệt giữa khóa công khai và khóa riêng. Chỉ có người giữ khóa riêng mới có thể tạo ra chữ ký số, trong khi bất kỳ ai cũng có thể sử dụng khóa công khai để xác minh. Chữ ký số giảm thiểu rủi ro giả mạo hoặc chỉnh sửa thông tin trong quá trình truyền tải.

b Xác thực danh tính

Chữ ký số giúp xác thực danh tính của người ký, đảm bảo rằng tài liệu hoặc giao dịch được thực hiện bởi đúng đối tượng. Chữ ký số giúp đảm bảo tính tin cậy trong giao dịch điện tử, ngăn chặn gian lận và giả mạo.

c. Tính toàn vẹn dữ liệu

Hàm băm trong quy trình tạo chữ ký số giúp phát hiện bất kỳ sự thay đổi nào đối với thông tin sau khi ký. Nếu dữ liệu bị chỉnh sửa sau khi ký, chữ ký số sẽ trở nên vô hiệu. Nó đảm bảo rằng thông tin không bị thay đổi trong quá trình truyền tải hoặc lưu trữ.

d. Tính pháp lý

Chữ ký số có tính pháp lý tại nhiều quốc gia, được coi là bằng chứng hợp pháp tương đương với chữ ký tay trong nhiều quy định và luật pháp liên quan đến giao dịch điện tử. Chữ ký số giúp người ký có thể ký kết hợp đồng và các thỏa thuận pháp lý từ xa, giúp tăng cường hiệu quả và tiết kiệm thời gian.

e. Tiết kiệm chi phí và thời gian

Sử dụng chữ ký số giúp loại bỏ nhu cầu in ấn, chuyển phát tài liệu vật lý, cũng như việc ký kết và xác minh thủ công. Chữ ký số giúp tăng cường tốc độ xử lý các giao dịch và giảm chi phí vận hành liên quan đến giấy tờ và chuyển phát.

g. Dễ dàng tích hợp với các hệ thống số hóa

Chữ ký số có thể dễ dàng tích hợp vào các hệ thống quản lý tài liệu, giao dịch điện tử, và các nền tảng thương mại điện tử. Nó giúp nâng cao hiệu suất hoạt động và tự động hóa nhiều quy trình kinh doanh.

1.3.6.2. Hạn chế của chữ ký số

a. Chi phí thiết lập ban đầu

Việc triển khai chữ ký số yêu cầu thiết lập hạ tầng khóa công khai (PKI), bao gồm việc cấp và quản lý chứng thư số (digital certificate) từ các cơ quan chứng thực (CA - Certificate Authority). Do đó chi phí thiết lập và duy trì hệ thống PKI có thể cao, đặc biệt là đối với các tổ chức nhỏ và vừa.

b. Phụ thuộc vào cơ quan chứng thực (CA)

Chữ ký số yêu cầu sự tin cậy vào cơ quan chứng thực (CA) để phát hành và xác nhận chứng thư số của người dùng. Do vậy nếu cơ quan chứng thực bị tấn công hoặc thao túng hoặc ngừng hoạt động, tính bảo mật và tính xác thực của chữ ký số có thể bị ảnh hưởng.

c. Khó khăn trong việc sử dụng cho người không quen thuộc với công nghệ

Người dùng không quen thuộc với các khái niệm liên quan đến chữ ký số, chứng thư số, và mã hóa có thể gặp khó khăn trong việc tạo, quản lý, và sử dụng chữ ký số. Vì vậy cần đào tạo và hỗ trợ kỹ thuật để người dùng nắm bắt cách sử dụng hiệu quả chữ ký số.

d. Thời hạn của chứng thư số

Chứng thư số có thời hạn hiệu lực, và sau khi hết hạn, người dùng cần gia hạn hoặc đăng ký lại chứng thư số mới. Do đó, việc quản lý thời hạn và gia hạn chứng thư số có thể gây ra sự bất tiện, đặc biệt nếu quá trình gia hạn không được thực hiện kịp thời.

e. Vấn đề pháp lý quốc tế

Mặc dù chữ ký số được công nhận tại nhiều quốc gia, nhưng vẫn tồn tại sự khác biệt trong quy định pháp lý giữa các quốc gia về việc công nhận chữ ký số, đặc biệt là trong các giao dịch quốc tế. Như vậy một hạn chế là giao dịch giữa các bên ở các quốc gia khác nhau có thể gặp rào cản pháp lý liên quan đến sự công nhận và sử dụng chữ ký số.

g. Rủi ro mất khóa riêng

Chữ ký số dựa trên việc giữ bí mật khóa riêng của người dùng. Nếu khóa riêng bị mất hoặc bị đánh cắp, chữ ký số của người đó có thể bị giả mạo. Do đó, người dùng cần quản lý khóa riêng một cách cẩn thận để tránh mất mát hoặc lạm dụng.

1.4. HỆ PHI TẬP TRUNG

1.4.1. Khái niệm hệ phi tập trung

Hệ phi tập trung (Decentralized System) là một hệ thống mà quyền kiểm soát và ra quyết định không tập trung vào một thực thể duy nhất, mà được phân chia giữa nhiều nút (nodes) hoặc thành phần riêng lẻ. Trong hệ thống này, không có một đơn vị quyền lực trung tâm có toàn quyền điều khiển, thay vào đó các nút trong hệ thống có vai trò tương đương và hoạt động độc lập hoặc cùng nhau để đạt được mục tiêu chung.

Hệ phi tập trung thường được áp dụng trong các lĩnh vực như blockchain, mạng máy tính, tổ chức tự trị phi tập trung (DAO), và quản trị phi tập trung. Trong hệ thống này, việc phân phối quyền kiểm soát và dữ liệu giúp giảm thiểu rủi ro tập trung, tăng cường bảo mật, và cải thiện tính minh bạch.

1.4.2. Đặc điểm của hệ phi tập trung

Không có trung tâm kiểm soát duy nhất: Quyền ra quyết định và dữ liệu không phụ thuộc vào một thực thể duy nhất.

Tự quản lý và phân tán: Các nút trong hệ thống tự hoạt động và quản lý mà không cần sự can thiệp của trung tâm.

Tăng cường khả năng chịu lỗi: Nếu một hoặc nhiều nút gặp sự cố, hệ thống vẫn có thể tiếp tục hoạt động, giúp tăng độ bền vững.

Minh bạch và không dễ bị giả mạo: Nhờ vào tính phân tán, mọi thay đổi trong hệ thống đều có thể được kiểm tra và theo dõi.

1.4.3. Cấu trúc và mô hình của hệ phi tập trung

Hệ phi tập trung có cấu trúc khác biệt so với hệ tập trung, vì quyền kiểm soát và tài nguyên không tập trung vào một thực thể duy nhất mà được phân phối giữa nhiều nút (nodes). Các thành phần chính trong cấu trúc của một hệ phi tập trung:

1.4.3.1. Các nút (Nodes)

Nút (node) là các thành phần cơ bản trong hệ phi tập trung, có thể là máy tính, máy chủ, hoặc thiết bị cá nhân, mỗi nút có khả năng xử lý và lưu trữ dữ liệu độc lập. Các nút có quyền và trách nhiệm tương đương nhau.

Các nút thực hiện các tác vụ như xác minh, xử lý giao dịch, lưu trữ dữ liệu, và đảm bảo tính toàn vẹn của hệ thống. Một số hệ thống có thể có các nút chuyên biệt như:

- Nút xác minh (Validators): Trong blockchain, các nút này tham gia vào quá trình xác thực giao dịch.

- Nút lưu trữ (Storage Nodes): Lưu trữ dữ liệu và phân phối lại khi được yêu cầu, ví dụ như trong các hệ thống mạng ngang hàng (P2P).

1.4.3.2. Giao thức đồng thuận (Consensus Protocol)

Trong hệ phi tập trung, các nút phải đồng thuận về trạng thái của hệ thống mà không cần sự can thiệp từ một thực thể trung tâm. Để làm điều này, một giao thức đồng thuận được sử dụng nhằm đạt được sự thống nhất giữa các nút về các hành động và thay đổi trong hệ thống.

Ví dụ: Các giao thức đồng thuận[2] phổ biến trong blockchain bao gồm:

- Proof of Work (PoW): Các nút giải các bài toán mật mã để xác nhận giao dịch (sử dụng trong Bitcoin).

- Proof of Stake (PoS): Các nút đóng góp theo số lượng tài sản kỹ thuật số để xác nhận giao dịch (sử dụng trong Ethereum 2.0).

- Delegated Proof of Stake (DPoS): Các nút bỏ phiếu chọn ra các đại diện xác thực giao dịch.

1.4.3.3. Sổ cái phân tán[3] (Distributed Ledger)

Sổ cái phân tán là nơi lưu trữ tất cả các giao dịch hoặc sự kiện đã được xác nhận bởi các nút trong hệ thống. Mỗi nút có một bản sao của sổ cái này và có quyền kiểm tra các giao dịch bất kỳ lúc nào.

Sổ cái phân tán đảm bảo tính minh bạch và toàn vẹn dữ liệu, vì mọi thay đổi đều được ghi lại và phân phối cho tất cả các nút.

Ví dụ: Blockchain là một dạng sổ cái phân tán phổ biến, trong đó mỗi khối (block) chứa các giao dịch và được liên kết với khối trước đó.

1.4.3.4. Cơ chế truyền thông giữa các nút (Peer-to-Peer Communication)

Các nút trong hệ phi tập trung giao tiếp trực tiếp với nhau mà không cần thông qua một máy chủ trung tâm. Giao tiếp giữa các nút thường diễn ra thông qua các giao thức mạng ngang hàng (P2P).

Cơ chế truyền thông giúp đảm bảo rằng các thông điệp và dữ liệu có thể được trao đổi nhanh chóng giữa các nút. Điều này giúp hệ thống tiếp tục hoạt động ngay cả khi một số nút bị ngắt kết nối.

Ví dụ: Trong các mạng P2P như BitTorrent, các máy tính chia sẻ tệp trực tiếp với nhau thay vì thông qua máy chủ trung tâm.

1.4.3.5. Tài nguyên phân tán (Distributed Resources)

Tài nguyên trong hệ phi tập trung không tập trung tại một nơi mà được phân tán giữa các nút. Điều này có thể bao gồm dữ liệu, băng thông, khả năng xử lý hoặc tài sản kỹ thuật số.

Phân tán tài nguyên giúp tăng cường khả năng chịu lỗi của hệ thống và đảm bảo tính sẵn có cao hơn so với hệ thống tập trung.

---

[2] Khái niệm này được trình bày chi tiết trong chương 4 của giáo trình này

[3] Khái niệm này được trình bày chi tiết trong chương 2 của giáo trình này

Ví dụ: Hệ thống lưu trữ phi tập trung như IPFS phân tán dữ liệu trên nhiều nút thay vì lưu trữ toàn bộ tệp tin tại một vị trí duy nhất.

1.4.3.6. Hợp đồng thông minh[4](Smart Contracts) (tùy chọn)

Hợp đồng thông minh là các chương trình tự động hóa các thỏa thuận hoặc giao dịch khi các điều kiện được đáp ứng. Chúng thường được triển khai trên các nền tảng phi tập trung như blockchain.

Hợp đồng thông minh cho phép tự động hóa các quy trình và thực hiện giao dịch mà không cần trung gian.

Ví dụ: Trên blockchain Ethereum, các hợp đồng thông minh có thể tự động thực hiện các giao dịch khi các điều kiện xác định trước được đáp ứng.

1.4.3.7. Bảo mật và mật mã hóa (Security and Cryptography)

Hệ phi tập trung dựa vào các kỹ thuật mật mã để đảm bảo rằng thông tin và giao dịch được bảo vệ khỏi các hành vi giả mạo và xâm nhập. Điều này bao gồm mã hóa dữ liệu, chữ ký số, và các hàm băm để bảo vệ tính toàn vẹn.

Mật mã giúp xác thực danh tính, bảo vệ quyền riêng tư, và đảm bảo tính toàn vẹn của dữ liệu trong hệ thống.

1.4.4. Ưu điểm của cấu trúc phi tập trung và hệ phi tập trung

Với đặc điểm, mô hình như trên cấu trúc phi tập trung có các ưu điểm sau:

- Chống lỗi và tấn công: Không có điểm thất bại duy nhất, hệ thống vẫn có thể hoạt động dù một số nút bị xâm nhập.

- Tăng cường bảo mật: Sử dụng mật mã mạnh và phân tán giúp ngăn ngừa các hành vi giả mạo và đảm bảo an toàn dữ liệu.

- Tính minh bạch cao: Tất cả các giao dịch và thay đổi đều có thể kiểm tra bởi các nút, giúp hệ thống trở nên minh bạch.

Cùng với đó hệ phi tập trung mang lại các lợi ích như:

- Bảo mật và riêng tư cao: Vì không có một điểm tập trung duy nhất để tấn công, hệ thống phi tập trung khó bị xâm phạm hoặc lạm dụng dữ liệu hơn so với hệ thống tập trung.

- Chống kiểm duyệt: Không có cơ quan trung tâm nào có thể can thiệp hoặc kiểm duyệt thông tin trong hệ thống.

- Tăng cường minh bạch và tin cậy: Tất cả các giao dịch hoặc thay đổi trong hệ thống đều có thể được ghi lại và kiểm chứng bởi tất cả các nút.

- Giảm rủi ro lỗi hệ thống: Hệ thống phi tập trung thường có khả năng chịu lỗi cao hơn, bởi không phụ thuộc vào một điểm duy nhất.

[4] Khái niệm hợp đồng thông minh được trình bày chi tiết ở chương xx của giáo trình này

1.4.5. Ứng dụng của hệ phi tập trung

Hệ phi tập trung (decentralized system) có rất nhiều ứng dụng trong các lĩnh vực khác nhau nhờ vào tính bảo mật, minh bạch, khả năng chịu lỗi cao, và khả năng loại bỏ sự phụ thuộc vào các trung gian. Dưới đây là các ứng dụng phổ biến của hệ phi tập trung:

1.4.5.1. Blockchain và tiền mã hóa

Blockchain là một dạng hệ phi tập trung trong đó các giao dịch được lưu trữ trong các khối và liên kết với nhau thành chuỗi. Không có một cơ quan trung ương nào kiểm soát toàn bộ hệ thống, mà thay vào đó các nút mạng (nodes) cùng xác minh và duy trì sổ cái. Ví dụ:

- Bitcoin: Một loại tiền mã hóa phi tập trung, nơi các giao dịch được xác minh thông qua cơ chế đồng thuận Proof of Work (PoW) và không có ngân hàng hoặc tổ chức tài chính trung gian.

- Ethereum: Nền tảng blockchain hỗ trợ hợp đồng thông minh (smart contracts), cho phép thực hiện các giao dịch phi tập trung tự động mà không cần trung gian.

1.4.5.2. Tổ chức tự trị phi tập trung (DAO - Decentralized Autonomous Organization)

DAO là các tổ chức tự vận hành mà không có một quản lý trung tâm. Các quy tắc và quá trình hoạt động của DAO được mã hóa trong các hợp đồng thông minh và các thành viên của DAO có quyền bỏ phiếu quyết định các vấn đề. Ví dụ:

- MakerDAO: Một tổ chức cho phép người dùng tạo ra stablecoin DAI thông qua hợp đồng thông minh mà không cần ngân hàng hoặc tổ chức tài chính.

- Aragon: Một nền tảng giúp dễ dàng tạo và quản lý các tổ chức phi tập trung trên blockchain.

1.4.5.3. Tài chính phi tập trung (DeFi - Decentralized Finance)

DeFi là hệ sinh thái tài chính mà không cần đến các trung gian truyền thống như ngân hàng, công ty tài chính. Các giao dịch như vay, cho vay, mua bán, bảo hiểm, và nhiều dịch vụ tài chính khác được thực hiện thông qua hợp đồng thông minh. Ví dụ:

- Uniswap: Một sàn giao dịch phi tập trung (DEX) cho phép người dùng mua bán tiền mã hóa mà không cần qua trung gian.

- Aave: Nền tảng cho vay phi tập trung cho phép người dùng vay và cho vay tiền mã hóa mà không cần qua ngân hàng.

1.4.5.4. Mạng ngang hàng (P2P - Peer-to-Peer)

Mạng P2P là mạng phi tập trung nơi các thiết bị có thể kết nối và chia sẻ tài nguyên trực tiếp với nhau mà không cần qua máy chủ trung tâm. Ví dụ:

- BitTorrent: Một giao thức chia sẻ tệp ngang hàng cho phép người dùng chia sẻ và tải xuống tệp mà không cần máy chủ tập trung.

- IPFS (InterPlanetary File System): Hệ thống lưu trữ và chia sẻ tệp phi tập trung, giúp cải thiện khả năng truy cập và bảo mật dữ liệu.

1.4.5.5. Truyền thông phi tập trung

Các nền tảng truyền thông phi tập trung không phụ thuộc vào các nhà cung cấp dịch vụ trung gian, giúp tăng cường quyền riêng tư và tránh sự kiểm duyệt. Ví dụ:

- Matrix: Một giao thức truyền thông mã nguồn mở phi tập trung cho phép các hệ thống truyền thông kết nối với nhau.

- Signal: Mặc dù chưa hoàn toàn phi tập trung, Signal sử dụng mã hóa đầu cuối (end-to-end encryption) và đang phát triển theo hướng tăng cường tính phi tập trung.

1.4.5.6. Mạng xã hội phi tập trung

Mạng xã hội phi tập trung cho phép người dùng kiểm soát hoàn toàn nội dung và dữ liệu cá nhân của họ mà không phụ thuộc vào các công ty hoặc nhà cung cấp dịch vụ trung gian. Điều này giúp tránh sự kiểm duyệt và bảo vệ quyền riêng tư tốt hơn. Ví dụ:

- Mastodon: Mạng xã hội phi tập trung nơi người dùng có thể tự tạo máy chủ riêng để quản lý và kiểm soát dữ liệu cá nhân.

- Steemit: Một nền tảng truyền thông xã hội phi tập trung chạy trên blockchain Steem, nơi người dùng được thưởng bằng tiền mã hóa khi đóng góp nội dung.

1.4.5.7. Lưu trữ dữ liệu phi tập trung

Hệ thống lưu trữ dữ liệu phi tập trung giúp phân tán dữ liệu trên nhiều nút, loại bỏ sự phụ thuộc vào các dịch vụ lưu trữ tập trung như Google Drive, Amazon S3. Điều này giúp bảo mật và đảm bảo rằng dữ liệu không dễ bị kiểm duyệt hay mất mát. Ví dụ:

- Storj: Nền tảng lưu trữ dữ liệu phi tập trung sử dụng blockchain và mạng P2P để lưu trữ dữ liệu một cách an toàn.

- Filecoin: Mạng lưu trữ phi tập trung cho phép người dùng thuê không gian lưu trữ từ những người khác trên toàn cầu, đồng thời đảm bảo dữ liệu an toàn và không bị kiểm duyệt.

1.4.5.8. Quản trị phi tập trung

Hệ phi tập trung có thể áp dụng vào các mô hình quản trị, nơi các quyết định được đưa ra dựa trên sự đồng thuận của cộng đồng hoặc tổ chức, mà không phụ thuộc vào một cơ quan hoặc lãnh đạo trung tâm. Ví dụ:

- Liquid Democracy: Mô hình quản trị phi tập trung cho phép công dân hoặc thành viên của một tổ chức bỏ phiếu trực tiếp hoặc ủy quyền cho người khác bỏ phiếu thay mình.

- Tezos: Một blockchain tự quản lý nơi người dùng có thể bỏ phiếu cho các thay đổi hoặc cải tiến của giao thức mà không cần sự can thiệp từ bên ngoài.

1.4.5.9. Hệ thống y tế phi tập trung

Các hệ thống y tế phi tập trung có thể cải thiện việc lưu trữ và chia sẻ dữ liệu bệnh nhân giữa các tổ chức y tế mà không cần phụ thuộc vào cơ quan trung ương. Điều này giúp bảo mật thông tin y tế và cho phép truy cập nhanh chóng đến hồ sơ bệnh nhân. Ví dụ:

- MedRec: Một dự án sử dụng blockchain để lưu trữ và quản lý hồ sơ y tế, cho phép bệnh nhân kiểm soát và chia sẻ dữ liệu y tế của họ.

1.4.5.10. Internet of Things (IoT) phi tập trung

Hệ thống IoT phi tập trung sử dụng blockchain hoặc mạng P2P để kết nối và quản lý các thiết bị mà không cần qua các máy chủ trung tâm. Điều này giúp tăng cường bảo mật và giảm thiểu các điểm thất bại duy nhất trong mạng lưới. Ví dụ:

- IOTA: Một nền tảng blockchain phi tập trung được thiết kế đặc biệt cho mạng IoT, cho phép các thiết bị giao tiếp và trao đổi dữ liệu một cách an toàn mà không cần trung gian.

Ứng dụng của hệ phi tập trung đang mở rộng mạnh mẽ trong nhiều lĩnh vực từ tài chính, y tế, lưu trữ dữ liệu cho đến quản trị. Với khả năng bảo mật cao, minh bạch và loại bỏ sự phụ thuộc vào các trung gian, hệ phi tập trung không chỉ giúp giảm chi phí mà còn tăng cường quyền kiểm soát của người dùng và tính bền vững của hệ thống.

1.5. HỆ PHÂN TÁN

1.5.1. Khái niệm hệ phân tán

Hệ phân tán (distributed system) là một tập hợp các máy tính độc lập kết hợp với nhau để tạo thành một hệ thống thống nhất, hoạt động như một thực thể duy nhất. Trong hệ thống này, các thành phần có thể nằm ở các vị trí khác nhau, và chúng giao tiếp với nhau qua mạng để thực hiện các tác vụ chung. Mục tiêu của hệ phân tán là cung cấp hiệu suất cao, tính sẵn sàng, và khả năng chịu lỗi trong khi hoạt động trên nhiều máy tính riêng biệt.

Một **hệ thống phi tập trung** là hệ thống trong đó **không có trung tâm điều khiển duy nhất** – thay vào đó, mọi thành phần trong hệ thống đều có quyền ra quyết định hoặc đóng vai trò quan trọng tương đương nhau.

Hãy tưởng tượng một công ty giao hàng như **GrabExpress**: mỗi tài xế hoạt động **độc lập**, không cần trở về "trung tâm" để nhận hàng. Họ nhận đơn từ ứng dụng, trực tiếp đi lấy hàng từ người gửi, rồi giao đến người nhận. Grab chỉ cung cấp nền tảng kết nối – không điều khiển từng bước chi tiết của tài xế.

Bảng 4: Mô tả hệ thống phi tập trung và một ứng dụng thực tế

So sánh chi tiết:		
Tiêu chí	**Hệ thống phi tập trung**	**Mạng lưới giao hàng Grab**
Trung tâm điều khiển	Không có trung tâm cố định, các nút cùng chia sẻ quyền xử lý	Grab chỉ đóng vai trò kết nối, không kiểm soát từng tài xế
Tính linh hoạt	Nếu một nút lỗi, hệ thống vẫn tiếp tục hoạt động	Nếu một tài xế huỷ đơn, đơn sẽ được chuyển cho tài xế khác
Phân tán nhiệm vụ	Các nút xử lý thông tin và đưa ra quyết định cục bộ	Mỗi tài xế tự quyết định nhận đơn nào, đi tuyến đường nào

Ứng dụng thực tế	Blockchain, mạng P2P, web 3.0	Giao hàng theo mô hình chia sẻ tài nguyên (sharing economy)

Mạng lưới giao hàng như Grab hoạt động theo mô hình **phi tập trung**: mỗi tài xế là một "nút" độc lập trong hệ thống, không cần quay về trung tâm để lấy hàng hay nhận lệnh. Tất cả được điều phối tự động qua ứng dụng, giúp hệ thống linh hoạt và mở rộng dễ dàng.

1.5.2. Đặc điểm của hệ phân tán

Tính độc lập: Các thành phần của hệ thống phân tán có thể hoạt động độc lập và không cần phải ở cùng một địa điểm.

Tính đồng thời: Các quá trình hoặc thành phần trong hệ phân tán có thể hoạt động đồng thời, thực hiện các tác vụ một cách song song.

Khả năng mở rộng: Hệ phân tán dễ dàng mở rộng bằng cách thêm các tài nguyên (máy tính hoặc phần cứng) mà không làm gián đoạn hệ thống.

Tính chịu lỗi: Hệ phân tán có khả năng chịu lỗi tốt, tức là nếu một hoặc một vài thành phần bị hỏng, hệ thống vẫn có thể hoạt động bình thường hoặc với hiệu suất giảm nhẹ.

1.5.3. Các mô hình hệ phân tán

Trong các hệ thống phân tán, có nhiều mô hình khác nhau để tổ chức và quản lý các thành phần của hệ thống. Mỗi mô hình sẽ phù hợp với các mục tiêu, yêu cầu khác nhau của hệ thống như hiệu suất, tính sẵn sàng, bảo mật, khả năng mở rộng, và độ phức tạp. Dưới đây là một số mô hình phổ biến trong hệ phân tán:

1.5.3.1. Mô hình Máy khách - Máy chủ (Client-Server)

Mô hình máy khách - máy chủ là một trong những mô hình đơn giản và phổ biến nhất trong hệ phân tán. Trong mô hình này, có hai loại nút chính:

- Máy khách (Client): Máy khách là các nút gửi yêu cầu đến máy chủ và nhận phản hồi từ máy chủ. Máy khách thường là các thiết bị đầu cuối như trình duyệt web hoặc ứng dụng người dùng.

- Máy chủ (Server): Máy chủ là các nút cung cấp dịch vụ hoặc tài nguyên cho các máy khách. Máy chủ nhận yêu cầu từ máy khách, xử lý chúng và trả về kết quả.

Ưu điểm của mô hình là dễ triển khai, dễ bảo trì, dễ kiểm soát vì có máy chủ trung tâm. Nhược điểm của nó là máy chủ có thể bị quá tải nếu có quá nhiều máy khách đồng thời yêu cầu dịch vụ, và mô hình này có thể không chịu lỗi tốt nếu máy chủ trung tâm gặp sự cố.

Ví dụ: Mô hình ứng dụng web truyền thống, nơi máy khách (trình duyệt) gửi yêu cầu HTTP đến máy chủ web và nhận lại trang web.

1.5.3.2. Mô hình Ngang hàng (Peer-to-Peer - P2P)

Trong mô hình Peer-to-Peer, tất cả các nút trong hệ thống đều có quyền và trách nhiệm như nhau. Không có một máy chủ trung tâm, và mỗi nút có thể vừa là máy khách vừa là máy chủ, chia sẻ tài nguyên và dịch vụ trực tiếp với các nút khác.

Ưu điểm của P2P là không có điểm thất bại duy nhất, dễ dàng mở rộng, và tài nguyên được phân phối đồng đều giữa các nút. P2P có nhược điểm là quản lý hệ thống và bảo mật phức tạp hơn do không có máy chủ trung tâm, và các nút có thể không luôn sẵn sàng hoặc đáng tin cậy.

Ví dụ: Mạng chia sẻ tệp như BitTorrent, nơi người dùng tải lên và tải xuống tệp từ các máy tính khác mà không cần một máy chủ trung tâm.

1.5.3.3. Mô hình Đa tầng (Multi-tier)

Mô hình đa tầng (hay còn gọi là mô hình ba tầng trong ứng dụng web) chia hệ thống phân tán thành nhiều tầng để phân chia các nhiệm vụ cụ thể, giúp hệ thống có tính linh hoạt và dễ bảo trì hơn.

Các tầng phổ biến trong mô hình đa tầng bao gồm:

- Tầng giao diện người dùng (Presentation Layer): Đây là tầng mà người dùng tương tác, chẳng hạn như trình duyệt web hoặc ứng dụng di động.

- Tầng logic xử lý (Business Logic Layer): Tầng này chứa các logic xử lý nghiệp vụ và quy trình xử lý yêu cầu từ người dùng.

- Tầng cơ sở dữ liệu (Data Layer): Tầng này quản lý cơ sở dữ liệu, nơi lưu trữ và truy xuất dữ liệu.

Mô hình này có ưu điểm là dễ dàng bảo trì, mở rộng và phân chia trách nhiệm giữa các tầng. Tuy vậy các tầng có thể tạo ra độ trễ do yêu cầu phải đi qua nhiều bước, đặc biệt là trong môi trường mạng.

Ví dụ: Ứng dụng web ba tầng (web application) với tầng giao diện người dùng (UI), tầng xử lý nghiệp vụ (Business Logic), và tầng cơ sở dữ liệu (Database).

1.5.3.4. Mô hình Hệ thống Tệp phân tán (Distributed File System - DFS)

Trong mô hình này, hệ thống tệp phân tán cung cấp một cách tiếp cận để lưu trữ và truy cập dữ liệu từ nhiều nút phân tán mà người dùng có thể truy cập như thể dữ liệu đó nằm trên một hệ thống tệp duy nhất.

Các tệp được chia thành các khối dữ liệu nhỏ, phân tán trên nhiều máy chủ, và người dùng có thể truy cập chúng thông qua một hệ thống giao diện chung.

Ưu điểm của mô hình là dễ dàng mở rộng, có khả năng chịu lỗi tốt, và cung cấp khả năng truy cập tệp từ bất kỳ nút nào trong hệ thống. Tuy vậy, trong mô hình này việc quản lý nhất quán tệp và đồng bộ hóa giữa các nút có thể gặp khó khăn.

Ví dụ: Hadoop Distributed File System (HDFS), Google File System (GFS).

1.5.3.5. Mô hình Hệ thống Cơ sở dữ liệu phân tán (Distributed Database System)

Hệ thống cơ sở dữ liệu phân tán chia cơ sở dữ liệu thành nhiều phần và phân phối chúng trên nhiều nút trong hệ thống. Các nút này có thể thực hiện các tác vụ lưu trữ và truy vấn dữ liệu đồng thời, nhằm cải thiện hiệu suất và khả năng chịu lỗi của hệ thống.

Ưu điểm của mô hình này là dễ dàng mở rộng, dữ liệu được phân phối đồng đều, và hệ thống có khả năng chịu lỗi cao. Tuy vậy sự đồng bộ hóa và duy trì tính nhất quán giữa các bản sao dữ liệu có thể phức tạp.

Ví dụ: Hệ thống cơ sở dữ liệu NoSQL như MongoDB, Cassandra, hoặc hệ thống cơ sở dữ liệu SQL phân tán như Google Spanner.

1.5.3.6. Mô hình Đám mây (Cloud Computing)

Mô hình đám mây sử dụng các tài nguyên phân tán từ nhiều máy chủ đặt tại các trung tâm dữ liệu khác nhau và cung cấp các dịch vụ qua Internet. Người dùng có thể truy cập các dịch vụ này mà không cần phải lo lắng về cơ sở hạ tầng phần cứng.

Mô hình đám mây có khả năng mở rộng linh hoạt, tiết kiệm chi phí phần cứng, và dễ dàng tiếp cận các dịch vụ và tài nguyên từ xa. Mô hình này phụ thuộc vào kết nối Internet, và các vấn đề bảo mật có thể phát sinh khi lưu trữ dữ liệu trên đám mây.

Ví dụ: Amazon Web Services (AWS), Microsoft Azure, Google Cloud.

1.5.3.7. Mô hình Tính toán đám mây phân tán (Edge Computing)

Trong mô hình tính toán đám mây phân tán, các tài nguyên và dịch vụ được phân tán ra gần với người dùng hoặc thiết bị (edge devices), thay vì tập trung vào các trung tâm dữ liệu lớn.

Ưu điểm của mô hình là giảm độ trễ, tiết kiệm băng thông, và xử lý dữ liệu nhanh chóng gần nguồn gốc. Mô hình có nhược điểm là quản lý và bảo mật dữ liệu trở nên phức tạp hơn.

Ví dụ: Các ứng dụng IoT, nơi dữ liệu được xử lý ngay tại các thiết bị cảm biến hoặc các nút mạng gần người dùng.

1.5.4. Tính chất của hệ phân tán

- Tính minh bạch (Transparency):

+ Minh bạch về truy cập: Người dùng không cần biết vị trí thực của tài nguyên (dữ liệu, dịch vụ) trong hệ phân tán, chỉ cần sử dụng như thể nó cục bộ.

+ Minh bạch về vị trí: Người dùng không cần biết tài nguyên đang nằm ở máy nào trong mạng.

+ Minh bạch về lỗi: Hệ thống có khả năng che giấu lỗi và phục hồi một cách tự động, giúp hệ thống vẫn duy trì hoạt động.

+ Minh bạch về tính di động: Tài nguyên hoặc tiến trình có thể di chuyển trong hệ thống mà không ảnh hưởng đến người dùng.

- Tính mở (Openness):

Hệ phân tán có thể dễ dàng mở rộng và kết hợp thêm các thành phần mới mà không ảnh hưởng đến hệ thống hiện tại.

Các thành phần trong hệ thống giao tiếp với nhau qua các giao thức chuẩn và dễ tương tác với các hệ thống khác.

- Tính đồng bộ và không đồng bộ (Synchronous and Asynchronous):

Trong hệ phân tán, có thể có các hệ thống đồng bộ, nơi các thành phần giao tiếp với nhau với một tốc độ xác định. Tuy nhiên, phần lớn hệ thống phân tán là không đồng bộ, trong đó các thành phần không cần phải chờ đợi nhau.

- Tính không tập trung (Decentralization):

Không có máy chủ trung tâm quản lý tất cả, các máy tính trong hệ phân tán thường có quyền quản lý và điều hành ngang nhau, giúp giảm thiểu rủi ro tập trung và tăng cường khả năng chịu lỗi.

- Tính chịu lỗi (Fault Tolerance):

Hệ phân tán có khả năng tiếp tục hoạt động dù một số thành phần bị lỗi. Các cơ chế như sao lưu, dự phòng và phát hiện lỗi giúp hệ thống duy trì được tính khả dụng cao.

- Tính nhất quán (Consistency):

Dữ liệu và trạng thái của hệ thống phải được duy trì nhất quán giữa các thành phần trong hệ phân tán. Có thể có nhiều mức độ nhất quán như nhất quán mạnh, nhất quán yếu hoặc nhất quán cuối cùng (eventual consistency).

- Tính khả dụng (Availability):

Hệ thống phải luôn sẵn sàng để phục vụ các yêu cầu của người dùng, ngay cả khi một số nút trong hệ thống không hoạt động.

- Tính mở rộng (Scalability):

Hệ phân tán có khả năng mở rộng dễ dàng khi nhu cầu tài nguyên tăng lên. Điều này bao gồm cả mở rộng về kích thước của hệ thống lẫn số lượng người dùng hoặc khối lượng công việc.

- Tính đối xứng (Symmetry):

Trong một số hệ phân tán, các thành phần có thể có vai trò tương đương nhau, không phân biệt rõ ràng máy chủ (server) và máy khách (client).

Những tính chất này giúp hệ phân tán trở thành một giải pháp hiệu quả trong nhiều tình huống, từ hệ thống lưu trữ dữ liệu, dịch vụ đám mây đến mạng lưới Internet of Things (IoT).

1.5.5. Quản lý đồng bộ và tính toàn vẹn

Quản lý đồng bộ (synchronization) và tính toàn vẹn (integrity) là những thách thức quan trọng trong hệ phân tán. Các khía cạnh này liên quan đến việc đảm bảo rằng các tiến trình hoặc nút trong hệ thống có thể hoạt động cùng nhau mà không xảy ra mâu thuẫn dữ liệu hay sai lệch trạng thái.

1.5.5.1. Quản lý đồng bộ trong hệ phân tán:

Đồng bộ trong hệ phân tán liên quan đến việc đảm bảo các tiến trình hoạt động một cách phối hợp và tránh xung đột truy cập tài nguyên hoặc dữ liệu dùng chung.

Cơ chế khóa (Locking Mechanisms): Một phương pháp phổ biến để quản lý đồng bộ là sử dụng các cơ chế khóa như mutexes, semaphores, hoặc giao thức phân phối token. Điều này ngăn chặn nhiều tiến trình cùng truy cập một tài nguyên tại cùng thời điểm, dẫn đến tranh chấp tài nguyên.

Đồng bộ theo thời gian (Clock Synchronization): Trong hệ phân tán, các tiến trình trên các máy khác nhau có thể có thời gian hệ thống không đồng bộ. Một số thuật toán được sử dụng để đồng bộ hóa thời gian giữa các nút như thuật toán NTP (Network Time Protocol), thuật toán Berkeley và Lamport Timestamps (để đồng bộ thứ tự các sự kiện).

1.5.5.2. Tính toàn vẹn dữ liệu trong hệ phân tán:

Tính toàn vẹn dữ liệu đảm bảo rằng dữ liệu không bị thay đổi hoặc hỏng hóc khi di chuyển qua các nút khác nhau của hệ phân tán.

Phân cấp đồng bộ hóa (Hierarchical Synchronization): Một số hệ phân tán sử dụng các phương pháp phân cấp để đảm bảo tính toàn vẹn dữ liệu trong các trường hợp không đồng bộ hoàn toàn giữa các nút.

Kiểm soát truy cập song song (Concurrency Control): Kiểm soát song song là một kỹ thuật đảm bảo rằng các giao dịch hoặc truy vấn từ nhiều người dùng được xử lý theo cách duy trì tính nhất quán của dữ liệu. Ví dụ: cơ chế Two-Phase Locking (2PL) thường được sử dụng trong hệ thống cơ sở dữ liệu phân tán.

Các mô hình nhất quán (Consistency Models): Trong hệ phân tán, có nhiều cấp độ nhất quán khác nhau, từ nhất quán mạnh (strong consistency) cho đến nhất quán cuối cùng (eventual consistency). Việc lựa chọn mô hình nhất quán phụ thuộc vào yêu cầu của hệ thống, giữa tính khả dụng và tính nhất quán.

1.5.5.3. Thách thức trong quản lý đồng bộ và tính toàn vẹn:

Độ trễ mạng (Network Latency): Do các nút trong hệ phân tán có thể nằm ở những vị trí địa lý khác nhau, độ trễ mạng và băng thông có thể ảnh hưởng đến việc đồng bộ hóa dữ liệu, dẫn đến sự sai lệch thời gian.

Phân vùng mạng (Network Partitioning): Các vấn đề về phân vùng mạng có thể gây ra các trạng thái không đồng bộ, ảnh hưởng đến tính toàn vẹn dữ liệu. Các thuật toán như Paxos và Raft được sử dụng để duy trì sự đồng thuận trong điều kiện mạng không đáng tin cậy.

1.5.5.4. Các giải pháp quản lý đồng bộ và tính toàn vẹn:

Thuật toán phân tán (Distributed Algorithms): Nhiều thuật toán đã được phát triển để quản lý đồng bộ và tính toàn vẹn như Chandy-Lamport Snapshot Algorithm, Bully Algorithm, và Paxos.

Replication: Bản sao (replica) dữ liệu trên nhiều nút giúp đảm bảo tính sẵn sàng và toàn vẹn. Tuy nhiên, việc đồng bộ giữa các bản sao cần các chiến lược mạnh mẽ để tránh các vấn đề về nhất quán.

Cơ chế đồng thuận (Consensus Mechanisms): Các hệ thống phân tán có thể sử dụng các cơ chế đồng thuận như Paxos hoặc Raft để đảm bảo rằng tất cả các nút đồng thuận về một giá trị cụ thể trước khi tiếp tục các tác vụ khác.

1.5.6. Ứng dụng của hệ phân tán

Hệ phân tán có nhiều ứng dụng trong các lĩnh vực khác nhau, từ công nghệ thông tin, tài chính, y tế đến giải trí và nghiên cứu khoa học. Dưới đây là một số ứng dụng phổ biến của hệ phân tán:

1.5.6.1. Điện toán đám mây (Cloud Computing):

Điện toán đám mây là một trong những ứng dụng phổ biến nhất của hệ phân tán, cho phép người dùng truy cập tài nguyên tính toán và lưu trữ dữ liệu qua mạng Internet.

Các nền tảng như Amazon Web Services (AWS), Google Cloud Platform (GCP) và Microsoft Azure đều dựa trên mô hình hệ phân tán để cung cấp dịch vụ cơ sở hạ tầng (IaaS), nền tảng (PaaS) và phần mềm (SaaS) cho người dùng toàn cầu.

Các dịch vụ như lưu trữ đám mây (cloud storage), tính toán đám mây (cloud computing), và mạng phân phối nội dung (Content Delivery Networks - CDN) đều sử dụng hệ phân tán để đảm bảo tính khả dụng và khả năng mở rộng.

1.5.6.2. Cơ sở dữ liệu phân tán (Distributed Databases):

Cơ sở dữ liệu phân tán cho phép lưu trữ và quản lý dữ liệu trên nhiều máy chủ trong một mạng. Điều này giúp tăng khả năng chịu lỗi, mở rộng dễ dàng và giảm độ trễ truy cập.

Các hệ thống như Google Spanner, Amazon DynamoDB, Apache Cassandra, và MongoDB sử dụng kiến trúc phân tán để quản lý dữ liệu hiệu quả và đảm bảo tính nhất quán.

Các cơ chế đồng bộ hóa và phân vùng dữ liệu giúp đảm bảo dữ liệu được sao lưu và đồng bộ giữa các máy chủ, phục vụ cho các ứng dụng yêu cầu hiệu suất cao.

1.5.6.3. Blockchain và tiền điện tử (Cryptocurrency):

Blockchain là một ứng dụng điển hình của hệ thống phân tán, nơi dữ liệu được lưu trữ trên một mạng các nút (nodes) và được duy trì thông qua các thuật toán đồng thuận như Proof of Work (PoW) hoặc Proof of Stake (PoS).

Các ứng dụng như Bitcoin, Ethereum và nhiều loại tiền điện tử khác hoạt động dựa trên hệ thống phân tán, không có một thực thể trung tâm quản lý, giúp tăng cường tính bảo mật, minh bạch và phi tập trung.

Blockchain cũng có các ứng dụng khác ngoài tiền điện tử, bao gồm hợp đồng thông minh (smart contracts), quản lý chuỗi cung ứng, và quản lý tài sản số.

1.5.6.4. Hệ thống file phân tán (Distributed File Systems):

Hệ thống file phân tán giúp lưu trữ và truy xuất dữ liệu trên nhiều máy chủ, cho phép các ứng dụng và người dùng có thể truy cập dữ liệu từ xa một cách dễ dàng.

Các hệ thống như Google File System (GFS), Hadoop Distributed File System (HDFS), và Ceph là những ví dụ điển hình về hệ thống file phân tán, thường được sử dụng trong các ứng dụng dữ liệu lớn (Big Data).

Những hệ thống này đảm bảo tính sẵn sàng và khả năng mở rộng, đồng thời giúp dữ liệu an toàn và đồng bộ.

1.5.6.5. Ứng dụng mạng xã hội và truyền thông (Social Networking and Communication):

Các mạng xã hội như Facebook, Twitter, Instagram, và các ứng dụng nhắn tin như WhatsApp, Telegram đều dựa vào hệ phân tán để xử lý hàng tỷ yêu cầu mỗi ngày.

Hệ thống phân tán giúp các mạng xã hội mở rộng quy mô, lưu trữ và quản lý lượng dữ liệu khổng lồ, đồng thời cung cấp nội dung theo thời gian thực cho người dùng trên toàn cầu.

Các dịch vụ truyền thông dựa trên hệ phân tán cũng sử dụng các kỹ thuật caching (bộ nhớ đệm) và CDN để cải thiện tốc độ truy cập và độ ổn định.

1.5.6.6. Hệ thống quản lý tài chính và ngân hàng (Financial and Banking Systems):

Các hệ thống thanh toán điện tử, ngân hàng trực tuyến và hệ thống giao dịch chứng khoán cũng sử dụng hệ phân tán để đảm bảo tính khả dụng, khả năng mở rộng và bảo mật.

Ví dụ, Visa, MasterCard, và các hệ thống giao dịch chứng khoán quốc tế đều dựa trên mô hình phân tán để xử lý hàng triệu giao dịch mỗi giây.

Các dịch vụ thanh toán như PayPal, Stripe, Square và các hệ thống quản lý tiền tệ khác cũng sử dụng hệ phân tán để đảm bảo giao dịch nhanh chóng và an toàn.

1.5.6.6. Ứng dụng dữ liệu lớn (Big Data Analytics):

Hệ phân tán là nền tảng của các ứng dụng dữ liệu lớn, nơi các công cụ như Apache Hadoop, Apache Spark, và Google MapReduce được sử dụng để xử lý và phân tích khối lượng lớn dữ liệu trên các hệ thống máy tính phân tán.

Các tổ chức như Google, Amazon, Facebook sử dụng các công cụ này để phân tích hành vi người dùng, tối ưu hóa hệ thống và cải thiện hiệu suất dịch vụ.

Hệ thống dữ liệu lớn yêu cầu khả năng mở rộng cao và chịu lỗi tốt, điều mà các hệ thống phân tán có thể cung cấp.

1.5.6.7. IoT (Internet of Things):

Mạng IoT là một hệ thống phân tán với hàng triệu thiết bị kết nối và chia sẻ dữ liệu với nhau. Các ứng dụng của IoT trong nhà thông minh, y tế, giao thông và công nghiệp đều dựa vào hệ thống phân tán để quản lý và xử lý dữ liệu từ các cảm biến và thiết bị.

Các nền tảng như AWS IoT, Google Cloud IoT, và Microsoft Azure IoT Hub cung cấp các dịch vụ dựa trên hệ phân tán để quản lý các thiết bị IoT và dữ liệu được tạo ra.

1.5.6.8. Trò chơi trực tuyến (Online Gaming):

Các trò chơi trực tuyến nhiều người chơi (MMO) như World of Warcraft, Fortnite, và League of Legends sử dụng hệ phân tán để quản lý hàng triệu người chơi trên toàn thế giới.

Hệ thống phân tán giúp giảm độ trễ và đảm bảo các trải nghiệm game thời gian thực ổn định cho người chơi dù họ ở các vị trí địa lý khác nhau.

Việc sử dụng các máy chủ phân tán cũng giúp trò chơi có khả năng mở rộng khi số lượng người chơi tăng lên.

1.5.6.9. Ứng dụng trí tuệ nhân tạo (Artificial Intelligence):

Các hệ thống AI và học máy (machine learning) thường yêu cầu khối lượng lớn tài nguyên tính toán và dữ liệu. Các mô hình như TensorFlow và PyTorch có thể được triển khai trên các hệ phân tán để đào tạo và suy luận trên dữ liệu lớn.

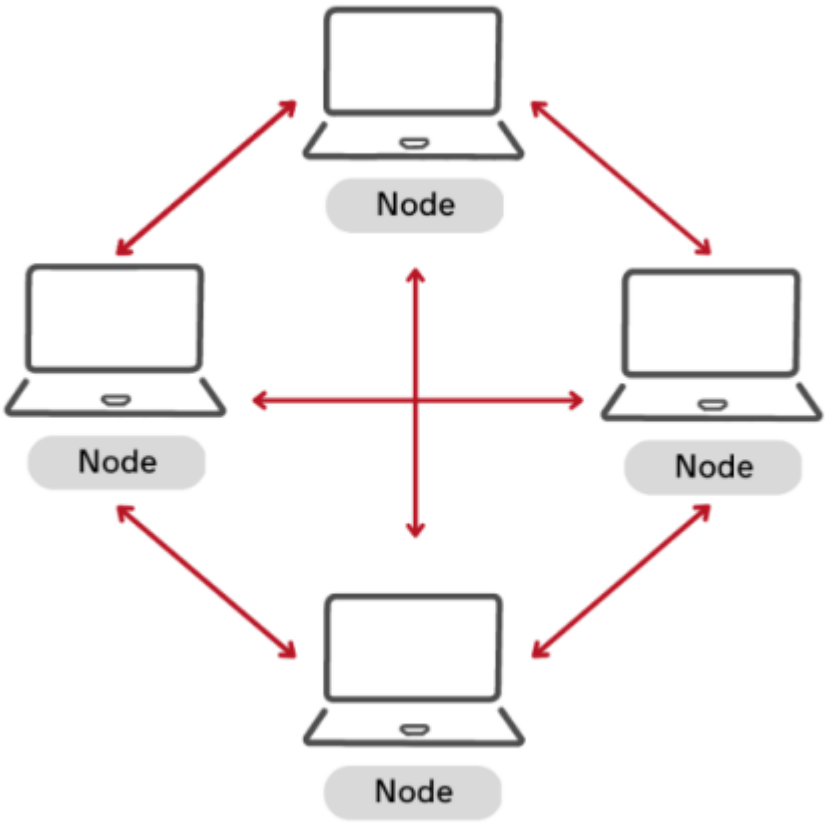
Các ứng dụng AI như nhận diện hình ảnh, xử lý ngôn ngữ tự nhiên và phân tích dữ liệu phức tạp đều có thể được triển khai trên hệ thống phân tán để tối ưu hóa hiệu suất.

Nhờ vào các đặc tính như khả năng chịu lỗi, mở rộng và tính khả dụng cao, hệ phân tán trở thành nền tảng quan trọng cho rất nhiều ứng dụng trong thế giới hiện đại.

1.6 MẠNG NGANG HÀNG

1.6.1. Khái niệm mạng ngang hàng

Mạng ngang hàng (Peer-to-Peer - P2P) là một mô hình mạng trong đó các nút (nodes) trong mạng đều có vai trò bình đẳng. Các nút này vừa có thể đóng vai trò là máy khách (client) vừa là máy chủ (server), tức là có thể vừa nhận vừa cung cấp tài nguyên. Không có máy chủ trung tâm quản lý, tất cả các thành viên trong mạng đều có thể trực tiếp trao đổi dữ liệu với nhau.



Hình 2: Một mô hình mạng ngang hàng

Mô hình P2P thường được sử dụng để chia sẻ tệp, tài nguyên tính toán hoặc kết nối giữa nhiều thiết bị trong hệ thống phân tán mà không cần trung gian.

1.6.2. Đặc điểm của mạng ngang hàng

Phân tán (Decentralized): Không có một máy chủ trung tâm quản lý toàn bộ hệ thống. Các thành viên đều bình đẳng và tự quản lý tài nguyên của mình.

Khả năng mở rộng (Scalability): Khi có nhiều nút tham gia mạng, khả năng mở rộng là rất cao. Điều này làm tăng băng thông và tài nguyên tính toán mà không cần thêm máy chủ trung tâm.

Chịu lỗi (Fault Tolerance): Mạng ngang hàng thường có khả năng chịu lỗi tốt, vì sự hỏng hóc của một vài nút không ảnh hưởng nhiều đến toàn bộ hệ thống.

Cân bằng tải (Load Balancing): Vì không có máy chủ trung tâm, việc lưu trữ và chia sẻ dữ liệu được phân phối đều trên các nút, giúp giảm tình trạng quá tải cho một máy chủ duy nhất.

Quản lý tài nguyên (Resource Management): Mỗi nút có thể quản lý tài nguyên của chính nó, bao gồm băng thông, bộ nhớ và dữ liệu.

1.6.3. Các loại mạng ngang hàng

- Mạng P2P không có cấu trúc (Unstructured P2P):

Trong mạng không có cấu trúc, các nút được sắp xếp ngẫu nhiên và không có quy tắc cố định để kết nối các nút với nhau. Mạng P2P không có cấu trúc dễ dàng thiết lập, không cần kiến trúc phức tạp. tuy vậy việc tìm kiếm tài nguyên có thể không hiệu quả, đặc biệt là khi số lượng nút tăng lên. Ví dụ: Gnutella, Napster.

- Mạng P2P có cấu trúc (Structured P2P):

Trong mạng có cấu trúc, các nút được sắp xếp theo một quy tắc nhất định, thường sử dụng bảng băm phân tán (Distributed Hash Table - DHT) để quản lý tài nguyên. Loại mạng này dễ dàng tìm kiếm và truy cập dữ liệu nhanh chóng nhưng phức tạp hơn trong việc thiết lập và bảo trì so với mạng không cấu trúc. Ví dụ: Chord, Kademlia.

- Mạng P2P lai (Hybrid P2P):

Kết hợp giữa mạng P2P và mạng máy khách-máy chủ, nơi một số nút đặc biệt đóng vai trò như máy chủ trung gian giúp điều phối và quản lý kết nối giữa các nút. Loại mạng này tận dụng được cả lợi ích của mô hình P2P và máy khách-máy chủ.

Ví dụ: BitTorrent (với các trackers đóng vai trò máy chủ trung gian).

1.6.4. Cơ chế hoạt động của mạng P2P

Kết nối giữa các nút: Các nút trong mạng P2P kết nối trực tiếp với nhau, tạo thành một mạng phân tán. Khi một nút tham gia mạng, nó tìm kiếm các nút khác để kết nối, và sau đó có thể chia sẻ hoặc yêu cầu tài nguyên.

Trao đổi dữ liệu: Dữ liệu hoặc tài nguyên có thể được chia sẻ giữa các nút bằng cách gửi yêu cầu đến các nút khác để tìm kiếm tài nguyên mong muốn. Các yêu cầu này có thể được phát sóng (broadcast) hoặc gửi theo cách có cấu trúc (structured search) tùy thuộc vào loại mạng P2P.

Tìm kiếm và phân phối dữ liệu: Một trong những cơ chế quan trọng trong P2P là tìm kiếm và định vị dữ liệu. Trong mạng P2P không cấu trúc, các yêu cầu tìm kiếm thường được phát đi khắp mạng. Trong mạng có cấu trúc, bảng băm phân tán DHT được sử dụng để tìm kiếm dữ liệu một cách nhanh chóng.

Chia nhỏ và ghép nối dữ liệu (Swarming): Trong các mạng như BitTorrent, các tệp tin lớn được chia thành nhiều phần nhỏ và các phần này được tải xuống từ nhiều nguồn khác nhau, giúp tăng tốc độ truyền tải.

1.6.5. Công nghệ và giao thức trong mạng ngang hàng

Bảng băm phân tán (Distributed Hash Table - DHT): DHT là công nghệ chính để định vị và quản lý dữ liệu trong các mạng P2P có cấu trúc. Các nút và tài nguyên trong mạng đều được ánh xạ tới một không gian địa chỉ ảo. Mỗi nút chỉ chịu trách nhiệm quản lý một phần của không gian này. Ví dụ: Kademlia, Chord.

Giao thức BitTorrent: BitTorrent là một giao thức phổ biến cho việc chia sẻ tệp tin trong mạng P2P. Các tệp tin được chia nhỏ thành nhiều mảnh, và người dùng có thể tải xuống các mảnh từ nhiều người khác nhau cùng lúc.

Gnutella: Là một trong những giao thức P2P không cấu trúc đầu tiên. Gnutella sử dụng mô hình phát sóng (broadcast) để tìm kiếm và trao đổi dữ liệu giữa các nút.

FastTrack: Giao thức được sử dụng bởi các mạng chia sẻ tệp tin nổi tiếng như Kazaa, sử dụng một số nút siêu cấp (supernodes) để quản lý và điều phối lưu lượng mạng.

1.6.6. Ứng dụng của mạng ngang hàng

- Chia sẻ tệp (File Sharing): Ứng dụng phổ biến nhất của mạng P2P là chia sẻ tệp tin, ví dụ như BitTorrent. Người dùng có thể chia sẻ tệp âm nhạc, video, phần mềm hoặc các tài liệu khác một cách dễ dàng và nhanh chóng. Ví dụ của ứng dụng hướng này có thể kể đến là BitTorrent, eMule.

- Truyền tải video và nội dung đa phương tiện (Media Streaming): Mạng P2P cũng được sử dụng cho các ứng dụng truyền tải video và phát trực tuyến nội dung đa phương tiện. Các nội dung được truyền tải qua mạng P2P có thể giảm tải cho máy chủ trung tâm và tăng tốc độ truy cập của người dùng. Ví dụ: Joost, Popcorn Time.

- Tính toán phân tán (Distributed Computing): Mạng P2P cho phép tận dụng sức mạnh tính toán của nhiều máy tính phân tán để thực hiện các tác vụ phức tạp. Ví dụ: SETI@home (tìm kiếm sự sống ngoài hành tinh), Folding@home (nghiên cứu về protein).

- Hệ thống blockchain và tiền điện tử (Blockchain & Cryptocurrency): Blockchain là một ứng dụng của mạng P2P, trong đó các giao dịch được xác nhận và ghi nhận trên một sổ cái phân tán mà không cần sự can thiệp của trung gian. Ví dụ: Bitcoin, Ethereum.

- Mạng truyền thông (Communication Networks): Mạng P2P được sử dụng trong các ứng dụng nhắn tin và truyền thông ngang hàng, nơi các tin nhắn và dữ liệu được truyền trực tiếp giữa các thiết bị mà không cần máy chủ trung gian. Các hệ thống Skype (trước đây sử dụng P2P), Tox là ví dụ của loại ứng dụng này.

CÂU HỎI VÀ BÀI TẬP

1. Sự khác biệt giữa mã hóa đối xứng và mã hóa bất đối xứng là gì?
2. Chế độ hoạt động của mã hóa khối (block cipher mode) là gì?
3. Vai trò của khóa phiên (session key) trong mã hóa đối xứng là gì?
4. Tính chất nào của hàm băm là quan trọng nhất?
5. Sự khác biệt giữa mã hóa và hàm băm là gì?
6. Tại sao va chạm hàm băm (hash collision) là một vấn đề trong bảo mật?
7. Chữ ký số hoạt động như thế nào?
8. Sự khác biệt giữa chữ ký số và chữ ký điện tử là gì?
9. Vai trò của hàm băm trong chữ ký số là gì?
10. Các thuật toán phổ biến sử dụng trong chữ ký số là gì?
11. Làm thế nào để xác minh tính hợp lệ của chữ ký số?
12. Chữ ký số giúp ngăn chặn các cuộc tấn công như thế nào?
13. Viết một chương trình để mã hóa và giải mã một thông điệp sử dụng thuật toán AES. Thử nghiệm với các chế độ hoạt động khác nhau như ECB, CBC, và GCM.
14. Viết một chương trình để tạo ra một hệ thống mã hóa lai, trong đó sử dụng mã hóa bất đối xứng để mã hóa khóa phiên (session key) và mã hóa đối xứng để mã hóa thông điệp.
15. Sử dụng thuật toán AES trong chế độ ECB để mã hóa một hình ảnh bitmap. Quan sát kết quả và giải thích lý do tại sao chế độ ECB không nên được sử dụng để mã hóa dữ liệu lớn có cấu trúc như hình ảnh.
16. Viết một chương trình đơn giản để tạo ra một hàm băm dựa trên chuỗi ký tự (ví dụ: sử dụng tổng của mã ASCII). Hãy thử nghiệm với một số chuỗi đầu vào khác nhau
17. Cho một chuỗi băm đã được cho trước (ví dụ: `d2d2d2...`), hãy tìm một chuỗi đầu vào có thể tạo ra băm này. Hãy thử với các hàm băm phổ biến như MD5, SHA-1, SHA-256 và ghi lại thời gian thực hiện.
18. Hãy thử tìm hai chuỗi khác nhau nhưng tạo ra cùng một giá trị băm sử dụng một hàm băm đơn giản tự viết. So sánh kết quả với các hàm băm mật mã phổ biến như MD5 hay SHA-1.

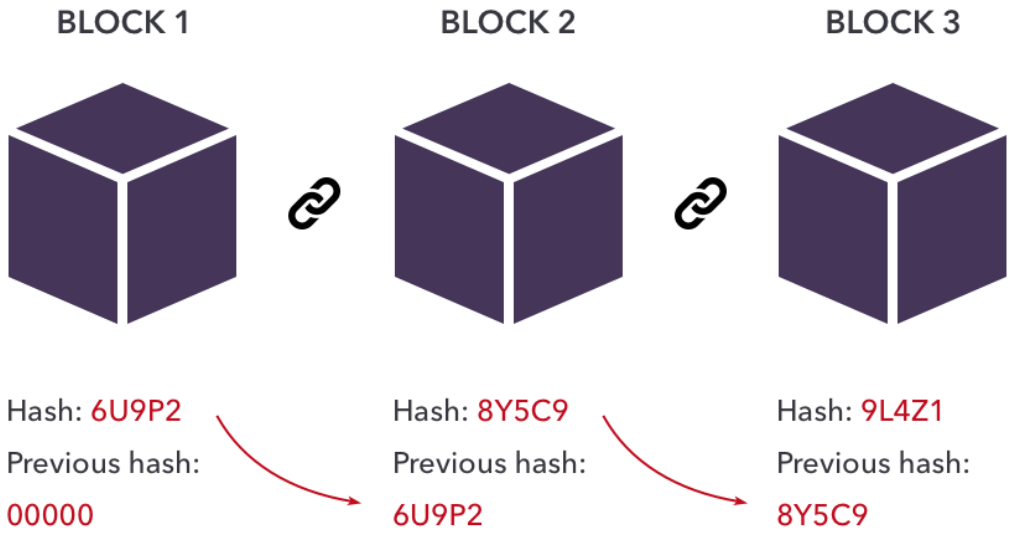
19. Viết một chương trình để kiểm tra tính toàn vẹn của tệp tin sử dụng hàm băm (ví dụ: SHA-256). Hãy thay đổi một số byte trong tệp tin và quan sát sự thay đổi của giá trị băm.
20. Giải thích tấn công Birthday và viết một chương trình mô phỏng nguyên lý tấn công này trên một hàm băm đơn giản, sau đó thực hiện với một hàm băm như MD5 hoặc SHA-1.
21. Viết một chương trình đơn giản sử dụng thuật toán RSA để tạo chữ ký số cho một chuỗi văn bản và sau đó xác minh chữ ký này. Thử nghiệm với các thư viện mật mã phổ biến như `PyCryptodome` hoặc `OpenSSL`.
22. Sử dụng thuật toán ECDSA để tạo và xác minh chữ ký số. So sánh hiệu suất của ECDSA với RSA khi ký cùng một thông điệp.
23. Tải về một chứng chỉ số từ một trang web (ví dụ: thông qua HTTPS) và viết một chương trình để trích xuất khóa công khai từ chứng chỉ này. Sử dụng khóa công khai để xác minh một chữ ký số.
24. Nghiên cứu cách chữ ký số được sử dụng trong các hợp đồng thông minh (smart contract) trên nền tảng blockchain. Viết một hợp đồng thông minh đơn giản có sử dụng chữ ký số để xác minh giao dịch.
25. Thực hiện bài tập thực hành để tạo và xác minh chữ ký số bằng cả RSA và ECDSA, sau đó so sánh về kích thước chữ ký, tốc độ ký, và tốc độ xác minh.

CHƯƠNG 2: CÁC KHÁI NIỆM CỦA BLOCKCHAIN

2.1. KHÁI NIỆM

2.1.1. Khái niệm

Blockchain (hay còn gọi là chuỗi khối) là một công nghệ lưu trữ và chia sẻ thông tin minh bạch trong một mạng lưới (network), dựa trên công nghệ dữ liệu phân tán (distributed database) và phi tập trung (decentralized), nơi dữ liệu được tổ chức thành các khối (blocks) liên kết với nhau bằng các hàm băm mật mã (cryptographic hashes). Mỗi khối chứa thông tin về các giao dịch (transaction) và tham chiếu đến khối trước đó, tạo thành một chuỗi liên tục. Do bản chất phân tán, blockchain tồn tại trên nhiều máy tính trong mạng lưới mà không phụ thuộc vào cơ quan trung tâm nào, giúp tăng tính bảo mật và chống gian lận.



Hình 2.1. Chuỗi khối

Blockchain được xem là bất biến vì khi dữ liệu đã được ghi vào, rất khó thay đổi hoặc xóa bỏ. Nó cũng mang tính minh bạch vì mọi người trong mạng lưới có thể xem và xác nhận các giao dịch. Đặc điểm này làm cho blockchain trở thành một công nghệ đáng tin cậy, lý tưởng cho việc ghi nhận giao dịch và theo dõi tài sản trong nhiều lĩnh vực như tài chính, chuỗi cung ứng, y tế và nhiều ứng dụng khác.

Một số nền tảng blockchain thế hệ mới hỗ trợ hợp đồng thông minh, cho phép tự động hóa giao dịch dựa trên các điều kiện xác định trước.

Các khái niệm cơ bản trong công nghệ blokchain:

Dữ liệu phân tán (Distributed Database): Trong hệ thống blockchain, dữ liệu không được lưu trữ ở một vị trí duy nhất mà được phân tán trên nhiều máy tính (hay nút - nodes) trong mạng lưới. Điều này có nghĩa là không có một trung tâm hay tổ chức nào kiểm soát toàn bộ dữ liệu, tạo ra tính phi tập trung và độ bền vững cao cho hệ thống.

Phi tập trung (Decentralized): Blockchain không phụ thuộc vào một cơ quan hay tổ chức trung ương để quản lý hoặc xác nhận thông tin. Thay vào đó, mạng lưới các nút phân tán sẽ tự động đồng thuận và xác minh thông tin.

Khối (Block): Mỗi khối trong blockchain chứa một nhóm các giao dịch hoặc dữ liệu đã được xác minh. Khối này không chỉ chứa thông tin về giao dịch mà còn có một mã băm (hash) của khối trước đó, tạo thành chuỗi liên kết các khối với nhau.

Hàm băm mật mã (Cryptographic Hash): Đây là một hàm toán học sử dụng mật mã để chuyển đổi một lượng dữ liệu (như thông tin trong khối) thành một chuỗi ký tự có độ dài cố định. Mỗi khối trong blockchain chứa một mã băm duy nhất được tính toán từ dữ liệu trong khối và mã băm của khối trước đó. Điều này giúp liên kết các khối với nhau và bảo vệ tính toàn vẹn của dữ liệu, vì nếu có thay đổi nhỏ trong dữ liệu của một khối, mã băm sẽ thay đổi, từ đó dễ dàng phát hiện sự giả mạo.

Giao dịch (Transaction): Mỗi giao dịch trong blockchain là một hành động hoặc sự kiện cần được ghi nhận, chẳng hạn như chuyển tiền, chuyển quyền sở hữu tài sản, hoặc cập nhật thông tin. Các giao dịch này được ghi lại trong các khối và liên kết với nhau thành chuỗi giao dịch.

2.1.2. Một số đặc điểm quan trọng của blockchain

Blockchain là một công nghệ nổi bật với nhiều đặc điểm quan trọng. Dưới đây là một số đặc điểm chính của blockchain:

1. Tính bất biến: Dữ liệu trong belockchain không thể thay đổi hay bị xóa sau khi đã được ghi nhận, đảm bảo tính toàn vẹn của sổ cái.

2. Phi tập trung: Blockchain không phụ thuộc vào một cơ quan trung ương hay tổ chức để quản lý, mà các giao dịch được phân phối và xác nhận qua nhiều nút mạng (nodes), đảm bảo tính minh bạch và giảm rủi ro lạm quyền.

3. Minh bạch và không thể thay đổi: Mọi giao dịch trên blockchain đều được ghi lại và công khai cho tất cả các bên tham gia mạng lưới, một khi thông tin được ghi vào blockchain, nó không thể bị thay đổi hoặc xóa bỏ.

4. Bảo mật cao: Blockchain sử dụng các thuật toán mật mã để bảo vệ dữ liệu và đảm bảo tính toàn vẹn của các giao dịch. Các khối dữ liệu trong blockchain được liên kết với nhau thông qua hàm băm (hash), khiến việc thay đổi dữ liệu trở nên gần như không thể.

5. Hợp đồng thông minh (Smart Contracts): Blockchain có thể hỗ trợ việc triển khai các hợp đồng thông minh, nó là các hợp đồng tự động thực hiện khi các điều kiện nhất định được đáp ứng. Điều này giúp tiết kiệm thời gian và các chi phí liên quan.

6. Khả năng mở rộng và ứng dụng rộng rãi: Mặc dù blockchain được biết đến nhiều trong các ứng dụng tiền mã hóa, nhưng công nghệ này cũng được áp dụng trong nhiều lĩnh vực khác nhau, từ quản lý chuỗi cung ứng, bầu cử điện tử cho đến bảo hiểm và chăm sóc sức khỏe.

7. Phân tán: Mỗi người tham gia blockchain (các nút mạng) đều có một bản sao của toàn bộ sổ cái (ledger), điều này giúp thông tin được phân tán và bảo vệ hệ thống khỏi các cuộc tấn công.

8. Tiết kiệm chi phí: Blockchain có thể giúp giảm chi phí giao dịch và xử lý thanh toán nhờ vào việc loại bỏ các trung gian và sử dụng các quy trình tự động. Điều này không chỉ nâng cao hiệu quả mà còn giảm sự phụ thuộc vào bên thứ ba.

2.1.3. Các thành phần cơ bản của blockchain

Blockchain được cấu thành từ một số thành phần cơ bản, mỗi thành phần đóng vai trò quan trọng trong việc đảm bảo tính bảo mật, minh bạch và hoạt động hiệu quả của hệ thống. Dưới đây là các thành phần cơ bản của blockchain:

2.1.3.1. Block (Khối):

Blockchain được chia thành các khối (block), mỗi khối chứa một nhóm các giao dịch. Mỗi khối bao gồm các thông tin như:

- Dữ liệu giao dịch: Các giao dịch được ghi lại trong khối, bao gồm thông tin về người gửi, người nhận, số tiền giao dịch và các thông tin liên quan.

- Chữ ký số (Digital Signature): Dùng để xác nhận tính hợp lệ của các giao dịch.

- Mã hash của khối trước: Mỗi khối lưu trữ mã hash của khối trước đó, tạo thành chuỗi liên kết.

- Mã hash của khối hiện tại: Mỗi khối có một mã hash riêng biệt, dùng để nhận diện và xác nhận tính toàn vẹn của dữ liệu.

2.1.3.2. Sổ cái phân tán (Distributed Ledger):

Blockchain là một sổ cái phân tán, có nghĩa là bản sao của dữ liệu được lưu trữ trên nhiều nút (nodes) trên toàn mạng.

Điều này đảm bảo tính minh bạch và giảm rủi ro từ việc một nút hoặc một phần của hệ thống bị tấn công.

2.1.3.3. Nút mạng (Node):

Các nút trong blockchain có thể là máy tính, thiết bị hoặc các tổ chức tham gia vào mạng. Chúng có nhiệm vụ lưu trữ và xử lý thông tin.

Các nút có thể là nút đầy đủ (full node) lưu trữ toàn bộ bản sao của blockchain, hoặc nút nhẹ (light node) chỉ lưu trữ một phần dữ liệu cần thiết.

2.1.3.4. Mã hash (Hash):

Hash là một giá trị số học do thuật toán hash tạo ra, dùng để đại diện cho dữ liệu của khối.

Mỗi khối trong blockchain có một mã hash độc nhất, giúp đảm bảo rằng bất kỳ thay đổi nào trong khối sẽ làm thay đổi mã hash và dễ dàng phát hiện sự giả mạo.

2.1.3.5. Thuật toán đồng thuận (Consensus Algorithm):

Thuật toán đồng thuận là cơ chế để các nút trong mạng blockchain thống nhất về các giao dịch hợp lệ và thêm chúng vào chuỗi.

Các thuật toán phổ biến bao gồm:

- Proof of Work (PoW): Yêu cầu các nút thực hiện các phép tính phức tạp để xác minh và thêm giao dịch vào blockchain (dùng trong Bitcoin).

- Proof of Stake (PoS): Các nút được chọn dựa trên lượng tiền tệ họ sở hữu và sẵn sàng tham gia vào quá trình xác thực (dùng trong Ethereum 2.0).

- Delegated Proof of Stake (DPoS): Mạng blockchain có thể ủy quyền cho một số nút đại diện để xử lý các giao dịch (thường thấy trong EOS).

2.1.3.6. Hợp đồng thông minh (Smart Contract):

Hợp đồng thông minh là các chương trình tự động thực hiện các điều kiện khi giao dịch xảy ra mà không cần sự can thiệp của bên thứ ba.

Chúng giúp tự động hóa các thỏa thuận và thực thi các quy tắc mà các bên tham gia đã đồng ý.

2.1.3.7. Kênh giao tiếp (P2P Network):

Blockchain sử dụng mạng ngang hàng (peer-to-peer) để các nút có thể trao đổi thông tin trực tiếp với nhau mà không cần qua một máy chủ trung gian. Điều này làm tăng tính phân tán và bảo mật của hệ thống.

2.1.3.8. Cơ chế mã hóa (Cryptography):

Mã hóa đóng vai trò quan trọng trong bảo vệ tính toàn vẹn của dữ liệu và xác thực giao dịch.

Các giao dịch và thông tin trên blockchain được mã hóa bằng các thuật toán như SHA-256, RSA, hoặc elliptic curve cryptography (ECC).

Các thành phần này phối hợp với nhau để tạo thành một hệ thống blockchain hoàn chỉnh, đảm bảo tính bảo mật, minh bạch và ổn định.

2.1.4. Quy trình hoạt động của blockchain

Quy trình hoạt động của blockchain có thể được tóm tắt qua một chuỗi các bước, từ khi một giao dịch được tạo ra cho đến khi nó được xác nhận và thêm vào sổ cái (ledger) vĩnh viễn. Dưới đây là quy trình hoạt động cơ bản của blockchain:

2.1.4.1. Tạo giao dịch

Quá trình bắt đầu khi người dùng (hoặc các hệ thống) tạo ra một giao dịch. Giao dịch có thể là chuyển tiền, chuyển nhượng quyền sở hữu tài sản, hoặc thực hiện các hành động khác tùy theo ứng dụng của blockchain. Giao dịch này sẽ được mã hóa bao gồm thông tin như người gửi, người nhận, số tiền, và các thông tin liên quan.

2.1.4.2. Xác nhận giao dịch

Giao dịch sau khi tạo ra sẽ được phát tán đến mạng lưới các nút (nodes) trong blockchain. Các nút trong mạng sẽ kiểm tra tính hợp lệ của giao dịch (ví dụ, xác minh rằng người gửi có đủ số dư để thực hiện giao dịch).

Một số blockchain sử dụng các thuật toán đồng thuận (như Proof of Work, Proof of Stake) để xác nhận giao dịch.

2.1.4.3. Tạo khối mới (Block)

Sau khi giao dịch được xác nhận, nó sẽ được nhóm lại với các giao dịch khác thành một khối (block).

2.1.4.4. Xác thực khối thông qua thuật toán đồng thuận

Sau khi khối được tạo ra, nó sẽ được gửi đến các nút trong mạng để xác nhận.

Quá trình xác nhận này thường sử dụng các thuật toán đồng thuận như Proof of Work (PoW) hoặc Proof of Stake (PoS) để đảm bảo rằng các nút đồng ý với khối và các giao dịch trong đó.

Ví dụ, trong hệ thống Proof of work, các nút (thợ mỏ) sẽ cạnh tranh để giải quyết các bài toán phức tạp (tìm một giá trị hash hợp lệ), và khi họ thành công, khối sẽ được chấp nhận và thêm vào chuỗi.

2.1.4.5. Thêm khối vào blockchain

Khi khối mới được xác nhận và thêm vào blockchain, các giao dịch trong khối sẽ được coi là hợp lệ và không thể thay đổi.

2.1.4.6. Phân phối bản sao sổ cái

Sau khi khối mới được thêm vào blockchain, bản sao của nó sẽ được phân phối đến tất cả các nút trong mạng.

Điều này đảm bảo rằng mọi nút đều có bản sao mới nhất của blockchain và giúp duy trì tính phân tán và minh bạch của hệ thống.

2.1.4.7. Giao dịch hoàn tất

Khi khối đã được xác nhận và thêm vào blockchain, giao dịch trong khối được xem là hoàn tất và không thể thay đổi.

Người nhận có thể xác nhận rằng họ đã nhận được giao dịch thông qua hệ thống, và tất cả các bên tham gia đều có thể truy cập vào bản sao của sổ cái để kiểm tra tính hợp lệ của giao dịch.

2.1.4.8. Quy trình tiếp tục

Sau mỗi giao dịch được thêm vào blockchain, quá trình sẽ tiếp tục từ bước 1 cho các giao dịch tiếp theo.

Các khối mới sẽ được tạo ra và xác nhận liên tục, duy trì sự phát triển của chuỗi blockchain.

Với quy trình trên, blockchain đảm bảo rằng mỗi giao dịch được ghi lại một cách minh bạch và an toàn mà không cần sự can thiệp của một tổ chức trung gian.

2.2. LỊCH SỬ RA ĐỜI CỦA BLOCKCHAIN

2.2.1. Sơ lược về lịch sử công nghệ blockchain

Ý tưởng về công nghệ blockchain bắt đầu từ cuối những năm 1980 và đầu 1990. Vào năm 1989, Leslie Lamport phát triển giao thức Paxos và mô hình đồng thuận trong mạng máy tính, giúp đạt được sự thống nhất dù có sự không đáng tin cậy. Vào năm 1991, chuỗi thông tin được ký điện tử đã được sử dụng để đảm bảo tính toàn vẹn của tài liệu số hóa. Những ý tưởng này kết hợp và ứng dụng vào tiền mã hóa, được mô tả trong bài báo "Bitcoin: A Peer-to-Peer

Electronic Cash System" của Satoshi Nakamoto vào năm 2008. Mạng blockchain của Bitcoin chính thức được thiết lập vào năm 2009, trở thành ứng dụng blockchain đầu tiên và mở đường cho các ứng dụng khác sau này.

Trước Bitcoin, đã có các hệ thống tiền điện tử khác như ecash, nhưng không hệ thống nào phổ biến rộng rãi. Blockchain cho phép Bitcoin hoạt động phân tán, không có điểm kiểm soát trung tâm, giúp giao dịch giữa người dùng mà không cần bên trung gian. Blockchain cũng hỗ trợ việc phát hành tiền mã hóa mới cho những người tham gia duy trì mạng. Hệ thống tự vận hành đảm bảo chỉ giao dịch hợp lệ mới được thêm vào blockchain.

Bitcoin là một trong những ứng dụng tiên phong của công nghệ blockchain, cung cấp mức độ ẩn danh cho người dùng. Trong đó, các tài khoản có thể được theo dõi thông qua mã định danh nhưng không thể nhận diện trực tiếp. Tính năng ẩn danh này không chỉ giúp bảo mật thông tin mà còn cho phép người dùng tạo tài khoản mà không cần phải xác minh theo các quy định *Know-Your-Customer* (KYC).

Do Bitcoin là ẩn danh một phần, việc tạo ra lòng tin trong một môi trường mà người dùng không dễ nhận dạng là rất quan trọng. Trước khi công nghệ blockchain ra đời, lòng tin này thường được cung cấp thông qua các bên trung gian đáng tin cậy của cả hai phía giao dịch. Trong blockchain, lòng tin được xây dựng dựa trên bốn đặc tính chính của công nghệ blockchain:

- Sổ cái (Ledger): Công nghệ này sử dụng một sổ cái chỉ cho phép ghi thêm, cung cấp lịch sử giao dịch đầy đủ. Không giống như cơ sở dữ liệu truyền thống, các giao dịch và giá trị trên blockchain không bị ghi đè.
- An toàn (Secure): Blockchain được bảo mật bằng các phương pháp mật mã, đảm bảo rằng dữ liệu trong sổ cái không thể bị can thiệp và luôn có thể kiểm chứng được.
- Chia sẻ (Shared): Sổ cái được chia sẻ giữa nhiều người tham gia, mang lại sự minh bạch trên tất cả các nút trong mạng lưới blockchain.
- Phân tán (Distributed): Blockchain có thể được phân tán, cho phép mở rộng số lượng nút trong mạng lưới, từ đó tăng khả năng chống lại các cuộc tấn công từ các tác nhân xấu. Khi số lượng nút tăng, khả năng tác nhân xấu ảnh hưởng đến giao thức đồng thuận của blockchain sẽ giảm.

Blockchain được giới thiệu chính thức vào năm 2009 cùng với sự ra mắt của Bitcoin, nhưng nguồn gốc của công nghệ này đã có từ nhiều thập kỷ trước. Nhiều công nghệ nền tảng của blockchain ngày nay đã được phát triển trước khi Bitcoin xuất hiện. Dù blockchain thường gắn liền với Bitcoin, nó đã trải qua nhiều thăng trầm, đặc biệt trong những năm đầu sau khi Bitcoin ra đời, với những rủi ro liên quan đến việc ứng dụng trong kinh doanh. Tuy nhiên, vào năm 2016, cộng đồng nguồn mở đã bắt đầu phát triển các nền tảng blockchain dành cho doanh nghiệp, giúp công nghệ này trở nên ứng dụng hơn.

Mặc dù blockchain có lịch sử tương đối ngắn, nhưng ảnh hưởng của nó ngày nay rất rộng rãi và các ứng dụng của nó đang ngày càng mở rộng và phát triển. Qua nhiều thập kỷ, sự phát triển và tiến hóa của blockchain đã chứng kiến một số bước tiến đáng chú ý sau:

- Những người tiên phong như Merkle với mô hình cây của ông, Chaum với tiền kỹ thuật số, Haber với dấu thời gian, Dwork với bằng chứng công việc (PoW), Black với hashcash, và Finney với PoW có thể tái sử dụng đã đóng góp từ những năm đầu trong bối cảnh phát triển của tiền điện tử và blockchain.
- Biệt danh Satoshi Nakamoto được sử dụng để giới thiệu khái niệm về tiền mã hóa và blockchain. Ngay sau đó, tiền mã hóa đã được ra mắt, Nakamoto thực hiện giao dịch *bitcoin* đầu tiên, một sàn giao dịch bitcoin được thành lập, và một lập trình viên đã chi *10.000 bitcoin* để mua hai chiếc pizza.
- Giá Bitcoin đã tăng vọt từ vài xu lên tới hàng chục nghìn đô la, đồng thời kéo theo nhiều tranh cãi, đóng cửa, đàn áp, phá sản, lừa đảo, bê bối và bắt giữ.
- Blockchain cùng với các công nghệ tiên tiến như trí tuệ nhân tạo (AI), Internet vạn vật (IoT), token không thể thay thế (NFT), tài chính phi tập trung (DeFi), và hợp đồng thông minh, cùng với các sáng kiến từ các tập đoàn lớn như Walmart và Amazon, blockchain đã trở thành một giải pháp hợp pháp, an toàn và khả thi, thay thế cho các phương pháp truyền thống trong việc thực hiện các giao dịch kinh doanh và cá nhân.

2.2.2. Quá trình hình thành và phát triển của công nghệ blockchain

1979: Cây Merkle, một trong những công nghệ tiền blockchain đầu tiên, được đặt theo tên của nhà khoa học Ralph Merkle. Ông đã mô tả phương pháp phân phối khóa công khai và chữ ký số trong luận án tiến sĩ tại Đại học Stanford. Merkle cấp bằng sáng chế cho phương pháp này, mở ra cách xác minh các bản ghi riêng lẻ thông qua cây Merkle.

1992: David Chaum mô tả hệ thống két trong luận án Tiến sĩ tại Đại học California, Berkeley, nhằm tạo dựng lòng tin giữa các hệ thống máy tính của các nhóm nghi ngờ lẫn nhau. Chaum cũng được ghi nhận là người sáng lập tiền kỹ thuật số và thành lập công ty DigiCash.

1991: Stuart Haber và W. Scott Stornetta xuất bản bài viết mô tả cách đóng dấu thời gian cho tài liệu kỹ thuật số, ngăn ngừa thay đổi ngày tháng mà không cần lưu hồ sơ của dịch vụ đóng dấu. Họ cũng tích hợp cây Merkle vào thiết kế này để có thể chứa nhiều chứng chỉ tài liệu trên một khối.

1993: Khái niệm PoW (Proof of Work) được công bố bởi Cynthia Dwork và Moni Naor nhằm chống thư rác và kiểm soát quyền truy cập tài nguyên chia sẻ.

1997: Adam Black giới thiệu Hashcash, một thuật toán PoW để đối phó với tình trạng từ chối dịch vụ (DoS).

1999: Markus Jakobsson và Ari Juels công bố thuật ngữ "Proof of Work". Cùng năm, mạng P2P được phổ biến qua ứng dụng chia sẻ tệp ngang hàng Napster, góp phần xây dựng các hệ thống phân tán.

2000: Stefan Konst giới thiệu chuỗi bảo mật bằng mật mã trong bài báo "Tệp nhật ký bảo mật". Mô hình của ông đã tạo nền tảng cho các mô hình blockchain ngày nay.

2004: Hal Finney giới thiệu PoW có thể tái sử dụng, cung cấp cơ chế nhận mã thông báo hashcash không thể trao đổi cho mã thông báo được ký bằng RSA, một yếu tố quan trọng trong khai thác Bitcoin.

2008: Satoshi Nakamoto xuất bản sách trắng về Bitcoin, giới thiệu khái niệm blockchain và tiền mã hóa. Nakamoto phát triển phần mềm Bitcoin đầu tiên, mở ra hệ sinh thái giao dịch P2P không cần bên thứ ba.

2009: Bitcoin ra mắt trong thời kỳ đại suy thoái. Nakamoto khai thác khối đầu tiên (khối Genesis), xác thực blockchain. Bitcoin được phát hành dưới dạng phần mềm nguồn mở.

2010: Lập trình viên Laszlo Hanyecz thực hiện giao dịch Bitcoin đầu tiên khi chi 10.000 bitcoin để mua 2 chiếc pizza Papa John's. Jed McCaleb ra mắt Mt. Gox, sàn giao dịch Bitcoin đầu tiên, nhưng sau đó bị hack nghiêm trọng.

2011: Bitcoin đạt mức ngang giá với đô la Mỹ. Mt. Gox bị hack và Litecoin ra đời như một loại tiền điện tử thay thế.

2012: Bitcoin duy trì giá trị quanh mức 5 USD, với sự quan tâm mạnh mẽ từ cộng đồng. Tạp chí Bitcoin được ra mắt và Quỹ Bitcoin được thành lập.

2013: Bitcoin tiếp tục tăng trưởng mạnh mẽ, giá trị vượt qua 1 tỷ USD. Tuy nhiên, các chính phủ như Thái Lan và Trung Quốc cấm tiền điện tử, trong khi WikiLeaks bắt đầu chấp nhận quyên góp bằng Bitcoin.

2014: Vitalik Buterin công bố Ethereum, nền tảng phi tập trung với hợp đồng thông minh, mở ra cơ hội ứng dụng blockchain ngoài tiền điện tử.

2015: Ethereum Frontier ra mắt, khởi động cho việc phát triển các ứng dụng phi tập trung (dApps). Các ngân hàng lớn cũng hợp tác để nghiên cứu ứng dụng blockchain trong tài chính.

2016: Ethereum đã trải qua một hard fork sau sự cố hack, trong khi sàn giao dịch Bitfinex bị tấn công và mất 120.000 bitcoin. Cũng trong năm này, blockchain bắt đầu được công nhận là một thuật ngữ độc lập.

2017: Bitcoin đạt mức cao gần 20.000 USD, Nhật Bản công nhận Bitcoin là tiền tệ hợp pháp. Blockchain bắt đầu được ứng dụng rộng rãi trong các lĩnh vực tài chính, ngân hàng, và thương mại.

2018: Bitcoin giảm mạnh về mức 3.800 USD, tuy nhiên blockchain vẫn tiếp tục phát triển. Chính phủ Trung Quốc và Hàn Quốc tiếp tục cam kết đầu tư vào blockchain.

2019: Walmart và Amazon bắt đầu ứng dụng blockchain. Ethereum ghi nhận kỷ lục giao dịch, và các tổ chức toàn cầu tiếp tục nghiên cứu blockchain.

2020: Blockchain đã được triển khai trong 40% các doanh nghiệp. Ethereum 2.0 ra mắt với mục tiêu cải thiện khả năng mở rộng và bảo mật. Đồng thời, Stablecoin và sự kết hợp giữa blockchain với AI phát triển mạnh mẽ.

2021: Bitcoin đạt mức cao kỷ lục 68.789 USD, và Coinbase được niêm yết trên sàn chứng khoán Hoa Kỳ. Cùng năm này, NFT và DeFi bùng nổ mạnh mẽ.

2022: NFT tiếp tục tăng trưởng. Các ứng dụng blockchain tiếp tục gia tăng trong các công ty. Bitcoin tiến gần đến giới hạn khai thác 21 triệu đồng, dự kiến đạt được vào khoảng năm 2140.

2023: Blockchain tiếp tục đối mặt với thách thức, trong khi các doanh nghiệp vẫn duy trì triển khai công nghệ. Web 3.0 và các ứng dụng blockchain trong nhiều lĩnh vực hứa hẹn sẽ thúc đẩy sự phát triển trong tương lai.

2024: Công nghệ blockchain tiếp tục phát triển mạnh mẽ, với việc ứng dụng trong các lĩnh vực như tài chính, y tế, chuỗi cung ứng, và quản lý dữ liệu. Các cải tiến trong khả năng mở rộng, bảo mật và tính hiệu quả của blockchain sẽ tạo ra cơ hội mới cho các doanh nghiệp và người dùng. Đồng thời, blockchain ngày càng được tích hợp với các công nghệ mới như AI, IoT và 5G, thúc đẩy sự chuyển đổi số và mang lại giá trị bền vững trong các hoạt động kinh doanh và cá nhân. Trong năm 2024, Bitcoin đã đạt mức giá cao nhất mọi thời đại vào ngày 5 tháng 12, khi vượt qua ngưỡng 100.000 USD và chạm mức 101.600 USD.

Sau năm 2024, một số xu hướng dự kiến sẽ đóng góp đáng kể vào việc đạt được mức định giá nghìn tỷ đô la của công nghệ blockchain, bao gồm:

- Mở rộng ứng dụng DeFi (Tài chính phi tập trung): Các giao thức DeFi tiếp tục phát triển, mang lại giải pháp tài chính minh bạch và phi tập trung cho người dùng toàn cầu.
- Sự phát triển của Web 3.0: Internet phi tập trung, với các ứng dụng dựa trên blockchain, sẽ mở ra tiềm năng to lớn trong việc bảo mật dữ liệu và quyền riêng tư.
- Tích hợp blockchain vào quản lý chuỗi cung ứng: Đảm bảo tính minh bạch và truy xuất nguồn gốc trong chuỗi cung ứng toàn cầu.
- NFT và tài sản kỹ thuật số: Sự phát triển của NFT tiếp tục định hình cách thức sở hữu và giao dịch tài sản kỹ thuật số trong các lĩnh vực như nghệ thuật, giải trí và thể thao.
- Ứng dụng trong lĩnh vực IoT: Kết hợp blockchain với Internet vạn vật (IoT) để cải thiện khả năng bảo mật và quản lý thiết bị.
- Hợp đồng thông minh nâng cao: Sử dụng các hợp đồng tự thực thi ngày càng phổ biến trong các lĩnh vực pháp lý, bất động sản và chăm sóc sức khỏe.
- Chuyển đổi kỹ thuật số trong chính phủ: Blockchain có tiềm năng cách mạng hóa quản lý dữ liệu, bầu cử và dịch vụ công tại nhiều quốc gia.

2.3. CÁC LOẠI MẠNG BLOCKCHAIN

Có bốn loại mạng blockchain chính: blockchain công khai, blockchain riêng tư, blockchain liên minh và blockchain lai. Mỗi loại mạng này có đặc điểm riêng, với các lợi ích,

nhược điểm và ứng dụng lý tưởng khác nhau. Chúng ta sẽ cùng khám phá chi tiết về từng nền tảng.

2.3.1. Blockchain công khai

Cách thức hoạt động: Blockchain công khai là nền tảng mà các loại tiền điện tử như Bitcoin được phát triển, đồng thời giúp phổ biến công nghệ Sổ cái phân tán (Distributed Ledger Technology - DLT). Công nghệ này khắc phục các vấn đề của tập trung hóa, bao gồm các yếu tố như bảo mật và minh bạch kém. DLT không lưu trữ thông tin tại một địa điểm duy nhất mà thay vào đó phân phối dữ liệu trên một mạng lưới ngang hàng (peer-to-peer).

Bản chất phi tập trung của blockchain yêu cầu các phương pháp xác minh tính xác thực của dữ liệu. Một trong những phương pháp này là thuật toán đồng thuận, giúp các thành viên trong mạng blockchain đạt được sự nhất trí về trạng thái hiện tại của sổ cái. Hai phương pháp đồng thuận phổ biến nhất là Bằng chứng công việc (Proof of Work - PoW) và Bằng chứng cổ phần (Proof of Stake - PoS).

Ưu điểm: Một trong những ưu điểm của blockchain công khai là tính độc lập hoàn toàn với các tổ chức. Điều này có nghĩa là, ngay cả khi tổ chức khởi tạo blockchain không còn tồn tại, mạng lưới blockchain công khai vẫn có thể hoạt động miễn là vẫn còn các máy tính kết nối với nó. Theo James Godefroy, hiệu trưởng và phó giám đốc thực thi tại Rouse, một nhà cung cấp dịch vụ sở hữu trí tuệ, "Một số blockchain khuyến khích người dùng cam kết sử dụng sức mạnh máy tính để bảo mật mạng bằng cách cung cấp phần thưởng."

Một lợi thế khác của blockchain công khai là tính minh bạch của mạng lưới. Miễn là người dùng tuân thủ chặt chẽ các giao thức và phương pháp bảo mật, blockchain công khai hầu như đều an toàn.

Nhược điểm: Mạng blockchain công khai có thể gặp phải vấn đề về tốc độ, và các công ty không thể hạn chế quyền truy cập hoặc sử dụng. Một trong những rủi ro tiềm ẩn là nếu tin tặc chiếm được 51% hoặc hơn sức mạnh tính toán của mạng, họ có thể đơn phương thay đổi dữ liệu trong blockchain. James Godefroy cho biết đây là một trong những nguy cơ mà các mạng blockchain công khai phải đối mặt.

Trường hợp sử dụng: Trường hợp sử dụng phổ biến nhất của blockchain công khai là khai thác và trao đổi tiền điện tử như Bitcoin. Tuy nhiên, blockchain công khai cũng có thể được áp dụng để tạo ra các hồ sơ cố định với chuỗi lưu ký có thể kiểm toán, chẳng hạn như công chứng điện tử các bản tuyên thệ hoặc tạo hồ sơ công khai về quyền sở hữu tài sản.

Loại blockchain này đặc biệt phù hợp với các tổ chức hoạt động dựa trên sự minh bạch và tin cậy, như các nhóm hỗ trợ xã hội hoặc các tổ chức phi chính phủ. Tuy nhiên, do tính chất công khai của mạng lưới, các doanh nghiệp tư nhân có thể sẽ muốn tránh sử dụng blockchain công khai.

2.3.2. Blockchain riêng tư

Cách thức hoạt động: Một blockchain riêng tư hoạt động trong một môi trường hạn chế, như một mạng lưới khép kín hoặc dưới sự kiểm soát của một thực thể duy nhất. Mặc dù sử dụng các kết nối ngang hàng và phi tập trung giống như blockchain công khai, nhưng blockchain riêng tư có quy mô nhỏ hơn nhiều. Thay vì cho phép bất kỳ ai tham gia và cung cấp

sức mạnh tính toán, blockchain riêng tư thường được vận hành trên một mạng lưới nhỏ trong nội bộ một công ty hoặc tổ chức. Loại blockchain này còn được gọi là blockchain được cấp phép hoặc blockchain doanh nghiệp.

Ưu điểm: Tổ chức kiểm soát blockchain riêng tư sẽ thiết lập các mức cấp phép, bảo mật, ủy quyền và khả năng truy cập. Ví dụ, tổ chức thiết lập mạng blockchain riêng tư có thể xác định các nút nào có quyền xem, thêm hoặc thay đổi dữ liệu, và cũng có thể ngăn chặn các bên thứ ba truy cập vào một số thông tin nhất định.

James Godefroy cho biết: "Bạn có thể coi blockchain riêng tư như mạng nội bộ, trong khi blockchain công khai giống như internet hơn."

Do có quy mô nhỏ hơn, blockchain riêng tư có thể rất nhanh và xử lý giao dịch hiệu quả hơn nhiều so với blockchain công khai.

Nhược điểm: Nhược điểm của blockchain riêng tư bao gồm một tuyên bố gây tranh cãi rằng chúng không phải là blockchain "thực sự", vì triết lý cốt lõi của blockchain là tính phi tập trung. Hơn nữa, việc đạt được sự tin tưởng hoàn toàn vào thông tin trở nên khó khăn hơn, do các nút tập trung quyết định thông tin nào là hợp lệ. Số lượng nút ít cũng có thể đồng nghĩa với bảo mật kém hơn. Nếu một vài nút hoạt động bất hợp pháp, phương pháp đồng thuận có thể bị xâm phạm.

Ngoài ra, mã nguồn của blockchain riêng tư thường là độc quyền và đóng, khiến người dùng không thể kiểm tra hoặc xác minh độc lập. Điều này có thể dẫn đến mức độ bảo mật thấp hơn. Thêm vào đó, blockchain riêng tư không hỗ trợ tính ẩn danh, điều này làm giảm khả năng bảo vệ quyền riêng tư của người dùng.

Các trường hợp sử dụng: Tốc độ của blockchain riêng tư làm cho chúng trở thành lựa chọn lý tưởng trong các trường hợp mà blockchain cần được bảo mật bằng mật mã nhưng thực thể kiểm soát không muốn thông tin bị công chúng truy cập.

James Godefroy cho biết: "Ví dụ, các công ty có thể chọn tận dụng công nghệ blockchain mà không từ bỏ lợi thế cạnh tranh của mình vào tay bên thứ ba. Họ có thể sử dụng blockchain riêng để quản lý bí mật thương mại, kiểm toán."

Các trường hợp sử dụng khác của blockchain riêng tư bao gồm quản lý chuỗi cung ứng, quyền sở hữu tài sản, và bỏ phiếu nội bộ, nơi tính bảo mật và kiểm soát quyền truy cập là yếu tố quan trọng.

2.3.3. Blockchain lai

Cách thức hoạt động: Blockchain lai kết hợp các yếu tố của cả blockchain riêng tư và blockchain công khai. Nó cho phép các tổ chức thiết lập một hệ thống riêng tư, dựa trên quyền cùng với một hệ thống công khai không cần quyền, cho phép họ kiểm soát những ai có thể truy cập dữ liệu cụ thể được lưu trữ trong blockchain và dữ liệu nào sẽ được mở công khai.

Thông thường, các giao dịch và hồ sơ trong một blockchain lai không được công khai nhưng có thể được xác minh khi cần, chẳng hạn như bằng cách cho phép truy cập thông qua hợp đồng thông minh . Thông tin bí mật được lưu giữ bên trong mạng nhưng vẫn có thể xác

minh được. Mặc dù một thực thể tư nhân có thể sở hữu blockchain lai, nhưng nó không thể thay đổi các giao dịch.

Khi người dùng tham gia vào một blockchain lai, họ có toàn quyền truy cập vào mạng. Danh tính của người dùng được bảo vệ khỏi những người dùng khác, trừ khi họ tham gia vào một giao dịch. Sau đó, danh tính của họ được tiết lộ cho bên kia.

Ưu điểm: Một trong những ưu điểm lớn của blockchain lai là vì nó hoạt động trong một hệ sinh thái khép kín nên tin tặc bên ngoài không thể thực hiện cuộc tấn công 51% vào mạng. Nó cũng bảo vệ quyền riêng tư nhưng cho phép giao tiếp với bên thứ ba. Giao dịch rẻ và nhanh, và nó cung cấp khả năng mở rộng tốt hơn so với mạng blockchain công khai.

Nhược điểm: Loại blockchain này không hoàn toàn minh bạch vì thông tin có thể bị che giấu. Việc nâng cấp cũng có thể là một thách thức và không có động lực nào để người dùng tham gia hoặc đóng góp vào mạng lưới.

Các trường hợp sử dụng: Blockchain lai có một số trường hợp sử dụng mạnh, bao gồm bất động sản. Các công ty có thể sử dụng blockchain lai để chạy hệ thống riêng tư nhưng hiển thị một số thông tin nhất định, chẳng hạn như danh sách, cho công chúng. Bán lẻ cũng có thể hợp lý hóa các quy trình của mình bằng blockchain lai và các thị trường được quản lý chặt chẽ như dịch vụ tài chính cũng có thể thấy được lợi ích khi sử dụng nó .

Theo Godefroy, hồ sơ y tế có thể được lưu trữ trong một blockchain lai. Hồ sơ không thể được xem bởi bên thứ ba ngẫu nhiên, nhưng người dùng có thể truy cập thông tin của họ thông qua hợp đồng thông minh. Chính phủ cũng có thể sử dụng nó để lưu trữ dữ liệu công dân một cách riêng tư nhưng chia sẻ thông tin một cách an toàn giữa các tổ chức.

2.3.4. Blockchain liên kết

Cách thức hoạt động: Loại blockchain thứ tư, blockchain liên minh, còn được gọi là blockchain liên bang, kết hợp các tính năng của blockchain công khai và blockchain riêng tư. Tuy nhiên, điểm khác biệt là nhiều tổ chức hợp tác trên một mạng phi tập trung. Về cơ bản, blockchain liên minh là blockchain riêng tư với quyền truy cập hạn chế, chỉ cho phép một nhóm cụ thể tham gia, giúp loại bỏ các rủi ro liên quan đến việc chỉ một thực thể kiểm soát mạng như trong blockchain riêng tư.

Trong blockchain liên minh, các thủ tục đồng thuận được kiểm soát bởi các nút đã được thiết lập sẵn. Nó có một nút xác thực khởi tạo, nhận và xác minh các giao dịch. Các nút thành viên có thể nhận hoặc khởi tạo các giao dịch trong mạng, tạo điều kiện cho sự hợp tác giữa các tổ chức trong một môi trường bảo mật và có kiểm soát.

Ưu điểm: Blockchain liên kết có xu hướng an toàn hơn, có khả năng mở rộng và hiệu quả hơn so với mạng blockchain công khai. Giống như blockchain riêng tư và blockchain lai, nó cũng cung cấp quyền kiểm soát truy cập.

Nhược điểm: Blockchain liên kết kém minh bạch hơn blockchain công khai. Nó vẫn có thể bị xâm phạm nếu một nút thành viên bị vi phạm và các quy định riêng của blockchain có thể làm suy yếu chức năng của mạng.

Các trường hợp sử dụng: Ngân hàng và thanh toán là hai ứng dụng của loại blockchain này. Các ngân hàng khác nhau có thể liên kết với nhau và thành lập một liên minh, quyết định nút nào sẽ xác thực các giao dịch. Các tổ chức nghiên cứu có thể tạo ra một mô hình tương tự. Blockchain liên minh lý tưởng cho chuỗi cung ứng, đặc biệt là các ứng dụng thực phẩm và thuốc.

2.4. TIỀN MÃ HÓA VÀ TOKENOMICS

2.4.1. Tiền mã hóa

2.4.1.1. Khái niệm

Tiền mã hóa hay tiền điện tử là loại tiền kỹ thuật số được thiết kế để hoạt động thông qua một mạng máy tính, không phụ thuộc vào bất kỳ cơ quan trung ương nào, chẳng hạn như chính phủ hay ngân hàng. Đây là một dạng tiền tệ kỹ thuật số sử dụng mật mã để bảo mật các quy trình liên quan đến việc tạo đơn vị, thực hiện giao dịch và xác minh quyền sở hữu của tiền tệ.

Hầu hết các loại tiền tệ hiện đại được gọi là tiền tệ fiat, được quản lý và sản xuất bởi các cơ quan chính phủ (ví dụ, đồng đô la Mỹ). Ngược lại, tiền mã hóa không được phát hành bởi cơ quan chính phủ nào và không có cơ quan duy nhất quản lý mà hoạt động dựa trên một phương pháp tiếp cận đồng thuận phân tán.

Tiền mã hóa được đặt tên từ sự kết hợp giữa "mật mã" và "tiền tệ". Trung tâm của tất cả các loại tiền mã hóa là một thuật toán mật mã với mã hóa phức tạp. Tiền mã hóa được tạo ra bằng cách giải quyết một phần thuật toán băm mật mã trong một chuỗi dài, thay vì là một đơn vị vật lý (như đồng xu hay tờ tiền). Tài sản tiền mã hóa thường được lưu trữ trong ví kỹ thuật số để theo dõi và quản lý.

Các giao dịch tiền mã hóa trên toàn cầu được giám sát bởi một sổ cái phân tán, phi tập trung, mà không có sự kiểm soát của bất kỳ cơ quan trung ương nào. Một trong những loại tiền mã hóa nổi tiếng nhất là Bitcoin, được giới thiệu vào năm 2009. Kể từ đó, tiền mã hóa đã trở nên cực kỳ phổ biến, và hiện nay có hơn 10.000 loại tiền kỹ thuật số đang lưu hành trên toàn cầu.

Tiền mã hóa hoạt động như thế nào?

Tiền mã hóa có thể hoạt động toàn cầu, không bị giới hạn bởi múi giờ, và hoạt động 24/7. Một điểm nổi bật là tiền mã hóa không cần các trung gian như ngân hàng, giúp giảm thiểu chi phí và thời gian xử lý giao dịch. Cũng chính vì vậy, tiền mã hóa hỗ trợ các giao dịch P2P (peer-to-peer), cho phép cá nhân giao dịch trực tiếp với nhau mà không cần bên trung gian.

Đồng tiền mã hóa đầu tiên?

Bitcoin là đồng tiền mã hóa đầu tiên và nổi tiếng nhất. Được tạo ra vào năm 2009 bởi một người hoặc nhóm người có tên là Satoshi Nakamoto, Bitcoin đã mở đường cho hàng nghìn loại tiền mã hóa khác. Mặc dù tiền mã hóa có thể được sử dụng làm phương tiện trao đổi như tiền tệ truyền thống, nhưng trong những năm qua, công dụng của nó đã phát triển rộng rãi, bao gồm ứng dụng trong các lĩnh vực tài chính phi tập trung (DeFi), trí tuệ nhân tạo, game, quản trị, chăm sóc sức khỏe, và đồ sưu tầm kỹ thuật số, cùng nhiều ngành khác.

2.4.1.2. Những đặc điểm chính của tiền mã hóa?

Một số đặc điểm nổi bật của tiền mã hóa:

Phi tập trung: Không có cơ quan trung ương nào điều hành tiền mã hóa, mà dựa vào hệ thống mạng phân tán.

Bảo mật cao: Các giao dịch được mã hóa mạnh mẽ và khó bị giả mạo, nhờ vào thuật toán mã hóa (cryptography).

Giao dịch nhanh chóng và toàn cầu: Tiền mã hóa có thể được giao dịch qua mạng internet, giúp quá trình chuyển tiền diễn ra nhanh chóng và không bị hạn chế bởi biên giới quốc gia.

Tính ẩn danh: Mặc dù các giao dịch được ghi nhận trên blockchain, thông tin về người dùng có thể được giữ ẩn, chỉ hiển thị dưới dạng địa chỉ ví.

Bitcoin (BTC) là đồng tiền mã hóa đầu tiên và phổ biến nhất, nhưng hiện nay có hàng nghìn loại tiền mã hóa khác nhau như Ethereum (ETH), ADA, Litecoin, Ripple, v.v.

Các thức hoạt động của tiền mã hóa?

Mạng lưới blockchain

Tiền mã hóa hoạt động trên một mạng lưới phân tán gồm các node (máy tính) có nhiệm vụ xác minh và xác thực giao dịch trong một sổ cái công khai gọi là blockchain. Mỗi node lưu trữ một bản sao của blockchain và cập nhật khi có giao dịch mới. Sau khi giao dịch được xác nhận, nó sẽ được ghi lại vĩnh viễn và không thể thay đổi.

Với kiến trúc phi tập trung, blockchain không có điểm lỗi duy nhất, giúp bảo mật hệ thống. Nếu một node thực hiện giao dịch không hợp lệ, nó sẽ bị loại khỏi mạng. Điều này đảm bảo tính bảo mật, minh bạch, và toàn vẹn của các giao dịch trên blockchain.

Mật mã học

Tiền mã hóa sử dụng mật mã để bảo mật các giao dịch, bảo vệ tính toàn vẹn dữ liệu và kiểm soát việc tạo ra các đơn vị mới. Khi bạn thực hiện giao dịch tiền mã hóa, bạn sử dụng khóa riêng tư của mình để tạo chữ ký số. Mạng lưới sẽ kiểm tra chữ ký này, và nếu hợp lệ, giao dịch của bạn sẽ được ghi vào một block mới và lưu trên mạng lưới blockchain.

2.4.1.3 Phân loại tiền mã hóa?

Cho đến nay, có nhiều loại tiền mã hóa khác nhau, cũng giống như có nhiều loại tiền pháp định khác nhau do các chính phủ toàn cầu phát hành. Trong khi Bitcoin được cho là loại tiền mã hóa nổi tiếng nhất, nhiều loại tiền mã hóa khác đã xuất hiện trong những năm qua. Bao gồm Dogecoin, Ethereum, Cardano ... phổ biến trên internet. Sau đây là các loại tiền mã hóa phổ biến:

Bitcoin

Bitcoin là loại tiền mã hóa đầu tiên, được ra mắt vào năm 2009 và được tạo ra bởi người hoặc nhóm người có tên Satoshi Nakamoto. Bitcoin (BTC) hiện là đồng tiền mã hóa nổi tiếng nhất và được sử dụng rộng rãi như một phương tiện lưu trữ giá trị và phương tiện trao đổi.

Bitcoin sử dụng cơ chế proof-of-work (PoW), trong đó các thợ đào cạnh tranh để xác thực giao dịch và nhận phần thưởng dưới dạng block. Quá trình đào yêu cầu sức mạnh tính toán lớn để giải các bài toán phức tạp, từ đó giúp bảo mật mạng lưới.

Với nguồn cung hạn chế chỉ 21 triệu coin, Bitcoin trở nên khan hiếm và được ví như "vàng kỹ thuật số". Tính khan hiếm này làm tăng giá trị và sự hấp dẫn của Bitcoin như một tài sản đầu tư dài hạn.

Tất cả các loại tiền mã hóa không phải ***Bitcoin*** thường được gọi là ***altcoin***.

Một số đồng tiền mã hóa altcoin phổ biến:

Ether (ETH)

Ether (ETH) là đồng coin gốc của blockchain Ethereum, được tạo ra bởi Vitalik Buterin. Ethereum cung cấp một mạng lưới phi tập trung, cho phép các nhà phát triển xây dựng DApp (ứng dụng phi tập trung) thông qua hợp đồng thông minh.

Ban đầu, Ethereum sử dụng cơ chế đồng thuận proof-of-work (PoW), nhưng sau đó đã chuyển sang proof-of-stake (PoS) để cải thiện hiệu quả và giảm mức tiêu thụ năng lượng. Với PoS, người dùng có thể stake ETH để xác thực giao dịch và bảo mật mạng lưới, thay vì dựa vào công suất tính toán của các node.

Cardano (ADA)

Cardano (ADA) ra mắt vào ngày 29 tháng 9 năm 2017, khi mạng Cardano chính thức đi vào hoạt động và đồng tiền ADA bắt đầu được giao dịch trên các sàn tiền mã hóa. Cardano được phát triển bởi IOHK (Input Output Hong Kong), với mục tiêu xây dựng một nền tảng blockchain an toàn, bền vững và có khả năng mở rộng cao.

Cardano là nền tảng blockchain mã nguồn mở do Charles Hoskinson sáng lập, nhằm cung cấp một hệ thống an toàn cho các ứng dụng phân tán và hợp đồng thông minh. Cardano sử dụng cơ chế đồng thuận Proof of Stake (PoS) mang tên Ouroboros, giúp tiết kiệm năng lượng và tăng khả năng mở rộng.

Cardano có kiến trúc phân tách thành hai tầng: Settlement Layer (SL) cho giao dịch và Computation Layer (CL) cho hợp đồng thông minh. Hệ thống hỗ trợ hợp đồng thông minh qua ngôn ngữ Plutus, với mục tiêu đảm bảo khả năng tương tác giữa các blockchain khác và phát triển bền vững. Token ADA là đồng tiền chính, được sử dụng trong các giao dịch và staking.

BNB

BNB ra mắt vào năm 2017 dưới dạng token ERC-20 trên blockchain Ethereum. Vào năm 2019, BNB chuyển sang blockchain riêng và hiện là đồng tiền mã hóa gốc của hệ sinh thái BNB Chain.

Tương tự như Ethereum, BNB Chain cung cấp môi trường cho hợp đồng thông minh và DApp, với phí giao dịch thấp và thời gian xử lý nhanh hơn các blockchain khác.

Tether (USDT)

USDT là một stablecoin neo vào đồng USD được Tether Limited Inc. ra mắt vào năm 2014. Stablecoin là loại tiền mã hoá được thiết kế để luôn duy trì giá trị với một tài sản dự trữ, chẳng hạn như đô la Mỹ hoặc một loại tiền pháp định khác.

Litecoin

Là một altcoin hoặc giải pháp thay thế Bitcoin ban đầu, Litecoin ban đầu nổi lên nhờ sử dụng thuật toán băm Scrypt, được những người ủng hộ cho là dễ quản lý hơn so với mã hóa SHA-256 mà Bitcoin sử dụng. Litecoin có mã là LTC được phát hành lần đầu tiên vào năm 2011 bởi tác giả Charlie Lee; vốn hóa thị trường ước tính khoảng 12 tỷ đô la mỹ.

2.4.1.4. Các ứng dụng của tiền mã hoá trong nền kinh tế

Tiền mã hoá ngày càng được chấp nhận và sử dụng rộng rãi bởi nhiều ngành nghề, thành phần khác nhau trong nền kinh tế trên nhiều quốc gia khác nhau, ứng dụng của tiền mã hoá trong nền kinh tế tập trung trong ba lĩnh vực chủ yếu gồm có: Thanh toán, chuyển tiền, và đầu tư.

Dịch vụ chuyển tiền

Một trong những ứng dụng lớn của các loại tiền mã hóa, đặc biệt là Litecoin (LTC), Stellar Lumen (XLM) và Bitcoin Cash (BCH), là khả năng thực hiện giao dịch quy mô lớn trong thời gian ngắn và chi phí thấp, nhờ nền tảng công nghệ chuỗi khối. Ví dụ, một giao dịch chuyển tiền bằng LTC trị giá 99 triệu USD được hoàn tất trong 2,5 phút với phí giao dịch chỉ 0,4 USD (Lielacher, 2018). Quy trình này, bao gồm cả thời gian và chi phí, được đánh giá vượt trội so với chi phí dịch vụ chuyển tiền tại các định chế tài chính truyền thống.

Thanh toán

Tiền mã hóa được một số tổ chức và đơn vị chấp nhận sử dụng cho thanh toán giao dịch hoặc trả thưởng cho nhân viên và thành viên tham gia. Ví dụ, nền tảng Steemit thưởng tiền mã hóa cho các thành viên đăng bài và quản lý nội dung, nhằm khuyến khích chất lượng nội dung trên trang web (Lielacher, 2018). Theo thống kê của Statista (2020), số lượng tài khoản ví điện tử Blockchain toàn cầu đã tăng gần 5 lần, từ 8,95 triệu ví (quý 3/2016) lên gần 44,7 triệu ví (quý 4/2019).

Một số công ty du lịch như CheapAir và Destinia chấp nhận Bitcoin trong thanh toán cho vé máy bay, thuê phương tiện và dịch vụ khách sạn (Lielacher, 2018). Sự phổ biến của các ATM Bitcoin trên thế giới giúp dễ dàng đổi tiền mã hóa sang tiền pháp định tại nhiều thành phố du lịch lớn. Thống kê từ coinmap cho thấy mức độ chấp nhận rộng rãi của các chủ thể tham gia nền kinh tế đối với Bitcoin và tiền mã hóa trong lĩnh vực thanh toán.

Huy động vốn và Đầu tư

Huy động vốn qua ICOs (Initial Coin Offerings) ngày càng trở nên phổ biến và quan trọng, đặc biệt đối với các doanh nghiệp khởi nghiệp trong lĩnh vực công nghệ chuỗi khối. Điều này đặc biệt có ý nghĩa đối với các doanh nghiệp nhỏ, khó tiếp cận các nguồn vốn truyền thống từ các định chế tài chính hoặc thị trường chứng khoán.

Thuật ngữ "tiền mã hóa" trong ICOs đề cập đến các token phát hành bởi các dự án hoặc tổ chức cụ thể, khác với các đồng tiền mã hóa như Bitcoin hay Ethereum. Mặc dù token và coin (tiền mã hóa) thường bị nhầm lẫn, chúng có tính chất và đặc điểm khác biệt.

Để huy động vốn qua ICOs, các tổ chức phát hành (doanh nghiệp khởi nghiệp blockchain) cần tạo ra hệ thống tiền tệ riêng (token), được định giá và bán cho nhà đầu tư bằng tiền mã hóa. Nhà đầu tư có thể nắm giữ hoặc bán token trên thị trường thứ cấp, nhưng thị trường này thường có thanh khoản kém (Lipush, 2018).

Khác với việc phát hành chứng khoán, yêu cầu tuân thủ quy định của Bộ Tài chính, ICOs không chịu sự quản lý chặt chẽ của cơ quan chức năng. Doanh nghiệp chỉ cần có sách trắng (whitepaper) để mô tả ý tưởng kinh doanh và mục đích sử dụng vốn, thay vì phải có báo cáo như trong phát hành chứng khoán.

2.4.2. Tokenomics

2.4.2.1. Khái niệm

Trong nền kinh tế học truyền thống, quá trình sản xuất, phân phối và tiêu thụ hàng hóa thường gắn liền với các phương tiện trao đổi như tiền tệ và hàng hóa. Tiền tệ là phương tiện trao đổi phổ biến, giúp đơn giản hóa việc mua bán và định giá hàng hóa, dịch vụ. Trước khi tiền tệ ra đời, việc trao đổi hàng hóa trực tiếp (barter) là hình thức phổ biến, trong đó một loại hàng hóa được đổi lấy một loại hàng hóa khác có giá trị tương đương.

Tương tự, trong hệ sinh thái blockchain, phương thức trao đổi, quản lý và lưu hành chủ yếu là các token kỹ thuật số (hay còn gọi là tokenomics). Tokenomics đề cập đến các yếu tố kinh tế liên quan đến sự phát triển, phân phối và sử dụng các token trong blockchain, nó đóng vai trò tương tự như tiền tệ trong nền kinh tế truyền thống.

Hiểu về tokenomics là điều quan trọng đối với những ai tham gia hoặc quan tâm đến tiền mã hóa, vì nó ảnh hưởng trực tiếp đến giá trị, tiện ích và tiềm năng của tài sản kỹ thuật số. Việc nắm vững các khái niệm cơ bản trong tokenomics sẽ giúp khám phá lý do tại sao nó đóng vai trò then chốt đối với tương lai của tài chính phi tập trung (DeFi) và nền kinh tế số.

Tokenomics là gì?

*"**Tokenomics** là thuật ngữ kết hợp giữa "token" và "economics" (kinh tế học), dùng để chỉ các yếu tố kinh tế liên quan đến việc tạo ra, phân phối, sử dụng và quản lý token trong các hệ sinh thái blockchain. Tokenomics đóng vai trò quan trọng trong việc đảm bảo sự phát triển và ổn định của một dự án tiền mã hóa, vì nó ảnh hưởng trực tiếp đến giá trị, tiện ích và tiềm năng của token trong hệ sinh thái đó."*

Chúng ta hãy cùng xem xét crypto token là gì?: Crypto token là đơn vị tiền tệ kỹ thuật số được các dự án tiền mã hóa xây dựng trên các blockchain hiện có. Giống như các loại tiền tệ truyền thống, crypto token có giá trị và có thể trao đổi được.

Về mặt kinh tế, sự khác biệt giữa kinh tế token và kinh tế truyền thống rất quan trọng. Trong lịch sử, các chính phủ đã tạo ra tiền mà không dựa vào cơ sở thực tế, thường thông qua việc đúc tiền để giải quyết các vấn đề như chiến tranh hay hạn hán. Tuy nhiên, việc tạo thêm tiền sẽ làm giảm giá trị đồng tiền hiện tại.

Ngược lại, các dự án tiền mã hóa xác định trước lịch phát hành và số lượng token thông qua thuật toán, giúp ta có thể dự đoán chính xác số lượng coin đang lưu hành tại một thời điểm cụ thể. Mặc dù có thể thay đổi lịch phát hành, nhưng quá trình này rất khó thực hiện và nó được kiểm soát chặt chẽ.

Ví dụ, Bitcoin có tổng nguồn cung tối đa là 21 triệu token, với số lượng Bitcoin được tạo ra thông qua quá trình đào. Phần thưởng được trao cho miners mỗi khi một block mới được khai thác, diễn ra trong khoảng thời gian 10 phút. Phần thưởng này sẽ giảm một nửa sau mỗi 210.000 block, tương đương với khoảng thời gian 4 năm. Dự kiến rằng Bitcoin sẽ được khai thác hết vào khoảng năm 2140.

Ngoài phần thưởng từ việc khai thác block, tokenomics của Bitcoin còn bao gồm phí giao dịch mà miners nhận được khi một khối mới được xác nhận. Phí giao dịch này sẽ tăng khi số lượng giao dịch và tình trạng tắc nghẽn mạng tăng lên. Điều này giúp ngăn chặn spam và đảm bảo tính hiệu quả của mạng lưới, đồng thời khuyến khích miners tiếp tục tham gia vào quá trình khai thác khi phần thưởng từ block subsidy[5] giảm theo thời gian.

2.4.2.2. Phân loại

Tokenomics (token economics) đề cập đến thiết kế, quản lý và phân tích hệ sinh thái của token trong các dự án blockchain. Việc phân loại tokenomics thường dựa trên các khía cạnh liên quan đến mục đích, chức năng, và cách thức hoạt động của token. Dưới đây là một cách phân loại phổ biến:

a) Phân loại theo mục đích sử dụng

Utility Token (Token tiện ích):

Utility Token hay còn gọi là Token tiện ích, là một loại cryptocurrency được tạo ra và sử dụng cho các mục đích cụ thể trong hệ sinh thái của một dự án blockchain. Utility Token không đại diện cho quyền sở hữu hoặc cổ phần trong doanh nghiệp.

Utility Token được thiết kế để cung cấp quyền truy cập vào một sản phẩm, dịch vụ, hoặc nền tảng blockchain.

Ví dụ: Ethereum (ETH) để thanh toán phí giao dịch, Binance Coin (BNB) để giảm phí giao dịch trên sàn Binance.

Security Tokens:

Token đại diện cho một tài sản thực hoặc quyền lợi đầu tư (ví dụ: cổ phiếu, trái phiếu). Chúng thường bị điều chỉnh bởi các quy định tài chính.

Security Token hay còn gọi là Token chứng khoán, là một loại cryptocurrency đại diện cho quyền sở hữu hoặc lợi ích kinh tế trong một tài sản hoặc dự án nào đó. Nó được phát hành trên nền tảng blockchain và tuân theo các quy định pháp lý về chứng khoán.

[5] *block subsidy*: là phần thưởng mà các **miners** nhận được khi khai thác thành công một khối (block) mới trong mạng lưới blockchain. Đây là một cơ chế quan trọng giúp khuyến khích các miners tham gia vào việc duy trì và bảo mật mạng lưới blockchain.

Security Token đại diện cho quyền sở hữu tài sản (cổ phiếu, trái phiếu, bất động sản…), được giao dịch trên các sàn giao dịch tập trung hoặc phi tập trung có hỗ trợ giao dịch Token chứng khoán nhưng phải quy định pháp lý về chứng khoán.

Ví dụ: Các token phát hành theo STO (Security Token Offering); Securitize; tZERO.

Governance Token (Token quản trị):

Token quản trị là loại token được các nhà phát triển tạo ra để cho phép người nắm giữ ảnh hưởng đến quyết định phát triển hoặc quản lý dự án. Những người nắm giữ token quản trị có thể tham gia vào các quyết định như đề xuất tính năng mới, thay đổi hệ thống quản trị, hoặc quyết định về các thay đổi trong dự án.

Trong nhiều trường hợp, các thay đổi sẽ được đề xuất, thẩm định và bỏ phiếu thông qua hệ thống quản trị trên chuỗi, với việc áp dụng tự động nhờ hợp đồng thông minh. Trong những trường hợp khác, nhóm phát triển dự án sẽ thực hiện các thay đổi theo yêu cầu.

Các hệ thống sử dụng token quản trị giúp phi tập trung và dân chủ hóa quyết định, phản ánh lý tưởng ban đầu của tiền điện tử. Các tổ chức như vậy thường được gọi là Tổ chức tự trị phi tập trung (DAO).

Một ví dụ điển hình về token quản trị là Maker (MKR), cho phép người nắm giữ tham gia vào quyết định liên quan đến giao thức tài chính phi tập trung (DeFi) của stablecoin DAI.

Mỗi token quản trị thường tương đương với một phiếu bầu cho các đề xuất, mặc dù có thể có những phương pháp khác. Người nắm giữ token có thể chấp nhận hoặc từ chối thay đổi đối với ứng dụng phi tập trung (dApp) hoặc blockchain trong các giai đoạn bỏ phiếu. Nhiều dApp cũng cho phép người dùng tạo sáng kiến và đưa chúng ra bỏ phiếu.

Payment Tokens (Token thanh toán):

Token thanh toán là loại token được sử dụng như phương tiện thanh toán và trao đổi thay thế. Khác với tiền tệ fiat như Đô la Mỹ, Euro hay Yên Nhật, token thanh toán như Bitcoin chưa phải là tiền tệ hợp pháp và chưa được chính phủ hỗ trợ. Mục tiêu chính của chúng là trở thành công cụ phi tập trung để mua bán hàng hóa và dịch vụ mà không cần trung gian truyền thống, với chức năng hạn chế hoặc không có chức năng bổ sung.

Ví dụ, vào tháng 1 năm 2019, FCA (Cơ quan Quản lý Tài chính Vương quốc Anh) xác nhận rằng token thanh toán (hoặc token trao đổi) "hiện nằm ngoài phạm vi quản lý", có nghĩa là các hoạt động liên quan đến chuyển nhượng, mua bán các token này, bao gồm hoạt động của các sàn giao dịch tiền điện tử, không được FCA quản lý. Tương tự, FINMA của Thụy Sĩ cũng không coi token thanh toán là chứng khoán, nhưng nếu có thay đổi trong luật hoặc văn bản pháp lý, FINMA sẽ điều chỉnh hoạt động của mình.

Ngoài ra, theo bản sửa đổi AMLD 5 của EU về chống rửa tiền, các quy tắc AML (Chống Rửa Tiền) sẽ được áp dụng chặt chẽ hơn đối với các thực thể thực hiện các hoạt động liên quan đến tiền mã hóa. Các quy định này yêu cầu các quốc gia thành viên thực hiện trước ngày 10 tháng 1 năm 2020, bao gồm các hoạt động như trao đổi giữa tài sản tiền mã hóa và tiền pháp định, quản lý tài sản tiền mã hóa, và cung cấp dịch vụ tài chính liên quan đến tài sản tiền mã hóa.

Stablecoin (Token ổn định giá):

Stablecoin (Token ổn định giá) là loại tiền điện tử có giá trị gắn liền với một tài sản ổn định, như tiền pháp định (USD, EUR) hoặc vàng. Ví dụ điển hình bao gồm Tether (USDT) và USD Coin (USDC).

Mục tiêu chính của stablecoin là duy trì giá trị ổn định bằng cách gắn giá trị thị trường của chúng với một tham chiếu bên ngoài, có thể là tiền pháp định, vàng hoặc các công cụ tài chính khác. Stablecoin nhằm giải quyết vấn đề biến động giá cao của các loại tiền điện tử phổ biến như Bitcoin (BTC), làm chúng ít phù hợp cho các giao dịch thông thường.

Stablecoin đóng vai trò quan trọng trong hệ sinh thái tiền mã hóa nhờ tính ổn định của chúng. Các loại tiền mã hóa như Bitcoin và Ether cung cấp nhiều lợi ích, như không cần trung gian trong thanh toán, nhưng giá của chúng có thể dao động mạnh, làm khó khăn cho việc sử dụng hàng ngày. Stablecoin giúp giải quyết vấn đề này bằng cách gắn giá trị với các tài sản ổn định, khuyến khích sử dụng trong các giao dịch thường xuyên và duy trì giá trị theo thời gian.

b) Phân loại theo cơ chế phát hành và quản lý

Inflationary Token (Token lạm phát):

Lạm phát token (Token Inflation) là sự gia tăng số lượng token lưu thông theo thời gian, làm giảm giá trị của từng token và ảnh hưởng đến giá trị tài sản của các nhà đầu tư khi cung vượt quá cầu.

Các yếu tố dẫn đến lạm phát token bao gồm:

- Gia tăng số lượng token do các hoạt động mở khóa token theo lộ trình roadmap.
- Tấn công dự án: Hacker có thể tạo ra nhiều token và đưa vào lưu thông.
- Khuyến khích staking và lock token: Nếu chính sách staking hoặc lock không hấp dẫn, lượng token mới đưa vào lưu thông sẽ vượt quá lượng token bị khoá, dẫn đến lạm phát.

Tóm lại, các yếu tố chính dẫn đến lạm phát token bao gồm tăng số lượng token, thiếu nhu cầu sử dụng, thay đổi chính sách phát hành, tác động của thị trường, tấn công và không đồng bộ với nhu cầu thị trường.

Deflationary Token (Token giảm phát):

Token giảm phát là loại token có giá trị gia tăng theo thời gian khi nguồn cung giảm hoặc không đổi. Mục tiêu của token giảm phát là giảm dần số lượng token trong lưu thông để đạt được sự khan hiếm, từ đó tăng giá trị theo thời gian.

Khác với token lạm phát, token giảm phát không có tỷ lệ giảm phát cố định trong giao thức mà thay vào đó, giao thức sẽ quy định các điều kiện để loại bỏ token khỏi lưu thông, thường thông qua quy trình đốt token. Cơ chế này giúp giảm nguồn cung theo thời gian, nhưng tốc độ giảm có thể thay đổi tùy thuộc vào hoạt động của mạng lưới.

Các token giảm phát có thể có giới hạn nguồn cung cố định hoặc biến đổi. Ví dụ, một token có tỷ lệ giảm phát 2% sẽ giảm tổng nguồn cung token của nó xuống 2% mỗi năm. Một số token giảm phát cũng đốt một phần token như phí gas trong các giao dịch trên blockchain.

Một ví dụ về token giảm phát là Binance Coin (BNB). Binance thực hiện sự kiện đốt coin hàng quý để loại bỏ lượng BNB dư thừa và cũng đốt một phần BNB như phí giao dịch. Binance cam kết sẽ đốt 50% tổng nguồn cung của BNB.

Fixed Supply Token (Token có cung cố định):

Một số loại tiền mã hóa, như Bitcoin, tuân theo mô hình cung cấp token cố định. Điều này có nghĩa là tổng số token sẽ tồn tại được xác định trước và không thể thay đổi. Ví dụ, Bitcoin có nguồn cung cố định là 21 triệu coin, và khi tất cả chúng được khai thác, sẽ không có Bitcoin mới nào được tạo ra.

Nguồn cung token cố định tạo ra sự khan hiếm, vì số lượng token có sẵn là hạn chế, dẫn đến giá trị tiềm năng tăng theo thời gian khi nhu cầu tăng lên. Sự khan hiếm này thường được coi là một trong những lý do đằng sau giá trị của Bitcoin, vì nó phản ánh đặc tính của kim loại quý như vàng, vốn cũng có nguồn cung hạn chế.

Các nhà đầu tư và người đam mê tin rằng sự khan hiếm này góp phần vào tiềm năng của Bitcoin như một kho lưu trữ giá trị và một hàng rào chống lại lạm phát trong các loại tiền tệ fiat truyền thống.

c) Phân loại theo phương thức phát hành

Pre-Mined Token:

Pre-mined tokens là những loại tiền mã hóa được khai thác trước khi dự án chính thức ra mắt. Ví dụ như Ripple (XRP), Cardano (ADA) và Stellar (XLM). Khác với Bitcoin, nơi tiền mới được phát hành thông qua khai thác (mining), các token này đã được tạo ra một phần và phân phối trước ngày ra mắt chính thức của dự án. Khi một loại tiền mã hóa được phát hành trước, có nghĩa là một phần token đã được tạo ra và trong một số trường hợp, đã được phân phối cho nhà đầu tư ICO, nhà phát triển và nhóm dự án.

Các token khai thác trước thường được phát hành trong khối đầu tiên của giao thức và phân phối cho các nhà đầu tư ICO, đội ngũ phát triển, và thành viên nhóm. Ripple (XRP) là một ví dụ, được phát triển như một hệ thống thanh toán tập trung cho phép chuyển tiền nhanh chóng và tiết kiệm chi phí. Tuy nhiên, phần lớn lượng tiền XRP vẫn do Ripple nắm giữ và công ty này kiểm soát việc phát hành token.

Trước khi chuyển sang Proof of Stake (PoS), Ethereum cũng là một ví dụ của tiền mã hóa khai thác trước. Ether đầu tiên được phát hành như một phần thưởng cho những người tham gia ICO vào tháng 7 và tháng 8 năm 2014.

Minted Token:

Minting là quá trình phát hành các tài sản số mới vào trong hệ sinh thái tiền mã hóa. Phương pháp này đưa các đồng tiền hoặc token mới vào lưu thông, cho phép chúng được giao dịch hoặc sử dụng trong hệ sinh thái. Minting tương tự như mining (khai thác), nhưng có một số điểm khác biệt quan trọng.

Trong các hệ thống Proof of Stake (PoS), minting được sử dụng để phát hành đồng tiền mới. Hệ thống này dựa vào validators (người xác thực) hoặc stakers (người đặt cọc) để xác minh giao dịch và thêm các khối mới vào blockchain. Ngược lại, mining gắn liền với cơ chế

Proof of Work (PoW), trong đó miners (thợ đào) sử dụng phần cứng chuyên dụng để giải quyết các bài toán mật mã phức tạp và tạo ra các khối mới trên blockchain.

Một sự khác biệt lớn là trong khi mining tiêu tốn nhiều năng lượng, minting lại thân thiện với môi trường hơn. Mining là quá trình liên tục, duy trì trong suốt thời gian mạng blockchain hoạt động, xác minh giao dịch và củng cố bảo mật của mạng lưới. Trong khi đó, minting diễn ra một lần khi token mới được tạo ra.

Airdrop Token:

Airdrop tiền điện tử là quá trình phân phối token hoặc coin miễn phí cho nhiều cá nhân trong cộng đồng tiền điện tử nhằm khuyến khích tham gia và quảng bá dự án. Đây là một chiến lược phổ biến giúp nâng cao nhận thức về dự án và thu hút người dùng hoặc nhà đầu tư.

Mặc dù tài sản airdrop được phát miễn phí, một số dự án yêu cầu người tham gia hoàn thành nhiệm vụ cụ thể trước khi nhận được token, ví dụ như tham gia nhóm Telegram, theo dõi dự án trên mạng xã hội, hoặc nắm giữ một số lượng nhất định token trong ví. Các airdrop cũng có thể chỉ trao cho ví đã tương tác với nền tảng dự án trước một ngày xác định.

Airdrop trở nên phổ biến trong ICO 2017 và vẫn được sử dụng trong các dự án hiện nay. Tuy nhiên, không có quy tắc cố định cho airdrop và mỗi dự án có thể thiết lập tiêu chí và phương pháp riêng.

d) Phân loại theo giá trị kinh tế

Asset-Backed Token (Token được đảm bảo tài sản):

Token được đảm bảo bởi tài sản (Asset-backed tokens) là các token số hóa đại diện cho tài sản vật lý, được bảo đảm bởi giá trị của tài sản đó. Các tài sản như vàng, dầu thô, bất động sản, cổ phiếu và nhiều tài sản vật lý khác có thể được mã hóa thành token. Các token này được phát triển nhờ công nghệ blockchain, cung cấp một cách tiếp cận ổn định hơn để lưu trữ giá trị và trao đổi tài sản mà không cần sự trung gian của tổ chức tài chính.

Giá trị của asset-backed tokens trực tiếp phụ thuộc vào giá trị của tài sản cơ sở. Quyền sở hữu token thường đại diện cho quyền sở hữu tài sản và có thể đi kèm với kỳ vọng lợi nhuận khi giá trị tài sản tăng. Các token này được phân loại là chứng khoán theo các cơ quan quản lý tài chính.

Phát triển các asset-backed tokens cho phép cá nhân, công ty hoặc tổ chức huy động vốn thông qua blockchain, phát hành token như một công cụ vốn chủ sở hữu mới. Doanh nghiệp cũng có thể token hóa tài sản hiện có để bán, giúp nhà đầu tư, kể cả các nhà đầu tư cá nhân, dễ dàng tham gia vào thị trường mà không cần lưu trữ hoặc trao đổi tài sản vật lý.

Ngoài ra, asset-backed tokens giúp giảm chi phí hậu cần và tăng hiệu quả giao dịch. Chúng cung cấp giải pháp thay thế tài chính cho các vấn đề như tiền tệ bị thổi phồng hoặc mất giá, và giúp cải thiện tính thanh khoản của các thị trường không thanh khoản.

Các chính phủ và thị trường bất động sản đang tiến tới việc sử dụng token hóa tài sản để cải thiện tính thanh khoản và thúc đẩy tính bảo mật và minh bạch trong các giao dịch. Điều này đang làm thay đổi cách thức kinh doanh và suy nghĩ về quyền sở hữu và tạo ra của cải trong tương lai.

Non-Asset-Backed Token (Token không đảm bảo tài sản):

Giá trị dựa vào cung và cầu, không gắn liền với tài sản thực tế. Ví dụ: Dogecoin (DOGE).

Non-Asset-Backed Token (Token không hỗ trợ bởi tài sản) là những loại token không có sự đảm bảo hoặc giá trị từ một tài sản vật lý cụ thể nào. Giá trị của chúng chủ yếu phụ thuộc vào yếu tố thị trường, sự chấp nhận của cộng đồng hoặc các yếu tố kỹ thuật, thay vì được bảo đảm bởi tài sản như vàng, bất động sản hay cổ phiếu.

Ví dụ về Non-Asset-Backed Token:

- Bitcoin (BTC): Là một loại tiền mã hóa không hỗ trợ bởi bất kỳ tài sản vật lý nào. Giá trị của Bitcoin phụ thuộc vào cung cầu và sự tin tưởng của cộng đồng người dùng.

- Ethereum (ETH): Cũng không phải là token hỗ trợ bởi tài sản, mà có giá trị nhờ vào việc sử dụng của nó trong các ứng dụng phân tán (dApps) và hợp đồng thông minh.

- Cardano (ADA): ADA là đồng tiền mã hóa gốc của blockchain cardano. ADA không gắn với một tài sản vật lý hoặc tài chính như Stablecoin (USDT hay USDC); giá trị của ADA đến từ:

+ *Việc sử dụng của blockchain Cardano*: Blockchain này hỗ trợ hợp đồng thông minh, ứng dụng phi tập trung (DApp), và nhiều dự án khác.

+ *Niềm tin cộng đồng*: Cardano được xem là một blockchain thế hệ mới với công nghệ dựa trên bằng chứng cổ phần (Proof of Stake - PoS), giúp tiết kiệm năng lượng và cải thiện khả năng mở rộng.

+ *Các tính năng kỹ thuật*: Cardano chú trọng vào nghiên cứu học thuật và xây dựng các giao thức blockchain bền vững.

Giá trị của ADA từng dao động mạnh, phụ thuộc vào sự phát triển của dự án và điều kiện thị trường; Ví dụ: Trong đợt bull run năm 2021, ADA tăng giá đáng kể nhờ các bản cập nhật quan trọng như Alonzo Hard Fork, cho phép chạy hợp đồng thông minh trên Cardano.

2.4.2.3. Các yếu tố chính của một tokenomics

Tokenomics (hoặc kinh tế học token) là nghiên cứu và thiết kế các yếu tố kinh tế liên quan đến một token trong hệ sinh thái blockchain hoặc cryptocurrency. Các yếu tố chính của tokenomics bao gồm:

Supply (Nguồn cung)

Cung cấp tối đa (Max Supply): Tổng số lượng token tối đa sẽ tồn tại trong suốt đời của dự án. Điều này giúp định hướng sự hiếm hoi của token.

Cung cấp lưu thông (Circulating Supply): Số lượng token hiện tại đang được giao dịch trên thị trường.

Cung cấp phát hành (Issuance Supply): Số lượng token sẽ được phát hành theo thời gian, có thể bao gồm các token đã được phát hành và token sẽ được phát hành trong tương lai.

Demand (Nhu cầu)

Đây là các yếu tố thúc đẩy nhu cầu sử dụng và nắm giữ token, bao gồm các ứng dụng trong hệ sinh thái, sự chấp nhận của cộng đồng và tính tiện ích của token trong các sản phẩm/dịch vụ.

Utility (Tính tiện ích)

Token phải có mục đích sử dụng cụ thể trong hệ sinh thái, chẳng hạn như thanh toán dịch vụ, quyền truy cập vào sản phẩm, staking để nhận thưởng, hoặc tham gia quản trị của hệ thống (governance).

Incentives (Khen thưởng)

Các cơ chế khuyến khích người dùng giữ token hoặc tham gia vào hệ sinh thái, ví dụ như phần thưởng từ staking, yield farming, hay các chương trình đào coin.

Governance (Quản trị)

Một số token có thể được sử dụng để tham gia vào việc quản lý dự án, chẳng hạn như bỏ phiếu về các thay đổi trong giao thức hoặc quyết định về sự phát triển của dự án.

Vesting (Lộ trình phát hành)

Quy trình phát hành token đối với đội ngũ sáng lập, nhà đầu tư và các bên liên quan khác trong một thời gian nhất định. Điều này giúp đảm bảo rằng các bên này không bán token ngay lập tức, giúp ổn định giá trị token trong dài hạn.

Burning (Đốt token)

Một số hệ thống áp dụng cơ chế đốt token (burn) nhằm giảm số lượng token lưu hành trên thị trường, giúp tăng giá trị của các token còn lại.

Distribution (Phân phối)

Cách thức phân phối token cho cộng đồng, nhà đầu tư và các bên liên quan khác. Có thể thông qua các ICO, airdrop, staking rewards hoặc các hình thức khác.

Tất cả các yếu tố này phải được thiết kế và tối ưu sao cho hợp lý để đảm bảo sự phát triển bền vững của dự án và tạo ra động lực cho người dùng tham gia vào hệ sinh thái.

2.5. NFT

2.5.1. Khái niệm

NFT (Non-Fungible Token) là tài sản kỹ thuật số độc nhất, được xây dựng trên công nghệ blockchain, đại diện cho quyền sở hữu hoặc quyền truy cập duy nhất vào sản phẩm hoặc dịch vụ số cụ thể. Điểm đặc trưng của NFT là tính không thể thay thế (non-fungible), nghĩa là mỗi NFT là duy nhất và không thể thay thế bằng NFT khác, khác với các tài sản có thể thay thế như tiền điện tử (ví dụ: 1 Bitcoin có giá trị ngang bằng với 1 Bitcoin khác).

NFT được sử dụng để tạo và xác thực quyền sở hữu đối với các tài sản số như hình ảnh, âm nhạc, video clip, và bất động sản ảo. Mỗi NFT có một mã nhận dạng duy nhất, được lưu trữ trên blockchain, giúp đảm bảo tính xác thực và quyền sở hữu tài sản. Công nghệ blockchain đóng vai trò quan trọng trong việc xác thực quyền sở hữu và tính nguyên bản của NFT.

Khác với tài sản truyền thống như cổ phiếu hoặc tiền tệ, NFT không thể thay thế hoặc trao đổi ngang giá với vật phẩm tương tự. Điều này khiến NFT giống như các vật phẩm sưu tầm quý hiếm trong thế giới thực. NFT thường không thể chia nhỏ, nhưng một số nền tảng như Fractional cho phép chia sẻ quyền sở hữu NFT, cho phép NFT được chia thành các phần nhỏ để bán cho nhiều người mua.

NFT cũng không thể thay đổi sau khi đã được mã hóa trên blockchain, và tính hợp pháp của nó được xác thực thông qua blockchain nơi nó được lưu trữ

Tại sao NFT lại quan trọng?

Justin Herzig, đồng sáng lập của Own the Moment NFT, cho rằng sự gia tăng mức độ phổ biến của NFT là kết quả của tính dễ sử dụng, bản chất đầu cơ như vật phẩm sưu tầm và đầu tư, cùng sự phát triển của cộng đồng xung quanh các sản phẩm này.

NFT cho phép cá nhân mua và bán tài sản kỹ thuật số theo cách mới, giúp nghệ sĩ và người sáng tạo nội dung thể hiện kỹ năng dưới dạng kỹ thuật số. Nó cung cấp khả năng định giá, mua bán, và trao đổi nghệ thuật kỹ thuật số một cách an toàn bằng sổ cái kỹ thuật số. NFT giúp phát triển các trao đổi giá trị sáng tạo, xây dựng các cấu trúc thị trường mới.

Herzig cũng nhấn mạnh rằng NFT là một hình thức đầu tư thay thế hấp dẫn, liên kết với sở thích cá nhân và đam mê của người mua, đồng thời mang lại giá trị tài chính và tiện ích. Người mua NFT hy vọng giá trị của token sẽ tăng theo thời gian, giống như bất kỳ khoản đầu tư nào khác, và giá trị của NFT phụ thuộc vào cung và cầu.

Theo Grand View Research, thị trường NFT được định giá 20,44 tỷ đô la vào năm 2022 và dự kiến sẽ đạt 211,72 tỷ đô la vào năm 2030.

NFT trên nền tảng cardano?

NFT đầu tiên trên Cardano, SpaceBudz, được ra mắt vào tháng 3 năm 2021. Đây là bộ sưu tập gồm 10.000 hình ảnh động vật phi hành gia độc đáo, mỗi hình ảnh được mã hóa dưới dạng NFT trên blockchain Cardano. SpaceBudz đã tiên phong trong việc áp dụng tiêu chuẩn siêu dữ liệu NFT và triển khai thị trường dựa trên hợp đồng thông minh đầu tiên trên Cardano.

Sự ra mắt của SpaceBudz đã đánh dấu một bước ngoặt quan trọng trong việc phát triển hệ sinh thái NFT trên Cardano, mở đường cho nhiều dự án NFT khác trên nền tảng này.

Để tham gia vào thị trường NFT trên Cardano, người dùng cần có ví tiền điện tử tương thích với Cardano, như Nami hoặc Daedalus, và kết nối với các sàn giao dịch NFT như CNFT.io hoặc jpg.store.

2.5.2. Đặc điểm

2.5.2.1. Tính độc nhất (Uniqueness)

Mỗi NFT là duy nhất và không thể sao chép. Thông tin metadata của NFT được lưu trữ trên blockchain, đảm bảo rằng mỗi token có các đặc điểm riêng biệt.

2.5.2.2. Không thể thay thế (Non-fungibility)

Không giống như các tài sản có thể thay thế (như Bitcoin hoặc tiền mặt), NFT không thể trao đổi ngang giá. Mỗi NFT có giá trị riêng dựa trên độ hiếm, tính độc đáo, hoặc giá trị thị trường.

2.5.2.3. Quyền sở hữu rõ ràng (Ownership)

NFT ghi lại quyền sở hữu trong blockchain. Người sở hữu có thể chứng minh quyền sở hữu của mình và chuyển nhượng token nếu muốn.

2.5.2.4. Tính bền vững và minh bạch (Immutability & Transparency)

Thông tin và lịch sử giao dịch của NFT được lưu trữ công khai trên blockchain, không thể bị thay đổi hoặc xóa bỏ.

2.5.2.5. Khả năng chia nhỏ hạn chế (Indivisibility)

Hầu hết NFT không thể chia nhỏ như tiền điện tử. Bạn chỉ có thể sở hữu toàn bộ NFT, không phải một phần của nó (trừ một số trường hợp đặc biệt).

2.5.2.6. Khả năng tương tác (Interoperability)

NFT có thể được sử dụng trên nhiều nền tảng và ứng dụng khác nhau, miễn là chúng tương thích với cùng một blockchain hoặc tiêu chuẩn.

Ví dụ:

- NFT trên Ethereum tuân theo tiêu chuẩn ERC-721 hoặc ERC-1155.

- NFT trên blockchain Cardano được gọi là CNFTs (Cardano Non-Fungible Tokens). Cardano sử dụng tiêu chuẩn CIP-721, tương tự ERC-721 trên Ethereum, để định nghĩa và quản lý NFT. Tiêu chuẩn này đảm bảo tính nhất quán và khả năng tương thích cho các dự án NFT trên mạng lưới.

2.5.2.7. Ứng dụng đa dạng

NFT không chỉ giới hạn trong nghệ thuật số mà còn áp dụng cho:

- Gaming (vật phẩm, nhân vật, tài sản trong game).
- Bất động sản ảo.
- Vé sự kiện hoặc tài sản trí tuệ.
- Sưu tập kỹ thuật số (thẻ bài, tác phẩm nghệ thuật).

2.5.2.8. Khả năng kiếm thu nhập thụ động

Một số NFT cho phép người sở hữu nhận hoa hồng hoặc thu nhập từ việc sử dụng tác phẩm, ví dụ khi tác phẩm được bán lại.

Ví dụ: Trung tuần tháng 3 năm 2022, rapper Binz (Việt nam) kết hợp cùng Công ty blockchain Tuniver ra mắt bộ sưu tập NFT cho ca khúc mới 'Don't Break My Heart'. Bản quyền bài hát này được anh phân chia thành các NFT với 4 hạng khác nhau, tương ứng với 4 mức tỷ lệ chia sẻ bản quyền doanh thu.

2.5.3. Ứng dụng

NFT (Non-Fungible Token) có rất nhiều ứng dụng thực tế trong các lĩnh vực khác nhau, từ nghệ thuật, giải trí đến giáo dục và tài chính. Dưới đây là các ứng dụng phổ biến của NFT:

2.5.3.1. Nghệ thuật số (Digital Art)

Sưu tầm và bán tác phẩm nghệ thuật số. Nghệ sĩ có thể bán tác phẩm của họ trực tiếp cho người mua dưới dạng NFT mà không cần thông qua trung gian. Ví dụ: Beeple đã bán tác phẩm “Everydays: The First 5000 Days” với giá 69,3 triệu USD.

Xác thực và bảo vệ bản quyền. NFT ghi lại nguồn gốc và quyền sở hữu của tác phẩm, giúp ngăn chặn sao chép hoặc giả mạo.

2.5.3.2. Gaming (Trò chơi)

Sở hữu vật phẩm trong game: Người chơi có thể mua, bán hoặc trao đổi tài sản trong game (vũ khí, nhân vật, trang phục) dưới dạng NFT. Ví dụ: Axie Infinity cho phép người chơi sở hữu và giao dịch các sinh vật kỹ thuật số trong game.

Play-to-Earn: Các trò chơi NFT thưởng cho người chơi bằng tiền điện tử, biến việc chơi game thành một nguồn thu nhập.

2.5.3.3. Metaverse và bất động sản ảo

Mua bán đất ảo: Người dùng có thể sở hữu và phát triển đất ảo trong các nền tảng metaverse. Ví dụ: Decentraland, The Sandbox, và Pavia (trên Cardano).

Tài sản kỹ thuật số trong metaverse: NFT được sử dụng để giao dịch các tài sản trong thế giới ảo, như nhà cửa, đồ nội thất, và vật phẩm trang trí.

2.5.3.4. Âm nhạc và giải trí

Bản quyền âm nhạc: Nghệ sĩ có thể phát hành các bài hát hoặc album dưới dạng NFT, cho phép người hâm mộ mua và sở hữu một phần doanh thu bản quyền. Ví dụ: Kings of Leon phát hành album dưới dạng NFT.

Vé sự kiện: NFT có thể được sử dụng như vé điện tử, chống gian lận và tạo trải nghiệm độc quyền cho người tham dự.

2.5.3.5. Sưu tập kỹ thuật số (Digital Collectibles)

Thẻ bài và đồ sưu tập: Các thẻ bài kỹ thuật số, hình ảnh hoặc video nổi bật được phát hành dưới dạng NFT.

Ví dụ: NBA Top Shot cung cấp các khoảnh khắc nổi bật của các trận đấu bóng rổ dưới dạng NFT.

2.5.3.6. Giáo dục và tài liệu số

Bằng cấp và chứng chỉ: NFT có thể dùng để lưu trữ và xác thực bằng cấp, chứng chỉ, đảm bảo không thể làm giả.

Tài liệu học tập: Sách giáo khoa, bài giảng có thể được phát hành dưới dạng NFT, cho phép theo dõi và quản lý bản quyền.

2.5.3.7. Tài chính (DeFi)

Tài sản thế chấp: NFT có thể được sử dụng làm tài sản thế chấp trong các giao dịch tài chính, vay mượn trên nền tảng blockchain.

Quản lý tài sản: NFT đại diện cho quyền sở hữu đối với tài sản trong thế giới thực như bất động sản hoặc cổ phiếu.

2.5.3.8. Thời trang và thương mại điện tử

Quần áo kỹ thuật số: Các thương hiệu thời trang lớn phát hành sản phẩm kỹ thuật số dưới dạng NFT để sử dụng trong metaverse. Ví dụ: Gucci và Nike đã bắt đầu thử nghiệm bán NFT thời trang.

Theo dõi và xác thực: NFT có thể được sử dụng để chứng minh tính xác thực và nguồn gốc của sản phẩm trong chuỗi cung ứng.

2.5.3.9. Từ thiện và gây quỹ cộng đồng

Gây quỹ thông qua NFT: NFT được bán để gây quỹ cho các tổ chức từ thiện hoặc các dự án cộng đồng.

Ví dụ: WWF phát hành NFT về các loài động vật đang bị đe dọa để kêu gọi bảo vệ môi trường.

2.5.3.10. Bản quyền và sở hữu trí tuệ

Bảo vệ bản quyền: Các tác phẩm sáng tạo như video, bài viết, hoặc hình ảnh có thể được lưu trữ dưới dạng NFT để theo dõi và quản lý bản quyền.

Phân phối lợi nhuận: Người sáng tạo có thể kiếm được tiền bản quyền mỗi khi NFT của họ được giao dịch trên thị trường.

2.5.4. Thách thức và cơ hội

2.5.4.1. Thách thức với NFT

Mặc dù NFT đã mang lại nhiều cơ hội sáng tạo và kinh tế, chúng cũng đối mặt với nhiều thách thức đáng chú ý. Dưới đây là các vấn đề chính mà NFT đang phải giải quyết:

a) Tính bất ổn của thị trường

- Biến động giá: Giá trị của NFT thường không ổn định, dễ tăng hoặc giảm mạnh trong thời gian ngắn. Điều này làm cho NFT trở thành một khoản đầu tư rủi ro.

- Thiếu tiêu chuẩn định giá: Việc đánh giá giá trị của một NFT phụ thuộc nhiều vào cảm nhận và thị hiếu của người mua, dẫn đến tình trạng đầu cơ.

- Ví dụ:

Beeple’s NFT - “Everydays: The First 5000 Days”:

Sự kiện: Tác phẩm này được bán với giá kỷ lục 69,3 triệu USD tại Christie's vào tháng 3/2021, gây chấn động thị trường NFT.

Tính bất ổn: Sau cơn sốt, hàng loạt NFT khác cũng ra đời nhưng không thể đạt được mức giá tương tự. Thị trường trở nên bão hòa và giảm nhiệt nhanh chóng.

b) Vấn đề bản quyền và quyền sở hữu

- Tranh chấp bản quyền: Một số NFT bị tạo ra từ tác phẩm của người khác mà không có sự cho phép, gây tranh cãi về quyền sở hữu trí tuệ.

Ví dụ: Hermès vs. Mason Rothschild: Hermès kiện nhà sáng tạo Mason Rothschild vì bộ sưu tập NFT "MetaBirkins" sử dụng hình ảnh của túi xách Birkin mà không được phép. Hermès thắng kiện vào năm 2023, khẳng định quyền sở hữu thương hiệu.

- Tách biệt giữa quyền sở hữu NFT và nội dung: Khi mua một NFT, người mua sở hữu token kỹ thuật số liên kết với một nội dung (tác phẩm nghệ thuật, âm nhạc, video, v.v.), nhưng không đồng nghĩa với việc sở hữu bản quyền của tác phẩm đó. Người mua thường hiểu lầm rằng họ có quyền sao chép, phân phối hoặc chỉnh sửa tác phẩm, trong khi các quyền này vẫn thuộc về người sáng tạo gốc, trừ khi có thỏa thuận khác.

Ví dụ: Bored Ape Yacht Club (BAYC): Chủ sở hữu NFT trong bộ sưu tập này được quyền thương mại hóa hình ảnh của các "Bored Ape" họ sở hữu. Tuy nhiên, điều này là ngoại lệ nhờ điều khoản rõ ràng do nhà sáng tạo đưa ra, không phải quy tắc chung của NFT.

c) Chi phí giao dịch cao

Chi phí giao dịch trong thị trường NFT thường rất cao, đặc biệt trên các nền tảng hoạt động dựa trên blockchain như Ethereum. Đây là một thách thức lớn đối với người dùng và nhà phát triển, gây ra rào cản trong việc mở rộng quy mô thị trường và khuyến khích sự tham gia của người dùng mới.

Ví dụ:

- OpenSea và phí gas cao trên Ethereum:

Trong thời kỳ bùng nổ NFT vào năm 2021, phí gas trên Ethereum từng đạt mức 200–300 USD chỉ để thực hiện một giao dịch đơn giản như mua hoặc bán NFT.

Người dùng nhỏ lẻ bị loại khỏi thị trường do không thể chi trả khoản phí cao này. Chẳng hạn, nếu một NFT có giá 50 USD nhưng phí giao dịch lên đến 200 USD, người mua sẽ khó chấp nhận.

- Mint NFT tốn kém:

Để mint một NFT trên Ethereum, người sáng tạo thường phải trả từ 50–200 USD phí gas, tùy thuộc vào mức độ tắc nghẽn mạng.

Một nghệ sĩ độc lập muốn mint 10 NFT sẽ phải trả 500–2.000 USD phí gas, khiến họ do dự trong việc tham gia thị trường.

d) Lo ngại về môi trường

Tiêu thụ năng lượng lớn: Công nghệ blockchain, đặc biệt là các mạng lưới dựa trên cơ chế Proof of Work (PoW), tiêu thụ một lượng lớn năng lượng, góp phần vào biến đổi khí hậu.

Áp lực chuyển đổi: Các mạng lưới đang phải tìm cách chuyển sang cơ chế thân thiện hơn như Proof of Stake (PoS), nhưng quá trình này không dễ dàng.

Ví dụ:

- Beeple và “Everydays: The First 5000 Days”:

Tác phẩm của Beeple được bán với giá kỷ lục 69,3 triệu USD trên Ethereum vào năm 2021;

Tác động môi trường: Các giao dịch đấu giá và chuyển quyền sở hữu tiêu thụ lượng lớn năng lượng, với tổng khí thải carbon tương đương hàng nghìn tấn CO_2.

- Bộ sưu tập NFT “Space Cat”:

NFT “Space Cat” (hình ảnh một con mèo du hành vũ trụ) được mint và phát hành trên Ethereum. Việc tạo ra và giao dịch Space Cat tiêu thụ **hơn 200 kWh**, tương đương với lượng điện năng tiêu thụ của một gia đình châu Âu trong một tháng.

e) Gian lận và lừa đảo

NFT giả: Một số người tạo NFT từ nội dung không thuộc sở hữu của họ hoặc sao chép NFT của người khác để lừa đảo người mua.

Sàn giao dịch không đáng tin cậy: Một số nền tảng giao dịch thiếu sự minh bạch, dễ bị tấn công hoặc sập đổ, gây thiệt hại cho người dùng.

Ví dụ:

- Frosties NFT (2022): Một trong những vụ rug pull lớn nhất trong năm 2022, nhóm sáng lập Frosties NFT đã lừa đảo người dùng hơn 1,3 triệu USD trước khi xóa bỏ các tài khoản mạng xã hội và ngừng giao tiếp.

- OpenSea và NFT giả mạo (2022): Một trong những sự cố lớn là các nghệ sĩ phát hiện ra rằng tác phẩm của họ đã bị sao chép và bán lại như NFT trên OpenSea mà không có sự cho phép. OpenSea đã phải xử lý hàng nghìn NFT giả mạo, khiến người mua gặp rủi ro lớn.

- Giả mạo MetaMask và OpenSea (2021): Trong một loạt các vụ lừa đảo, hacker gửi email giả mạo OpenSea và MetaMask, yêu cầu người dùng xác minh tài khoản hoặc cung cấp thông tin cá nhân. Sau khi người dùng làm theo, hacker lấy được khóa riêng và chiếm đoạt NFT từ ví của họ.

- The Evolved Apes (2021): Một dự án NFT tên là Evolved Apes đã thu hút hàng triệu USD từ các nhà đầu tư, nhưng nhóm phát triển đột ngột biến mất và không có gì thực sự được phát triển. Người dùng không thể tiếp tục giao dịch NFT và dự án đã chết ngay sau khi thu tiền.

f) Thiếu tính tiện dụng

Độ phức tạp kỹ thuật: Việc tạo, giao dịch hoặc lưu trữ NFT yêu cầu người dùng hiểu biết về công nghệ blockchain, ví tiền điện tử, và các quy trình liên quan.

Hạn chế về trải nghiệm người dùng: Giao diện của các nền tảng NFT hiện tại còn khó sử dụng đối với người mới.

Ví dụ:

- Khó khăn trong việc sử dụng MetaMask và ví tiền mã hóa khác

Một người mới tham gia vào thị trường NFT có thể gặp khó khăn trong việc thiết lập ví MetaMask, kết nối ví với các nền tảng như OpenSea, và thực hiện giao dịch. Quá trình này có thể mất thời gian và dễ gây nhầm lẫn nếu người dùng không có kinh nghiệm.

Người dùng có thể bỏ lỡ cơ hội đầu tư hoặc thậm chí mất tài sản do không thể thực hiện giao dịch chính xác.

- Quá trình mint NFT tốn thời gian và phức tạp

Một nghệ sĩ muốn mint một NFT nhưng gặp khó khăn trong việc tạo và cấu hình hợp đồng thông minh, lựa chọn nền tảng, và thanh toán phí gas. Điều này có thể làm họ cảm thấy bối rối và dễ từ bỏ.

Người sáng tạo không thể phát triển dự án của mình, dẫn đến sự thiếu tham gia của các nghệ sĩ độc lập vào thị trường NFT.

- Phí gas cao gây khó chịu cho người dùng

Một nhà đầu tư muốn mua một NFT có giá 100 USD nhưng phải trả thêm 80 USD phí gas để hoàn tất giao dịch trên Ethereum. Điều này làm giảm tính tiện dụng và có thể khiến người dùng không hài lòng với chi phí giao dịch.

Nhà đầu tư có thể quyết định không mua hoặc bỏ lỡ các cơ hội tiềm năng vì phí giao dịch quá cao.

2.5.4.1. Cơ hội với NFT

NFT (Token không thể thay thế) không chỉ là một phần của thị trường đầu tư tài sản số mà còn mở ra nhiều cơ hội mới trong các lĩnh vực nghệ thuật, giải trí, bất động sản, game và nhiều ngành công nghiệp khác. Dưới đây là một số cơ hội tiềm năng của NFT trong tương lai.

a) NFT trong ngành nghệ thuật và sáng tạo

NFT tạo ra một cơ hội lớn cho các nghệ sĩ và nhà sáng tạo nội dung khi cho phép họ bán và phân phối tác phẩm nghệ thuật dưới dạng tài sản số. Điều này giúp nghệ sĩ tiếp cận một thị trường toàn cầu và nhận được sự công nhận xứng đáng.

- Cơ hội:

+) Nghệ sĩ có thể bảo vệ bản quyền và nhận doanh thu từ việc bán tác phẩm nghệ thuật mà không bị can thiệp.

+) NFT cho phép phân phối và chứng minh quyền sở hữu đối với tác phẩm nghệ thuật số.

+) Các nghệ sĩ không còn phụ thuộc vào các nhà đấu giá hay các công ty lớn để bán tác phẩm của mình.

- Ví dụ: Beeple: Một nghệ sĩ kỹ thuật số nổi tiếng đã bán tác phẩm "Everydays: The First 5000 Days" dưới dạng NFT với giá 69 triệu USD vào năm 2021. Điều này đã mở ra một cơ hội lớn cho các nghệ sĩ số khác để tiếp cận thị trường và kiếm tiền từ các tác phẩm của mình mà không cần qua các trung gian.

b) NFT trong ngành game

NFT có thể thay đổi hoàn toàn cách thức trao đổi tài sản trong các trò chơi điện tử. Người chơi có thể sở hữu và giao dịch các vật phẩm trong game dưới dạng NFT, mang lại cho họ quyền kiểm soát và sở hữu tài sản số lâu dài.

- Cơ hội:

+) Người chơi có thể sở hữu, mua bán và trao đổi vật phẩm trong game như vũ khí, nhân vật, trang phục hoặc đất đai dưới dạng NFT.

+) NFT có thể làm cho các trò chơi có giá trị hơn khi cho phép người chơi sở hữu các vật phẩm có thể giao dịch với người khác.

- Ví dụ: Axie Infinity, đây là một trò chơi blockchain cho phép người chơi nuôi, huấn luyện và chiến đấu với các sinh vật gọi là Axies. Các Axies được đại diện dưới dạng NFT, và người chơi có thể mua bán chúng trên thị trường. Trò chơi này đã thu hút hàng triệu người tham gia và trở thành một ví dụ điển hình về NFT trong game.

c) NFT trong bất động sản

NFT có thể được áp dụng trong ngành bất động sản để đại diện cho quyền sở hữu tài sản vật lý, giúp đơn giản hóa các giao dịch và giảm thiểu thủ tục hành chính phức tạp.

- Cơ hội:

+) Bất động sản có thể được token hóa và đại diện dưới dạng NFT, giúp việc chuyển nhượng quyền sở hữu và giao dịch tài sản trở nên nhanh chóng và minh bạch.

+) NFT có thể giúp giảm thiểu các vấn đề về pháp lý và giấy tờ, đồng thời tạo điều kiện cho những người đầu tư nhỏ lẻ tham gia vào thị trường bất động sản.

- Ví dụ: RealT: Đây là một nền tảng cho phép các nhà đầu tư mua cổ phần bất động sản thông qua các NFT. Người sở hữu NFT có thể nhận phần lợi nhuận từ bất động sản mà họ đầu tư vào. Nền tảng này đang thử nghiệm với việc token hóa bất động sản và đã thu hút sự quan tâm từ các nhà đầu tư.

d) NFT trong âm nhạc và giải trí

NFT đang mở ra cơ hội mới cho các nghệ sĩ âm nhạc và nhà sản xuất nội dung để bán sản phẩm của họ trực tiếp cho người hâm mộ mà không cần thông qua các trung gian như các công ty thu âm hoặc nền tảng trực tuyến.

- Cơ hội:

+) Nghệ sĩ có thể phát hành album, bài hát, video âm nhạc và thậm chí là vé concert dưới dạng NFT, giúp họ giữ lại phần lớn doanh thu và xây dựng một cộng đồng fan trung thành.

+) NFT có thể tạo ra các cơ hội độc quyền cho người hâm mộ, chẳng hạn như quyền truy cập sớm vào các sự kiện hoặc các bản thu âm đặc biệt.

- Ví dụ: Kings of Leon, ban nhạc này đã phát hành album "When You See Yourself" dưới dạng NFT, cung cấp quyền truy cập đặc biệt cho người mua, bao gồm những nội dung độc quyền và vé tham dự các buổi hòa nhạc.

f) NFT trong ngành thể thao

NFT có thể được sử dụng để tạo ra các thẻ giao dịch thể thao kỹ thuật số, các bộ sưu tập hoặc các vật phẩm lưu niệm độc đáo liên quan đến các vận động viên và sự kiện thể thao.

- Cơ hội:

+) Người hâm mộ có thể mua và sở hữu các thẻ cầu thủ hoặc các khoảnh khắc nổi bật trong các trận đấu thể thao dưới dạng NFT.

+) Các đội thể thao và vận động viên có thể tạo ra các nguồn thu mới từ việc bán các NFT đặc biệt như thẻ cầu thủ hoặc video khoảnh khắc đáng nhớ.

- Ví dụ: NBA Top Shot, đây là một nền tảng cho phép người hâm mộ NBA mua, bán và trao đổi các khoảnh khắc đặc biệt từ các trận đấu của NBA dưới dạng NFT. Các video khoảnh khắc như các cú dunk nổi bật hay các pha bóng quyết định có thể được sở hữu như một tài sản kỹ thuật số duy nhất.

g) NFT trong việc xác thực danh tính và chứng nhận

NFT có thể giúp xác thực danh tính hoặc chứng nhận các thành tích, chứng chỉ trong nhiều lĩnh vực như giáo dục, công nghệ hoặc y tế, giúp việc xác nhận các thông tin trở nên nhanh chóng và bảo mật hơn.

- Cơ hội:

+) NFT có thể được sử dụng để tạo ra các chứng chỉ học vấn, giải thưởng, hoặc các danh hiệu được lưu trữ an toàn và không thể làm giả.

+) Những tổ chức, trường học, công ty có thể sử dụng NFT để cấp phát chứng chỉ hoặc danh hiệu, giúp việc xác thực trở nên dễ dàng và minh bạch.

- Ví dụ: Coursera và các nền tảng giáo dục khác: Một số nền tảng giáo dục trực tuyến đang thử nghiệm với việc phát hành chứng chỉ khóa học dưới dạng NFT, giúp học viên có thể chứng minh thành tích học tập mà không lo bị làm giả.

Tóm lại:

NFT mở ra nhiều cơ hội tiềm năng trong các ngành nghệ thuật, giải trí, game, bất động sản và nhiều lĩnh vực khác. Bằng cách cung cấp các giải pháp sáng tạo, NFT có thể giúp các nghệ sĩ, nhà sáng tạo, vận động viên, và người tiêu dùng xây dựng các giá trị mới và cải thiện các mô hình kinh doanh truyền thống. Khi công nghệ blockchain phát triển và các quy định pháp lý rõ ràng hơn, thị trường NFT có thể tiếp tục mở rộng và mang lại nhiều cơ hội hơn nữa.

2.6. VÍ VÀ ĐỊA CHỈ

Ví và địa chỉ là hai khái niệm quan trọng trong thế giới blockchain và tài sản kỹ thuật số, bao gồm cả tiền mã hóa (cryptocurrency) và NFT. Các ví và địa chỉ đóng vai trò quan trọng trong việc quản lý tài sản kỹ thuật số, giao dịch và bảo mật thông tin.

2.6.1 Ví (wallet)

2.6.1.1 Khái niệm

Ví (wallet) trong ngữ cảnh của tài sản kỹ thuật số là một phần mềm, thiết bị hoặc dịch vụ giúp người dùng lưu trữ, gửi và nhận tài sản số, bao gồm tiền mã hóa (cryptocurrency) và NFT. Ví không phải là nơi lưu trữ tài sản thực sự, mà là công cụ để quản lý và truy cập vào tài sản đó thông qua các khóa riêng (private key) và khóa công khai (public key).

Ví có thể được sử dụng cho nhiều mục đích khác nhau, từ việc giao dịch tiền mã hóa cho đến việc quản lý các tài sản kỹ thuật số khác, như các bộ sưu tập NFT hoặc chứng chỉ số.

Với tiền mã hóa, không có loại tiền tệ hữu hình, không có tiền giấy để đặt trong ví hoặc túi xách vật lý. Tiền mã hóa tồn tại trên blockchain và không có biểu hiện vật lý nào mà người dùng chạm vào. Nhưng vẫn cần có cá nhân và tổ chức hiểu được quyền sở hữu tài sản tiền mã hóa và có thể biết được số tiền được nắm giữ, giống như tài khoản ngân hàng cung cấp số dư ngân hàng.

Ví tiền mã hóa cung cấp cho người dùng cách xác thực số dư tài khoản để cung cấp khả năng hiển thị số tiền mã hóa mà người dùng sở hữu. Ví tiền mã hóa cho phép người dùng gửi và nhận các giao dịch tiền mã hóa, một cách tiếp cận tương tự về khái niệm là cách một tài khoản ngân hàng truyền thống cho phép người dùng thực hiện giao dịch. Đối với nhiều người dùng, ví tiền mã hóa là cơ chế chính để quản lý số dư tiền mã hóa.

Tại sao ví tiền mã hóa lại quan trọng?

Giống như bất kỳ loại tiền tệ nào, tiền mã hóa có thể được tích lũy và sử dụng cho nhiều mục đích và giao dịch khác nhau. Ví tiền mã hóa đóng vai trò nền tảng trong việc cho phép tài sản tiền mã hóa và tiền mã hóa có chức năng hữu ích cho cá nhân và tổ chức, giống như tài khoản ngân hàng là nền tảng cho tiền pháp định.

Ví tiền mã hóa là cần thiết cho một số mục đích quan trọng giúp tận dụng tiện ích thực tế của tài sản số, bao gồm:

- *Quản lý tiền mã hóa:* Ví tiền điện tử cung cấp cho người dùng khả năng theo dõi số dư tài sản tiền mã hóa.

- *Giao dịch:* Gửi và nhận thanh toán bằng tiền điện tử là một tính năng quan trọng của ví tiền mã hóa.

- *Kết nối với các ứng dụng phi tập trung (dApp)*: Cần có ví tiền mã hóa để kết nối và tương tác với các dApp Web 3.0 .

- *Nhận dạng tên người dùng:* Tất cả tiền mã hóa đều được lưu trữ trên blockchain. Ví tiền mã hóa cho phép giao dịch bằng tên người dùng có thể được liên kết với địa chỉ khóa công khai trên blockchain.

- *Quản lý khóa*: Về mặt chức năng, tiền mã hóa tồn tại trên blockchain dưới dạng địa chỉ khóa công khai. Ví tiền mã hóa giúp người dùng quản lý khóa mã hóa riêng được sử dụng để truy cập vào một địa chỉ nhất định và cho phép giao dịch.

2.6.1.2 Phân loại ví

Ví (wallet) trong thế giới tài sản kỹ thuật số có thể được phân loại theo các tiêu chí khác nhau, chủ yếu là dựa trên cách thức lưu trữ, mức độ bảo mật và khả năng sử dụng. Dưới đây là phân loại ví và các loại ví phổ biến hiện nay:

1. Ví Phần Mềm (Software Wallet)

Ví phần mềm là loại ví phổ biến, được cài đặt trên máy tính, điện thoại hoặc thiết bị di động. Ví này cung cấp cho người dùng khả năng truy cập vào tài sản kỹ thuật số và dễ dàng giao dịch. Ví phần mềm có thể kết nối với internet để thực hiện các giao dịch.

Các loại ví phần mềm:

a) Ví di động (Mobile Wallet): Cài đặt trên điện thoại di động, giúp người dùng có thể thực hiện giao dịch mọi lúc, mọi nơi. Đây là lựa chọn phổ biến cho người dùng tiền mã hóa khi di chuyển.

Ví phổ biến:

- Trust Wallet: Một ví di động phổ biến hỗ trợ nhiều loại tiền mã hóa và NFT.

- MetaMask: Một ví di động và trình duyệt dành cho Ethereum và các token ERC-20.

- Yoroi Wallet: Yoroi Wallet là một ví phần mềm nhẹ dành cho Cardano, được phát triển bởi Emurgo (một tổ chức con của Cardano). Yoroi hỗ trợ người dùng quản lý ADA và các tài sản Cardano khác. Đây là một ví thân thiện với người dùng và dễ dàng truy cập qua trình duyệt web hoặc ứng dụng di động.

b) Ví Desktop (Desktop Wallet): Cài đặt trên máy tính để bàn hoặc laptop. Ví desktop thường an toàn hơn ví trực tuyến nhưng có thể dễ bị mất nếu máy tính bị hỏng hoặc bị tấn công.

Ví phổ biến: Exodus, Electrum, Yoroi Wallet, ..

2. Ví Cứng (Hardware Wallet)

Ví cứng là thiết bị vật lý được thiết kế để lưu trữ tiền mã hóa và NFT ngoại tuyến, giúp bảo vệ tài sản khỏi các mối đe dọa trực tuyến như phần mềm độc hại hoặc hack. Ví cứng được coi là lựa chọn bảo mật nhất vì nó không kết nối trực tiếp với internet khi lưu trữ khóa riêng.

Các loại ví cứng:

a) Ví Ledger:

Là một trong những ví cứng phổ biến nhất, hỗ trợ nhiều loại tiền mã hóa và cung cấp bảo mật cao với khóa riêng được lưu trữ trong thiết bị.

Ví phổ biến: Ledger Nano S, Ledger Nano X,…

b) Ví Trezor:

Một ví cứng khác với bảo mật cao, hỗ trợ nhiều đồng tiền và token khác nhau.

Ví phổ biến: Trezor One, Trezor Model T, …

3. Ví Trực Tuyến (Web Wallet)

Ví trực tuyến (hoặc ví web) là ví được lưu trữ trên các nền tảng trực tuyến, cho phép người dùng truy cập và quản lý tài sản kỹ thuật số thông qua trình duyệt web. Ví trực tuyến có thể dễ dàng sử dụng nhưng bảo mật thấp hơn vì các khóa riêng có thể bị lộ nếu nền tảng bị hack.

Các loại ví trực tuyến:

a) Ví Blockchain: Một ví trực tuyến đơn giản cho phép người dùng lưu trữ và giao dịch tiền mã hóa như Bitcoin và Ethereum.

Ví phổ biến: Blockchain Wallet, ví dễ sử dụng với giao diện thân thiện và khả năng lưu trữ Bitcoin, Ethereum.

b) Ví Coinbase: Là ví trực tuyến và cũng là một nền tảng trao đổi tiền mã hóa, cho phép người dùng dễ dàng giao dịch và lưu trữ các loại tiền mã hóa.

Ví phổ biến: Coinbase Wallet, ví di động và ví web giúp người dùng lưu trữ tài sản và tương tác với các ứng dụng phi tập trung (dApp).

c) Daedalus Wallet: Daedalus là ví chính thức của Cardano, được phát triển bởi IOHK (Input Output Hong Kong), công ty đứng sau Cardano. Đây là một ví đầy đủ tính năng, chạy trên desktop và cung cấp cho người dùng khả năng lưu trữ toàn bộ blockchain Cardano, giúp đồng bộ hóa và xác nhận giao dịch trực tiếp từ mạng Cardano.

Các nền tảng hỗ trợ: Máy tính để bàn (Windows, macOS, Linux

d) Adalite Wallet: Adalite là một ví Cardano web nhẹ, dễ sử dụng và không yêu cầu tải toàn bộ blockchain. Nó cho phép người dùng tương tác với mạng Cardano, gửi và nhận ADA, cũng như tham gia vào các hoạt động staking mà không cần phải cài đặt phần mềm nặng.

Các nền tảng hỗ trợ: Trình duyệt web (Chrome, Firefox, Safari)

4. Ví Giấy (Paper Wallet)

Ví giấy là một phương pháp lưu trữ khóa riêng và khóa công khai dưới dạng bản in vật lý. Ví này giúp lưu trữ tài sản ngoài mạng internet, nhưng người dùng phải rất cẩn thận khi lưu trữ vì dễ bị mất hoặc hư hỏng.

Ví giấy Bitcoin (Bitcoin Paper Wallet): Đây là ví giấy đơn giản được tạo ra bằng cách in khóa công khai và khóa riêng của Bitcoin. Các dịch vụ như *bitaddress.org* giúp người dùng tạo ví giấy miễn phí.

Ví phổ biến: *Bitaddress.org,* dịch vụ tạo ví giấy Bitcoin miễn phí, giúp người dùng tạo ví an toàn và bảo mật.

5. Ví Thẻ (Card Wallet)

Ví thẻ là loại ví mới và tương đối ít phổ biến, giúp người dùng lưu trữ tiền mã hóa và NFT trong một thẻ vật lý tương tự như thẻ ngân hàng. Đây là một phương pháp lưu trữ tiện lợi, an toàn và dễ dàng mang theo.

Ví thẻ Trezor: Một loại ví cứng tích hợp dưới dạng thẻ, cho phép người dùng lưu trữ tiền mã hóa trên một thẻ vật lý.

Ví phổ biến: *Trezor Model T (thẻ),*cung cấp bảo mật cao cho tiền mã hóa và có màn hình cảm ứng để dễ dàng kiểm tra giao dịch.Ví (wallet) trong thế giới tài sản kỹ thuật số có thể được phân loại theo các tiêu chí khác nhau, chủ yếu là dựa trên cách thức lưu trữ, mức độ bảo mật và khả năng sử dụng. Dưới đây là phân loại ví và các loại ví phổ biến hiện nay:

1. Ví Phần Mềm (Software Wallet)

Ví phần mềm là loại ví phổ biến, được cài đặt trên máy tính, điện thoại hoặc thiết bị di động. Ví này cung cấp cho người dùng khả năng truy cập vào tài sản kỹ thuật số và dễ dàng giao dịch. Ví phần mềm có thể kết nối với internet để thực hiện các giao dịch.

Các loại ví phần mềm:

a) Ví di động (Mobile Wallet): Cài đặt trên điện thoại di động, giúp người dùng có thể thực hiện giao dịch mọi lúc, mọi nơi. Đây là lựa chọn phổ biến cho người dùng tiền mã hóa khi di chuyển.

Ví phổ biến:

- Trust Wallet: Một ví di động phổ biến hỗ trợ nhiều loại tiền mã hóa và NFT.

- MetaMask: Một ví di động và trình duyệt dành cho Ethereum và các token ERC-20.

- Yoroi Wallet: Yoroi Wallet là một ví phần mềm nhẹ dành cho Cardano, được phát triển bởi Emurgo (một tổ chức con của Cardano). Yoroi hỗ trợ người dùng quản lý ADA và

các tài sản Cardano khác. Đây là một ví thân thiện với người dùng và dễ dàng truy cập qua trình duyệt web hoặc ứng dụng di động.

b) Ví Desktop (Desktop Wallet): Cài đặt trên máy tính để bàn hoặc laptop. Ví desktop thường an toàn hơn ví trực tuyến nhưng có thể dễ bị mất nếu máy tính bị hỏng hoặc bị tấn công.

Ví phổ biến: Exodus, Electrum, Yoroi Wallet, ..

2. Ví Cứng (Hardware Wallet)

Ví cứng là thiết bị vật lý được thiết kế để lưu trữ tiền mã hóa và NFT ngoại tuyến, giúp bảo vệ tài sản khỏi các mối đe dọa trực tuyến như phần mềm độc hại hoặc hack. Ví cứng được coi là lựa chọn bảo mật nhất vì nó không kết nối trực tiếp với internet khi lưu trữ khóa riêng.

Các loại ví cứng:

a) Ví Ledger:

Là một trong những ví cứng phổ biến nhất, hỗ trợ nhiều loại tiền mã hóa và cung cấp bảo mật cao với khóa riêng được lưu trữ trong thiết bị.

Ví phổ biến: Ledger Nano S, Ledger Nano X,…

b) Ví Trezor:

Một ví cứng khác với bảo mật cao, hỗ trợ nhiều đồng tiền và token khác nhau.

Ví phổ biến: Trezor One, Trezor Model T, …

3. Ví Trực Tuyến (Web Wallet)

Ví trực tuyến (hoặc ví web) là ví được lưu trữ trên các nền tảng trực tuyến, cho phép người dùng truy cập và quản lý tài sản kỹ thuật số thông qua trình duyệt web. Ví trực tuyến có thể dễ dàng sử dụng nhưng bảo mật thấp hơn vì các khóa riêng có thể bị lộ nếu nền tảng bị hack.

Các loại ví trực tuyến:

a) Ví Blockchain: Một ví trực tuyến đơn giản cho phép người dùng lưu trữ và giao dịch tiền mã hóa như Bitcoin và Ethereum.

Ví phổ biến: Blockchain Wallet, ví dễ sử dụng với giao diện thân thiện và khả năng lưu trữ Bitcoin, Ethereum.

b) Ví Coinbase: Là ví trực tuyến và cũng là một nền tảng trao đổi tiền mã hóa, cho phép người dùng dễ dàng giao dịch và lưu trữ các loại tiền mã hóa.

Ví phổ biến: Coinbase Wallet, ví di động và ví web giúp người dùng lưu trữ tài sản và tương tác với các ứng dụng phi tập trung (dApp).

c) Daedalus Wallet: Daedalus là ví chính thức của Cardano, được phát triển bởi IOHK (Input Output Hong Kong), công ty đứng sau Cardano. Đây là một ví đầy đủ tính năng, chạy trên desktop và cung cấp cho người dùng khả năng lưu trữ toàn bộ blockchain Cardano, giúp đồng bộ hóa và xác nhận giao dịch trực tiếp từ mạng Cardano.

Các nền tảng hỗ trợ: Máy tính để bàn (Windows, macOS, Linux

d) Adalite Wallet: Adalite là một ví Cardano web nhẹ, dễ sử dụng và không yêu cầu tải toàn bộ blockchain. Nó cho phép người dùng tương tác với mạng Cardano, gửi và nhận ADA, cũng như tham gia vào các hoạt động staking mà không cần phải cài đặt phần mềm nặng.

Các nền tảng hỗ trợ: Trình duyệt web (Chrome, Firefox, Safari)

4. Ví Giấy (Paper Wallet)

Ví giấy là một phương pháp lưu trữ khóa riêng và khóa công khai dưới dạng bản in vật lý. Ví này giúp lưu trữ tài sản ngoài mạng internet, nhưng người dùng phải rất cẩn thận khi lưu trữ vì dễ bị mất hoặc hư hỏng.

Ví giấy Bitcoin (Bitcoin Paper Wallet): Đây là ví giấy đơn giản được tạo ra bằng cách in khóa công khai và khóa riêng của Bitcoin. Các dịch vụ như *bitaddress.org* giúp người dùng tạo ví giấy miễn phí.

Ví phổ biến: *Bitaddress.org,* dịch vụ tạo ví giấy Bitcoin miễn phí, giúp người dùng tạo ví an toàn và bảo mật.

5. Ví Thẻ (Card Wallet)

Ví thẻ là loại ví mới và tương đối ít phổ biến, giúp người dùng lưu trữ tiền mã hóa và NFT trong một thẻ vật lý tương tự như thẻ ngân hàng. Đây là một phương pháp lưu trữ tiện lợi, an toàn và dễ dàng mang theo.

Ví thẻ Trezor: Một loại ví cứng tích hợp dưới dạng thẻ, cho phép người dùng lưu trữ tiền mã hóa trên một thẻ vật lý.

Ví phổ biến: *Trezor Model T (thẻ),*cung cấp bảo mật cao cho tiền mã hóa và có màn hình cảm ứng để dễ dàng kiểm tra giao dịch.

2.6.1.3 Nguyên lý hoạt động

Ví (wallet) trong thế giới blockchain và tài sản kỹ thuật số hoạt động dựa trên các nguyên lý bảo mật mạnh mẽ và cấu trúc của mạng blockchain. Dưới đây là cách thức hoạt động cơ bản của một ví kỹ thuật số:

1. Khóa Công Khai và Khóa Riêng

Ví kỹ thuật số chủ yếu dựa trên hai thành phần quan trọng: khóa công khai (public key) và khóa riêng (private key). Chúng tạo ra một cặp khóa cho mỗi ví.

Khóa công khai (Public Key): Đây là địa chỉ ví mà người khác có thể gửi tiền hoặc tài sản kỹ thuật số (như tiền mã hóa hoặc NFT). Khóa công khai là công khai và có thể chia sẻ với bất kỳ ai.

Khóa riêng (Private Key): Đây là khóa bí mật, chỉ người sở hữu ví mới biết được. Khóa riêng dùng để xác thực giao dịch và chứng minh quyền sở hữu tài sản. Nếu mất khóa riêng, người dùng sẽ mất quyền truy cập vào tài sản của mình.

2. Quản lý Tài Sản (Chữ Ký Số)

Khi một người dùng muốn thực hiện một giao dịch (ví dụ: gửi ADA hoặc NFT cho người khác), họ sẽ phải sử dụng khóa riêng của mình để ký giao dịch đó. Việc ký giao dịch bằng khóa riêng giúp đảm bảo rằng chỉ người sở hữu ví mới có thể thực hiện các giao dịch liên quan đến tài sản của mình. Đây là quá trình xác thực quyền sở hữu tài sản.

Quy trình giao dịch:

Tạo giao dịch: Người dùng tạo giao dịch bằng cách nhập địa chỉ ví người nhận và số lượng tài sản muốn chuyển.

Chữ ký số: Giao dịch được ký bằng khóa riêng của người gửi, giúp chứng minh rằng họ có quyền chuyển giao tài sản.

Xác nhận giao dịch: Giao dịch sau đó được phát lên mạng blockchain để được xác nhận bởi các nút (nodes) trong mạng (ví dụ, qua cơ chế Proof of Work hoặc Proof of Stake).

Giao dịch sẽ chỉ được chấp nhận khi ký số của người gửi hợp lệ và phù hợp với khóa riêng của họ.

3. Lưu trữ và Quản lý Khóa Riêng

Khóa riêng không được lưu trữ trong ví dưới dạng thông tin dễ nhìn thấy. Thay vào đó, nó được bảo mật trong ví và có thể được mã hóa, giúp bảo vệ người dùng khỏi các mối đe dọa từ bên ngoài.

Ví phần mềm: Thông tin khóa riêng được lưu trữ cục bộ trên máy tính hoặc điện thoại của người dùng. Ví phần mềm sử dụng các biện pháp bảo mật, như mã hóa, để bảo vệ khóa riêng khỏi bị truy cập trái phép.

Ví cứng: Ví cứng lưu trữ khóa riêng trong một thiết bị ngoại vi không kết nối với internet. Điều này giúp bảo vệ tài sản khỏi các mối đe dọa từ phần mềm độc hại hoặc hack.

4. Quản lý Tài Sản (Blockchain và Giao Dịch)

Khi giao dịch được thực hiện, ví sẽ không thực sự chuyển tài sản (ví dụ: ADA hoặc NFT) giữa các ví, mà nó sẽ thay đổi trạng thái của tài sản trên blockchain.

Tài sản không thực sự tồn tại trong ví. Thay vào đó, ví chỉ lưu trữ thông tin về quyền sở hữu tài sản, được xác nhận thông qua các giao dịch trên blockchain.

Địa chỉ ví: là nơi tài sản "sống", và ví chỉ giúp người dùng truy cập vào các tài sản này bằng cách ký các giao dịch và quản lý quyền sở hữu.

5. Xác Thực và Bảo Mật

Các ví sử dụng nhiều biện pháp bảo mật để bảo vệ tài sản kỹ thuật số của người dùng như mã hóa, xác thực hai yếu tố (2FA) hay phục hồi ví (khóa dự phòng).

6. Giao dịch và Tương tác với dApps

Ví không chỉ dùng để lưu trữ tiền mã hóa mà còn hỗ trợ người dùng tương tác với các ứng dụng phi tập trung (DApps) trên blockchain.

Ví như một cổng kết nối: Ví là cổng kết nối giữa người dùng và các ứng dụng phi tập trung trên mạng blockchain. Người dùng có thể sử dụng ví để thực hiện các giao dịch, tham gia staking, giao dịch NFT, hoặc tương tác với các smart contract.

Các DApp hỗ trợ ví: Ví như MetaMask (trên Ethereum) hoặc Yoroi (trên Cardano) cho phép người dùng tương tác trực tiếp với DApps mà không cần phải rời khỏi ứng dụng ví.

Tóm lại ví hoạt động theo nguyên lý:

1. Cặp khóa công khai và khóa riêng giúp người dùng quản lý quyền truy cập và bảo mật tài sản.

2. Chữ ký số đảm bảo giao dịch chỉ có thể thực hiện bởi chủ sở hữu khóa riêng.

3. Ví phần mềm và ví cứng bảo mật khóa riêng và lưu trữ tài sản trong mạng blockchain.

4. Tài sản kỹ thuật số không thực sự lưu trữ trong ví mà được ghi lại trong blockchain.

5. Biện pháp bảo mật như mã hóa, xác thực hai yếu tố và từ khóa phục hồi giúp bảo vệ tài sản của người dùng.

6. Ví còn giúp người dùng tương tác với các DApp và tham gia vào các hoạt động staking, giao dịch, hoặc quản lý NFT trên blockchain.

Nguyên lý hoạt động của ví đảm bảo tính an toàn và bảo mật cho người dùng khi họ thực hiện giao dịch hoặc quản lý tài sản kỹ thuật số.

2.6.1.4 Vấn đề bảo mật và rủi ro

Khi sử dụng ví kỹ thuật số để lưu trữ và giao dịch tài sản trên các blockchain như Bitcoin, Ethereum, Cardano, hay bất kỳ nền tảng nào, người dùng cần phải cẩn thận với các mối nguy cơ bảo mật. Mặc dù ví mang lại nhiều tiện ích, nhưng chúng cũng tiềm ẩn các rủi ro có thể dẫn đến mất mát tài sản hoặc dữ liệu cá nhân. Dưới đây là một số vấn đề bảo mật và các rủi ro phổ biến mà người dùng ví cần lưu ý:

1. Mất hoặc lộ khóa riêng (Private Key)

Mất khóa riêng: Nếu người dùng mất khóa riêng của mình, họ sẽ không thể truy cập vào tài sản kỹ thuật số của mình. Điều này rất nghiêm trọng vì blockchain là hệ thống phân tán và không thể khôi phục giao dịch hoặc tài sản một khi khóa riêng đã bị mất.

Lộ khóa riêng: Nếu khóa riêng bị lộ (do người dùng chia sẻ sai, bị hack, hoặc lưu trữ không an toàn), kẻ xấu có thể chiếm đoạt tài sản của người dùng.

Ví dụ:

Ví phần mềm bị hack: Một số ví phần mềm như Exodus hoặc Electrum đã bị các nhóm hacker tấn công, và nếu người dùng không bảo vệ khóa riêng của mình bằng mã hóa hoặc các phương pháp bảo mật khác, họ có thể mất tài sản. Một ví dụ đáng chú ý là vụ hack MyEtherWallet vào năm 2018, nơi các hacker đã tấn công DNS và lừa người dùng cung cấp khóa riêng.

2. Mất ví hoặc hư hỏng thiết bị

Mất ví cứng: Nếu người dùng mất ví cứng (như Ledger hoặc Trezor) và không sao lưu đủ thông tin (như từ khóa phục hồi), họ sẽ không thể phục hồi tài sản.

Hư hỏng thiết bị: Ví cứng hoặc ví phần mềm có thể hỏng hoặc bị mất nếu không sao lưu dữ liệu ví một cách an toàn.

Ví dụ:

Mất ví cứng Trezor: Một người dùng có thể vô tình làm rơi hoặc mất ví Trezor của mình. Nếu không sao lưu cụm từ khôi phục, họ sẽ không thể khôi phục quyền truy cập vào tài sản của mình.

Hư hỏng ví phần mềm: Ví như Exodus có thể gặp sự cố nếu máy tính hoặc điện thoại của người dùng bị hỏng và không có bản sao lưu khóa riêng hoặc từ khóa phục hồi.

3. Tấn công phishing và lừa đảo

Tấn công Phishing: Đây là một kỹ thuật lừa đảo nơi hacker giả mạo các trang web hoặc email từ các ví nổi tiếng như MetaMask, Trust Wallet, hoặc Coinbase Wallet để lấy cắp khóa riêng hoặc thông tin cá nhân.

Lừa đảo qua liên kết giả mạo: Người dùng có thể bị lừa nhấp vào các liên kết giả mạo trong email hoặc tin nhắn và nhập thông tin vào các trang web không chính thức.

Ví dụ:

MetaMask Phishing: Một số người dùng MetaMask đã bị lừa khi nhấp vào các liên kết phishing và nhập mật khẩu hoặc khóa riêng vào các trang web giả mạo, dẫn đến mất hết tài sản.

Lừa đảo qua email giả mạo Coinbase: Có các cuộc tấn công phishing, nơi hacker giả mạo email từ Coinbase và yêu cầu người dùng cung cấp thông tin đăng nhập ví hoặc mã xác thực 2FA.

4. Tấn công mạng và Malware (Phần mềm độc hại)

Phần mềm độc hại: Máy tính hoặc điện thoại của người dùng có thể bị nhiễm phần mềm độc hại (malware) để theo dõi hoạt động ví, đánh cắp thông tin khóa riêng, và thực hiện các giao dịch mà người dùng không hề hay biết.

Tấn công từ xa: Nếu ví được lưu trữ trên máy tính hoặc điện thoại có phần mềm độc hại, hacker có thể xâm nhập và rút tiền mà không cần sự đồng ý của người dùng.

Ví dụ:

Malware trên máy tính: Một người dùng đã tải xuống một phần mềm miễn phí, nhưng phần mềm này thực chất là malware đã theo dõi các hoạt động của ví Bitcoin và rút tiền từ ví mà không có sự đồng ý của chủ sở hữu.

Tấn công man-in-the-middle (MITM): Khi người dùng thực hiện giao dịch qua một mạng không an toàn, như Wi-Fi công cộng, hacker có thể nghe lén và can thiệp vào giao dịch của người dùng.

5. Các lỗ hổng bảo mật trong ví

Lỗ hổng phần mềm: Ví phần mềm có thể gặp phải các lỗ hổng bảo mật trong mã nguồn, giúp hacker có thể khai thác và chiếm đoạt tài sản của người dùng.

Lỗ hổng trong giao thức: Các giao thức blockchain hoặc ví có thể có lỗi lập trình hoặc thiếu sót, dẫn đến việc tài sản bị rút ra mà không có sự đồng ý của người dùng.

Ví dụ:

Lỗi bảo mật trong ví Ethereum: Trước đây, một số ví Ethereum đã gặp phải các lỗi bảo mật trong hợp đồng thông minh (smart contracts), khiến người dùng có thể bị mất tiền trong các giao dịch hoặc khi tham gia staking.

6. Nguy cơ từ mạng xã hội và Quảng cáo giả mạo

Quảng cáo giả mạo: Một số quảng cáo trên mạng xã hội hoặc các trang web không chính thống có thể dụ dỗ người dùng tải xuống ví hoặc ứng dụng giả mạo.

Lừa đảo đầu tư (Ponzi scheme): Các mánh lừa đảo liên quan đến việc đầu tư vào các tài sản kỹ thuật số hoặc NFT với lời hứa lợi nhuận cao, chỉ để người dùng mất tiền.

Ví dụ:

Ví giả mạo trên Twitter: Có những tài khoản giả mạo ví nổi tiếng như MetaMask hoặc Trust Wallet trên Twitter hoặc Telegram, quảng cáo các chương trình khuyến mãi hoặc giảm giá, và khi người dùng tải về, họ cài đặt ứng dụng giả mạo để lấy cắp tài sản.

2.6.1.5 Các ứng dụng

Ví kỹ thuật số không chỉ đơn thuần là công cụ lưu trữ tài sản kỹ thuật số mà còn đóng vai trò quan trọng trong nhiều ứng dụng khác nhau trong thế giới blockchain và tài sản mã hóa.

Các ứng dụng thông dụng của ví:

1. Lưu trữ và quản lý tài sản kỹ thuật số (Bitcoin, Ethereum, ADA, NFT).

2. Giao dịch và thanh toán tiền mã hóa.

3. Tham gia DApp (DeFi, trò chơi blockchain, NFT).

4. Staking tài sản để nhận phần thưởng.

5. Quản lý NFT (Non-Fungible Tokens).

6. Giao dịch ngoài hệ sinh thái blockchain.

7. Lưu trữ token bảo mật và chứng nhận quyền sở hữu tài sản.

8. Xác thực danh tính (KYC).

Ví kỹ thuật số là một công cụ mạnh mẽ không chỉ để lưu trữ và giao dịch tiền mã hóa, mà còn hỗ trợ người dùng tham gia vào các ứng dụng phi tập trung, staking, quản lý NFT, và nhiều dịch vụ tài chính khác.

2.6.2. Địa chỉ

Trong hệ sinh thái blockchain, địa chỉ (address) là một chuỗi các ký tự hoặc mã nhận dạng duy nhất, dùng để xác định vị trí nơi người dùng có thể nhận hoặc gửi tài sản kỹ thuật số, như tiền mã hóa, token hoặc NFT. Địa chỉ này thường liên quan trực tiếp đến các ví kỹ thuật số và đóng vai trò quan trọng trong các giao dịch blockchain.

2.6.2.1. Khái niệm

Địa chỉ blockchain có thể được coi như một "số tài khoản" trong ngân hàng hoặc "số điện thoại" dùng để nhận tiền hoặc tài sản. Tuy nhiên, thay vì sử dụng tên hoặc số tài khoản, blockchain sử dụng các chuỗi ký tự số và chữ để làm địa chỉ.

Một địa chỉ thường được tạo ra thông qua các hàm băm (hashing) từ khóa công khai (public key) và các thuật toán mã hóa mạnh mẽ để đảm bảo tính bảo mật và bảo vệ quyền sở hữu tài sản.

Ví dụ:

Bitcoin Address (BTC): Địa chỉ Bitcoin thường bắt đầu bằng ký tự "1" hoặc "3", ví dụ: 1A1Z6MEAnqvhwxc9u3Uuu62W8AQu2D9UuC.

Ethereum Address (ETH): Địa chỉ Ethereum bắt đầu bằng "0x", ví dụ: 0x740ECBbCe82c3F000E01a0038e281f3097d403C5.

Cardano (ADA): Địa chỉ Cardano có thể bắt đầu bằng "addr1" và được mã hóa theo một cấu trúc khác so với Bitcoin và Ethereum. ví dụ: addr1q9knwn2jptp5eqlk5jlg8ldqu8pndw4fkp9dyxj69f9pdhpyh98ak8wjl5qlfuwqkcl96f40h5r

2.6.2.2. Phân loại

Địa chỉ blockchain có thể được phân loại theo từng loại blockchain và cách mà địa chỉ được sử dụng trong mỗi hệ thống. Các loại địa chỉ phổ biến bao gồm:

a) Địa chỉ Bitcoin (BTC)

Khái niệm: Địa chỉ Bitcoin dùng để nhận và gửi Bitcoin trong mạng lưới Bitcoin.

Đặc điểm: Địa chỉ Bitcoin có thể bắt đầu bằng ký tự "1", "3" hoặc "bc1".

Ví dụ: 1A1Z6MEAnqvhwxc9u3Uuu62W8AQu2D9UuC

Ví: Các địa chỉ "P2PKH" (Pay-to-PubKey-Hash) bắt đầu bằng "1", "P2SH" (Pay-to-Script-Hash) bắt đầu bằng "3", và địa chỉ SegWit bắt đầu bằng "bc1".

b) Địa chỉ Ethereum (ETH)

Khái niệm: Địa chỉ Ethereum là một chuỗi 40 ký tự (không tính tiền tố "0x") được sử dụng để nhận và gửi Ethereum và các token ERC-20.

Đặc điểm: Địa chỉ Ethereum bắt đầu bằng "0x".

Ví dụ: 0x740ECBbCe82c3F000E01a0038e281f3097d403C5

c) Địa chỉ Cardano (ADA)

Khái niệm: Địa chỉ Cardano là một chuỗi ký tự được tạo ra từ các quy tắc đặc biệt của blockchain Cardano.

Đặc điểm: Địa chỉ Cardano có thể bắt đầu bằng "addr1" và được mã hóa theo một cấu trúc khác so với Bitcoin và Ethereum.

Ví dụ: addr1q9knwn2jptp5eqlk5jlg8ldqu8pndw4fkp9dyxj69f9pdhpyh98ak8wjl5qlfuwqkcl96f40h5r

d) Địa chỉ Binance Smart Chain (BSC)

Khái niệm: Địa chỉ BSC là địa chỉ dùng để nhận và gửi tài sản trên mạng Binance Smart Chain.

Đặc điểm: Địa chỉ BSC tương tự như địa chỉ Ethereum, bắt đầu bằng "0x".

Ví dụ: 0x6f99fcd64af42c4e2c7289cab0f039080d997f21

e) Địa chỉ Solana (SOL)

Khái niệm: Địa chỉ Solana là một chuỗi ký tự dài được sử dụng trong hệ sinh thái Solana.

Đặc điểm: Địa chỉ Solana dài khoảng 32 ký tự và không có tiền tố đặc biệt.

Ví dụ: 6rKWh6j8jfTpzcsYXsdvxdTt2EZSY61qbb9XfX5g97DE

2.6.2.3. Nguyên lý hoạt động

Địa chỉ blockchain hoạt động chủ yếu dựa trên nguyên lý liên kết giữa khóa công khai (public key) và khóa riêng tư (private key). Quy trình này giúp xác thực và bảo vệ giao dịch:

1. Tạo địa chỉ

Bước 1: Tạo khóa công khai (public key): Quá trình tạo địa chỉ bắt đầu từ việc tạo khóa công khai thông qua các thuật toán như Elliptic Curve Cryptography (ECC) (trong Bitcoin, Ethereum, v.v.).

Bước 2: Băm và mã hóa: Để tạo địa chỉ, khóa công khai được băm lại bằng các hàm băm như SHA-256 và RIPEMD-160, sau đó mã hóa thành địa chỉ.

Bước 3: Kết quả, địa chỉ sẽ là một chuỗi ký tự đại diện cho một địa chỉ duy nhất trong mạng blockchain, có thể gửi và nhận tài sản.

2. Giao dịch với địa chỉ

Khi bạn muốn gửi tiền hoặc tài sản đến một địa chỉ blockchain, bạn sử dụng khóa riêng để ký xác thực giao dịch.

Giao dịch này được truyền tải qua mạng lưới và được xác nhận bởi các node (nút) trên blockchain.

Khi giao dịch hoàn tất, tài sản sẽ chuyển từ ví của bạn sang địa chỉ đích. Quá trình này được ghi lại trên sổ cái công khai của blockchain.

3. Bảo mật và xác thực

Khóa riêng (private key): Chỉ người sở hữu khóa riêng mới có thể ký và phê duyệt giao dịch từ địa chỉ của mình. Việc bảo mật khóa riêng cực kỳ quan trọng, nếu mất khóa riêng, bạn sẽ mất quyền truy cập vào tài sản trong ví.

Khóa công khai (public key): Đây là thông tin công khai và được sử dụng để tạo địa chỉ nhận tiền từ các giao dịch khác. Khóa công khai không thể dùng để ký giao dịch, mà chỉ để nhận tài sản.

2.6.2.4. Vấn đề bảo mật và các rủi ro

Địa chỉ trên blockchain đóng vai trò quan trọng trong việc nhận và gửi tài sản kỹ thuật số. Tuy nhiên, như với bất kỳ công nghệ nào, vấn đề bảo mật và các rủi ro liên quan đến địa chỉ trên blockchain là rất lớn và có thể gây thiệt hại nghiêm trọng nếu không được quản lý đúng cách. Dưới đây là các vấn đề bảo mật và các rủi ro chính của địa chỉ trên blockchain.

1. Mất khóa riêng (Private Key)

Khóa riêng là yếu tố bảo mật quan trọng nhất để quản lý tài sản trong ví blockchain. Nếu bạn mất khóa riêng của mình, bạn sẽ không thể truy cập vào tài sản của mình. Điều này có thể xảy ra khi:

Mất hoặc quên khóa riêng.

Khóa riêng bị xóa mà không sao lưu.

Khóa riêng bị đánh cắp do vi phạm bảo mật hoặc hành vi lừa đảo.

Ví dụ: Một người dùng Bitcoin mất khóa riêng của mình và không có bản sao lưu, dẫn đến việc mất toàn bộ số Bitcoin trong ví mà không thể khôi phục lại.

Giải pháp: Sao lưu khóa riêng ở nhiều nơi an toàn, chẳng hạn như giấy, phần mềm bảo mật hoặc thiết bị phần cứng. sSử dụng các ví phần cứng (hardware wallet) để lưu trữ khóa riêng một cách an toàn.

2. Tấn công lừa đảo (Phishing)

Phishing là phương thức mà kẻ lừa đảo giả mạo các trang web hoặc dịch vụ ví, yêu cầu người dùng nhập khóa riêng hoặc thông tin nhạy cảm của họ.

Kẻ tấn công có thể giả mạo địa chỉ ví của người dùng và thay đổi địa chỉ ví nhận trong một giao dịch, khiến tài sản bị gửi vào ví của kẻ lừa đảo.

Ví dụ: Một người dùng nhận được email giả mạo từ một sàn giao dịch, yêu cầu cập nhật thông tin tài khoản và nhập khóa riêng của mình. Sau khi làm theo hướng dẫn, tài sản của người dùng bị chuyển vào ví của kẻ lừa đảo.

Giải pháp: Luôn kiểm tra URL và các liên kết trước khi nhập thông tin vào các trang web hoặc dịch vụ ví. Kích hoạt xác thực hai yếu tố (2FA) để bảo vệ tài khoản ví.

3. Tấn công 51% (51% Attack)

Một tấn công 51% có thể xảy ra nếu kẻ tấn công kiểm soát hơn 50% sức mạnh tính toán của mạng blockchain. Điều này có thể dẫn đến khả năng thay đổi lịch sử giao dịch, thao túng giao dịch hoặc gây ra các vấn đề bảo mật nghiêm trọng khác.

Nếu có một số địa chỉ ví bị tấn công hoặc bị kiểm soát bởi một nhóm tấn công, có thể dẫn đến việc lừa đảo hoặc chi tiêu gấp đôi (double-spending).

Ví dụ: Mạng Bitcoin Cash từng phải đối mặt với cuộc tấn công 51% vào năm 2018, dẫn đến việc một số giao dịch bị đảo ngược và tiền bị chi tiêu gấp đôi.

Giải pháp: Sử dụng các blockchain có sức mạnh tính toán phân tán cao hoặc chuyển sang proof-of-stake (PoS) thay vì proof-of-work (PoW) để giảm thiểu nguy cơ này.

4. Lỗi phát sinh trong quá trình tạo địa chỉ (Address Generation Flaws)

Các lỗi trong quá trình tạo địa chỉ có thể xảy ra khi phần mềm tạo địa chỉ không đúng cách hoặc sử dụng thuật toán không bảo mật. Điều này có thể dẫn đến việc tạo ra các địa chỉ ví có thể bị dễ dàng dự đoán hoặc thậm chí bị tấn công.

Ví dụ: Một số ví lỗi có thể tạo ra địa chỉ dễ dàng đoán được, làm tăng khả năng tấn công từ kẻ xấu.

Giải pháp: Sử dụng các công cụ và phần mềm ví có chứng nhận bảo mật cao, luôn cập nhật các bản vá bảo mật mới nhất.

5. Giao dịch sai địa chỉ (Wrong Address Transactions)

Việc gửi tài sản đến địa chỉ sai có thể xảy ra nếu người dùng sao chép và dán sai địa chỉ ví, hoặc khi có sự nhầm lẫn giữa các địa chỉ ví (ví dụ: địa chỉ Bitcoin và Ethereum có cấu trúc tương tự).

Các giao dịch trên blockchain là không thể hoàn tác (irreversible), vì vậy nếu tài sản được gửi nhầm, người dùng sẽ không thể lấy lại.

Ví dụ: Người dùng gửi Bitcoin đến một địa chỉ Ethereum, và do sự khác biệt giữa các blockchain, giao dịch không thể thực hiện được, gây mất mát tài sản.

Giải pháp: Kiểm tra kỹ địa chỉ ví trước khi gửi giao dịch. Sử dụng mã QR hoặc các công cụ hỗ trợ để tránh lỗi nhập sai địa chỉ.

6. Rủi ro từ các ví trung gian (Hot Wallets)

Ví nóng (Hot Wallets) là các ví được kết nối trực tiếp với internet và dễ bị tấn công từ các mối đe dọa bên ngoài như virus, phần mềm độc hại hoặc hacker. Các ví trung gian trên các sàn giao dịch cũng có thể là mục tiêu tấn công.

Ví dụ: Vào năm 2014, sàn giao dịch Mt. Gox bị hack và mất 850.000 Bitcoin, phần lớn tài sản này là của người dùng đang lưu trữ trong ví nóng của sàn.

Giải pháp: Lưu trữ tài sản trên ví lạnh (cold wallet), đặc biệt là các tài sản lớn, và chỉ sử dụng ví nóng cho giao dịch ngắn hạn hoặc thử nghiệm. Kích hoạt xác thực hai yếu tố (2FA) và bảo vệ tài khoản ví với các phương thức bảo mật khác.

Tóm lại

Bảo mật địa chỉ trên blockchain là vấn đề quan trọng đối với người dùng và các tổ chức sử dụng công nghệ này. Việc hiểu rõ các rủi ro và cách thức bảo vệ tài sản là rất cần thiết để tránh mất mát tài sản và các cuộc tấn công có thể xảy ra.

2.6.2.5. Ứng dụng

Địa chỉ trên blockchain không chỉ là nơi lưu trữ tài sản, mà còn đóng vai trò quan trọng trong nhiều ứng dụng và dịch vụ khác nhau.

1. Giao dịch tiền mã hóa (Cryptocurrency Transactions)

Ứng dụng: Địa chỉ trên blockchain chủ yếu được sử dụng để gửi và nhận tiền mã hóa (cryptocurrency). Mỗi địa chỉ ví trên blockchain là một điểm nhận tài sản, cho phép các giao dịch tiền mã hóa diễn ra giữa các người dùng.

Ví dụ:

Một người dùng Bitcoin có thể gửi BTC từ địa chỉ 1A1Z6MEAnqvhwxc9u3Uuu62W8AQu2D9UuC tới địa chỉ của người nhận.

Tương tự, người dùng Ethereum gửi ETH từ địa chỉ 0x740ECBbCe82c3F000E01a0038e281f3097d403C5 tới một địa chỉ Ethereum khác.

Mục đích: Thực hiện các giao dịch thanh toán trực tuyến. Chuyển tiền xuyên biên giới mà không cần sự tham gia của các tổ chức tài chính trung gian.

2. Sử dụng trong hợp đồng thông minh (Smart Contracts)

Ứng dụng: Các hợp đồng thông minh (smart contracts) trên blockchain sử dụng địa chỉ ví để thực hiện các giao dịch tự động khi điều kiện nhất định được đáp ứng. Địa chỉ trong trường hợp này có thể là địa chỉ của hợp đồng thông minh hoặc địa chỉ của người tham gia hợp đồng.

Ví dụ: Một hợp đồng thông minh trên Ethereum có thể nhận các khoản thanh toán từ người dùng và sau đó tự động thực hiện một hành động (ví dụ: giao hàng hoặc cấp phép) khi thanh toán hoàn tất.

Mục đích: Tự động hóa các thỏa thuận mà không cần bên trung gian. Đảm bảo tính minh bạch và đáng tin cậy trong các giao dịch phức tạp.

3. Địa chỉ liên kết với NFT (Non-Fungible Tokens)

Ứng dụng: Trong hệ sinh thái NFT, địa chỉ ví được sử dụng để mua, bán và lưu trữ các NFT. Mỗi NFT có thể được chuyển từ địa chỉ này sang địa chỉ khác khi giao dịch được thực hiện. Người dùng sở hữu các NFT sẽ giữ chúng trong ví của mình dưới các địa chỉ ví riêng biệt.

Ví dụ: Một nghệ sĩ có thể tạo ra và bán NFT trên các nền tảng như OpenSea, nơi địa chỉ ví của người mua và người bán đóng vai trò quyết định trong việc chuyển nhượng quyền sở hữu NFT.

Mục đích: Chuyển nhượng tài sản số độc nhất (NFT). Xác nhận quyền sở hữu và tính xác thực của các vật phẩm kỹ thuật số.

4. Quản lý và lưu trữ tài sản kỹ thuật số (Digital Asset Management)

Ứng dụng: Địa chỉ blockchain cũng được sử dụng trong việc quản lý các tài sản kỹ thuật số ngoài tiền mã hóa, như token hóa tài sản (real estate, cổ phiếu, hoặc vật phẩm số). Các tài sản này có thể được chuyển nhượng hoặc bán lại dưới dạng các token, và việc quản lý những token này được thực hiện qua địa chỉ ví blockchain.

Ví dụ: Các tổ chức tài chính có thể phát hành Security Tokens để đại diện cho các cổ phiếu hoặc tài sản. Các nhà đầu tư sẽ sở hữu các token này thông qua địa chỉ ví của mình.

Mục đích: Đảm bảo quyền sở hữu và tính hợp pháp của các tài sản kỹ thuật số. Tạo điều kiện thuận lợi cho việc giao dịch các tài sản trong môi trường blockchain.

5. Giao địch và quản lý Token trong các DApp (Decentralized Applications)

Ứng dụng: Các ứng dụng phi tập trung (DApp) sử dụng địa chỉ ví để thực hiện giao dịch token, tham gia vào các trò chơi blockchain, staking, hay voting. Người dùng tương tác với các DApp thông qua địa chỉ ví của mình, qua đó thực hiện các hành động như đặt cược token, tham gia quản trị, hoặc kiếm phần thưởng.

Ví dụ: Trong trò chơi blockchain như Axie Infinity, người chơi có thể sở hữu các token trong ví và sử dụng chúng để mua các vật phẩm hoặc tham gia chiến đấu. Trong các dự án DeFi (tài chính phi tập trung), người dùng có thể sử dụng ví của mình để staking hoặc cho vay token.

Mục đích:Tạo ra các dịch vụ tài chính phi tập trung (DeFi) mà không cần sự tham gia của ngân hàng hoặc tổ chức tài chính trung gian. Đảm bảo quyền kiểm soát hoàn toàn tài sản và thông tin cá nhân cho người dùng.

6. Quyền sở hữu và quản lý danh tính (Identity Management)

Ứng dụng: Blockchain cung cấp một cách thức để người dùng có thể quản lý danh tính của mình một cách an toàn thông qua địa chỉ ví. Các địa chỉ này có thể được sử dụng để xác minh danh tính, lưu trữ và bảo vệ thông tin cá nhân trên các nền tảng blockchain mà không cần phải dựa vào các tổ chức trung gian.

Ví dụ: Self-sovereign identity (SSO) cho phép người dùng kiểm soát thông tin cá nhân của mình và chia sẻ chúng khi cần thiết mà không cần phải thông qua cơ quan chứng nhận tập trung.

Mục đích: Cung cấp một phương thức bảo mật cho việc xác minh danh tính trực tuyến. Giảm thiểu các vấn đề về lừa đảo và bảo vệ quyền riêng tư của người dùng.

7. Thanh toán và Microtransactions

Ứng dụng: Địa chỉ ví trên blockchain cũng được sử dụng để thực hiện thanh toán và microtransactions. Các dịch vụ thanh toán như Lightning Network (Bitcoin) hoặc các giao thức thanh toán trên các nền tảng blockchain khác cho phép thanh toán nhanh chóng và chi phí thấp, giúp người dùng giao dịch một cách tiện lợi và dễ dàng.

Ví dụ: Sử dụng Bitcoin Lightning Network để thực hiện các giao dịch nhỏ với chi phí thấp, ví dụ: trả tiền cho nội dung số, sử dụng dịch vụ trực tuyến, hoặc gửi tiền nhỏ cho bạn bè.

Mục đích: Tăng cường khả năng thanh toán trực tuyến với các khoản tiền nhỏ mà không gặp phải phí giao dịch cao. Đẩy mạnh ứng dụng blockchain trong các dịch vụ thanh toán truyền thống.

8. Tạo và quản lý mã thẻ quà tặng (Gift Cards)

Ứng dụng: Một số nền tảng sử dụng blockchain để phát hành và quản lý thẻ quà tặng (gift cards). Địa chỉ ví blockchain có thể được sử dụng để nhận và thanh toán bằng các thẻ quà tặng này.

Ví dụ: Một dịch vụ thẻ quà tặng có thể phát hành mã thẻ dưới dạng token trên blockchain, và người nhận có thể sử dụng ví blockchain để thanh toán các sản phẩm và dịch vụ.

Mục đích: Giảm thiểu rủi ro gian lận và nâng cao tính bảo mật trong việc trao đổi thẻ quà tặng. Sử dụng blockchain để minh bạch hóa và bảo mật quá trình phát hành và sử dụng thẻ.

Tóm lại: Địa chỉ trên blockchain không chỉ đóng vai trò như một công cụ để lưu trữ và chuyển nhượng tài sản mà còn hỗ trợ rất nhiều ứng dụng khác nhau từ tài chính phi tập trung (DeFi), trò chơi blockchain, cho đến các nền tảng quản lý danh tính và thẻ quà tặng. Việc sử dụng địa chỉ ví blockchain mở ra rất nhiều cơ hội cho việc phát triển và ứng dụng công nghệ blockchain trong đời sống thực tế, đồng thời giúp tạo ra các giao dịch an toàn, minh bạch và hiệu quả.

2.7. SỔ CÁI (LEDGER)

2.7.1. Khái niệm

Trong blockchain, **sổ cái (ledger)** là một cơ sở dữ liệu phân tán, liên tục được cập nhật và lưu trữ tất cả các giao dịch đã được xác thực trên mạng lưới blockchain. Khác với sổ cái truyền thống, sổ cái trong blockchain không được kiểm soát bởi một tổ chức trung gian, mà thay vào đó được duy trì và xác nhận bởi tất cả các nút (nodes) tham gia trong mạng lưới. Mỗi giao dịch trên blockchain sẽ được ghi nhận trong các khối (blocks) và liên kết với nhau thành một chuỗi (chain), tạo thành một "sổ cái" công khai, không thể thay đổi, giúp đảm bảo tính toàn vẹn và bảo mật của các giao dịch.

2.7.2. Đặc điểm của Sổ Cái trong Blockchain?

1. Phân tán và không có trung gian:

Blockchain là một hệ thống phân tán, nghĩa là không có một cơ quan hoặc tổ chức trung gian nào kiểm soát sổ cái. Mỗi nút trong mạng đều có một bản sao của sổ cái, giúp tăng cường tính minh bạch và an toàn.

2. Không thể thay đổi (immutability):

Một khi giao dịch đã được ghi nhận và xác thực trong blockchain, nó không thể bị thay đổi hoặc xóa bỏ. Điều này đảm bảo tính toàn vẹn của dữ liệu và ngăn chặn các hành vi gian lận.

3. Công khai và minh bạch:

Sổ cái blockchain là công khai, có thể truy cập và kiểm tra bởi bất kỳ ai. Tuy nhiên, các thông tin nhạy cảm như danh tính của người tham gia giao dịch thường được bảo vệ thông qua các mã hóa và địa chỉ ví.

4. Bảo mật:

Sổ cái blockchain sử dụng các phương pháp mã hóa mạnh mẽ để bảo vệ dữ liệu khỏi bị thay đổi hoặc truy cập trái phép. Các giao dịch được xác nhận bởi các nút mạng thông qua các cơ chế đồng thuận như Proof of Work (PoW) hoặc Proof of Stake (PoS).

5. Tự động hóa và không cần sự tin cậy vào bên thứ ba:

Các giao dịch trên blockchain được xác thực và ghi nhận tự động mà không cần phải có sự tham gia của bên thứ ba trung gian, giúp giảm thiểu chi phí và rủi ro liên quan đến các bên trung gian.

2.7.3. Nguyên lý hoạt động của Sổ Cái trong Blockchain?

1. Giao dịch và khối:

Mỗi giao dịch trên blockchain được ghi nhận và xác nhận bởi các nút trong mạng lưới. Sau khi giao dịch được xác nhận, chúng sẽ được gom lại thành một "khối" (block) và được thêm vào sổ cái.

2. Cơ chế đồng thuận (Consensus Mechanism):

Các nút trong mạng lưới phải đạt được sự đồng thuận để chấp nhận một khối giao dịch mới. Các cơ chế đồng thuận phổ biến như Proof of Work (PoW), Proof of Stake (PoS) giúp đảm bảo rằng các giao dịch là hợp lệ và không có sự gian lận.

3. Xác thực và ghi nhận:

Sau khi đạt được đồng thuận, giao dịch trong khối sẽ được ghi nhận vào blockchain. Mỗi khối đều chứa một mã băm (hash) của khối trước đó, tạo ra một chuỗi liên kết chặt chẽ giữa các khối, giúp bảo vệ sự toàn vẹn của dữ liệu.

4. Chống gian lận và bảo mật:

Các giao dịch trong blockchain sử dụng mã hóa bất đối xứng để bảo vệ danh tính và các thông tin quan trọng. Một khi thông tin đã được ghi vào blockchain, nó không thể bị thay đổi mà không làm thay đổi tất cả các khối phía sau, điều này giúp bảo vệ khỏi các hành vi gian lận.

Tóm lại: Sổ cái trong blockchain là một hệ thống phân tán, bảo mật, và không thể thay đổi, giúp ghi nhận và lưu trữ tất cả các giao dịch trong mạng lưới. Với các đặc điểm như tính minh bạch, bảo mật, và không cần sự tin cậy vào bên trung gian, blockchain đã mang lại những lợi ích đáng kể trong nhiều lĩnh vực và mở ra các cơ hội mới cho các ứng dụng tài chính và phi tài chính.

2.8. CÁC LĨNH VỰC ỨNG DỤNG BLOCKCHAIN

Blockchain có nhiều lĩnh vực ứng dụng thực tiễn, bao gồm cả các ngành công nghiệp truyền thống lẫn các lĩnh vực công nghệ mới. Dưới đây là một số lĩnh vực cụ thể:

2.8.1. Tài chính và ngân hàng

Blockchain đã mang đến nhiều đột phá trong lĩnh vực tài chính và ngân hàng, giúp tối ưu hóa các quy trình, giảm chi phí và tăng tính minh bạch. Các lĩnh vực cụ thể như: thanh toán quốc tế, hợp đồng thông minh, quản lý tài sản, quản lý dữ liệu khách hàng, tự động hóa các quy trình bồi thường thông qua hợp đồng thông minh, …

Ví dụ: Bitcoin, Ethereum và các loại tiền điện tử khác sử dụng blockchain để cung cấp một phương thức thanh toán an toàn, nhanh chóng và không phụ thuộc vào ngân hàng trung gian. Ethereum**:** Cho phép xây dựng các hợp đồng thông minh để tự động xử lý khoản vay, bảo hiểm, hoặc phân bổ cổ tức.

2.8.2. Quản lý chuỗi cung ứng (Supply Chain Management)

Quản lý chuỗi cung ứng (Supply Chain Management - SCM) là một trong những lĩnh vực quan trọng và đang được cải thiện mạnh mẽ nhờ sự ứng dụng của công nghệ blockchain. Blockchain giúp cải thiện các vấn đề về minh bạch, bảo mật, hiệu quả và khả năng truy xuất trong quản lý chuỗi cung ứng. Dưới đây là một số ứng dụng của blockchain trong SC:

1. Tăng cường minh bạch và truy xuất nguồn gốc

Blockchain giúp các doanh nghiệp theo dõi toàn bộ quá trình sản xuất và vận chuyển của sản phẩm từ nhà cung cấp đến người tiêu dùng cuối cùng. Với tính chất không thể thay đổi và minh bạch của blockchain, mọi giao dịch sẽ được ghi lại trên một cuốn sổ điện tử công khai và có thể kiểm tra được.

Ví dụ: *IBM Food Trust* là một nền tảng blockchain được sử dụng để theo dõi các sản phẩm thực phẩm từ trang trại đến bàn ăn của người tiêu dùng. Điều này giúp đảm bảo chất lượng sản phẩm, kiểm soát an toàn thực phẩm và hạn chế gian lận.

2. Giảm chi phí và thời gian giao dịch

Blockchain giúp giảm chi phí và thời gian giao dịch bằng cách loại bỏ các trung gian (ví dụ: ngân hàng, nhà cung cấp dịch vụ chứng thực) trong quá trình thanh toán và vận chuyển.

Ví dụ: *VeChain* là một công ty sử dụng blockchain để theo dõi và quản lý chuỗi cung ứng, đặc biệt trong các ngành công nghiệp như ô tô và thời trang. Blockchain giúp giảm chi phí hành chính và giảm thiểu sai sót.

3. Bảo mật và giảm thiểu gian lận

Các giao dịch trong chuỗi cung ứng có thể bị gian lận hoặc giả mạo, nhưng với blockchain, mỗi giao dịch được xác nhận và lưu trữ một cách an toàn, không thể thay đổi. Điều này giúp ngăn chặn gian lận và đảm bảo tính trung thực của dữ liệu.

Ví dụ: *Everledger* là một công ty sử dụng blockchain để theo dõi và xác thực nguồn gốc của kim cương. Mỗi viên kim cương có một hồ sơ trên blockchain, giúp ngăn chặn việc trao đổi kim cương giả và xác nhận nguồn gốc hợp pháp.

4. Cải thiện quản lý hợp đồng và thanh toán

Thông qua việc sử dụng hợp đồng thông minh (smart contracts), blockchain có thể tự động hóa quá trình thực hiện hợp đồng và thanh toán mà không cần sự can thiệp của bên thứ ba. Các hợp đồng này có thể tự động thực thi khi các điều kiện đã được đáp ứng.

Ví dụ: Một nhà sản xuất có thể thiết lập hợp đồng thông minh với các nhà cung cấp vật liệu, yêu cầu thanh toán khi hàng hóa được giao đủ số lượng và chất lượng. Blockchain sẽ ghi lại tất cả các bước và điều kiện, giúp tự động thực hiện các giao dịch mà không cần người kiểm soát trung gian.

5. Xác minh sản phẩm và chứng nhận

Blockchain có thể hỗ trợ chứng nhận chất lượng sản phẩm, từ đó nâng cao niềm tin của người tiêu dùng. Các thông tin như tiêu chuẩn chất lượng, quy trình sản xuất, và thành phần sản phẩm sẽ được ghi lại trên blockchain.

Ví dụ: Các sản phẩm như cà phê, hạt ca cao, hoặc sản phẩm hữu cơ có thể được xác minh nguồn gốc thông qua blockchain, giúp người tiêu dùng yên tâm rằng họ đang mua các sản phẩm đáp ứng tiêu chuẩn đạo đức và môi trường.

Tóm lại: Blockchain giúp tối ưu hóa rất nhiều khía cạnh trong quản lý chuỗi cung ứng từ việc tăng cường minh bạch, bảo mật, giảm chi phí, đến việc tự động hóa và quản lý hợp đồng. Các công ty hiện nay đang ngày càng nhận thức rõ hơn về tiềm năng của công nghệ này trong việc tối ưu hóa các quy trình chuỗi cung ứng, tạo ra môi trường giao dịch an toàn và minh bạch hơn.

2.8.3. Quản trị và hợp đồng thông minh

Quản trị và hợp đồng thông minh (Smart Contracts) là một trong những ứng dụng nổi bật và quan trọng của blockchain, giúp tự động hóa các quy trình quản trị và thực thi hợp đồng mà không cần sự can thiệp của bên thứ ba. Dưới đây là một cái nhìn chi tiết về cách blockchain hỗ trợ quản trị và hợp đồng thông minh:

2.8.3.1. Quản trị với Blockchain

Quản trị trong bối cảnh blockchain không chỉ đề cập đến việc quản lý các giao dịch mà còn là sự quản lý quy trình và quyết định trong các hệ thống phân tán. Các tổ chức và dự án có thể sử dụng blockchain để đảm bảo rằng các quyết định được đưa ra một cách minh bạch, công bằng và không bị can thiệp bởi bất kỳ ai.

Ví dụ: DAO (Decentralized Autonomous Organization): Là một tổ chức tự trị phi tập trung, nơi các quyết định quan trọng được thực hiện qua các cuộc bỏ phiếu do các thành viên tổ chức quyết định. Các quyết định này thường được thực hiện tự động thông qua hợp đồng thông minh.

2.8.3.2. Hợp đồng thông minh (Smart Contracts)

Hợp đồng thông minh là các hợp đồng tự động thực thi khi các điều kiện đã được xác nhận. Thay vì phải thông qua các bên trung gian như luật sư hay ngân hàng để thực thi một hợp đồng, blockchain giúp tự động hóa mọi quy trình và giao dịch mà không cần sự can thiệp của con người.

Ví dụ ứng dụng hợp đồng thông minh:

Sử dụng trong tài chính (DeFi - Tài chính phi tập trung): Các hợp đồng thông minh trong lĩnh vực tài chính giúp thực hiện các giao dịch tự động như cho vay, vay, và giao dịch chứng khoán mà không cần sự tham gia của ngân hàng hay các tổ chức tài chính truyền thống. Ví dụ như **Compound**, nơi người dùng có thể cho vay và vay tiền điện tử mà không cần thông qua một tổ chức tài chính trung gian.

Hợp đồng lao động và thanh toán: Các hợp đồng thông minh có thể tự động thanh toán cho nhân viên khi công việc đã hoàn thành hoặc khi các điều kiện hợp đồng được thực thi. Ví dụ, nếu một freelancer hoàn thành một nhiệm vụ, hợp đồng thông minh có thể tự động thanh toán cho họ ngay lập tức.

2.8.4. Sở hữu và sưu tầm tài sản Kỹ thuật số (NFT)

Sở hữu và sưu tầm tài sản kỹ thuật số (NFTs - Non-Fungible Tokens) là một trong những ứng dụng nổi bật của công nghệ blockchain, đặc biệt trong lĩnh vực nghệ thuật, giải trí, và các ngành công nghiệp sáng tạo. NFTs đã tạo ra một xu hướng mới trong việc mua, bán và sưu tầm tài sản kỹ thuật số với tính chất duy nhất và không thể thay thế.

Các ứng dụng của NFT trong sở hữu và sưu tầm tài sản kỹ thuật số:

2.8.4.1. Nghệ thuật số (Digital Art)

NFTs đã tạo ra một cuộc cách mạng trong lĩnh vực nghệ thuật, giúp các nghệ sĩ bán tác phẩm của mình dưới dạng kỹ thuật số và nhận được thanh toán trực tiếp mà không cần qua các nhà đấu giá hoặc các bên trung gian.

Ví dụ: Một trong những nghệ sĩ nổi tiếng nhất trong thế giới NFT là Beeple, người đã bán một tác phẩm nghệ thuật kỹ thuật số của mình, "Everydays: The First 5000 Days", với giá gần 70 triệu USD tại một buổi đấu giá của Christie's.

Ứng dụng: Mỗi tác phẩm nghệ thuật kỹ thuật số được mã hóa thành một NFT duy nhất, giúp người mua xác nhận quyền sở hữu và đảm bảo tính độc đáo của tác phẩm.

2.8.4.2. Sưu tầm và Vật phẩm hiếm

NFTs cũng được sử dụng để sưu tầm các vật phẩm kỹ thuật số hiếm, chẳng hạn như thẻ giao dịch thể thao, vật phẩm trong game, hay thậm chí các video, âm nhạc, và các tác phẩm sáng tạo khác.

Ví dụ: CryptoKitties là một trong những trò chơi sưu tầm NFT nổi tiếng, nơi người chơi có thể mua, bán và lai tạo những con mèo kỹ thuật số độc đáo. Mỗi con mèo là một NFT duy nhất.

Ứng dụng: Các vật phẩm trong trò chơi như skin, nhân vật, hay vũ khí cũng có thể được mã hóa thành NFT, giúp người chơi sở hữu và giao dịch chúng.

2.8.4.3. Thế giới ảo và Metaverse

NFTs đóng một vai trò quan trọng trong các thế giới ảo và Metaverse, nơi người dùng có thể sở hữu đất đai, vật phẩm, hoặc các tài sản kỹ thuật số khác trong một không gian ảo.

Ví dụ: Trong các thế giới như Decentraland hoặc Sandbox, người dùng có thể mua và sở hữu đất ảo dưới dạng NFT, xây dựng các dự án và giao dịch chúng.

Ứng dụng: NFTs cung cấp chứng nhận quyền sở hữu tài sản ảo trong các môi trường 3D, giúp người dùng tạo dựng tài sản và giá trị trong Metaverse.

2.8.5. Ứng dụng trong Y tế

Blockchain ứng dụng trong y tế là một lĩnh vực đang ngày càng nhận được sự quan tâm và phát triển, nhờ vào khả năng bảo mật, minh bạch và khả năng xử lý dữ liệu hiệu quả của công nghệ này. Blockchain có thể giúp cải thiện nhiều khía cạnh trong ngành y tế, từ việc quản lý dữ liệu bệnh nhân đến cải thiện quy trình thanh toán và bảo hiểm.

2.8.5.1. Quản lý và chia sẻ dữ liệu bệnh nhân

Blockchain có thể giúp cải thiện việc quản lý và chia sẻ dữ liệu bệnh nhân, đảm bảo rằng thông tin bệnh nhân được bảo vệ, minh bạch và dễ dàng truy cập khi cần thiết. Các dữ liệu như hồ sơ y tế, kết quả xét nghiệm, và thông tin điều trị có thể được lưu trữ một cách an toàn trên blockchain.

Minh bạch và bảo mật: Dữ liệu được lưu trữ trên blockchain không thể thay đổi hoặc xóa bỏ, giúp bảo vệ sự toàn vẹn của thông tin bệnh nhân. Chỉ những người có quyền truy cập mới có thể xem hoặc thay đổi dữ liệu.

Chia sẻ thông tin nhanh chóng và dễ dàng: Các bệnh viện, phòng khám và bác sĩ có thể chia sẻ thông tin với nhau một cách nhanh chóng và bảo mật mà không cần qua các hệ thống trung gian phức tạp.

Ví dụ: Dự án MedRec là một nền tảng dựa trên blockchain cho phép bệnh nhân kiểm soát hồ sơ y tế của mình, đồng thời cho phép bác sĩ và các cơ sở y tế khác dễ dàng truy cập thông tin khi cần thiết, giúp giảm thiểu sai sót và cải thiện chăm sóc sức khỏe.

2.8.5.2. An toàn và bảo mật thông tin y tế

Thông tin y tế là một trong những loại dữ liệu nhạy cảm nhất và thường xuyên là mục tiêu của các cuộc tấn công mạng. Blockchain có thể cung cấp một giải pháp bảo mật mạnh mẽ, đảm bảo rằng dữ liệu bệnh nhân được lưu trữ an toàn và chỉ có những người được phép mới có quyền truy cập.

Chống gian lận và truy xuất nguồn gốc: Blockchain có khả năng ghi lại tất cả các giao dịch và thay đổi, giúp dễ dàng theo dõi và xác minh các thay đổi đối với hồ sơ y tế, ngăn chặn gian lận và đảm bảo tính chính xác của dữ liệu.

Ví dụ: Các nền tảng như Healthereum sử dụng blockchain để bảo mật thông tin bệnh nhân và theo dõi việc tham gia vào các chương trình y tế, giúp đảm bảo rằng tất cả các hành động đều minh bạch và không thể thay đổi.

2.8.5.3. Quản lý dược phẩm và chuỗi cung ứng thuốc

Blockchain có thể giúp theo dõi và quản lý chuỗi cung ứng thuốc, từ khi sản xuất đến khi đến tay người tiêu dùng. Việc theo dõi này có thể giúp ngăn chặn thuốc giả, đảm bảo chất lượng và tính hợp pháp của thuốc.

Ngăn chặn thuốc giả: Các thông tin về nguồn gốc của thuốc và quá trình vận chuyển có thể được ghi lại trên blockchain, giúp đảm bảo rằng thuốc không bị giả mạo hoặc bị can thiệp trong quá trình vận chuyển.

Theo dõi thuốc và thiết bị y tế: Blockchain giúp theo dõi tình trạng thuốc và thiết bị y tế từ khi sản xuất đến khi sử dụng, đảm bảo rằng các sản phẩm luôn ở trong tình trạng tốt nhất.

Ví dụ: Modum sử dụng blockchain để theo dõi các sản phẩm dược phẩm và đảm bảo rằng các điều kiện lưu trữ được đáp ứng trong suốt quá trình vận chuyển.

2.8.5.4. Thanh toán và bảo hiểm y tế

Blockchain có thể cải thiện quy trình thanh toán và xử lý bảo hiểm y tế, giúp giảm chi phí, thời gian xử lý và tăng cường sự minh bạch trong các giao dịch này. Blockchain có thể hỗ trợ các hợp đồng thông minh (smart contracts) để tự động hóa các quy trình này.

Tự động hóa thanh toán: Các hợp đồng thông minh có thể tự động xử lý các khoản thanh toán giữa bệnh nhân, nhà cung cấp dịch vụ y tế và công ty bảo hiểm, giúp giảm thiểu sai sót và gian lận.

Quy trình bảo hiểm nhanh chóng và chính xác: Các công ty bảo hiểm có thể sử dụng blockchain để lưu trữ và truy xuất thông tin bệnh nhân, giúp quá trình thanh toán yêu cầu bảo hiểm trở nên nhanh chóng và chính xác hơn.

Ví dụ: Solve.Care là một nền tảng sử dụng blockchain để quản lý các dịch vụ chăm sóc sức khỏe và bảo hiểm y tế, giúp tự động hóa quá trình thanh toán và giảm thiểu chi phí hành chính.

2.8.5.5. Quản lý quyền sở hữu và chia sẻ thông tin gen di truyền

Với sự phát triển của y học chính xác, việc chia sẻ và quản lý thông tin gen di truyền trở nên rất quan trọng. Blockchain có thể giúp bảo vệ thông tin này và đảm bảo quyền sở hữu và quyền riêng tư cho các cá nhân.

Bảo vệ quyền riêng tư: Blockchain có thể giúp bệnh nhân kiểm soát quyền truy cập vào thông tin gen của họ và quyết định ai có thể xem hoặc sử dụng dữ liệu gen này cho mục đích nghiên cứu hoặc điều trị.

Ví dụ: Nebula Genomics sử dụng blockchain để bảo mật dữ liệu gen của người dùng và cung cấp cho họ quyền kiểm soát dữ liệu của mình.

2.8.6. Bầu cử và Quản lý chính phủ

2.8.6.1. Bầu cử và bỏ phiếu điện tử (e-Voting)

Blockchain có thể giúp cải thiện quy trình bầu cử và bỏ phiếu điện tử bằng cách cung cấp một hệ thống an toàn và minh bạch cho việc ghi nhận và xác minh phiếu bầu.

Bảo mật và chống gian lận: Mỗi lá phiếu có thể được mã hóa thành một transaction (giao dịch) và lưu trữ trên blockchain, giúp bảo vệ dữ liệu khỏi bị thay đổi hoặc xóa bỏ. Điều này ngăn ngừa các hành vi gian lận như việc thay đổi phiếu bầu hoặc giả mạo kết quả bầu cử.

Minh bạch và công khai: Mọi thông tin về phiếu bầu và kết quả sẽ được ghi lại trên blockchain, giúp mọi người có thể kiểm tra và xác minh kết quả mà không cần phụ thuộc vào một bên thứ ba. Blockchain đảm bảo tính minh bạch và chính xác trong toàn bộ quá trình.

Bỏ phiếu từ xa: Blockchain có thể giúp triển khai hệ thống bỏ phiếu từ xa, cho phép cử tri bỏ phiếu từ bất kỳ đâu mà không phải đến các điểm bỏ phiếu truyền thống. Điều này đặc biệt hữu ích trong các cuộc bầu cử toàn cầu, nơi cử tri có thể bỏ phiếu từ nước ngoài.

Ví dụ: Dự án Voatz là một nền tảng bỏ phiếu điện tử dựa trên blockchain đã được thử nghiệm trong một số cuộc bầu cử ở Mỹ, cho phép người dân bỏ phiếu qua ứng dụng di động với mức độ bảo mật cao.

2.8.6.2. Quản lý hồ sơ công dân và giấy tờ điện tử

Blockchain có thể được sử dụng để quản lý hồ sơ công dân, giấy tờ điện tử và các thông tin quan trọng khác mà chính phủ lưu trữ.

Hồ sơ công dân an toàn: Các hồ sơ công dân như giấy khai sinh, chứng minh nhân dân, hộ khẩu, hay thông tin thuế có thể được lưu trữ trên blockchain, giúp bảo vệ thông tin cá nhân khỏi bị làm giả hoặc mất mát.

Giảm thiểu thủ tục hành chính: Chính phủ có thể giảm thiểu các thủ tục hành chính phức tạp và tiết kiệm thời gian cho người dân bằng cách sử dụng blockchain để tự động hóa các quy trình liên quan đến việc cấp phát các giấy tờ hoặc chứng nhận.

Ví dụ: **Estonia** là quốc gia tiên phong trong việc sử dụng blockchain cho các dịch vụ công cộng, bao gồm việc cấp thẻ căn cước điện tử, quản lý hồ sơ công dân và các dịch vụ y tế.

2.8.6.3. Quản lý ngân sách và tài chính công

Blockchain có thể giúp cải thiện quy trình quản lý ngân sách và tài chính công của chính phủ, từ việc theo dõi thu chi đến việc phân phối ngân sách.

Minh bạch trong chi tiêu công: Blockchain giúp theo dõi mọi khoản chi tiêu của chính phủ, giúp người dân và các tổ chức giám sát việc sử dụng ngân sách công một cách minh bạch và chính xác.

Giảm thiểu tham nhũng: Blockchain đảm bảo rằng mọi giao dịch tài chính công đều được ghi lại một cách rõ ràng và không thể thay đổi, từ đó giảm thiểu khả năng tham nhũng và lạm dụng quyền lực trong việc phân phối ngân sách.

Ví dụ: Các quốc gia như Georgia đã sử dụng blockchain trong việc quản lý đất đai và tài chính công để tăng cường tính minh bạch và giảm thiểu tham nhũng.

2.8.6.4. Hợp đồng thông minh (Smart Contracts) trong quản lý chính phủ

Hợp đồng thông minh có thể được sử dụng trong các quy trình hành chính và pháp lý của chính phủ, giúp tự động hóa việc thực thi các hợp đồng mà không cần đến sự can thiệp của bên thứ ba.

Tự động hóa quy trình pháp lý: Các hợp đồng thông minh có thể tự động thực thi các điều khoản trong hợp đồng mà không cần sự can thiệp của luật sư hay tổ chức trung gian. Điều này giúp tiết kiệm chi phí và thời gian cho các quy trình pháp lý.

Chuyển nhượng tài sản công: Blockchain và hợp đồng thông minh có thể hỗ trợ việc chuyển nhượng tài sản công một cách nhanh chóng và hiệu quả. Ví dụ, khi một công dân mua tài sản công hoặc tham gia các chương trình nhà ở xã hội, hợp đồng thông minh có thể tự động xử lý các điều khoản hợp đồng mà không cần phải qua các thủ tục phức tạp.

Ví dụ: Ukraine đã thử nghiệm sử dụng hợp đồng thông minh để tự động hóa quy trình cấp giấy chứng nhận quyền sở hữu đất đai.

2.8.6.5. Quản lý quyền sở hữu và phân phối tài sản công

Blockchain có thể giúp quản lý quyền sở hữu các tài sản công, chẳng hạn như đất đai, tài nguyên thiên nhiên và các tài sản quốc gia khác. Nó giúp xác định rõ quyền sở hữu, tránh tranh chấp và cung cấp một hệ thống phân phối tài sản công minh bạch.

Quản lý tài nguyên thiên nhiên: Blockchain có thể giúp chính phủ theo dõi việc khai thác tài nguyên thiên nhiên và đảm bảo rằng việc phân phối tài nguyên này là hợp pháp và công bằng.

Quản lý đất đai: Các hồ sơ đất đai có thể được lưu trữ trên blockchain, giúp giảm thiểu tình trạng tranh chấp quyền sở hữu đất và đảm bảo tính minh bạch trong việc giao dịch đất đai.

Ví dụ: Ghana và Rwanda là hai quốc gia đã bắt đầu triển khai blockchain trong việc quản lý quyền sở hữu đất đai, giúp giảm thiểu tranh chấp và tăng cường tính minh bạch trong giao dịch đất đai.

Tóm lại, *Ứng dụng blockchain trong bầu cử và quản lý chính phủ có thể giúp cải thiện tính minh bạch, bảo mật và hiệu quả của các quy trình chính trị và hành chính. Mặc dù blockchain mang lại nhiều lợi ích đáng kể, nhưng việc triển khai công nghệ này vẫn gặp phải một số thách thức, bao gồm sự thay đổi trong cơ cấu tổ chức, vấn đề về pháp lý và bảo mật, và việc đảm bảo sự chấp nhận của người dân. Tuy nhiên, với những lợi ích mà blockchain mang lại, các quốc gia có thể tận dụng công nghệ này để xây dựng một hệ thống chính phủ minh bạch và công bằng hơn.*

2.8.7. Bảo mật và quyền sở hữu dữ liệu

Ứng dụng blockchain trong bảo mật và quyền sở hữu dữ liệu là một trong những lĩnh vực quan trọng, khi công nghệ blockchain có thể giải quyết các vấn đề về bảo mật, quyền riêng tư

và kiểm soát dữ liệu trong một thế giới ngày càng số hóa. Blockchain giúp người dùng kiểm soát dữ liệu cá nhân của mình, đảm bảo rằng thông tin không bị thay đổi, sao chép hay truy cập trái phép.

2.8.7.1. Bảo mật dữ liệu cá nhân và quyền riêng tư

Blockchain giúp bảo vệ dữ liệu cá nhân của người dùng bằng cách lưu trữ thông tin trong một mạng lưới phân tán, nơi không có một cơ sở dữ liệu trung tâm duy nhất, điều này giúp giảm thiểu rủi ro bị tấn công hoặc xâm phạm.

Mã hóa dữ liệu: Blockchain sử dụng các phương pháp mã hóa mạnh mẽ để đảm bảo rằng dữ liệu chỉ có thể được truy cập bởi người có quyền. Khi thông tin được lưu trữ trên blockchain, nó được phân mảnh và mã hóa, khiến cho việc truy cập trái phép trở nên rất khó khăn.

Kiểm soát quyền truy cập: Người dùng có thể tự quyết định ai có quyền truy cập vào dữ liệu của mình thông qua việc sử dụng khóa riêng và công nghệ mã hóa. Điều này giúp họ giữ quyền kiểm soát và bảo vệ dữ liệu cá nhân khỏi sự xâm phạm của các bên thứ ba.

Ví dụ: **SelfKey** là một nền tảng cho phép người dùng kiểm soát quyền sở hữu và truy cập thông tin cá nhân của mình. Thông qua blockchain, người dùng có thể chia sẻ hoặc giữ lại dữ liệu của mình mà không cần dựa vào các tổ chức trung gian.

2.8.7.2. Quản lý quyền sở hữu tài sản dữ liệu

Blockchain có thể cung cấp một cách thức để chứng nhận quyền sở hữu đối với tài sản số, bao gồm dữ liệu, tệp tin, hình ảnh, video, và các tài nguyên kỹ thuật số khác. Thông qua blockchain, người dùng có thể xác minh quyền sở hữu và bảo vệ tài sản số của mình.

Chứng nhận quyền sở hữu dữ liệu: Blockchain giúp ghi lại quyền sở hữu tài sản số bằng cách mã hóa tài sản dưới dạng token và lưu trữ nó trên một blockchain. Mỗi tài sản sẽ có một mã nhận dạng duy nhất và không thể thay đổi, giúp xác định ai là chủ sở hữu của tài sản.

Quản lý bản quyền và quyền sử dụng: Blockchain có thể giúp các tổ chức và cá nhân quản lý quyền bản quyền của các tài sản kỹ thuật số. Hợp đồng thông minh (smart contracts) có thể tự động xác nhận và thực thi các thỏa thuận về quyền sử dụng, phân phối và trả phí cho việc sử dụng tài sản.

Ví dụ: Filecoin là một dự án sử dụng blockchain để tạo ra một nền tảng lưu trữ phi tập trung, nơi người dùng có thể lưu trữ và truy cập dữ liệu trong khi duy trì quyền sở hữu và bảo mật thông tin.

2.8.7.3. Quản lý quyền sở hữu trong các ngành công nghiệp sáng tạo

Blockchain có thể giúp bảo vệ quyền sở hữu trí tuệ trong các ngành công nghiệp sáng tạo như âm nhạc, nghệ thuật số, phim ảnh, và văn học. Thông qua blockchain, các nghệ sĩ và tác giả có thể chứng nhận quyền sở hữu và kiểm soát việc sử dụng tác phẩm của họ.

Chứng nhận quyền sở hữu tác phẩm: Các tác phẩm nghệ thuật số, âm nhạc, video và các sản phẩm sáng tạo khác có thể được mã hóa thành các token NFT (Non-Fungible Token) trên blockchain, giúp xác minh quyền sở hữu và giúp các nghệ sĩ nhận được lợi nhuận từ việc bán và chuyển nhượng tác phẩm.

Quản lý bản quyền: Các hợp đồng thông minh có thể tự động thực thi các điều khoản bản quyền, giúp các nghệ sĩ và tác giả quản lý và bảo vệ quyền lợi của mình.

Ví dụ: Audius là một nền tảng âm nhạc phi tập trung, nơi các nghệ sĩ có thể đăng tải và quản lý nhạc của mình, bảo vệ quyền sở hữu và nhận thù lao trực tiếp từ người nghe.

Tóm lại, Ứng dụng blockchain trong bảo mật và quyền sở hữu dữ liệu mở ra một tương lai sáng lạn cho việc quản lý và bảo vệ dữ liệu trong nhiều lĩnh vực khác nhau, từ y tế, tài chính, đến ngành công nghiệp sáng tạo. Blockchain không chỉ giúp bảo mật và bảo vệ quyền riêng tư mà còn giúp người dùng duy trì quyền kiểm soát đối với dữ liệu của chính mình. Với những lợi ích này, blockchain đang dần trở thành công cụ quan trọng trong việc giải quyết các vấn đề về bảo mật và quyền sở hữu dữ liệu trong kỷ nguyên số.

CÂU HỎI VÀ BÀI TẬP

1. Blockchain là gì? Hãy giải thích ngắn gọn khái niệm này.

2. Nêu các đặc điểm quan trọng của blockchain và giải thích tại sao tính bất biến là yếu tố quan trọng nhất.

3. Mô tả cách các khối (blocks) liên kết với nhau trong blockchain.

4. Năm nào bài báo "Bitcoin: A Peer-to-Peer Electronic Cash System" được xuất bản?
a. 1991
b. 2008
c. 2009
d. 2016

5. Đặc điểm nào dưới đây không thuộc tính chất của công nghệ blockchain?
a. Sổ cái chỉ cho phép ghi thêm (Ledger)
b. Bảo mật bằng mật mã (Secure)
c. Tập trung hóa quản lý
d. Phân tán và chia sẻ thông tin

6. Ứng dụng blockchain đầu tiên là gì?
a. Ethereum
b. Bitcoin
c. NFT
d. Hashcash

7. So sánh sự khác biệt cơ bản giữa blockchain công khai và blockchain riêng tư.

8. Blockchain lai có thể được ứng dụng vào lĩnh vực bất động sản như thế nào? Đưa ra một ví dụ minh họa.

9. Tiền mã hóa là gì?

10. Tiền mã hóa hoạt động như thế nào?

11. Kể tên một số loại tiền mã hóa phổ biến.

12. Phân biệt tiền mã hóa và tiền fiat.
Hãy trình bày sự khác biệt giữa tiền mã hóa và tiền fiat, đặc biệt là trong các yếu tố như cơ chế phát hành, kiểm soát và tính thanh khoản.

13. Tokenomics là gì?
Giải thích một cách đơn giản về tokenomics và tầm quan trọng của nó trong hệ sinh thái blockchain.

14. So sánh sự khác biệt giữa kinh tế token (tokenomics) và kinh tế truyền thống?
Hãy giải thích những điểm khác biệt chính giữa việc sử dụng tiền tệ trong nền kinh tế truyền thống và sử dụng token trong blockchain.

15. Bitcoin có một số đặc điểm quan trọng trong tokenomics. Bạn có thể liệt kê và giải thích các đặc điểm này không?
Đưa ra các yếu tố chính trong tokenomics của Bitcoin và cách chúng ảnh hưởng đến giá trị của Bitcoin.

16. NFT là gì?
Giải thích khái niệm NFT và sự khác biệt giữa NFT và các tài sản có thể thay thế như tiền điện tử.

17. Hãy nêu ví dụ về một dự án NFT trên nền tảng Cardano và cách nó đã phát triển hệ sinh thái NFT trên Cardano.
Giới thiệu về dự án NFT đầu tiên trên nền tảng Cardano và những tác động của nó đối với sự phát triển của hệ sinh thái NFT trên Cardano.

18. Thách thức lớn nhất của NFT trong thị trường hiện tại là gì?

a) Tính bất ổn của thị trường
b) Tính bảo mật của blockchain
c) Giá trị nghệ thuật của NFT
d) Khả năng xác thực danh tính

19. Tại sao phí giao dịch cao lại là một thách thức lớn đối với người dùng NFT? a) Phí giao dịch cao chỉ ảnh hưởng đến người bán
b) Phí giao dịch làm giảm lợi nhuận từ việc đầu tư vào NFT
c) Phí giao dịch làm giảm sự tham gia của người tiêu dùng và tạo ra rào cản đầu vào
d) Phí giao dịch không ảnh hưởng đến sự phát triển của NFT

20. NFT có thể giúp nghệ sĩ trong việc bảo vệ bản quyền của tác phẩm như thế nào?

a) Bằng cách cho phép nghệ sĩ sao chép tác phẩm của mình dưới dạng NFT
b) Bằng cách giúp nghệ sĩ nhận doanh thu trực tiếp từ việc bán NFT
c) Bằng cách cho phép nghệ sĩ bán tác phẩm qua các công ty lớn
d) Bằng cách giảm giá trị tác phẩm nghệ thuật gốc

21. Ví trong blockchain là gì? Giải thích tầm quan trọng của ví đối với người dùng tiền mã hóa.

22. Phân biệt các loại ví phần mềm, ví cứng, ví trực tuyến và ví giấy. Nêu ưu nhược điểm của từng loại ví.

23. Khóa công khai và khóa riêng trong ví có vai trò như thế nào trong việc bảo mật tài sản kỹ thuật số?

24. Ví tiền mã hóa có ảnh hưởng gì đến việc giao dịch và quản lý tài sản số như tiền mã hóa hoặc NFT?

25. Hãy giải thích nguyên lý hoạt động của ví trong thế giới blockchain, đặc biệt trong việc ký giao dịch và bảo mật tài sản.

26. Tại sao địa chỉ trên blockchain lại quan trọng đối với giao dịch tiền mã hóa?

27. Hợp đồng thông minh có thể sử dụng địa chỉ ví blockchain như thế nào để tự động thực hiện các hành động?

28. Ứng dụng của địa chỉ trên blockchain trong các DApp là gì và nó mang lại lợi ích gì cho người dùng?

29. Những ứng dụng nào có thể sử dụng blockchain để quản lý danh tính cá nhân và bảo vệ quyền riêng tư?

30. Sổ cái trong blockchain khác với sổ cái truyền thống như thế nào?

31. Tại sao blockchain không cần một tổ chức trung gian để duy trì sổ cái?

32. Giải thích khái niệm "immutability" trong blockchain và tại sao nó quan trọng đối với tính bảo mật của giao dịch?

33. Những đặc điểm nào của sổ cái blockchain giúp tăng cường tính minh bạch và bảo mật?

34. Cơ chế đồng thuận như Proof of Work (PoW) hoặc Proof of Stake (PoS) hoạt động như thế nào trong việc xác nhận các giao dịch trên blockchain?

35. Giải thích các lợi ích mà sổ cái blockchain mang lại cho các ứng dụng tài chính và phi tài chính.

CHƯƠNG 3: MỘT SỐ NỀN TẢNG BLOCKCHAIN

Blockchain, từ khi ra đời, đã trải qua một hành trình phát triển đầy dấu ấn, mỗi giai đoạn mở ra một chương mới cho công nghệ này. Chương này sẽ đưa người đọc khám phá những cột mốc quan trọng đó.

Bitcoin, thế hệ đầu tiên, đã chứng minh tiềm năng của sổ cái phi tập trung, nhưng bộc lộ hạn chế về mở rộng. Ethereum, thế hệ thứ hai, mở ra kỷ nguyên dApps với hợp đồng thông minh, nhưng vẫn đối mặt thách thức về hiệu suất. Cardano, thế hệ thứ ba, hướng đến sự bền vững và khoa học, xây dựng cơ chế đồng thuận Ouroboros.

Chương này sẽ phân tích từng thế hệ, khám phá đặc điểm, ưu nhược điểm, và tiềm năng tương lai của blockchain.

3.1. Thế hệ đầu tiên: Bitcoin – Blockchain đầu tiên

3.1.1. Giới thiệu về Bitcoin

Bitcoin là đồng tiền điện tử phi tập trung đầu tiên trên thế giới, được tạo ra bởi một cá nhân hoặc nhóm người ẩn danh mang tên Satoshi Nakamoto. Ra mắt vào năm 2009, Bitcoin không chỉ là một loại tiền kỹ thuật số mà còn đánh dấu sự khởi đầu của công nghệ blockchain – nền tảng cho các ứng dụng phi tập trung sau này.

Nguồn gốc và lịch sử phát triển

Bitcoin được giới thiệu lần đầu trong tài liệu khoa học mang tên "Bitcoin: A Peer-to-Peer Electronic Cash System" do Satoshi Nakamoto công bố vào năm 2008. Tài liệu này đã mô tả một hệ thống thanh toán điện tử ngang hàng (peer-to-peer) cho phép giao dịch trực tiếp giữa hai bên mà không cần bên trung gian. Ngày 3 tháng 1 năm 2009, khối đầu tiên của Bitcoin, gọi là Genesis Block, đã được khai thác, đánh dấu sự khởi đầu cho một kỷ nguyên tài chính mới.

Satoshi Nakamoto đã tạo ra Bitcoin với mục tiêu giải quyết những vấn đề của hệ thống tài chính truyền thống, đặc biệt là vấn đề "chi tiêu gấp đôi" (double spending) trong giao dịch kỹ thuật số. Khác với các hệ thống thanh toán truyền thống phụ thuộc vào các bên trung gian như ngân hàng hoặc công ty tài chính, Bitcoin cho phép giao dịch trực tiếp mà không cần sự tin cậy vào bên thứ ba.

Đặc điểm nổi bật của Bitcoin

Bitcoin sở hữu những đặc điểm nổi bật làm nên tên tuổi và tầm ảnh hưởng của nó trong thế giới tài chính và công nghệ:

- **Phi tập trung**:
    - Bitcoin không được quản lý bởi bất kỳ cá nhân hoặc tổ chức nào.

    - Tất cả các giao dịch và khai thác đều được xử lý bởi các nút (nodes) trong mạng lưới ngang hàng.
- **Minh bạch**:
    - Mọi giao dịch Bitcoin đều được ghi lại trên blockchain, cho phép bất kỳ ai cũng có thể kiểm tra.
    - Tuy nhiên, danh tính của các bên giao dịch được bảo mật nhờ vào hệ thống địa chỉ mã hóa.
- **Bảo mật cao**:
    - Bitcoin sử dụng thuật toán mã hóa SHA-256 để bảo vệ dữ liệu và giao dịch.
    - Các khối trong blockchain liên kết với nhau bằng các hàm băm mã hóa, tạo ra một chuỗi không thể sửa đổi.
- **Nguồn cung giới hạn**:
    - Bitcoin có nguồn cung tối đa là 21 triệu đơn vị, được dự kiến khai thác hết vào năm 2140.
    - Tính khan hiếm này khiến Bitcoin trở thành một phương tiện lưu trữ giá trị tương tự như vàng.

Vai trò của Bitcoin trong hệ sinh thái blockchain

Bitcoin đã mở ra một kỷ nguyên mới trong công nghệ và tài chính, đặt nền móng cho sự phát triển của hàng ngàn loại tiền điện tử và ứng dụng blockchain khác. Một số vai trò quan trọng của Bitcoin bao gồm:

- **Tiên phong trong công nghệ blockchain**:
    - Bitcoin là ứng dụng đầu tiên của công nghệ blockchain, giới thiệu cơ chế đồng thuận Proof of Work (PoW).
    - Cơ chế này đảm bảo tính toàn vẹn và bảo mật cho các giao dịch mà không cần bên thứ ba.
- **Công cụ lưu trữ giá trị**:
    - Với nguồn cung giới hạn và tính khan hiếm, Bitcoin được ví như "vàng kỹ thuật số".
    - Nhiều nhà đầu tư coi Bitcoin là một công cụ phòng ngừa lạm phát và lưu trữ giá trị lâu dài.
- **Hệ thống thanh toán toàn cầu**:
    - Bitcoin cho phép giao dịch xuyên biên giới nhanh chóng với chi phí thấp hơn so với các hệ thống truyền thống.
    - Điều này đặc biệt hữu ích cho các quốc gia có hệ thống tài chính kém phát triển.

- **Nền tảng cho đổi mới**:
    - Sự thành công của Bitcoin đã thúc đẩy sự phát triển của các nền tảng blockchain khác như Ethereum, Cardano, và Binance Smart Chain.
    - Các ứng dụng phi tập trung (dApps) và hợp đồng thông minh (smart contracts) đều lấy cảm hứng từ Bitcoin.

Thách thức và hạn chế của Bitcoin

Mặc dù có nhiều ưu điểm, Bitcoin cũng đối mặt với một số thách thức lớn:

- **Khả năng mở rộng**:
    - Mạng lưới Bitcoin chỉ có thể xử lý khoảng 4-7 giao dịch mỗi giây, thấp hơn nhiều so với các hệ thống thanh toán truyền thống như Visa. Điều này là do kích thước khối 1 MB và thời gian tạo khối khoảng 10 phút.
    - Điều này dẫn đến thời gian xử lý giao dịch chậm và phí giao dịch cao trong thời gian mạng lưới tắc nghẽn.
- **Tiêu thụ năng lượng**:
    - Cơ chế đồng thuận POW (Proof of Work) yêu cầu một lượng lớn năng lượng để khai thác, gây ra những lo ngại về môi trường.
- **Tính pháp lý và chấp nhận**:
    - Bitcoin vẫn chưa được công nhận hoặc chấp nhận rộng rãi tại nhiều quốc gia.
    - Một số chính phủ lo ngại về việc sử dụng Bitcoin trong các hoạt động bất hợp pháp.

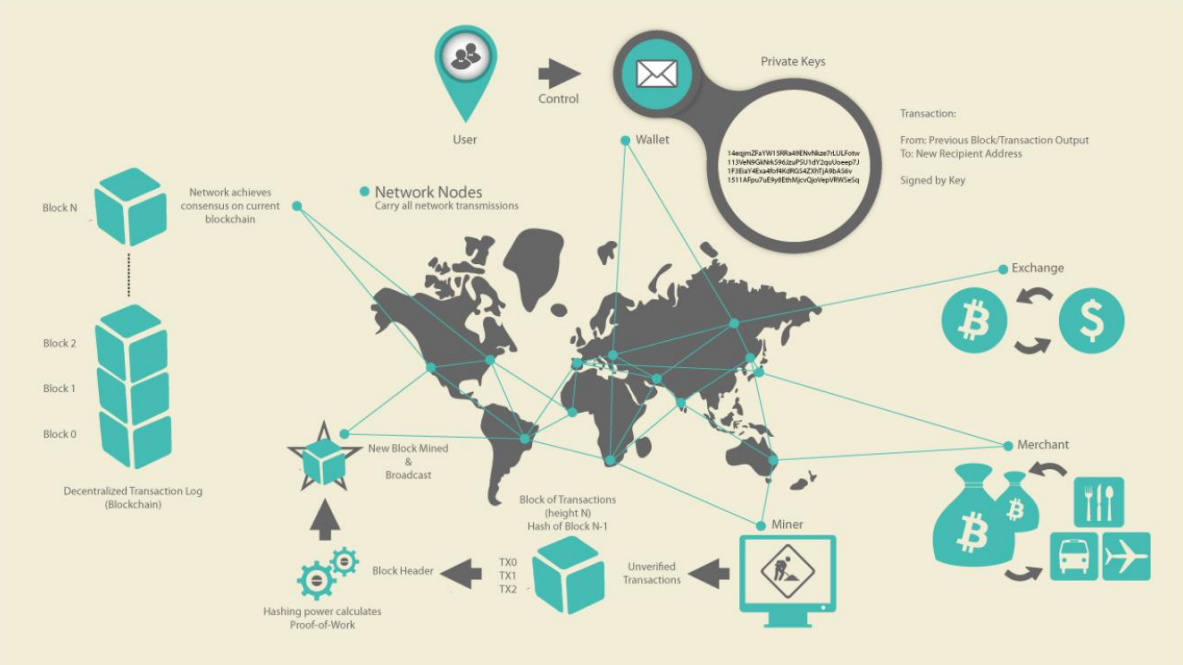
3.1.2. Nguyên lý hoạt động và cơ chế giao dịch của Bitcoin

Hệ thống Bitcoin, không giống như các hệ thống ngân hàng và thanh toán truyền thống, dựa trên sự tin tưởng phi tập trung. Thay vì có một cơ quan trung ương đáng tin cậy, trong Bitcoin, sự tin tưởng được hình thành như một thuộc tính nổi lên từ sự tương tác giữa các thành phần khác nhau trong hệ thống Bitcoin. Trong chương này, chúng ta sẽ xem xét Bitcoin từ góc độ tổng quan bằng cách theo dõi một giao dịch đơn lẻ qua hệ thống Bitcoin, quan sát cách giao dịch đó trở nên "đáng tin cậy" và được chấp nhận thông qua cơ chế đồng thuận phân tán của Bitcoin, cuối cùng được ghi lại trên blockchain – sổ cái phân tán của tất cả các giao dịch. Các chương sau sẽ đi sâu vào công nghệ đằng sau giao dịch, mạng lưới và khai thác.

3.1.2.1. Mô hình tổng quan về Bitcoin

Trong sơ đồ tổng quan được minh họa trong Hình 3-1, chúng ta thấy rằng hệ thống Bitcoin bao gồm các người dùng với ví chứa khóa, các giao dịch được truyền tải trên mạng, và các thợ đào (miners) tạo ra blockchain đồng thuận thông qua tính toán cạnh tranh. Blockchain này là sổ cái chính thức của tất cả các giao dịch.

Mỗi ví dụ trong chương này dựa trên một giao dịch thực tế được thực hiện trên mạng Bitcoin, mô phỏng các tương tác giữa người dùng (Joe, Alice, Bob và Gopesh) bằng cách chuyển tiền từ ví này sang ví khác. Trong khi theo dõi một giao dịch qua mạng Bitcoin đến blockchain, chúng ta sẽ sử dụng một trang web khám phá blockchain để hình dung từng bước. Trình khám phá blockchain là một ứng dụng web hoạt động như một công cụ tìm kiếm Bitcoin, cho phép bạn tìm kiếm địa chỉ, giao dịch và khối, đồng thời xem các mối quan hệ và luồng giữa chúng.



Hình 3-1. Bitcoin overview

Các trình khám phá blockchain phổ biến bao gồm:

Bitcoin Block Explorer: https://www.blockexplorer.com/

BlockCypher Explorer: https://live.blockcypher.com/

https://blockchain.info

Mỗi trình khám phá này đều có chức năng tìm kiếm, cho phép bạn nhập một địa chỉ Bitcoin, mã băm giao dịch (transaction hash), số khối (block number) hoặc mã băm khối (block hash) để truy xuất thông tin tương ứng từ mạng Bitcoin. Với mỗi ví dụ về giao dịch hoặc khối, chúng tôi sẽ cung cấp một URL để bạn có thể tự tra cứu và nghiên cứu chi tiết.

3.1.2.2. Giao dịch Bitcoin

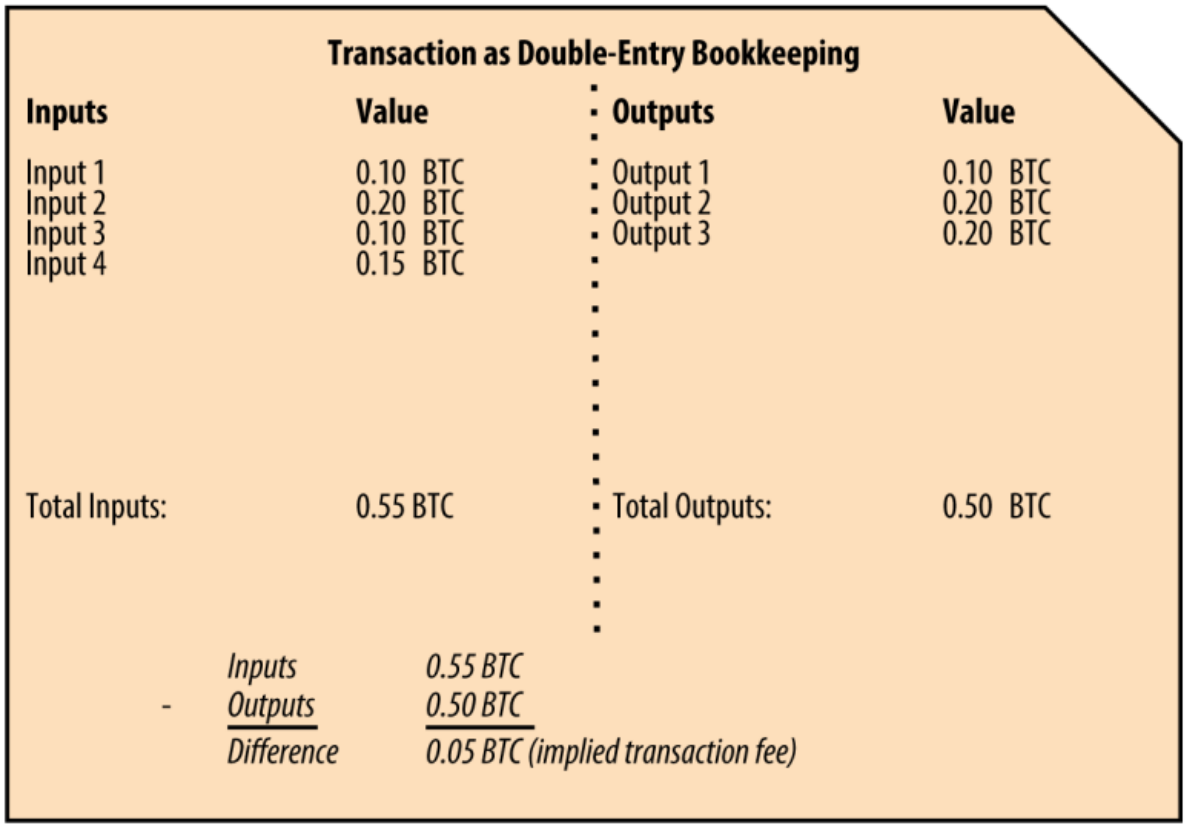
Một cách đơn giản, giao dịch Bitcoin là thông báo đến mạng lưới rằng một chủ sở hữu đã chấp thuận chuyển một lượng giá trị Bitcoin của mình cho một chủ sở hữu khác. Chủ sở hữu mới

sau đó có thể tiếp tục sử dụng số Bitcoin này bằng cách tạo ra một giao dịch mới, cho phép chuyển giá trị đó đến một người khác, hình thành nên một chuỗi liên tục của quyền sở hữu.

3.1.2.3. Đầu vào và đầu ra của giao dịch

Giao dịch Bitcoin có thể được hình dung như các dòng trong một sổ kế toán kép. Mỗi giao dịch bao gồm một hoặc nhiều "đầu vào" (inputs), tương tự như các khoản ghi nợ từ một tài khoản Bitcoin. Ở phía ngược lại, giao dịch có một hoặc nhiều "đầu ra" (outputs), giống như các khoản ghi có vào một tài khoản Bitcoin. Tuy nhiên, tổng số lượng đầu vào và đầu ra không nhất thiết phải bằng nhau. Thông thường, tổng các đầu ra sẽ nhỏ hơn tổng các đầu vào một chút, phần chênh lệch này được xem là phí giao dịch, một khoản thanh toán nhỏ được thợ đào (miner) thu về khi họ thêm giao dịch này vào sổ cái. Một giao dịch Bitcoin được thể hiện như một mục trong sổ kế toán được minh họa trong Hình 3-2.

Ngoài ra, mỗi giao dịch còn chứa bằng chứng về quyền sở hữu đối với lượng Bitcoin được sử dụng (đầu vào) dưới dạng chữ ký số của chủ sở hữu. Chữ ký này có thể được xác minh độc lập bởi bất kỳ ai. Trong ngữ cảnh Bitcoin, "sử dụng" có nghĩa là ký một giao dịch mới để chuyển giá trị từ một giao dịch trước đó đến một chủ sở hữu mới, được xác định thông qua địa chỉ Bitcoin của họ.



Hình 3-2. Giao dịch như sổ kế toán kép

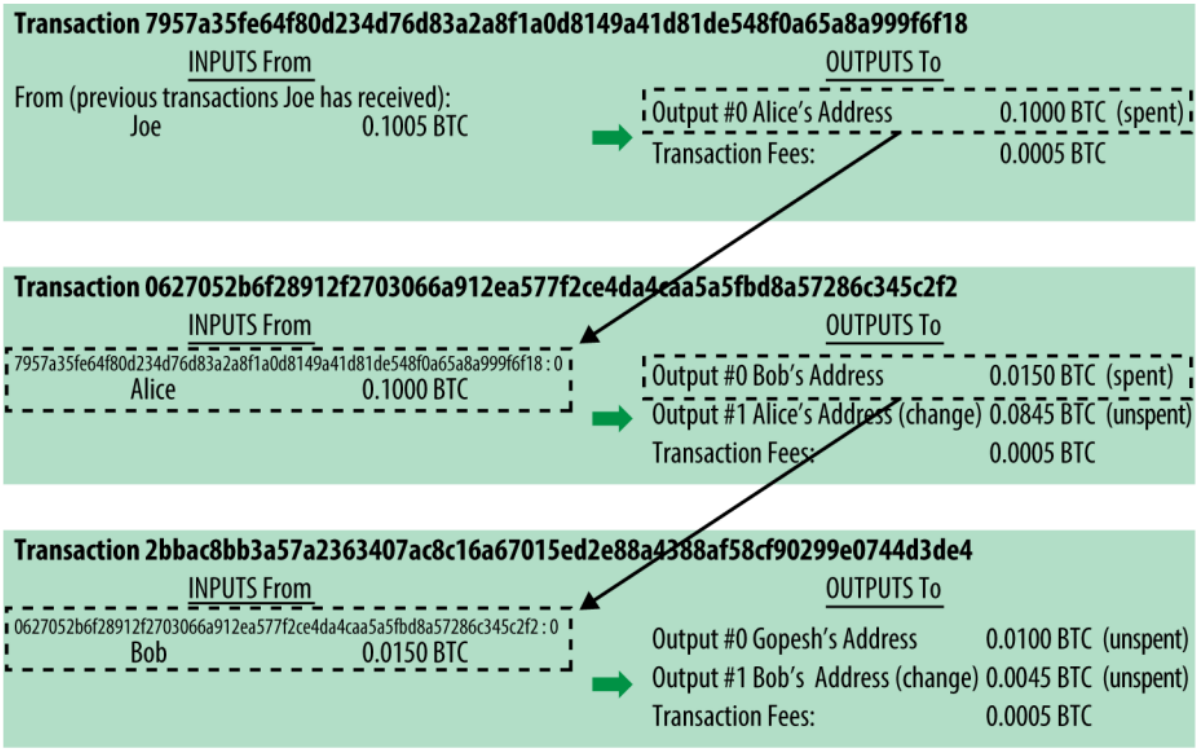
3.1.2.4. Chuỗi giao dịch (Transaction Chains)

Ví dụ: Khi Alice thanh toán cho quán cà phê của Bob, cô sử dụng đầu ra từ một giao dịch trước đó làm đầu vào. Giả sử trước đó, Alice đã nhận Bitcoin từ Joe, bạn của cô. Giao

dịch này đã tạo ra một giá trị Bitcoin được khóa bằng khóa của Alice. Trong giao dịch mới, Alice tham chiếu đến giao dịch trước đó làm đầu vào, đồng thời tạo ra các đầu ra mới để thanh toán cho cốc cà phê và nhận lại tiền thừa.

Các giao dịch này tạo thành một chuỗi liên kết, trong đó các đầu vào của giao dịch hiện tại gắn liền với các đầu ra từ các giao dịch trước đó. Khóa của Alice đóng vai trò cung cấp chữ ký số, mở khóa các đầu ra của giao dịch trước, qua đó chứng minh với mạng lưới Bitcoin rằng cô là chủ sở hữu hợp pháp của số tiền này. Alice sau đó gắn khoản thanh toán cho cốc cà phê vào địa chỉ của Bob, tạo điều kiện "ràng buộc" đầu ra với yêu cầu rằng Bob phải cung cấp chữ ký số của mình để sử dụng số tiền đó. Quá trình này minh họa rõ nét sự chuyển giao giá trị từ Alice sang Bob.

Chuỗi các giao dịch, từ Joe đến Alice và sau đó đến Bob, được minh họa trong Hình 3-3.



Hình 3-3. Chuỗi các giao dịch

3.1.2.5. Thêm Giao Dịch vào Sổ Cái

Giao dịch được tạo bởi ứng dụng ví của Alice có kích thước 258 byte, chứa tất cả các thông tin cần thiết để xác nhận quyền sở hữu số tiền và chỉ định chủ sở hữu mới. Bây giờ, giao dịch này cần được truyền tới mạng lưới Bitcoin để trở thành một phần của chuỗi khối (blockchain).

Trong phần tiếp theo, chúng ta sẽ tìm hiểu cách một giao dịch trở thành một phần của khối mới và cách khối này được "đào" (mined). Cuối cùng, chúng ta sẽ thấy cách khối mới, sau khi được thêm vào blockchain, dần dần nhận được sự tin cậy ngày càng tăng từ mạng lưới khi có thêm nhiều khối mới được bổ sung.

3.1.2.6. Truyền Giao Dịch

Vì giao dịch chứa tất cả thông tin cần thiết để xử lý, nên không quan trọng giao dịch được truyền tới mạng lưới Bitcoin như thế nào hoặc từ đâu. Mạng lưới Bitcoin là một mạng ngang hàng (peer-to-peer), trong đó mỗi máy khách Bitcoin tham gia bằng cách kết nối với một số máy khách Bitcoin khác. Mục đích của mạng này là để truyền tải giao dịch và các khối đến tất cả các thành viên tham gia.

3.1.2.7. Cách Giao Dịch Được Lan truyền

Bất kỳ hệ thống nào, như máy chủ, ứng dụng máy tính để bàn, hoặc ví điện tử, tham gia vào mạng lưới Bitcoin bằng cách sử dụng giao thức Bitcoin đều được gọi là một **nút Bitcoin** (bitcoin node). Ứng dụng ví của Alice có thể gửi giao dịch mới tới bất kỳ nút Bitcoin nào mà nó được kết nối, thông qua bất kỳ loại kết nối nào: có dây, WiFi, mạng di động, v.v.

Ví Bitcoin của Alice không cần phải kết nối trực tiếp với ví Bitcoin của Bob, và cô cũng không cần sử dụng kết nối internet của quán cà phê, mặc dù cả hai phương thức này đều có thể thực hiện được.

Bất kỳ nút Bitcoin nào nhận được một giao dịch hợp lệ mà nó chưa từng thấy trước đây sẽ ngay lập tức chuyển tiếp giao dịch đó tới tất cả các nút khác mà nó kết nối. Đây là một kỹ thuật truyền tải được gọi là **flooding** (truyền lan). Nhờ đó, giao dịch nhanh chóng được lan truyền khắp mạng ngang hàng, đạt tới một phần lớn các nút trong vòng vài giây.

3.1.2.8. Khai thác Bitcoin

Quá trình giao dịch của Alice hiện đã được truyền tải trên mạng Bitcoin. Tuy nhiên, giao dịch này chỉ trở thành một phần của blockchain khi nó được xác minh và đưa vào một khối thông qua một quá trình gọi là khai thác (mining).

Hệ thống tin cậy của Bitcoin dựa trên tính toán. Các giao dịch được gộp thành các khối, yêu cầu một lượng lớn tính toán để chứng minh, nhưng chỉ cần một lượng nhỏ tính toán để xác minh tính chính xác. Quá trình khai thác phục vụ hai mục đích chính trong Bitcoin:

- Các nút khai thác xác minh tất cả các giao dịch dựa trên các quy tắc đồng thuận của Bitcoin. Do đó, khai thác đảm bảo an ninh cho các giao dịch bằng cách loại bỏ các giao dịch không hợp lệ hoặc sai định dạng.
- Khai thác tạo ra Bitcoin mới trong mỗi khối, tương tự như cách ngân hàng trung ương in tiền mới. Số lượng Bitcoin được tạo ra trong mỗi khối bị giới hạn và giảm dần theo thời gian, tuân theo lịch trình phát hành cố định.

Khai thác đạt được sự cân bằng tinh tế giữa chi phí và phần thưởng. Quá trình này tiêu tốn điện năng để giải một bài toán toán học. Một thợ đào thành công sẽ nhận được phần thưởng dưới dạng Bitcoin mới và phí giao dịch. Tuy nhiên, phần thưởng chỉ được nhận nếu thợ đào xác minh đúng tất cả các giao dịch theo các quy tắc đồng thuận. Sự cân bằng này cung cấp an ninh cho Bitcoin mà không cần cơ quan trung ương.

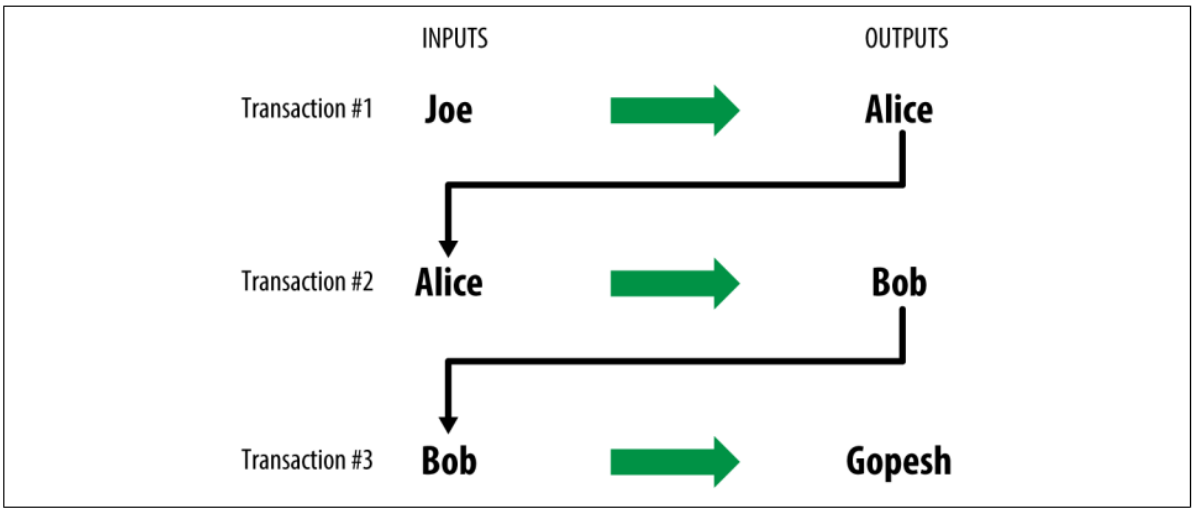
Một cách dễ hiểu để mô tả khai thác là giống như một trò chơi sudoku khổng lồ, cạnh tranh liên tục và đặt lại mỗi khi ai đó tìm được lời giải. Độ khó của trò chơi được điều chỉnh tự động để mất khoảng 10 phút để tìm ra lời giải. Hãy tưởng tượng một bảng sudoku khổng lồ, có hàng ngàn hàng và cột. Nếu bạn đưa ra một bảng hoàn chỉnh, người khác có thể kiểm tra rất nhanh. Tuy nhiên, nếu bảng chỉ có vài ô được điền, phần còn lại trống, thì cần rất nhiều công sức để giải! Độ khó của sudoku có thể được điều chỉnh bằng cách thay đổi kích thước của nó, nhưng vẫn dễ dàng xác minh ngay cả khi bảng rất lớn.

3.1.2.9. Chi tiêu Giao dịch

Khi giao dịch của Alice được ghi vào blockchain, nó trở thành một phần của sổ cái phân tán Bitcoin và hiển thị cho tất cả các ứng dụng Bitcoin. Các nút đầy đủ (full-node) có thể xác minh giao dịch là hợp lệ bằng cách theo dõi nguồn gốc của số Bitcoin từ khi được tạo ra trong khối đầu tiên, qua từng giao dịch cho đến địa chỉ của Bob. Trong khi đó, các ứng dụng khách nhẹ (lightweight clients) sử dụng phương pháp xác minh thanh toán đơn giản (SPV), xác nhận giao dịch nằm trên blockchain và được bổ sung bởi nhiều khối khác, đảm bảo rằng các thợ đào đã chấp nhận nó.

Giờ đây, Bob có thể chi tiêu số Bitcoin nhận từ Alice hoặc các giao dịch khác. Ví dụ, Bob có thể chuyển khoản thanh toán từ Alice đến các nhà cung cấp hoặc nhà thầu. Phần mềm Bitcoin của Bob thường gộp nhiều giao dịch nhỏ trong ngày thành một giao dịch lớn, hợp nhất thành một đầu ra và một địa chỉ duy nhất.

Khi Bob chi tiêu số Bitcoin này, chuỗi giao dịch tiếp tục mở rộng. Ví dụ, nếu Bob trả tiền cho nhà thiết kế web Gopesh, giao dịch này trở thành một phần của chuỗi từ Alice đến Gopesh. Chuỗi giao dịch minh họa cách giá trị di chuyển từ người này sang người khác, liên tục xây dựng trên blockchain.



Hình 3-4: Giao dịch của Alice là một phần trong chuỗi giao dịch từ Alice đến Gopesh.

3.1.3. Khóa, địa chỉ và ví

Quyền sở hữu Bitcoin được xác định qua các khóa số, địa chỉ Bitcoin và chữ ký số. Các khóa số được tạo và lưu trữ trong ví của người dùng, độc lập với mạng Bitcoin. Chúng cung

cấp các tính năng như kiểm soát phi tập trung, chứng thực quyền sở hữu và bảo mật bằng mật mã.

Mỗi giao dịch Bitcoin cần một chữ ký số hợp lệ, được tạo từ khóa bí mật. Ai sở hữu khóa bí mật có thể kiểm soát Bitcoin liên quan. Cặp khóa gồm khóa bí mật (giống mã PIN) và khóa công khai (giống số tài khoản), thường được phần mềm ví quản lý. Người dùng chỉ cần quan tâm đến địa chỉ Bitcoin – một dạng dấu vân tay số của khóa công khai – để nhận tiền.

Địa chỉ Bitcoin đơn giản hóa giao dịch, tương tự như tên người nhận trên một tấm séc, và có thể đại diện cho các script phức tạp. Chúng ta sẽ tìm hiểu cách tạo, lưu trữ, và quản lý khóa, định dạng mã hóa và ứng dụng nâng cao như địa chỉ đa chữ ký hay ví giấy.

Trong Bitcoin, mật mã khóa công khai được sử dụng để tạo một cặp khóa kiểm soát quyền truy cập vào Bitcoin. Cặp khóa bao gồm:

- **Khóa bí mật (private key):** dùng để ký giao dịch khi chi tiêu Bitcoin.
- **Khóa công khai (public key):** được tạo ra từ khóa bí mật và dùng để nhận Bitcoin.

Mối quan hệ toán học giữa khóa công khai và khóa bí mật cho phép sử dụng khóa bí mật để tạo chữ ký số. Chữ ký này có thể được xác minh bằng khóa công khai mà không cần tiết lộ khóa bí mật.

Khi chi tiêu Bitcoin, người sở hữu hiện tại trình bày khóa công khai và chữ ký (chữ ký thay đổi mỗi lần nhưng đều được tạo từ cùng một khóa bí mật) trong giao dịch. Nhờ đó, toàn bộ mạng Bitcoin có thể xác minh giao dịch là hợp lệ và xác nhận người chuyển sở hữu Bitcoin tại thời điểm giao dịch.

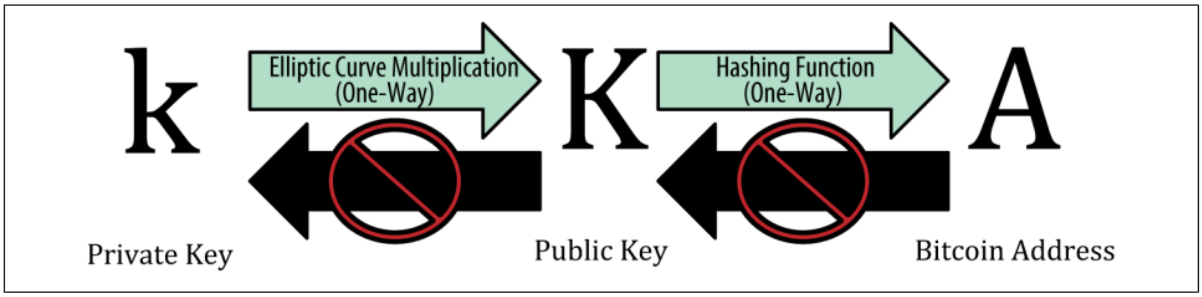
Trong hầu hết các ví Bitcoin, khóa bí mật và khóa công khai được lưu trữ cùng nhau dưới dạng cặp khóa để tiện lợi. Tuy nhiên, vì khóa công khai có thể được tính toán từ khóa bí mật, nên cũng có thể chỉ cần lưu trữ khóa bí mật.

Khóa Bí Mật và Khóa Công Khai của Ví Bitcoin

Bitcoin sử dụng mã hõa bất đối xứng đã được mô tả chi tiết tại mục 1.1.5 của tài liệu này. Sau đây chúng ta sẽ thấy rằng một ví Bitcoin chứa một tập hợp các cặp khóa, mỗi cặp bao gồm:

- **Khóa bí mật (k):** là một số, thường được chọn ngẫu nhiên.
- **Khóa công khai (K):** được tạo từ khóa bí mật thông qua phép nhân đường cong elliptic, một hàm mật mã một chiều.

Từ khóa công khai (K), một hàm băm mật mã một chiều sẽ được sử dụng để tạo ra địa chỉ Bitcoin (A). Mối quan hệ giữa khóa bí mật, khóa công khai và địa chỉ Bitcoin được minh họa trong Hình 3-5.



Hình 3-5: Private key, public key, and bitcoin address

Bitcoin hoạt động dựa trên hai loại khóa quan trọng: **khóa bí mật** và **khóa công khai**. Hai loại khóa này giúp đảm bảo an toàn, xác thực quyền sở hữu và quản lý tài sản Bitcoin một cách hiệu quả.

Khóa bí mật là một con số ngẫu nhiên rất lớn, được phần mềm ví Bitcoin tạo ra. Bạn có thể hình dung nó giống như một mật khẩu cá nhân mà chỉ mình bạn biết. Khóa bí mật đóng vai trò như chìa khóa chính để kiểm soát và chi tiêu Bitcoin.

Từ khóa bí mật, hệ thống sẽ tạo ra **khóa công khai**. Đây là một dạng thông tin có thể chia sẻ công khai, giống như số tài khoản ngân hàng mà bạn cung cấp cho người khác để họ gửi Bitcoin cho bạn. Khóa công khai được tạo ra từ khóa bí mật thông qua một phép toán đặc biệt, gọi là **phép nhân đường cong elliptic**. Điều đặc biệt ở đây là phép toán này chỉ hoạt động theo một chiều: từ khóa bí mật có thể tạo ra khóa công khai, nhưng không ai có thể làm ngược lại để tìm ra khóa bí mật từ khóa công khai.

Từ khóa công khai, hệ thống tiếp tục thực hiện một phép toán mật mã khác, gọi là **hàm băm**, để tạo ra **địa chỉ Bitcoin**. Địa chỉ này là nơi bạn nhận Bitcoin từ người khác.

Cụ thể, quy trình như sau: phần mềm ví Bitcoin sẽ tạo ra một số ngẫu nhiên (khóa bí mật). Từ đó, nó áp dụng phép nhân đường cong elliptic để tạo ra khóa công khai. Cuối cùng, từ khóa công khai, hệ thống áp dụng hàm băm để tạo ra địa chỉ Bitcoin.

Hệ thống này rất an toàn vì các phép toán chỉ hoạt động theo một chiều. Điều đó có nghĩa là, ngay cả khi ai đó biết khóa công khai hoặc địa chỉ Bitcoin của bạn, họ cũng không thể tìm ra khóa bí mật của bạn. Chỉ người nắm giữ khóa bí mật mới có thể tạo ra chữ ký số để xác nhận quyền sở hữu và chi tiêu Bitcoin.

Nói cách khác, khóa bí mật là chìa khóa duy nhất giúp bạn kiểm soát tài sản Bitcoin của mình, trong khi khóa công khai và địa chỉ Bitcoin là những thông tin có thể chia sẻ mà không ảnh hưởng đến bảo mật. Nhờ cơ chế này, Bitcoin đảm bảo được tính minh bạch và an toàn cho toàn bộ hệ thống.

Địa Chỉ Bitcoin

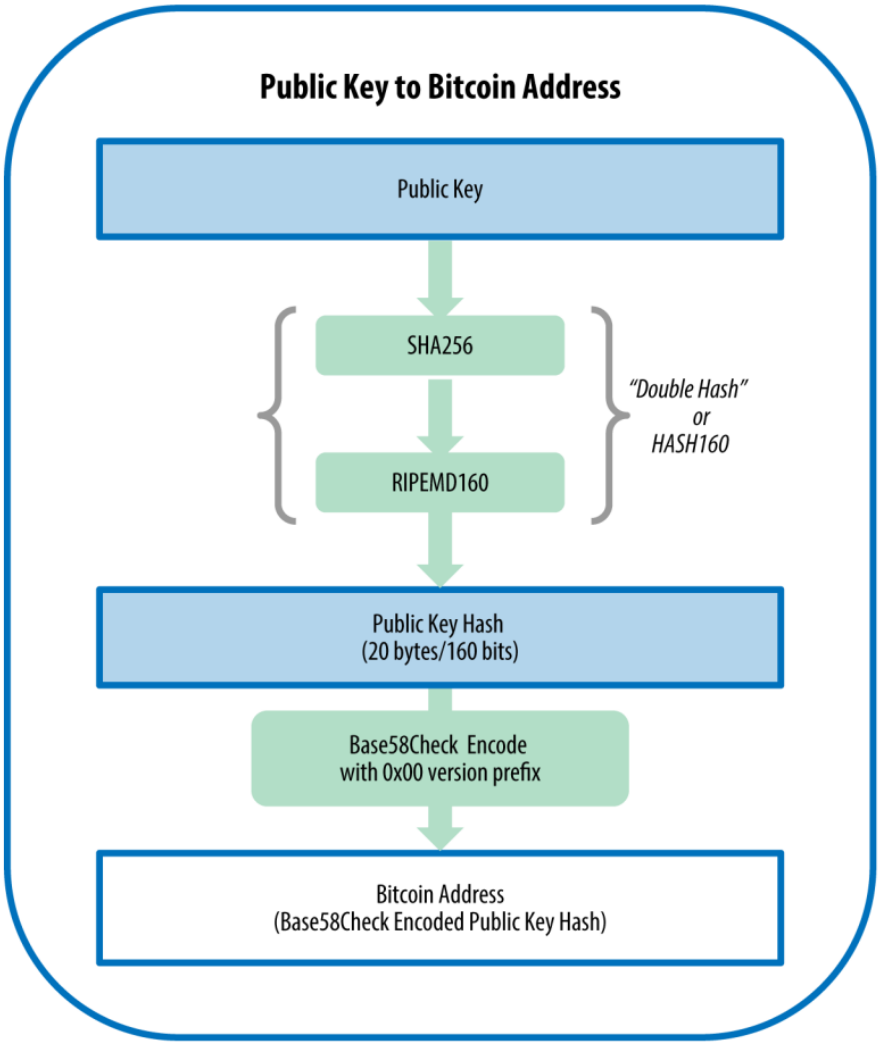
Địa chỉ Bitcoin là một chuỗi ký tự dùng để nhận tiền từ người khác. Được tạo ra từ khóa công khai, địa chỉ Bitcoin thường bắt đầu bằng số "1", Ví dụ về một địa chỉ Bitcoin: **1J7mdg5rbQyUHENYdx39WVWK7fsLpEoXZy** và có thể được so sánh với "người thụ hưởng" trong một tờ séc giấy. Nó đại diện cho nơi nhận tiền trong một giao dịch Bitcoin.

Quá trình tạo địa chỉ bắt đầu từ khóa công khai. Khóa này được băm hai lần: lần đầu sử dụng thuật toán SHA256, và lần thứ hai sử dụng RIPEMD160, tạo ra một chuỗi 160-bit gọi là địa chỉ Bitcoin.

Để dễ sử dụng và tránh nhầm lẫn, địa chỉ Bitcoin thường được mã hóa bằng Base58Check. Hệ thống này giúp địa chỉ dễ đọc hơn, tránh nhầm lẫn giữa các ký tự tương tự, đồng thời bổ sung kiểm tra tổng (checksum) để phát hiện lỗi nhập liệu.

Địa chỉ Bitcoin không phải là khóa công khai mà là phiên bản rút gọn và được bảo mật thông qua các hàm băm. Nó là phần duy nhất người dùng cần chia sẻ để nhận tiền.

Cơ chế mã hóa và giải mã Base58Check cũng như các biểu diễn kết quả được mô tả ở Hình 3-6. Nó minh họa quá trình chuyển đổi từ khóa công khai thành địa chỉ Bitcoin.



Hình 3-6: Mô tả quá trình chuyển đổi từ khóa công khai thành địa chỉ Bitcoin

Để hiểu sâu hơn về mối liên hệ giữa khóa riêng tư (private key), khóa công khai (public key) và địa chỉ Bitcoin, bạn có thể tìm hiểu thông qua BIP-38. BIP-38 là một tiêu chuẩn đề xuất (Bitcoin Improvement Proposal) được sử dụng để mã hóa khóa riêng tư bằng một mật khẩu (passphrase), sau đó mã hóa kết quả bằng Base58Check. Mục đích chính của BIP-38 là

tăng cường bảo mật cho khóa riêng tư, đặc biệt là khi chúng được lưu trữ ở những nơi không an toàn như trên giấy, USB, hoặc khi di chuyển giữa các ví. Bằng cách mã hóa khóa riêng tư, ngay cả khi ai đó có được bản sao của nó, họ cũng không thể sử dụng được nếu không có mật khẩu giải mã. Điều này giúp bảo vệ tài sản Bitcoin của bạn khỏi nguy cơ bị đánh cắp do lộ khóa riêng tư. Tóm lại, BIP-38 cung cấp một phương pháp an toàn và tiện lợi để bảo vệ khóa riêng tư bằng cách mã hóa chúng.

3.1.4. Mạng lưới Bitcoin

Bitcoin được xây dựng dựa trên kiến trúc mạng ngang hàng (peer-to-peer - P2P đã được giới thiệu ở Chương 1) hoạt động trên nền tảng internet. Kiến trúc mạng P2P của Bitcoin không chỉ là một lựa chọn về cấu trúc mà còn phản ánh và hỗ trợ cho đặc tính cốt lõi của Bitcoin: một hệ thống tiền mặt kỹ thuật số phi tập trung. Nguyên tắc thiết kế quan trọng của Bitcoin là phi tập trung quyền kiểm soát, điều này chỉ có thể đạt được và duy trì thông qua một mạng P2P, phi tập trung dựa trên sự đồng thuận.

Thuật ngữ "mạng Bitcoin" đề cập đến tập hợp các nút đang chạy giao thức P2P của Bitcoin. Ngoài giao thức P2P của Bitcoin, còn có các giao thức khác như Stratum được sử dụng cho khai thác (mining) và ví nhẹ (lightweight wallets) hoặc ví di động. Những giao thức bổ sung này được cung cấp bởi các máy chủ định tuyến cổng kết nối với mạng Bitcoin qua giao thức P2P và sau đó mở rộng mạng này tới các nút sử dụng các giao thức khác.

Ví dụ, các máy chủ Stratum kết nối các nút khai thác sử dụng giao thức Stratum với mạng Bitcoin chính và làm cầu nối giữa giao thức Stratum và giao thức P2P của Bitcoin. Thuật ngữ "mạng mở rộng của Bitcoin" được dùng để chỉ toàn bộ mạng, bao gồm giao thức P2P của Bitcoin, các giao thức khai thác trong nhóm (pool-mining), giao thức Stratum và các giao thức liên quan khác kết nối các thành phần của hệ thống Bitcoin.

Các loại Nút và vai trò của chúng trong mạng Bitcoin.

Dù các nút (node) trong mạng P2P của Bitcoin được xem là bình đẳng, chúng có thể đảm nhận các vai trò khác nhau dựa trên chức năng mà chúng hỗ trợ. Một nút Bitcoin là sự kết hợp của các chức năng: định tuyến, cơ sở dữ liệu blockchain, khai thác (mining), và dịch vụ ví (wallet). Một nút đầy đủ với cả bốn chức năng này được minh họa trong Hình 8-1.

- **Chức năng Định Tuyến**

Tất cả các nút đều bao gồm chức năng định tuyến để tham gia vào mạng và có thể có thêm các chức năng khác. Các nút đều thực hiện việc xác minh, lan truyền giao dịch và khối, cũng như tìm kiếm và duy trì kết nối với các nút đồng cấp (peers). Trong ví dụ về nút đầy đủ, chức năng định tuyến được biểu thị bằng vòng tròn màu cam có tên “Nút Định Tuyến Mạng” hoặc ký hiệu “N.”

- **Nút Đầy Đủ (Full Node)**

Một số nút, được gọi là nút đầy đủ (full node), duy trì một bản sao đầy đủ và luôn được cập nhật của blockchain. Các nút này có thể tự động và độc lập xác minh bất kỳ giao dịch nào

mà không cần tham chiếu bên ngoài. Trong hình minh họa, chức năng cơ sở dữ liệu blockchain đầy đủ được biểu thị bằng vòng tròn màu xanh dương có tên "Blockchain Đầy Đủ" hoặc ký hiệu "B."

- **Nút SPV (Simplified Payment Verification)**

Một số nút chỉ duy trì một phần của blockchain và xác minh giao dịch bằng phương pháp gọi là xác minh thanh toán đơn giản (Simplified Payment Verification - SPV). Các nút này thường được gọi là nút SPV hoặc nút nhẹ (lightweight nodes). Trong các hình minh họa, nút SPV được biểu thị mà không có vòng tròn màu xanh dương, cho thấy chúng không có bản sao đầy đủ của blockchain.

- **Nút Khai Thác (Mining Node)**

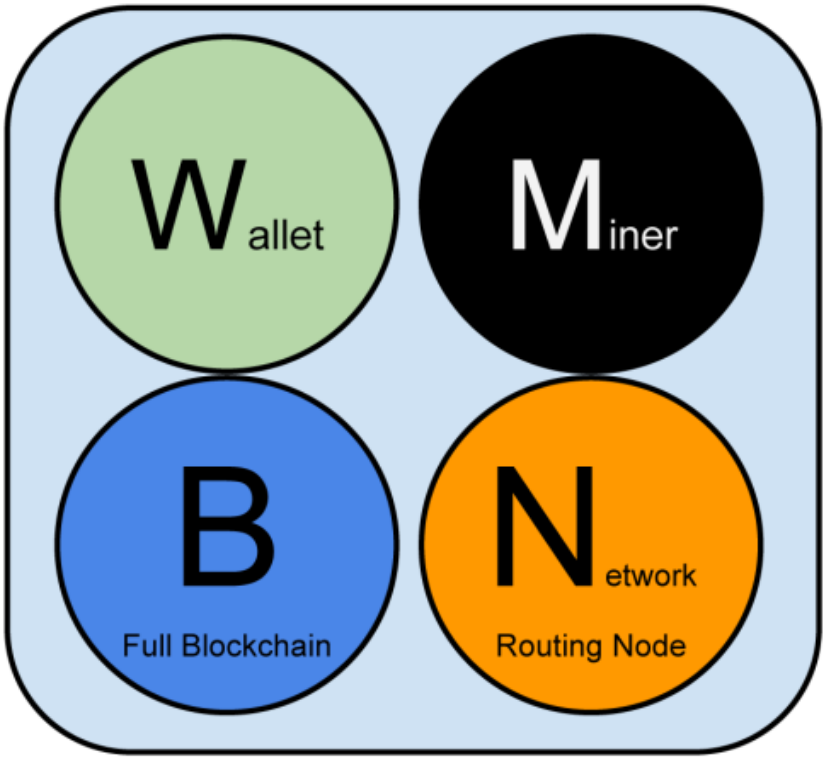
Các nút khai thác cạnh tranh để tạo ra các khối mới bằng cách chạy phần cứng chuyên dụng để giải thuật toán Proof-of-Work. Một số nút khai thác cũng là nút đầy đủ, duy trì bản sao đầy đủ của blockchain, trong khi một số khác là nút nhẹ tham gia khai thác nhóm (pool mining) và phụ thuộc vào máy chủ nhóm (pool server) để duy trì một nút đầy đủ. Chức năng khai thác được biểu thị bằng vòng tròn màu đen có tên "Khai Thác" hoặc ký hiệu "M."

- **Ví Người Dùng (User Wallets)**

Ví người dùng có thể là một phần của nút đầy đủ, như thường thấy trong các ứng dụng khách Bitcoin trên máy tính để bàn. Tuy nhiên, ngày càng nhiều ví người dùng, đặc biệt là trên các thiết bị có tài nguyên hạn chế như điện thoại thông minh, là các nút SPV. Chức năng ví được biểu thị bằng vòng tròn màu xanh lá cây có tên "Ví" hoặc ký hiệu "W."

- **Nút và Máy Chủ Khác**

Ngoài các loại nút chính trong giao thức P2P của Bitcoin, còn có các máy chủ và nút chạy các giao thức khác, như các giao thức dành riêng cho khai thác nhóm (mining pool) và giao thức truy cập khách hàng nhẹ (lightweight client-access).



Hình 3-7: Một nút mạng Bitcoin với đầy đủ bốn chức năng: Ví (Wallet), khai thác (Miner), cơ sở dữ liệu blockchain đầy đủ (B), và định tuyến mạng (Network).

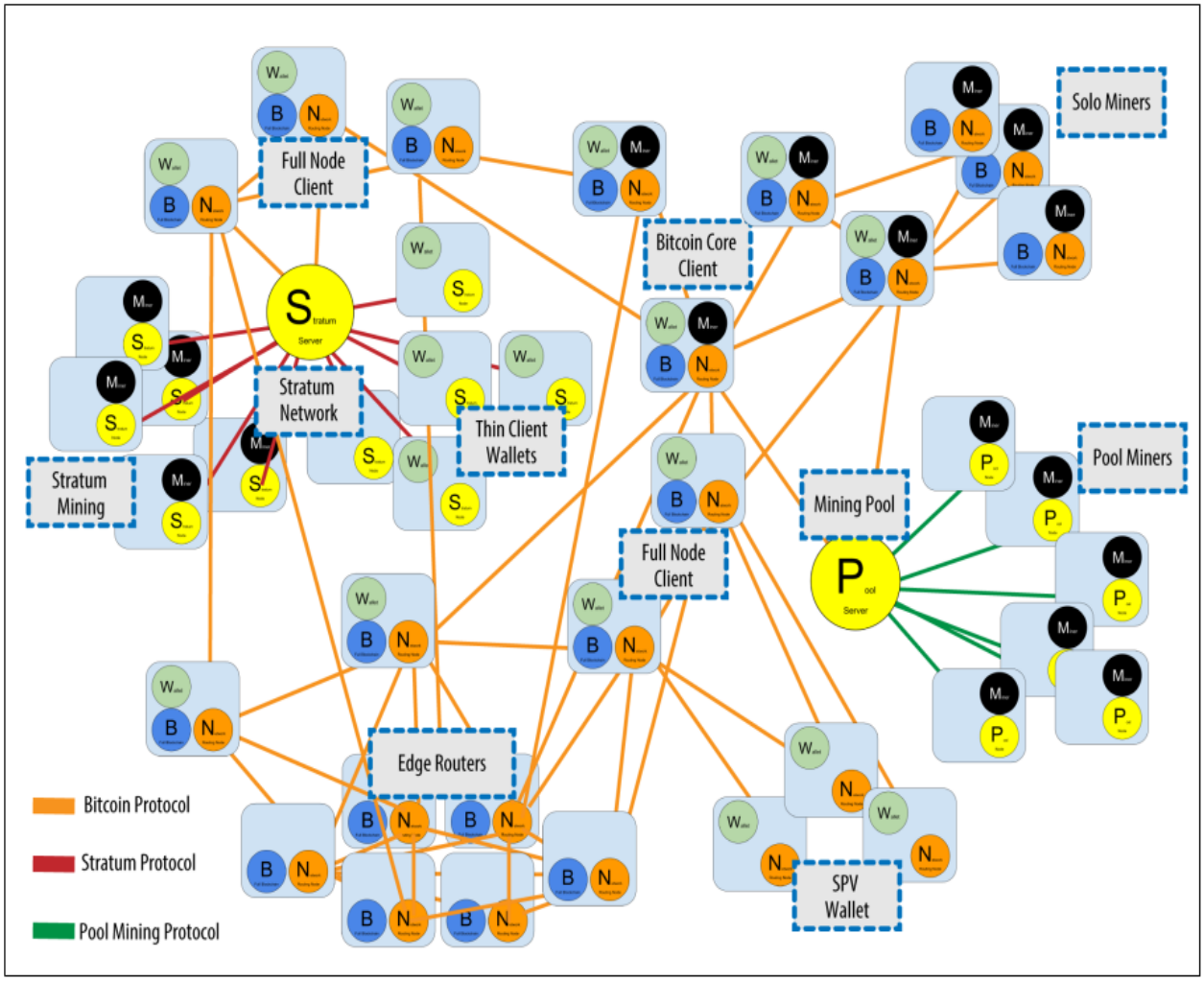
Mạng Bitcoin Mở Rộng

Mạng Bitcoin chính, chạy giao thức P2P của Bitcoin, bao gồm từ 5.000 đến 8.000 nút đang lắng nghe, chạy nhiều phiên bản khác nhau của ứng dụng tham chiếu Bitcoin (Bitcoin Core) và một vài trăm nút chạy các phiên bản khác của giao thức P2P Bitcoin như Bitcoin Classic, Bitcoin Unlimited, BitcoinJ, Libbitcoin, btcd, và bcoin. Một tỷ lệ nhỏ các nút trong mạng P2P Bitcoin là các nút khai thác, tham gia quá trình khai thác, xác thực giao dịch và tạo ra các khối mới.

Nhiều công ty lớn kết nối với mạng Bitcoin bằng cách chạy các ứng dụng khách nút đầy đủ dựa trên ứng dụng Bitcoin Core, với bản sao đầy đủ của blockchain và chức năng nút mạng, nhưng không có chức năng khai thác hoặc ví. Những nút này hoạt động như các bộ định tuyến biên của mạng, cho phép xây dựng các dịch vụ khác (sàn giao dịch, ví, trình khám phá khối, xử lý thanh toán thương mại) trên nền tảng của chúng.

Mạng Bitcoin mở rộng bao gồm mạng chạy giao thức P2P của Bitcoin như đã mô tả ở trên, cũng như các nút chạy các giao thức chuyên biệt khác. Gắn liền với mạng P2P chính của Bitcoin là một số máy chủ nhóm (pool servers) và các cổng giao thức kết nối các nút chạy các giao thức khác. Các nút này chủ yếu là các nút khai thác nhóm (pool mining nodes) và các ví nhẹ (lightweight wallet clients), không lưu trữ toàn bộ bản sao của blockchain.

Hình 3-8 Minh họa mạng Bitcoin mở rộng, bao gồm các loại nút khác nhau, máy chủ cổng, bộ định tuyến biên, và các ví khách, cũng như các giao thức khác nhau mà chúng sử dụng để kết nối với nhau.



Hình 3-8. *Mạng Bitcoin mở rộng minh họa các loại nút, cổng kết nối và giao thức khác nhau.*

3.1.5. Ý nghĩa và tác động của Bitcoin

Bitcoin không chỉ là một loại tiền kỹ thuật số mà còn mang lại những ý nghĩa và tác động sâu rộng đối với công nghệ, tài chính, kinh tế và xã hội.

Về mặt công nghệ, Bitcoin là ứng dụng đầu tiên của công nghệ blockchain – một hệ thống sổ cái phi tập trung, minh bạch và an toàn. Công nghệ này không chỉ giới hạn trong lĩnh vực tài chính mà còn có tiềm năng ứng dụng rộng rãi trong các ngành khác như chuỗi cung ứng, y tế, và quản trị.

Về tài chính, Bitcoin cung cấp một phương thức giao dịch ngang hàng không cần thông qua ngân hàng hay các tổ chức trung gian. Điều này đặc biệt hữu ích cho những người ở các khu vực không được tiếp cận với hệ thống ngân hàng truyền thống. Đồng thời, Bitcoin được xem như một công cụ lưu trữ giá trị, tương tự như "vàng kỹ thuật số", giúp chống lại lạm phát và sự mất giá của tiền tệ pháp định.

Về kinh tế, Bitcoin đã tạo ra một nền kinh tế hoàn toàn mới, thu hút sự tham gia của nhiều ngành công nghiệp như khai thác Bitcoin (mining), giao dịch tiền mã hóa, và phát triển công nghệ blockchain. Những ngành này không chỉ thúc đẩy đổi mới mà còn tạo ra nhiều cơ hội việc làm và đầu tư.

Về xã hội, Bitcoin mang lại sự tự do tài chính, cho phép mọi người kiểm soát tài sản của mình mà không phụ thuộc vào chính phủ hay ngân hàng. Điều này thúc đẩy quyền tự do cá nhân và giảm sự phụ thuộc vào các hệ thống tập trung.

Tuy nhiên, Bitcoin cũng đối mặt với nhiều thách thức và tranh cãi. Quá trình khai thác Bitcoin tiêu thụ lượng lớn năng lượng, gây lo ngại về tác động môi trường. Việc thiếu quy định rõ ràng khiến Bitcoin dễ bị lạm dụng cho các hoạt động phi pháp. Ngoài ra, giá Bitcoin thường xuyên biến động mạnh, gây khó khăn trong việc sử dụng như một đồng tiền thanh toán ổn định.

Dù vậy, Bitcoin vẫn được kỳ vọng sẽ tiếp tục đóng vai trò trung tâm trong hệ sinh thái tiền mã hóa. Sự phát triển của công nghệ và sự chấp nhận ngày càng tăng có thể biến Bitcoin thành nền tảng cho các giải pháp tài chính phi tập trung, đồng thời thay đổi cách chúng ta suy nghĩ về tiền tệ và giá trị.

Tóm lại, Bitcoin không chỉ là một công cụ tài chính mà còn là biểu tượng của sự đổi mới và tự do, góp phần định hình lại cách thế giới vận hành trong tương lai.

3.2. Ethereum: Hợp đồng thông minh và DApps

3.2.1 Ethereum

Nếu cần trả lời câu hỏi "*Ai là người có vai trò và tầm ảnh hưởng lớn nhất sau nhân vật ẩn danh Satoshi Nakamoto của Bitcoin?*", thì câu trả lời chính là **Vitalik Buterin**, một lập trình viên tài năng sinh năm 1994, mang quốc tịch Canada và có gốc Nga. Vào năm 2011, chỉ hai năm sau khi Bitcoin được tạo ra, Vitalik đã chăm chỉ viết bài cho trang web *Bitcoin Magazine,* với mức thù lao 5 Bitcoin cho mỗi bài đăng. Không lâu sau, anh trở thành đồng sáng lập của tạp chí này.

Sự gắn bó với *Bitcoin Magazine* cùng các chuyến du lịch khắp thế giới để học hỏi, gặp gỡ, và trao đổi với các nhà phát triển Bitcoin đã giúp Buterin trở thành một chuyên gia về Bitcoin. Đồng thời, anh cũng sớm nhận ra những hạn chế trong tính năng của Bitcoin. Từ đó, Buterin nhận thấy rằng mình có thể xây dựng một phiên bản blockchain mới với tiềm năng vượt trội hơn bằng cách cải tiến dựa trên Bitcoin.

Năm 2013, Buterin lần đầu tiên giới thiệu dự án Ethereum của mình đến cộng đồng blockchain qua một **tài liệu trắng** (white paper). Tầm nhìn của Buterin dành cho Ethereum là trở thành "**máy tính toàn cầu**" (the World computer) khi hệ thống phi tập trung này hoạt động trên nhiều nút (node) trên toàn thế giới và mọi tính toán hay giao dịch trên đó đều diễn ra trên toàn bộ mạng lưới khổng lồ như một thực thể.

Bản whitepaper đưa ra tầm nhìn và một số khái niệm ban đầu về Ethereum bao gồm các điểm chính:

- Cung cấp một *ngôn ngữ lập trình* **Turing hoàn chỉnh (**Turing complete), ngôn ngữ có khả năng thực hiện bất kỳ phép tính hoặc thuật toán nào nếu có đủ thời gian và tài nguyên. Nói cách khác, ngôn ngữ này có thể mô phỏng mọi chương trình máy tính có thể tưởng tượng được. Ethereum sử dụng ngôn ngữ này để xây dựng "hợp đồng thông minh" (smart contracts) – các chương trình tự thực thi chạy trên blockchain.
- **Thiết lập các giao dịch ngang hàng (peer-to-peer) trong blockchain:** Nền tảng này cho phép tạo ra và triển khai hợp đồng thông minh cùng các ứng dụng phi tập trung (DApps). Bất kỳ ai cũng có thể định nghĩa, tạo ra và trao đổi các loại giá trị trên Ethereum, bao gồm tiền điện tử, cổ phiếu, và nhiều loại tài sản khác.

Ý tưởng của Buterin không hoàn toàn mới; giống như Bitcoin, Ethereum tiếp tục kế thừa các ý tưởng của những người tiên phong blockchain và phát triển chúng trong hệ sinh thái mới. Ví dụ, trước đó Nick Szabo đã từng đề xuất ý tưởng về **hợp đồng thông minh** (smart contract) và quản lý tài sản trên cơ sở dữ liệu phân tán. Ngoài ra, với các **ứng dụng phân tán phi tập trung** (DApps), một bước phát triển của các blockchain trước đó (như Namecoin, Colored Coins và Metacoins, phần lớn là chỉ cố gắng mô phỏng tiền tệ) Buterin và cộng sự muốn hợp nhất và cải tiến tất cả các khái niệm này để làm cho **blockchain có thể lập trình và sử dụng rộng rãi**.

Đồng hành cùng **Vitalik Buterin** trong những năm đầu phát triển Ethereum là những tên tuổi lừng danh, bao gồm **Gavin Wood** (sau này sáng lập Polkadot), **Charles Hoskinson** (sau này sáng lập Cardano), **Anthony Di Iorio** (sáng lập Decentral Inc), và **Joseph Lubin** (sáng lập ConsenSys) …

Ngay sau khi tài liệu trắng được phát hành, Gavin Wood đã xuất bản **tài liệu vàng** (Yellow Paper) – một tài liệu kỹ thuật chuyên sâu với tiêu đề *Ethereum: A Secure Decentralised Generalised Transaction Ledger*.

Trong tài liệu này, Wood không chỉ mô tả chi tiết về Ethereum mà còn giải thích cụ thể về **Máy ảo Ethereum (Ethereum Virtual Machine - EVM)**, cùng với các cơ chế vận hành của hệ thống. Tài liệu vàng đóng vai trò bổ sung cho tài liệu trắng, cung cấp các mô tả kỹ thuật chính xác hơn về cách hệ thống hoạt động dựa trên những ý tưởng đã được giới thiệu trong tài liệu trắng.

Vào tháng 7 và tháng 8 năm 2014, sự kiện bán trước Ethereum cho công chúng (crowdsale) đã được tổ chức, trong đó một số lượng Ether nhất định được bán ra trước khi dự án chính thức khởi chạy. Những sự kiện bán trước như vậy thường được gọi là đợt phát hành token đầu tiên (ICO) hoặc bán token lần đầu (ITS) trong lĩnh vực blockchain.

Sự kiện bán trước này đã rất thành công. Nhóm của Vitalik Buterin đã huy động được 18,4 triệu USD, đảm bảo nguồn lực để phát triển Ethereum. Việc này được thực hiện dưới sự bảo trợ của tổ chức phi lợi nhuận Ethereum Foundation, được thành lập ngay trước sự kiện crowdsale và có trụ sở tại Thụy Sĩ.

Phiên bản thử nghiệm đầu tiên

Tháng 5 năm 2015, phiên bản thử nghiệm đầu tiên của Ethereum đã hoạt động trực tuyến. Được biết đến với tên gọi "Olympic," phiên bản này cho phép người dùng kiểm tra khả năng chịu tải và tính bảo mật của hệ thống. Người tham gia còn nhận được các phần thưởng khuyến khích nếu phát hiện ra các lỗi hoặc vấn đề nghiêm trọng.

Phiên bản chính thức: Frontier

Vào ngày 30 tháng 7 năm 2015, phiên bản chính thức đầu tiên của Ethereum được phát hành với tên gọi "Frontier." Đây là bước khởi đầu chính thức của mạng lưới Ethereum, mở ra khả năng xây dựng và triển khai các ứng dụng phi tập trung (DApps) thông qua việc sử dụng hợp đồng thông minh.

Từ đó, Ethereum tiếp tục phát triển qua nhiều giai đoạn nâng cấp lớn, bao gồm:

Homestead (2016): Tăng cường tính ổn định và cải thiện các tính năng bảo mật.

Metropolis (Byzantium và Constantinople, 2017-2019): Cung cấp các tính năng mới như zk-SNARKs và cải thiện hiệu suất mạng lưới.

Serenity (Ethereum 2.0, 2022): Thay đổi hoàn toàn từ cơ chế PoW sang PoS, giảm tiêu thụ năng lượng và cải thiện khả năng mở rộng.

Ethereum, sau khi chuyển đổi thành công sang POS, tiếp tục hướng đến mục tiêu cải thiện hiệu suất, khả năng mở rộng, và tính bền vững với các giai đoạn phát triển tiếp theo như:

Sharding: Giúp phân mảnh dữ liệu để xử lý hiệu quả hơn và tăng dung lượng mạng lưới.

Layer 2 Solutions: Các giải pháp mở rộng như Optimism và zk-Rollups giúp giảm tải cho mạng chính Ethereum.

Chúng ta sẽ tìm hiểu các nội dung mở rộng Ethereum và những hướng phát triển trong tương lai trong các chương tiếp theo. Trước khi đến với phần tiếp, chúng ta tiếp tục làm quen với một số thuật ngữ cơ bản:

Máy trạng thái (State Machine)

Ethereum tự xem mình như một máy trạng thái dựa trên giao dịch, bắt đầu với trạng thái ban đầu (genesis state) và được chuyển đổi thành trạng thái cuối cùng thông qua các giao dịch. Trạng thái cuối cùng này không phải là trạng thái mà hệ thống kết thúc, mà luôn là trạng thái cập nhật nhất của nền tảng (xem thêm ở yellow paper)

Bitcoin cũng có thể được mô tả như một máy trạng thái, với trạng thái được đại diện bởi tập hợp toàn cầu của tất cả các đầu ra giao dịch chưa được chi tiêu (UTXOs). Trạng thái của Bitcoin cũng bị thay đổi bởi các giao dịch trên mạng.

Để bắt đầu các giao dịch này, người tham gia phải sử dụng khóa của họ để truy cập vào một hoặc nhiều UTXOs và chuyển đổi chúng thành các UTXOs mới. Như ở các phần trên về Bitcoin đã trình bày, với Bitcoin, người dùng không có số dư tài khoản liên kết với địa chỉ của

họ. Họ chỉ quản lý các khóa trong ví của mình để có thể mở khóa các UTXOs được gán cho họ.

Vì vậy, trong khi trạng thái của Bitcoin khá trừu tượng, Ethereum xem trạng thái như một khái niệm cơ bản mà toàn bộ dự án của nó được xây dựng. Khác với Bitcoin, các tài khoản là một cấu trúc cơ bản quan trọng trong mạng Ethereum. Các tài khoản này đại diện cho địa chỉ của những người tham gia trong mạng, nhưng có thể chứa nhiều thông tin hơn.

Ethereum và tính chất Turing hoàn chỉnh

Ngay khi bạn bắt đầu tìm hiểu về Ethereum, bạn sẽ lập tức gặp thuật ngữ "Turing hoàn chỉnh" (**Turing complete**). Người ta thường nói rằng Ethereum, không giống như Bitcoin, là Turing hoàn chỉnh. Vậy điều này thực sự có ý nghĩa gì?

Thuật ngữ này liên quan đến nhà toán học người Anh **Alan Turing**, người được xem là cha đẻ của ngành khoa học máy tính. Vào năm 1936, ông đã tạo ra một mô hình toán học của một chiếc máy tính, bao gồm một máy trạng thái (state machine) thao tác với các ký hiệu bằng cách đọc và ghi chúng lên bộ nhớ tuần tự (giống như một cuộn băng giấy vô tận). Với mô hình này, Turing đã cung cấp cơ sở toán học để trả lời (theo hướng tiêu cực) các câu hỏi về khả năng tính toán phổ quát, tức là liệu mọi vấn đề đều có thể giải quyết được hay không. Ông chứng minh rằng có những lớp vấn đề không thể tính toán được.

Cụ thể, Turing đã chứng minh rằng **bài toán dừng (halting problem)** - liệu có thể xác định được, với một chương trình và một đầu vào bất kỳ, rằng chương trình đó sẽ kết thúc hay tiếp tục chạy mãi - là không thể giải quyết.

Alan Turing cũng định nghĩa một hệ thống là **Turing hoàn chỉnh** nếu nó có thể được sử dụng để mô phỏng bất kỳ máy Turing nào. Một hệ thống như vậy được gọi là **Máy Turing Phổ quát (Universal Turing Machine - UTM)**.

Khả năng của Ethereum trong việc thực thi một chương trình lưu trữ, trong một máy trạng thái gọi là **Ethereum Virtual Machine (EVM)**, đồng thời đọc và ghi dữ liệu vào bộ nhớ, biến nó thành một hệ thống Turing hoàn chỉnh và do đó là một UTM. Ethereum có thể tính toán bất kỳ thuật toán nào mà bất kỳ máy Turing nào có thể thực hiện, trong giới hạn của bộ nhớ hữu hạn.

Đột phá của Ethereum nằm ở việc kết hợp kiến trúc máy tính đa năng của một chiếc máy tính lưu trữ chương trình với một blockchain phi tập trung, từ đó tạo ra một "máy tính thế giới" phân tán với trạng thái duy nhất (singleton). Các chương trình Ethereum chạy "ở mọi nơi" nhưng tạo ra một trạng thái chung được bảo vệ bởi các quy tắc đồng thuận.

Turing hoàn chỉnh như một “Tính năng”

Khi nghe rằng Ethereum là Turing hoàn chỉnh, bạn có thể kết luận rằng đây là một tính năng mà các hệ thống Turing không hoàn chỉnh còn thiếu. Nhưng thực ra, điều này hoàn toàn ngược lại. Turing hoàn chỉnh rất dễ đạt được; thực tế, máy trạng thái Turing hoàn chỉnh đơn giản nhất được biết đến chỉ có **4 trạng thái và sử dụng 6 ký hiệu**, với định nghĩa trạng thái chỉ dài **22 hướng dẫn**.

Đôi khi, thậm chí có những hệ thống được phát hiện là **"Turing hoàn chỉnh một cách tình cờ"**. Một danh sách thú vị về các hệ thống như vậy có thể được tìm thấy tại: http://beza1e1.tuxen.de/articles/accidentally_turing_complete.html

Tuy nhiên, Turing hoàn chỉnh lại rất nguy hiểm, đặc biệt trong các hệ thống truy cập mở như blockchain công khai, bởi vì vấn đề **halting problem** đã được đề cập ở phần trước.

Ví dụ, các máy in hiện đại là Turing hoàn chỉnh và có thể bị đưa vào trạng thái "đóng băng" bởi các tập tin in phức tạp.

Việc Ethereum là Turing hoàn chỉnh có nghĩa là bất kỳ chương trình nào với bất kỳ độ phức tạp nào đều có thể được tính toán bởi Ethereum. Nhưng sự linh hoạt này mang lại những vấn đề nan giải về bảo mật và quản lý tài nguyên. Một chiếc máy in không phản hồi có thể được tắt đi và bật lại. Nhưng điều đó là không thể đối với một blockchain công khai.

Hệ quả của tính Turing hoàn chỉnh

Turing đã chứng minh rằng bạn không thể dự đoán liệu một chương trình có kết thúc hay không bằng cách mô phỏng nó trên một máy tính. Nói cách đơn giản, chúng ta không thể dự đoán được hành trình của một chương trình mà không thực sự chạy nó. Các hệ thống Turing hoàn chỉnh có thể chạy trong "vòng lặp vô hạn" (**infinite loops**) – một thuật ngữ được sử dụng (theo cách đơn giản hóa) để mô tả một chương trình không bao giờ kết thúc.

Việc tạo ra một chương trình chạy mãi mãi là điều rất dễ dàng. Tuy nhiên, những vòng lặp vô hạn không mong muốn có thể xuất hiện mà không có dấu hiệu báo trước, do các tương tác phức tạp giữa điều kiện ban đầu và mã chương trình. Trong Ethereum, điều này đặt ra một thách thức lớn: mỗi nút (client) tham gia vào mạng phải xác minh mọi giao dịch, bao gồm cả việc chạy các hợp đồng thông minh mà giao dịch đó gọi.

Tuy nhiên, như Turing đã chứng minh, Ethereum không thể dự đoán trước liệu một hợp đồng thông minh có kết thúc hay không, hoặc sẽ chạy trong bao lâu, mà không thực sự chạy nó (và có thể chạy mãi mãi).

Cho dù do vô tình hay cố ý, một hợp đồng thông minh có thể được tạo ra để chạy mãi mãi khi một nút cố gắng xác minh nó. Đây thực chất là một hình thức **tấn công từ chối dịch vụ (DoS)**. Ngoài ra, giữa một chương trình chỉ mất vài mili giây để xác minh và một chương trình chạy mãi mãi, còn tồn tại một loạt các chương trình tiêu tốn tài nguyên nặng nề, làm tăng bộ nhớ, quá tải CPU, và lãng phí tài nguyên.

Trong một "máy tính thế giới," một chương trình lạm dụng tài nguyên chính là lạm dụng tài nguyên của toàn thế giới. Vậy làm thế nào Ethereum có thể hạn chế tài nguyên mà một hợp đồng thông minh sử dụng nếu nó không thể dự đoán trước mức sử dụng tài nguyên?

Cơ chế giới hạn tài nguyên: Gas

Để giải quyết vấn đề này, Ethereum đã giới thiệu một cơ chế đo lường tài nguyên gọi là **gas**. Khi EVM thực thi một hợp đồng thông minh, nó cẩn thận tính toán từng lệnh (bao gồm tính toán, truy cập dữ liệu, v.v.).

Mỗi lệnh có một chi phí cố định tính bằng đơn vị gas. Khi một giao dịch kích hoạt việc thực thi hợp đồng thông minh, nó phải đi kèm với một lượng gas, đặt ra giới hạn tối đa về tài nguyên mà hợp đồng thông minh đó có thể tiêu thụ.

EVM sẽ dừng việc thực thi nếu lượng gas tiêu thụ vượt quá lượng gas khả dụng trong giao dịch. **Gas** chính là cơ chế mà Ethereum sử dụng để cho phép tính toán Turing hoàn chỉnh trong khi vẫn giới hạn tài nguyên mà bất kỳ chương trình nào có thể sử dụng.

Làm thế nào để có Gas?

Câu hỏi tiếp theo là, làm thế nào để người dùng có gas để chi trả cho việc tính toán trên "máy tính thế giới" Ethereum? Bạn sẽ không tìm thấy gas trên bất kỳ sàn giao dịch nào. Gas chỉ có thể được mua như một phần của giao dịch và chỉ có thể được mua bằng **ether**.

Ether cần được gửi kèm với giao dịch, và cần được chỉ định rõ ràng để mua gas cùng với một mức giá gas chấp nhận được. Cũng giống như giá nhiên liệu tại trạm xăng, giá gas không cố định.

Gas được mua để thực hiện giao dịch, quá trình tính toán được thực hiện, và bất kỳ lượng gas nào không sử dụng sẽ được hoàn trả lại cho người gửi giao dịch.

3.2.2. Hợp đồng thông minh (Smart Contract)

Ngay trong tiêu đề của tài liệu trắng về Ethereum, Vitalik Buterin đã đề cập đến Hợp đồng thông minh (Smart contract) thế hệ mới. Tài liệu đã mô tả giao thức Bitcoin như một **phiên bản yếu** của khái niệm hợp đồng thông minh mà Nick Szabo đã định nghĩa. Theo đó, Buterin đã đề xuất một phiên bản *thế hệ mới* mạnh mẽ hơn dựa trên ngôn ngữ lập trình **Solidity**, vốn là ngôn ngữ Turing hoàn chỉnh (*Turing Complete*). Kể từ đó, nhiều loại tiền mã hóa khác đã hỗ trợ các ngôn ngữ lập trình cho phép phát triển các hợp đồng thông minh phức tạp hơn giữa các bên không tin cậy lẫn nhau.

Hợp đồng thông minh là gì?

Trước hết, hãy nhìn lại khái niệm về “hợp đồng.” Chúng ta có thể dễ dàng nhận thấy trong cuộc sống hàng ngày, có nhiều loại hợp đồng như hợp đồng thuê nhà, hợp đồng vay tiền, hợp đồng thuê xe, hay hợp đồng thuê khoán chuyên môn… Trong hợp đồng, thường sẽ có các nội dung và điều khoản để các bên thực hiện. Một hợp đồng hiệu quả sẽ mô tả chi tiết các yêu cầu chính thức, trách nhiệm của mỗi bên, thời điểm và cách thức thực hiện các điều khoản, cũng như hậu quả nếu các quy tắc này không được tuân thủ. Do đó, hợp đồng là một tài liệu đáng tin cậy, đảm bảo rằng các bên liên quan thực hiện đúng như kế hoạch đã định.

Hợp đồng thông minh có nhiều điểm tương đồng với hợp đồng truyền thống, nhưng được triển khai thông qua mã máy tính. Một khi đã được tạo trên mạng blockchain phi tập trung, hợp đồng thông minh không thể thay đổi. Khi các điều kiện được đáp ứng, hợp đồng thông minh sẽ tự động thực thi mà không cần sự can thiệp của bên thứ ba. Trong các tài liệu của Ethereum, các tác giả nêu rõ rằng, trong bối cảnh Ethereum, thuật ngữ này thực chất hơi sai lệch. Bởi vì các hợp đồng thông minh trên Ethereum không thực sự "thông minh" và cũng không phải là các hợp đồng pháp lý. Tuy nhiên, thuật ngữ này vẫn được sử dụng rộng rãi để chỉ các chương trình máy tính bất biến, hoạt động một cách xác định trong bối cảnh của

Ethereum Virtual Machine (EVM), như một phần của giao thức mạng Ethereum, tức là trên máy tính toàn cầu phi tập trung Ethereum.

Vì blockchain có tính phi tập trung, không thể thay đổi và minh bạch, mọi người trong mạng lưới đều có thể công khai xác minh kết quả giao dịch của hợp đồng thông minh.

Nick Szabo là người đầu tiên mô tả khái niệm hợp đồng thông minh. Năm 1997, ông đã xuất bản bài viết **"The Idea of Smart Contracts"** (Ý tưởng về hợp đồng thông minh). Ông hình dung việc *chuyển đổi hợp đồng thành mã lập trình để tạo ra các hợp đồng tự thực thi mà không cần sự tin tưởng giữa các bên.*

Để minh họa khái niệm của mình, Nick Szabo sử dụng máy bán hàng tự động làm ví dụ về cách hợp đồng thông minh hoạt động. Khi bạn đưa số tiền chính xác vào máy, bạn sẽ nhận được sản phẩm mong muốn. Các hướng dẫn lập trình bên trong máy bán hàng đảm bảo rằng hợp đồng sẽ được thực hiện như dự định.

Sự khác biệt giữa Bitcoin và Ethereum về Smart Contract

Bitcoin: Chỉ hỗ trợ một số chức năng hợp đồng thông minh cơ bản (như giao dịch có điều kiện), giới hạn trong việc lập trình và khả năng mở rộng.

Ethereum: Đưa khái niệm hợp đồng thông minh lên một tầm cao mới với khả năng lập trình Turing hoàn chỉnh, cho phép tạo ra các ứng dụng phi tập trung (**DApps**) và các hệ sinh thái tài chính phi tập trung (**DeFi**) phong phú. Bất kỳ ai cũng có thể tạo hợp đồng thông minh trên blockchain Ethereum. Mã nguồn của hợp đồng thông minh minh bạch và có thể được công khai xác minh. Mọi người đều có thể xem logic thực thi của các hợp đồng thông minh được xây dựng như thế nào.

Cấu trúc của Smart Contract

Smart contract trong Ethereum là các chương trình máy tính được viết bằng mã nguồn (code) và được triển khai trên blockchain Ethereum. Mỗi smart contract có ba thành phần chính:

- **Hàm (Functions):** Hàm là các phần mã thực hiện các hành động cụ thể, chẳng hạn như thay đổi trạng thái của contract, chuyển tiền từ người này sang người khác, hoặc kiểm tra điều kiện nhất định. Các hàm có thể được gọi trực tiếp từ bên ngoài hợp đồng hoặc được kích hoạt bởi các sự kiện khác trong hệ thống. Ví dụ, một smart contract có thể có hàm "transfer" để chuyển tiền giữa hai tài khoản.
- **Trạng thái (State):** Trạng thái là các biến lưu trữ thông tin về dữ liệu của contract. Trạng thái này có thể được thay đổi bởi các hàm trong smart contract. Ví dụ, nếu smart contract là một hợp đồng tài chính, trạng thái có thể là số dư tài khoản của người dùng hoặc số lượng token mà một người sở hữu.
- **Sự kiện (Events):** Sự kiện là các thông báo hoặc tín hiệu được phát ra từ smart contract khi có một hành động hoặc điều kiện nào đó xảy ra. Các sự kiện giúp người

dùng hoặc các ứng dụng khác có thể theo dõi hoạt động của hợp đồng. Ví dụ, khi một giao dịch thành công, smart contract có thể phát ra một sự kiện để thông báo rằng giao dịch đã được thực hiện.

Ethereum Virtual Machine (EVM)

Ethereum Virtual Machine (EVM) là môi trường thực thi của smart contract trên Ethereum. EVM giống như một máy tính ảo có thể thực hiện các chương trình được viết bằng mã bytecode trong Ethereum. Khi một smart contract được triển khai trên blockchain, mã bytecode của nó được tải lên EVM để thực thi. EVM chịu trách nhiệm chạy các smart contract, xử lý các giao dịch và cập nhật trạng thái của blockchain.

EVM có khả năng tương tác với các dữ liệu và các hợp đồng khác trên blockchain Ethereum, đồng thời đảm bảo tính bảo mật và sự minh bạch của các giao dịch. Mỗi lần một smart contract được thực thi, EVM sẽ tính toán các chi phí sử dụng tài nguyên hệ thống, bao gồm gas, và xác nhận rằng hợp đồng hoạt động đúng như yêu cầu.

Quy trình thực thi Smart Contract

Khi một người dùng muốn tương tác với smart contract trong Ethereum, họ sẽ gửi một giao dịch đến mạng lưới Ethereum. Giao dịch này có thể là yêu cầu thực thi một hàm trong smart contract, chẳng hạn như chuyển một lượng ether từ người này sang người khác. Sau khi giao dịch được phát ra, quá trình thực thi sẽ diễn ra theo các bước sau:

1. **Gửi giao dịch:** Người dùng tạo và gửi giao dịch đến mạng Ethereum thông qua ví điện tử của họ (ví dụ: MetaMask, MyEtherWallet).
2. **Ký duyệt giao dịch:** Giao dịch sẽ được ký bởi người dùng bằng khóa riêng tư của họ để xác nhận tính hợp pháp của giao dịch.
3. **Phát giao dịch trên mạng lưới:** Giao dịch được phát tán trên mạng lưới Ethereum và các nút (nodes) trong mạng sẽ bắt đầu xử lý giao dịch.
4. **Chạy hợp đồng trong EVM:** Khi giao dịch liên quan đến một smart contract, EVM sẽ tìm smart contract tương ứng, đọc mã bytecode của nó, và thực thi các hàm mà người dùng yêu cầu. Các thay đổi về trạng thái (như chuyển tiền) sẽ được ghi lại trong block mới của blockchain.

5. **Chi phí gas:** Để thực thi các hàm trong smart contract, người dùng phải trả chi phí gas, tương đương với tài nguyên hệ thống được tiêu thụ. Nếu gas không đủ, quá trình thực thi sẽ dừng lại và giao dịch sẽ bị thất bại.
6. **Cập nhật trạng thái và tạo block mới:** Khi smart contract thực hiện các hành động thành công, như chuyển tiền, EVM sẽ cập nhật trạng thái của blockchain và tạo ra một block mới chứa thông tin về giao dịch đó.
7. **Phát lại sự kiện:** Nếu smart contract phát ra sự kiện, các ứng dụng khác có thể lắng nghe và xử lý thông tin từ sự kiện đó. Ví dụ, một DApp có thể cập nhật giao diện người dùng của nó dựa trên các sự kiện mà smart contract phát ra.

Mối quan hệ giữa Smart Contract và Gas

Mỗi khi một smart contract được gọi và thực thi, chi phí gas sẽ được tính toán. Gas là đơn vị đo lường tài nguyên mà một giao dịch tiêu thụ khi thực hiện trên blockchain Ethereum. Mỗi thao tác trong smart contract, từ việc tính toán đến việc đọc và ghi dữ liệu, đều yêu cầu một lượng gas nhất định.

Gas có hai yếu tố chính:

- **Gas Limit:** Là mức tối đa lượng gas mà người dùng sẵn sàng chi trả cho giao dịch. Nếu một smart contract yêu cầu nhiều hơn mức gas limit này, giao dịch sẽ bị hủy.
- **Gas Price:** Là giá trị mà người dùng sẵn sàng trả cho mỗi đơn vị gas. Gas price thường được tính bằng đơn vị gwei (1 gwei = 10^-9 ether).

Công thức chi phí giao dịch sẽ là:
Chi phí = Gas Limit × Gas Price
Ví dụ, nếu gas limit là 50,000 và gas price là 20 gwei, chi phí giao dịch sẽ là 1,000,000 gwei (hoặc 0.001 ether).

Như đã trình bày ở trên, Gas giúp bảo vệ mạng Ethereum khỏi các smart contract không được tối ưu hoặc chạy vô tận. Nếu một smart contract không được tối ưu hoặc không có điều kiện dừng hợp lý, gas limit sẽ ngừng thực thi, tránh việc chiếm dụng tài nguyên hệ thống.

Smart Contract "Hello World"

Dưới đây là một ví dụ cơ bản về "Hello World" trong Solidity:

// SPDX-License-Identifier: MIT

```
pragma solidity ^0.8.18;
```

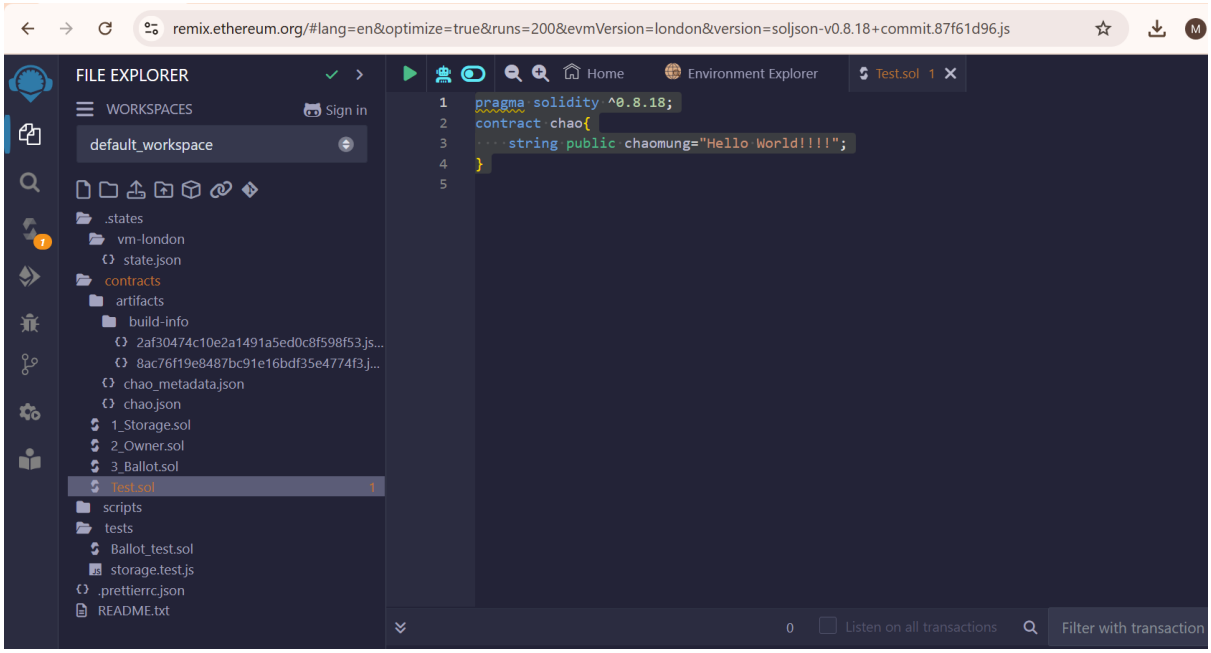
```
contract chao{
    string public chaomung="Hello World!!!!";
}
```

Chi tiết từng phần trong contract:

1. **pragma solidity**: Định nghĩa phiên bản Solidity sẽ được sử dụng. Ví dụ: ^0.8.0 đảm bảo code chạy trên các phiên bản từ 0.8.0 trở lên.
2. **string public chaomung**: Biến message lưu trữ thông điệp "Hello World!!!!" và có thể được truy cập công khai.

Quy trình triển khai và thử nghiệm trên Remix

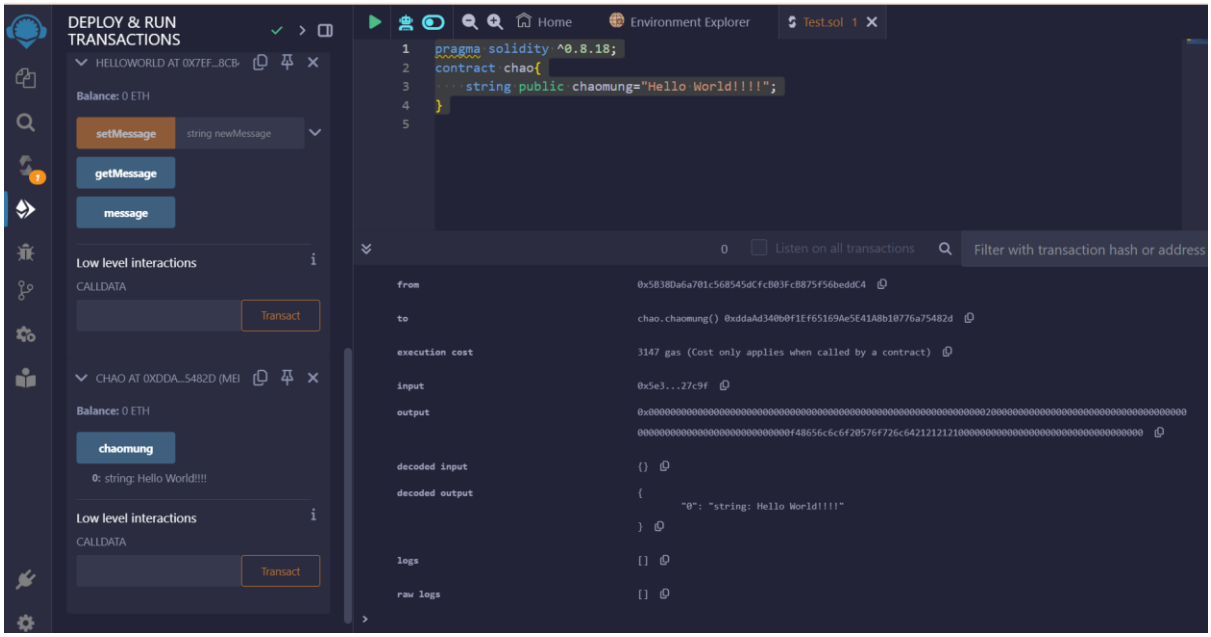
1. **Mở Remix IDE**:
    - Truy cập Remix IDE tại địa chỉ https://remix.ethereum.org/
    - Tạo một file mới (ví dụ: Test.sol).
    - Dán đoạn mã trên vào file.



2. **Biên dịch (Compile)**:
    - Chọn tab "Compiler" trong Remix.
    - Chọn phiên bản Solidity phù hợp và nhấn "Compile Test.sol".
3. **Triển khai (Deploy)**:

- Chuyển sang tab "Deploy & Run Transactions".
- Chọn môi trường là "JavaScript VM (London)" để thử nghiệm trên mạng giả lập.
- Nhấn nút "Deploy" để triển khai contract.

4. **Tương tác**:
   - Sau khi triển khai, bạn sẽ thấy các nút và trường liên quan đến contract trong Remix.
   - Nhấn Chaomung để đọc thông điệp mặc định ("Hello World!!!").



3.2.3. Các ứng dụng phi tập trung (DApps)

Trong phần này chúng ta sẽ khám phá thế giới của các ứng dụng phi tập trung, hay còn gọi là DApps. Từ những ngày đầu của Ethereum, tầm nhìn của các nhà sáng lập đã vượt xa khái niệm "hợp đồng thông minh": đó là tái tạo lại web và tạo ra một thế giới mới của các DApps, được gọi một cách phù hợp là web3. Hợp đồng thông minh là cách để phi tập trung hóa logic điều khiển và các chức năng thanh toán của ứng dụng. DApps trong web3 còn đi xa hơn bằng cách phi tập trung hóa tất cả các khía cạnh khác của một ứng dụng: lưu trữ, nhắn tin, đặt tên, v.v

DApp là gì?

Một DApp là ứng dụng được xây dựng chủ yếu hoặc hoàn toàn theo cách phi tập trung. Hãy xem xét các khía cạnh của một ứng dụng có thể được phi tập trung hóa:

- **Phần mềm backend (logic ứng dụng)**

- **Phần mềm frontend**
- **Lưu trữ dữ liệu**
- **Giao tiếp tin nhắn**
- **Giải quyết tên miền**

Mỗi khía cạnh này có thể được phát triển theo hướng tập trung hoặc phi tập trung. Ví dụ:

- **Frontend**: Có thể là một ứng dụng web chạy trên máy chủ tập trung hoặc một ứng dụng di động chạy trên thiết bị người dùng.
- **Backend và lưu trữ**: Có thể được đặt trên các máy chủ riêng và cơ sở dữ liệu độc quyền hoặc sử dụng hợp đồng thông minh và lưu trữ P2P.

Lợi ích của việc xây dựng một DApp

So với kiến trúc tập trung thông thường, DApps mang lại nhiều lợi ích vượt trội:

1. **Khả năng chống lỗi**
    - Logic kinh doanh được kiểm soát bởi hợp đồng thông minh, backend của DApp hoàn toàn phân tán và quản lý trên nền tảng blockchain.
    - DApp không có thời gian ngừng hoạt động (downtime) và sẽ tiếp tục khả dụng miễn là nền tảng vẫn hoạt động.
2. **Tính minh bạch**
    - Bản chất của DApp trên chuỗi khối cho phép mọi người kiểm tra mã nguồn để hiểu rõ hơn về cách hoạt động.
    - Mọi tương tác với DApp được lưu giữ vĩnh viễn trên blockchain.
3. **Khả năng chống kiểm duyệt**
    - Chỉ cần người dùng truy cập được một node Ethereum (hoặc tự chạy node nếu cần), họ luôn có thể tương tác với DApp mà không bị cản trở bởi bất kỳ cơ quan tập trung nào.
    - Ngay cả chủ sở hữu hợp đồng thông minh cũng không thể thay đổi mã sau khi nó được triển khai lên mạng.

Thực trạng và tương lai của DApps

Hiện tại, trong hệ sinh thái Ethereum, rất ít ứng dụng **thực sự phi tập trung** — hầu hết vẫn dựa vào các dịch vụ và máy chủ tập trung ở một phần nào đó. Trong tương lai, chúng ta hy vọng mọi thành phần của DApp có thể hoạt động hoàn toàn phi tập trung.

Backend (Hợp đồng thông minh)

- Trong một DApp, hợp đồng thông minh được sử dụng để lưu trữ logic kinh doanh (mã chương trình) và trạng thái liên quan đến ứng dụng.
- Hợp đồng thông minh có thể thay thế **backend server-side** trong ứng dụng truyền thống. Tuy nhiên, cần lưu ý:
    1. Mọi tính toán trong hợp đồng thông minh rất tốn kém, vì vậy cần giữ cho nó tối thiểu.
    2. Phải xác định rõ các phần của ứng dụng cần nền tảng thực thi phi tập trung và đáng tin cậy.

Thiết kế kiến trúc hợp đồng thông minh

1. **Hạn chế chỉnh sửa mã**
    - Sau khi triển khai, mã hợp đồng thông minh không thể thay đổi. Nó chỉ có thể bị xóa nếu được lập trình với lệnh **SELFDESTRUCT**, nhưng ngoài việc xóa hoàn toàn, không có cách nào để chỉnh sửa mã.
2. **Kích thước DApp**
    - Một hợp đồng thông minh lớn có thể tiêu tốn nhiều gas để triển khai và sử dụng. Vì vậy, một số ứng dụng có thể lựa chọn tính toán ngoài chuỗi và sử dụng nguồn dữ liệu bên ngoài.
    - Tuy nhiên, nếu logic kinh doanh cốt lõi của DApp phụ thuộc vào dữ liệu bên ngoài (ví dụ: từ máy chủ tập trung), người dùng sẽ phải tin tưởng vào các nguồn tài nguyên này.

Tóm lại, việc xây dựng và triển khai một DApp cần chú ý đến tính phi tập trung, hiệu quả gas, và tính toàn vẹn của dữ liệu. Mặc dù có những thách thức, nhưng DApps đang mở ra một kỷ nguyên mới của các ứng dụng web phi tập trung và minh bạch.

3.3. Thế hệ thứ ba: Cardano – Xây dựng từ nghiên cứu học thuật

3.3.1. Giới thiệu về Cardano

Cardano được coi là một trong những blockchain tiên tiến và độc đáo nhất hiện nay, nổi bật với cách tiếp cận dựa trên nghiên cứu học thuật nghiêm ngặt trước khi triển khai công nghệ. Được thiết kế để khắc phục những hạn chế của các blockchain thế hệ trước, Cardano đặt trọng tâm vào tính bền vững, tính minh bạch và sự đổi mới khoa học. Với sự kết hợp giữa nghiên cứu lý thuyết và áp dụng thực tế, dự án này đã định hình lại cách phát triển blockchain một cách có hệ thống và đáng tin cậy. Bây giờ, chúng ta sẽ cùng tìm hiểu về lịch sử ra đời và quá trình phát triển của blockchain Cardano.

3.3.1.1. Bối Cảnh Ra Đời

Vào năm 2015, Charles Hoskinson – một trong những người đồng sáng lập Ethereum – đã quyết định khởi động một blockchain mới. Sau khi rời Ethereum do một số bất đồng về hướng phát triển, Hoskinson nhận thấy cơ hội tạo ra một nền tảng blockchain được xây dựng bởi khoa học và nghiên cứu cẩn thận.

Cardano được thiết kế như một blockchain thế hệ thứ ba, nhằm khắc phục những vấn đề của Bitcoin (thế hệ thứ nhất) và Ethereum (thế hệ thứ hai). Mục tiêu chính là đạt được tính bền vững, khả năng mở rộng, và tính phân quyền cao trong khi vẫn bảo đảm tính bảo mật và minh bạch.

3.3.1.2. Giai Đoạn Khởi Động (2015-2017)

Cardano được phát triển, thúc đẩy bởi ba tổ chức chính:

- **IOG (Input Output Global):** Input Output là một công ty nghiên cứu và kỹ thuật và studio mạo hiểm xây dựng các sản phẩm blockchain và Web3 để trao quyền cho mọi người, ở mọi nơi.

  Được thành lập bởi Charles Hoskinson và Jeremy Wood, Input Output là một trong ba đơn vị tiên phong đằng sau Cardano, ban đầu được ký hợp đồng thiết kế, xây dựng và giúp duy trì nền tảng Cardano. Là một công ty hoàn toàn phi tập trung, Input Output bao gồm các nhóm năng động, sáng tạo - có trụ sở trên toàn thế giới, cùng nhau cam kết đổi mới thông qua việc cung cấp các tiêu chuẩn cao nhất về kỹ thuật phần mềm dựa trên khoa học được đánh giá ngang hàng nghiêm ngặt.

  Input Output là công ty hàng đầu trong việc xây dựng các hệ thống máy tính phân tán và các giải pháp công nghệ phi tập trung. Công ty tiếp tục nghiên cứu và xây dựng các mô hình và sản phẩm mới trong lĩnh vực công nghệ sổ cái phân tán và kiến trúc của Web3. Input Output cam kết tuân thủ các nguyên tắc nguồn mở và kinh doanh có đạo đức, có mục đích, tạo ra công nghệ mang lại lợi ích cho nhiều người chứ không phải cho số ít. Giống như Cardano Foundation và EMURGO, thúc đẩy giáo dục blockchain là cốt lõi trong triết lý của Input Output. IO Research tập trung vào việc thúc đẩy nghiên cứu học thuật về blockchain, được hỗ trợ bởi một nhóm các nhà giáo dục, đối tác học thuật và các khóa học được phát triển đặc biệt.

- **The Cardano Foundation:** Cardano Foundation là một tổ chức phi lợi nhuận độc lập có trụ sở tại Thụy Sĩ. Quỹ có nhiệm vụ thúc đẩy cơ sở hạ tầng kỹ thuật số công cộng Cardano và hoạt động để neo nó như một tiện ích cho các hệ thống tài chính và xã hội, do đó trao quyền cho các kiến trúc sư kỹ thuật số của tương lai.

  Quỹ tạo điều kiện cho sự tiến bộ của Cardano trên toàn thế giới trong các ứng dụng doanh nghiệp. Quỹ phát triển các công cụ cơ sở hạ tầng—bao gồm cả những nơi có thể không có trường hợp sử dụng thương mại ngay lập tức—cộng với việc tăng cường khả năng phục hồi hoạt động và thúc đẩy sự đa dạng của các trường hợp sử dụng trên cơ sở hạ tầng cũng như phát triển quản trị lành mạnh và đại diện.

  Một phần quan trọng khác trong sứ mệnh của Cardano Foundation là tương tác và hỗ trợ cộng đồng Cardano. Quỹ hỗ trợ phát triển các công cụ mà cộng đồng có thể sử dụng để tận dụng Cardano để giải quyết các vấn đề theo những cách mới.

- **Emurgo:** EMURGO là một công ty công nghệ blockchain và là đơn vị sáng lập của blockchain Cardano, cung cấp các sản phẩm và dịch vụ để thúc đẩy việc áp dụng hệ sinh thái Web3 của Cardano. Được thành lập vào năm 2015 tại Nhật Bản, sứ mệnh của EMURGO là tạo điều kiện cho việc áp dụng thương mại thông qua quan hệ đối tác năng động với các thành viên hệ sinh thái hiện tại và sự tích hợp liền mạch của những người mới tham gia.

Bằng cách ưu tiên đầu tư, cung cấp giáo dục liên tục và cung cấp các dịch vụ cơ sở hạ tầng, EMURGO hướng đến mục tiêu mở khóa toàn bộ tiềm năng của hệ sinh thái Cardano.

Năm 2017, Cardano chính thức ra mắt với việc phát hành token ADA, tiền mã hóa chính thức của nền tảng. ADA được đặt tên theo Ada Lovelace, người được coi là nhà lập trình viên máy tính đầu tiên trên thế giới.

Blockchain Cardano đã được phát triển với giao thức đồng thuận Ouroboros, giao thức đầu tiên trên thế giới được chứng minh bằng phương pháp toán học, nhấn mạnh vào khả năng mở rộng và bảo mật.

3.3.1.3. Lộ trình phát triển của Cardano

Lộ trình phát triển của Cardano đã được chia thành năm kỷ nguyên, mỗi kỷ nguyên tập trung vào một bộ tính năng khác nhau:

- Byron tập trung vào việc thiết lập một nền tảng.
- Shelley tập trung vào phân quyền, phi tập trung.
- Goguen là tất cả về các hợp đồng thông minh.
- Basho là động lực để đạt được khả năng mở rộng thực sự.
- Voltaire dựa trên việc thực hiện quản trị phi tập trung.

Mỗi thời đại được xây dựng xung quanh một tập hợp các tính năng được triển khai và cải thiện qua nhiều bản phát hành mã. Mặc dù công việc cho mỗi luồng phát triển này được phân phối theo thứ tự, nhưng nó thường được thực hiện đồng thời, với nghiên cứu, tạo mẫu và phát triển xảy ra đồng thời cùng một lúc.

Hình 3-9: Các kỷ nguyên phát triển của Cardano

- **Byron (Đặt Nền Tảng)**

Giai đoạn Byron, ra mắt vào năm 2017, đánh dấu sự khởi đầu của Cardano với các tính năng cơ bản. Người dùng có thể giao dịch ADA thông qua ví Daedalus (phiên bản ví đầy đủ) hoặc Yoroi (phiên bản ví nhẹ).

Giai đoạn này tập trung vào việc xây dựng cơ sở hạ tầng blockchain và giới thiệu giao thức Ouroboros, đảm bảo tính bảo mật và khả năng hoạt động bền vững. Byron cũng đặt nền móng cho sự phát triển của mạng lưới bằng cách tạo ra một cộng đồng người dùng ADA toàn cầu.

- **Shelley (Phân Quyền)**

Giai đoạn Shelley, ra mắt vào năm 2020, đánh dấu bước chuyển từ hệ thống tập trung sang phân quyền. Một trong những cải tiến lớn nhất là việc giới thiệu cơ chế staking và các nhóm cổ phần (stake pools). Người dùng Cardano có thể tham gia vào mạng lưới bằng cách ủy quyền cổ phần của mình cho các nhóm hoặc tự vận hành nhóm cổ phần riêng.

Shelley đã chứng minh khả năng hoạt động mạnh mẽ của Cardano với hàng ngàn nhóm cổ phần được thiết lập, giúp gia tăng sự phân quyền và bảo mật của mạng lưới. Giai đoạn này cũng cải thiện hiệu suất và sự ổn định của hệ thống.

- **Goguen (Hợp Đồng Thông Minh)**

Giai đoạn Goguen, ra mắt vào năm 2021, mở ra kỷ nguyên mới cho Cardano bằng cách giới thiệu tính năng hợp đồng thông minh. Với sự ra đời của Plutus, một nền tảng lập trình hợp đồng thông minh mạnh mẽ, Cardano đã trở thành một nền tảng phù hợp để xây dựng các ứng dụng phi tập trung (DApps).

Goguen cũng giới thiệu Marlowe, một ngôn ngữ lập trình đặc thù dành cho các hợp đồng tài chính, giúp người dùng không có kỹ năng lập trình vẫn có thể tạo và thực thi các hợp đồng phức tạp. Nhờ Goguen, Cardano đã tiến gần hơn đến việc cạnh tranh với các nền tảng blockchain lớn khác như Ethereum.

- **Basho (Tối Ưu Hóa)**

Giai đoạn Basho tập trung vào việc tối ưu hóa hiệu suất và khả năng mở rộng của Cardano. Các cải tiến bao gồm việc giới thiệu Hydra, một giải pháp lớp 2 giúp tăng tốc độ xử lý giao dịch và giảm chi phí.

Hydra cho phép mạng lưới Cardano xử lý hàng triệu giao dịch mỗi giây bằng cách sử dụng các kênh trạng thái (state channels). Điều này giúp Cardano trở thành một trong những blockchain có khả năng mở rộng tốt nhất, phục vụ nhu cầu ngày càng tăng của người dùng và doanh nghiệp.

- **Voltaire (Quản Trị)**

Giai đoạn Voltaire, giai đoạn cuối cùng trong lộ trình phát triển, tập trung vào việc xây dựng một hệ thống quản trị phi tập trung hoàn chỉnh. Người dùng ADA sẽ có quyền tham gia vào các quyết định quan trọng của mạng lưới thông qua cơ chế bỏ phiếu.

Voltaire giới thiệu hệ thống ngân quỹ, nơi mà một phần phí giao dịch được phân bổ để tài trợ cho các dự án và sáng kiến phát triển cộng đồng. Điều này giúp Cardano duy trì sự phát triển bền vững và linh hoạt trong tương lai.

3.3.1.4. Tác động và Tầm nhìn tương lai của Blockchain Cardano

Cardano không chỉ là một blockchain, mà còn là một hệ sinh thái với tầm nhìn xa về công nghệ và xã hội. Với sự kết hợp giữa nghiên cứu khoa học, thiết kế module, và cộng đồng phát triển mạnh mẽ, Cardano đã và đang định hình lại cách chúng ta nghĩ về blockchain.

- Tác động hiện tại

Cardano đã đạt được những thành tựu ấn tượng trong việc mang lại giải pháp blockchain bền vững và an toàn. Hàng ngàn nhóm cổ phần trên toàn thế giới đã tham gia vào mạng lưới, chứng minh tính phân quyền và khả năng mở rộng của nền tảng.

Ngoài ra, Cardano đã thu hút sự chú ý từ các tổ chức phi lợi nhuận và chính phủ ở nhiều quốc gia, đặc biệt là các nước đang phát triển. Ví dụ, dự án Atala Prism của Cardano đã được sử dụng để triển khai hệ thống nhận dạng số ở Ethiopia, giúp cải thiện việc tiếp cận giáo dục và dịch vụ công.

- Tầm nhìn tương tai

Trong tương lai, Cardano đặt mục tiêu trở thành một nền tảng blockchain toàn diện, hỗ trợ các ứng dụng thực tế trong nhiều lĩnh vực như tài chính, giáo dục, y tế, và quản trị. Một số hướng phát triển chính bao gồm:

Hỗ trợ DApps và DeFi: Với tính năng hợp đồng thông minh mạnh mẽ, Cardano sẽ tiếp tục hỗ trợ việc phát triển các ứng dụng phi tập trung và tài chính phi tập trung, cạnh tranh trực tiếp với các nền tảng như Ethereum.

Tăng cường khả năng mở rộng: Hydra và các giải pháp lớp 2 khác sẽ tiếp tục được phát triển để đảm bảo khả năng xử lý giao dịch nhanh chóng và chi phí thấp.

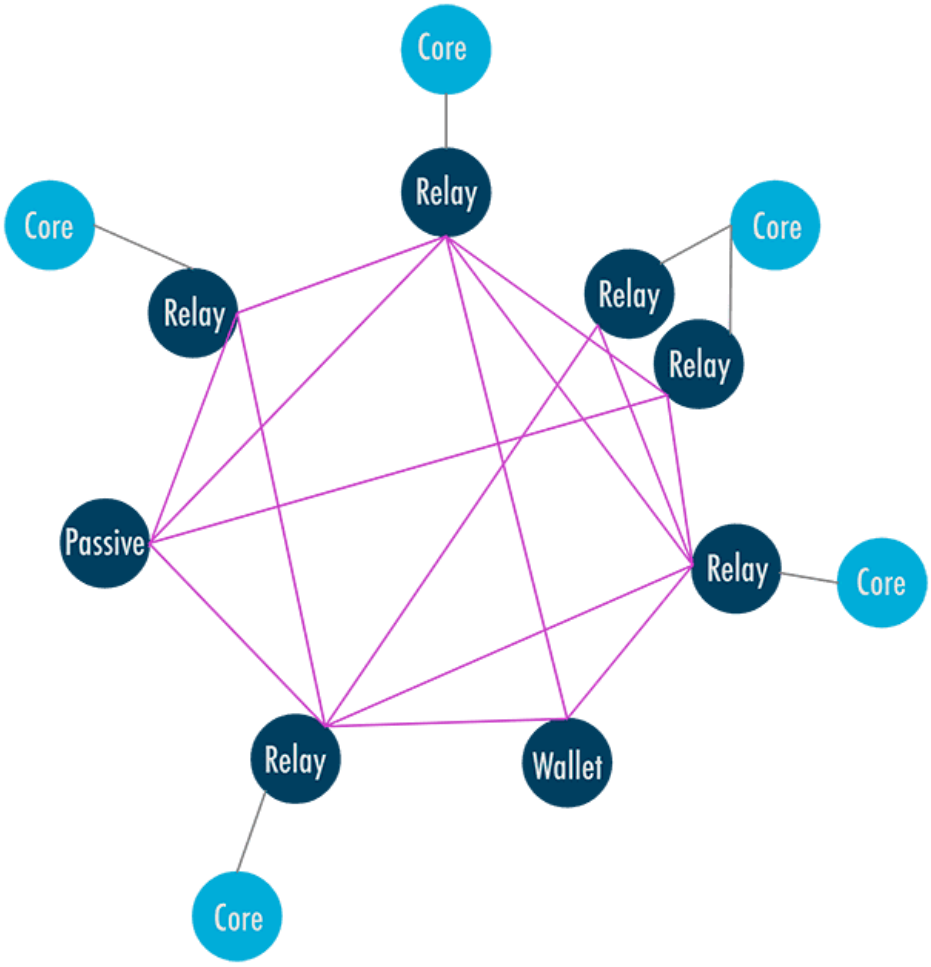
Phát triển cộng đồng: Cardano sẽ tiếp tục mở rộng cộng đồng người dùng và nhà phát triển, thúc đẩy sự tham gia từ các tổ chức và cá nhân trên toàn thế giới.

Ứng dụng thực tiễn: Cardano sẽ tập trung vào việc tạo ra các giải pháp blockchain thực tế, giúp giải quyết các vấn đề toàn cầu như nhận dạng số, quản lý tài nguyên, và minh bạch trong quản trị.

Với sự cam kết về nghiên cứu khoa học và phát triển bền vững, Cardano được kỳ vọng sẽ đóng vai trò quan trọng trong việc định hình tương lai của công nghệ blockchain và thúc đẩy sự đổi mới trên toàn cầu

3.3.2. Nguyên lý hoạt động và cơ chế giao dịch của Cardano

Cardano được xây dựng dựa trên giao thức đồng thuận **Ouroboros**, một hệ thống Proof of Stake (PoS) tiên phong được phát triển thông qua các nghiên cứu học thuật được đánh giá bởi cộng đồng khoa học. Trọng tâm của Ouroboros là cơ chế các nhóm cổ phần, nơi các nút máy chủ đáng tin cậy được quản lý bởi những nhà điều hành chuyên trách. Chủ sở hữu ADA có thể ủy quyền cổ phần của mình cho các nhóm này, giúp đảm bảo rằng bất kỳ ai cũng có thể tham gia vào giao thức mà không yêu cầu kiến thức kỹ thuật cao hay khả năng duy trì một nút trực tuyến. Các nhóm cổ phần đóng vai trò quan trọng trong việc bảo trì mạng lưới và quản lý cổ phần kết hợp của nhiều bên liên quan trong một thực thể thống nhất.



Hình 3-10: Hình ảnh tổng quan mạng Blockchain Cardano

Mạng lưới Cardano

Cardano là sổ cái blockchain công khai nên có thể dễ dàng theo dõi mọi giao dịch, chi tiết khối và dữ liệu kỷ nguyên bằng nhiều công cụ khác nhau.

Cardano Explorer là một công cụ hướng đến người dùng, lấy dữ liệu từ cơ sở dữ liệu chính và phản ánh dữ liệu đó trên một giao diện web đơn giản và tiện lợi.

Trình khám phá hiển thị chi tiết kỷ nguyên mới nhất. Bạn có thể xem các thông tin sau:

- Các khối được sản xuất.
- Thời gian Epoch bắt đầu.
- Thời gian của khối được tạo.
- Số lượng giao dịch đã xử lý

…

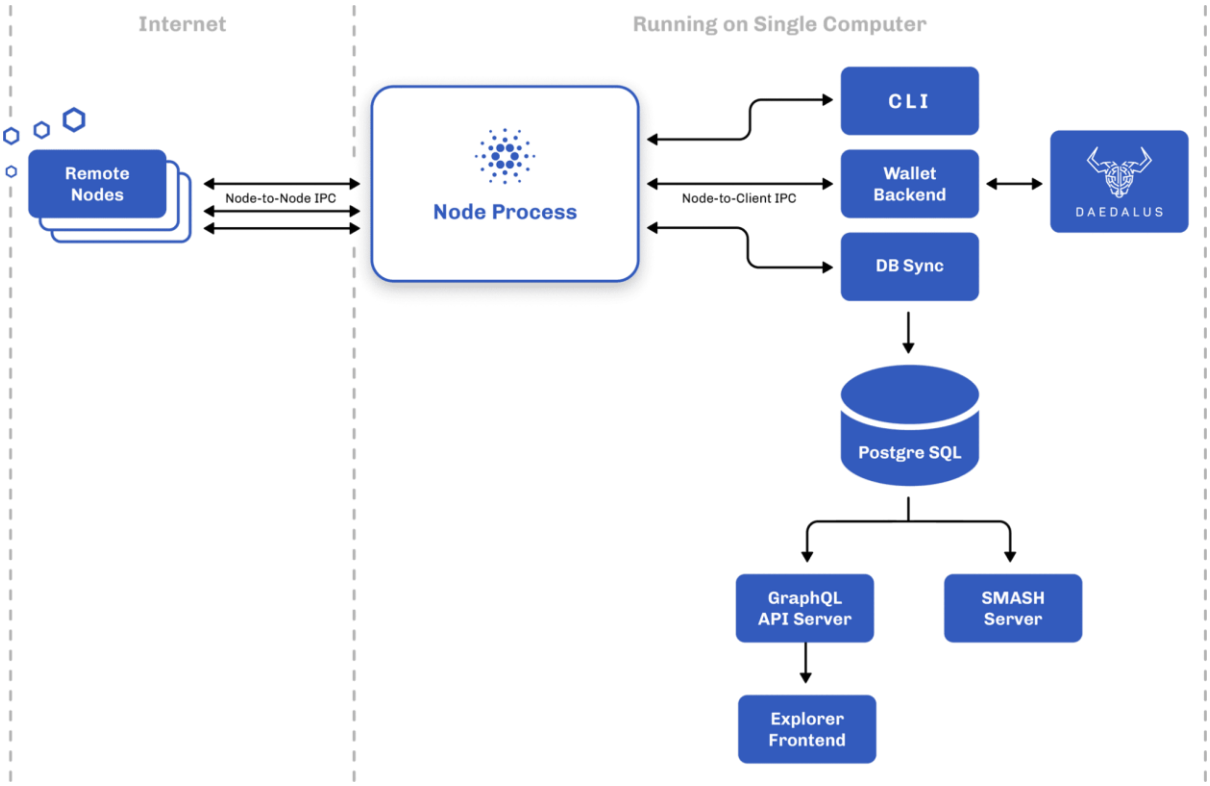
Bằng cách chọn một khối cụ thể, bạn có thể khám phá khối đó chi tiết hơn để xem ID, kích thước, Epoch và thông tin chi tiết về khối, số lượng giao dịch.

Bạn cũng có thể tìm kiếm các Epoch, giao dịch hoặc khối cụ thể bằng cách dán ID của chúng vào trường tìm kiếm.

Sau đây là một số Trình Khám phá bạn có thể truy cập:

- AdaStat
- Cardanoscan
- Cexplorer
- Cardano Assets
- Pool.pm

Hoạt động của Cardano dựa trên một kiến trúc được thiết kế chi tiết, mô tả cách thức hoạt động ở cấp cao. Kiến trúc này cung cấp cái nhìn sâu sắc về các thành phần cốt lõi và cách chúng tương tác với nhau.



Hình 3-11: Kiến trúc của Blockchain cardano.

Hiện tại, việc triển khai Cardano được thiết kế theo kiến trúc mô-đun cao, bao gồm nhiều thành phần khác nhau. Tùy thuộc vào các trường hợp sử dụng cụ thể, các thành phần này có thể được kết hợp linh hoạt để đáp ứng nhu cầu triển khai.

- **Nodes and remote nodes**

Một hệ thống blockchain bao gồm một tập hợp các nút (nodes) được phân phối trên mạng, giao tiếp với nhau để đạt được sự đồng thuận về trạng thái của hệ thống.

Các nút đảm nhận các nhiệm vụ sau:

- Thực thi giao thức Ouroboros
- Xác thực và truyền tải các khối
- Sản xuất các khối (một số nút đảm nhận nhiệm vụ này)
- Cung cấp thông tin về trạng thái của blockchain cho các khách hàng cục bộ khác.

- **Node Process**

cardano-node là thành phần cấp cao nhất của hệ thống Cardano, bao gồm các hệ thống phụ khác, trong đó các thành phần quan trọng nhất là đồng thuận (consensus), sổ cái (ledger), và mạng (networking). Ngoài ra, nó còn tích hợp các thành phần hỗ trợ như cấu hình, giao diện dòng lệnh (CLI), ghi log, và giám sát.

- **Giao thức IPC giữa các nút (Node-to-Node IPC Protocol)**

Mục đích của giao thức (IPC) giữa các nút là trao đổi các khối và giao dịch giữa các nút, đóng vai trò trong thuật toán đồng thuận Ouroboros.

Giao thức này bao gồm ba mini-protocol:

- **chain-sync:** Được sử dụng để theo dõi chuỗi và nhận tiêu đề khối (block headers).
- **block-fetch:** Được sử dụng để lấy nội dung khối (block bodies).
- **tx-submission:** Được sử dụng để chuyển tiếp các giao dịch.

Các mini-protocol này được ghép đa kênh (multiplexed) trên một kết nối TCP (Transmission Control Protocol) chạy liên tục giữa các nút. Chúng có thể chạy hai chiều trên cùng một kết nối TCP để hỗ trợ thiết lập ngang hàng (P2P).

Giao thức tổng thể và từng mini-protocol được thiết kế cho môi trường không cần tin cậy (trustless), trong đó cả hai phía đều cần bảo vệ chống lại các cuộc tấn công từ chối dịch vụ (DoS). Ví dụ, mỗi mini-protocol sử dụng luồng điều khiển do phía nhận điều khiển (consumer-driven control flow), nghĩa là một nút chỉ yêu cầu thêm công việc khi nó đã sẵn sàng, thay vì bị ép phải nhận thêm công việc.

Thiết kế của giao thức mang tính mô-đun và có khả năng phát triển cho phép thêm hoặc cập nhật các mini-protocol mới theo thời gian mà không gây ra vấn đề tương thích.

- **Giao thức IPC giữa nút và Client (Node-to-Client IPC Protocol)**

Mục đích của giao thức IPC giữa nút và Client là cho phép các ứng dụng cục bộ tương tác với blockchain thông qua nút. Điều này bao gồm các ứng dụng như backend của ví hoặc các công cụ khám phá blockchain. Giao thức này cho phép các ứng dụng truy cập dữ liệu thô của chuỗi và truy vấn trạng thái hiện tại của sổ cái. Ngoài ra, nó cũng cung cấp khả năng gửi các giao dịch mới vào hệ thống.

Giao thức này sử dụng cùng một thiết kế như giao thức giữa các nút, nhưng với một tập hợp mini-protocol khác và sử dụng các kênh cục bộ (local pipes) thay vì kết nối TCP. Vì vậy, đây là một giao diện hẹp, cấp thấp, chỉ cung cấp những gì mà nút có thể cung cấp. Ví dụ, nút cung cấp quyền truy cập vào tất cả dữ liệu thô của chuỗi, nhưng không cung cấp cách truy vấn dữ liệu trên chuỗi. Nhiệm vụ cung cấp dịch vụ dữ liệu và các API cấp cao hơn được giao cho các khách hàng chuyên dụng, như cardano-db-sync và backend của ví.

Giao thức này bao gồm ba mini-protocol:

- **chain-sync:** Được sử dụng để theo dõi chuỗi và nhận các khối.
- **local-tx-submission**: Được sử dụng để gửi giao dịch.
- **local-state-query:** Được sử dụng để truy vấn trạng thái sổ cái.

Phiên bản ***chain-sync*** trong giao thức **node-client** sử dụng toàn bộ các khối (full blocks), thay vì chỉ tiêu đề khối, do đó không cần giao thức block-fetch riêng biệt. Giao thức ***local-tx-submission*** tương tự như giao thức tx-submission giữa các nút nhưng đơn giản hơn và trả về thông tin chi tiết về lỗi xác thực giao dịch. Giao thức ***local-state-query*** cung cấp khả năng truy vấn trạng thái sổ cái hiện tại, chứa nhiều dữ liệu thú vị không được phản ánh trực tiếp trên chuỗi.

- **Giao diện dòng lệnh (CLI)**

Công cụ CLI của node được ví như "swiss army knife" của hệ thống. Nó có thể thực hiện hầu hết mọi tác vụ, nhưng lại ở cấp độ thấp và không mấy tiện lợi vì dựa trên văn bản (text-based) và không có giao diện đồ họa (GUI).

Công cụ CLI có thể:

- Truy vấn node để lấy thông tin.
- Xây dựng và ký giao dịch.
- Gửi giao dịch.
- Quản lý các khóa mã hóa.

- **Ví Daedalus**

Daedalus là một ví full-node hỗ trợ người dùng quản lý ADA và thực hiện gửi, nhận thanh toán trên blockchain Cardano. Daedalus bao gồm hai phần: giao diện ví (frontend) và backend.

- Frontend: Là ứng dụng đồ họa mà người dùng có thể nhìn thấy và tương tác trực tiếp.
- Backend: Là một tiến trình dịch vụ giám sát trạng thái ví của người dùng và thực hiện các tác vụ phức tạp như chọn đồng tiền (coin selection), xây dựng giao dịch (transaction construction), và gửi giao dịch (submission).

Backend tương tác với một node cục bộ thông qua giao thức IPC giữa nút và khách hàng (node-to-client IPC protocol) và kết nối với frontend thông qua một API HTTP. Backend cũng cung cấp một công cụ CLI cho phép tương tác với ví. Ngoài ra, backend của ví có thể được sử dụng riêng biệt – không cần đến Daedalus – thông qua API của nó. Đây là một cách tiện lợi để các nhà phát triển phần mềm tích hợp Cardano vào các ứng dụng và hệ thống khác.

Ngoài ví Daedalus là ví full-node ra còn rất nhiều ví khác như

Ví Hardware

Sau đây là danh sách các ví phần cứng cần cân nhắc để lưu trữ và giao dịch ada:

- Trezor Model T
- Ledger Nano S Plus
- Ledger Nano X

Ví nhẹ

Ngoài ví Daedalus và các ví cứng, Blockchain Cardano còn có nhiều ví nhẹ được phát triển bởi cộng đồng, hoạt động trên trình duyệt hoặc ứng dụng di động, bao gồm:

- Lace
- Nami
- Eternl
- GeroWallet
- Typhon
- Ellipal
- AdaLite
- Infinito Wallet
- Atomic Wallet

DB Sync

Node của Cardano chỉ lưu trữ blockchain cùng với thông tin liên quan cần thiết để xác thực chuỗi khối. Nguyên tắc thiết kế này nhằm giảm thiểu độ phức tạp của mã nguồn (code complexity), giảm chi phí tính toán và sử dụng tài nguyên, giữ cho các giao diện cục bộ của node đơn giản nhất có thể, và sử dụng các client bên ngoài để cung cấp nhiều giao diện tiện dụng hơn và chức năng bổ sung.

Đặc biệt, node không cung cấp giao diện truy vấn thuận tiện cho thông tin lịch sử trên blockchain. Dịch vụ dữ liệu **DB-Sync** này được cung cấp bởi một thành phần riêng biệt sử dụng cơ sở dữ liệu SQL (Structured Query Language). Dữ liệu này có đặc tính một chiều. Nó chỉ có chiều ghi từ Node Cardano và đọc từ User.

3.3.3 Mô hình EUTxO của Blockchain Cardano

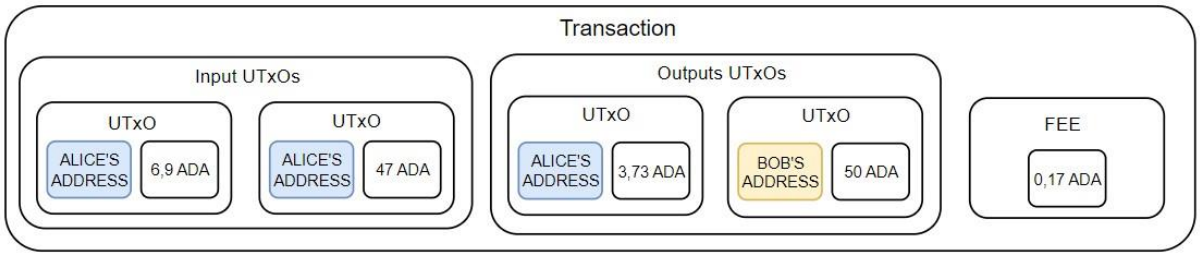
3.3.3.1 Thông tin cơ bản về UTXO

UTXO (Unspent Transaction Output) là đầu ra từ một giao dịch trước đó, có thể được sử dụng làm đầu vào cho các giao dịch trong tương lai. UTxO là mô hình sổ cái được sử dụng cho Blockchain Bitcoin

Mô hình UTXO không dựa trên khái niệm tài khoản hay số dư, mà hoạt động như tiền mặt, với mỗi UTXO mang một giá trị cụ thể, ví dụ: 6,9 ADA, 47 ADA, hoặc 459,7 ADA. Ví Cardano quản lý UTXO và hiển thị tổng số như một số dư, chẳng hạn 513,6 ADA từ ba UTXO.

Khi gửi 50 ADA, ví sẽ chọn UTXO đủ giá trị để chi trả, ví dụ: sử dụng hai UTXO (6,9 ADA và 47 ADA) để tạo giao dịch tổng cộng 53,9 ADA. Giao dịch tạo ra hai UTXO đầu ra: 50 ADA cho người nhận và 3,73 ADA trả lại cho người gửi sau khi trừ phí giao dịch.

UTXO đầu vào được sử dụng hoàn toàn, và UTXO đầu ra mới được tạo ra từ giao dịch, phản ánh nguyên tắc cơ bản của mô hình UTXO.



Hình 3-12: Mô tả một giao dịch trên Blockchain Cardano

3.3.3.2 Sự khác biệt giữa EUTxO và Mô hình dựa trên tài khoản

Mô hình dựa trên tài khoản hoạt động dựa trên khái niệm tài khoản và số dư, tương tự như cách thức hoạt động của hệ thống ngân hàng. **Ethereum** áp dụng mô hình này, trong đó mỗi người dùng có một tài khoản lưu giữ số dư token của mình. Các giao dịch trong mô hình này thực

hiện bằng cách cập nhật số dư của tài khoản người gửi và người nhận, đây là một **atomic operation** phụ thuộc vào trạng thái toàn cầu.

- **Atomic operation** là một khái niệm trong khoa học máy tính, mô tả các thao tác hoặc hành động được thực hiện mà không bị ngắt quãng hay can thiệp. Điều này đảm bảo tính toàn vẹn dữ liệu và sự nhất quán của hệ thống, đặc biệt trong môi trường có nhiều luồng hoặc tiến trình thao tác trên cùng một tài nguyên.

Ngược lại, mô hình eUTxO (Extended Unspent Transaction Output) là sự mở rộng của mô hình UTxO được sử dụng trong Bitcoin. Trong mô hình này, tài sản được lưu trữ dưới dạng UTxO thay vì số dư tài khoản. Mỗi UTxO đại diện cho một lượng giá trị cụ thể, có thể được sử dụng làm đầu vào cho các giao dịch mới. Giao dịch sử dụng UTxO từ các giao dịch trước đó và tạo ra UTxO mới để sử dụng trong tương lai.

Hai mô hình này đại diện cho những cách tiếp cận khác biệt trong việc quản lý tài sản trên blockchain, mỗi mô hình phù hợp với các mục tiêu và ứng dụng cụ thể của từng nền tảng.

3.3.3.3 Mô hình EUTxO của Cardano

Cardano sử dụng mô hình EUTxO cải tiến từ UTxO của Blockchain Bitcoin, để hỗ trợ nhiều tài sản và hợp đồng thông minh. Nó khác với mô hình dựa trên tài khoản (Accounting) được các ngân hàng hoặc **Ethereum** sử dụng. Trong phần này, sẽ giải thích ngắn gọn sự khác biệt giữa mô hình dựa trên tài khoản và mô hình EUTxO. Mục đích là giải thích chi tiết cách người dùng chi tiêu EUTxO.

Hình 3-13: Cấu tạo của EUTxO

Mô hình EUTxO được mở rộng mô hình UTxO theo hai cách:

- *Khái quát hóa khái niệm "địa chỉ" bằng cách sử dụng phép ẩn dụ khóa và chìa khóa.* Thay vì giới hạn khóa chỉ là khóa công khai và chìa khóa chỉ là chữ ký, các địa chỉ trong mô hình EUTxO có thể chứa logic tùy ý dưới dạng các tập lệnh (scripts). Ví dụ, khi một node xác thực giao dịch, node sẽ xác định liệu giao dịch có được phép sử dụng một đầu ra cụ thể làm đầu vào hay không. Giao dịch sẽ tra cứu tập lệnh được cung cấp bởi địa chỉ của đầu ra và thực thi tập lệnh nếu giao dịch có thể sử dụng đầu ra làm đầu vào.
- *Đầu ra có thể mang theo (gần như) dữ liệu tùy ý, ngoài địa chỉ và giá trị.* Điều này làm cho các tập lệnh trở nên mạnh mẽ hơn nhờ khả năng mang theo thông tin trạng thái.

Hơn nữa, mô hình EUTxO mở rộng mô hình UTxO bằng cách cho phép các địa chỉ đầu ra chứa logic phức tạp để quyết định giao dịch nào có thể mở khóa chúng và bằng cách thêm dữ liệu tùy chỉnh vào tất cả các đầu ra. Khi xác thực một địa chỉ, tập lệnh sẽ truy cập dữ liệu được mang theo bởi đầu ra, giao dịch đang được xác thực, và một số dữ liệu bổ sung gọi là **"Redeemer"** được giao dịch cung cấp cho mỗi đầu vào. Bằng cách tra cứu tất cả thông tin này, tập lệnh có đủ ngữ cảnh để đưa ra câu trả lời "đồng ý" hoặc "từ chối" ngay cả trong các tình huống và trường hợp sử dụng phức tạp.

EUTxO cho phép thực hiện logic tùy ý dưới dạng các tập lệnh. Logic này kiểm tra giao dịch và dữ liệu để quyết định liệu giao dịch có được phép sử dụng một đầu vào hay không.

Mô hình UTxO với cấu trúc đồ thị của nó khác biệt cơ bản so với mô hình dựa trên tài khoản được sử dụng bởi một số blockchain hỗ trợ hợp đồng thông minh hiện tại. Do đó, các mẫu thiết kế hoạt động cho DApp trên blockchain dựa trên tài khoản không thể áp dụng trực tiếp cho Cardano. Các mẫu thiết kế mới là cần thiết vì cách biểu diễn dữ liệu cơ bản là khác nhau.

EUTxO kế thừa thiết kế phân nhánh của mô hình UTxO (Bitcoin), trong đó một nhánh được định nghĩa là một chuỗi giao dịch yêu cầu một chuỗi xác thực. Để phân tách logic qua các nhánh khác nhau và tăng cường tính song song, điều quan trọng là xây dựng DApp và các giải pháp khác bằng cách sử dụng nhiều UTxO. Điều này mang lại lợi ích về khả năng mở rộng, tương tự như việc phát triển các dịch vụ Bitcoin yêu cầu chia một ví thành nhiều ví con.

3.3.3.4 Các thành phần cơ bản của EUTxO

Hình 3-14: Các Thành phần cơ bản của EUTxO

- **Hợp đồng thông minh (Contract)**: Dùng để khóa UTxO chứa các ADA, tài sản gốc và NFT.
- **Redeemer**: Dữ liệu do người dùng cung cấp để mở khóa tài sản đã bị khóa và chi tiêu chúng.
- **Datum**: Dữ liệu như điểm số, thông tin người dùng hoặc các thông tin liên quan đến ứng dụng của bạn. Nó là các thông tin được gắn cùng với UTxO mà muốn chi tiêu UTxO đó cần thỏa mãn các điều kiện trong Scripts mà Datum là một tham số.
- **Ngữ cảnh (Context)**: Thông tin như siêu dữ liệu về giao dịch đang được xác thực.

3.3.3.5 Lợi ích của mô hình EUTxO

Mô hình EUTxO của Cardano cung cấp một môi trường an toàn và linh hoạt để xử lý nhiều hoạt động mà không gặp sự cố hệ thống. Mô hình này mang lại khả năng mở rộng và bảo mật cao hơn, cùng với logic giao dịch đơn giản hơn, vì mỗi UTxO chỉ có thể được tiêu thụ một lần và hoàn toàn, giúp việc xác minh giao dịch trở nên dễ dàng hơn.

Mô hình EUTxO có những lợi thế độc đáo so với các mô hình kế toán khác. Sự thành công hay thất bại của việc xác thực giao dịch chỉ phụ thuộc vào bản thân giao dịch và các đầu vào của nó, không liên quan đến bất kỳ yếu tố nào khác trên blockchain. Do đó, tính hợp lệ của một giao dịch có thể được kiểm tra ngoài chuỗi trước khi gửi lên blockchain. Giao dịch vẫn có thể thất bại nếu một giao dịch khác tiêu thụ đồng thời một đầu vào mà giao dịch đang chờ, nhưng nếu tất cả các đầu vào vẫn còn, giao dịch được đảm bảo sẽ thành công.

Điều này trái ngược với mô hình dựa trên tài khoản (như Ethereum), nơi một giao dịch có thể thất bại trong quá trình thực thi script. Điều này không bao giờ xảy ra trong mô hình EUTxO.

Nhờ vào tính chất "cục bộ" của việc xác thực giao dịch, một mức độ song song cao có thể đạt được. Về nguyên tắc, một node có thể xác thực các giao dịch song song, miễn là các giao dịch đó không cố gắng tiêu thụ cùng một đầu vào. Điều này mang lại hiệu quả cao hơn và đơn giản hóa việc phân tích các kết quả có thể xảy ra, đồng thời chứng minh rằng không có sự cố không mong muốn nào xảy ra. Bạn có thể tìm hiểu thêm trong bài viết blog về mô hình EUTxO.

Một tính năng mạnh mẽ của mô hình EUTxO là phí cần thiết cho một giao dịch hợp lệ có thể được dự đoán chính xác trước khi đăng giao dịch. Đây là một tính năng độc đáo không có trong các mô hình dựa trên tài khoản. Các blockchain dựa trên tài khoản, như Ethereum, mang tính không xác định, có nghĩa là chúng không thể đảm bảo hiệu quả của giao dịch trên chuỗi. Sự không chắc chắn này gây ra rủi ro mất tiền, phí cao không mong muốn và các cơ hội hành vi đối kháng.

Tóm lại, EUTxO mang lại mức độ bảo mật cao hơn, khả năng dự đoán chi phí thực thi hợp đồng thông minh (không có bất ngờ khó chịu) và khả năng song song mạnh mẽ hơn.

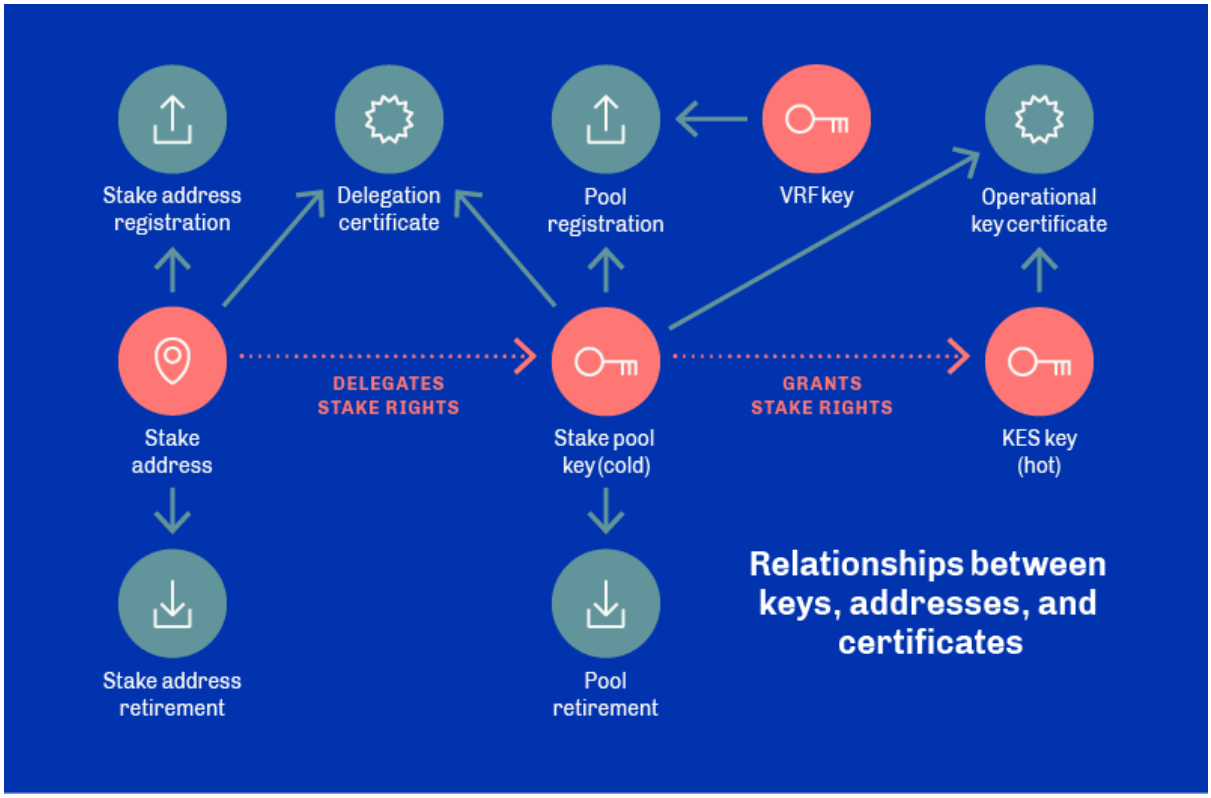
3.3.4. Khóa, địa chỉ của Blockchain cardano.

Khóa của Cardano

Khóa của Cardano là các cặp khóa mật mã bất đối xứng (chi tiết mô tả trong mục 1.1.5) được sử dụng cho nhiều mục đích trên blockchain Cardano, bao gồm:

- Ký và xác minh các giao dịch thanh toán và chứng chỉ staking.
- Nhận diện và định nghĩa các địa chỉ trên blockchain Cardano.

Dưới đây là sơ đồ minh họa mối quan hệ giữa các khóa, địa chỉ và chứng chỉ:



Hình 3-15: Mối quan hệ giữa các khóa, địa chỉ và chứng chỉ

Các loại khóa trong Cardano

Trong hệ sinh thái Cardano, có hai loại khóa chính:

- **Khóa của Node**
- **Khóa địa chỉ**

Khóa của node

Các khóa này được sử dụng để xác thực và ủy quyền các hoạt động của một nút Cardano, đặc biệt là các nút vận hành nhóm cổ phần (stake pools).

Chúng cho phép nút thực hiện các tác vụ quan trọng như tạo khối (block production) và tham gia vào quá trình đồng thuận.

Quan trọng nhất là, chúng tách biệt quyền vận hành node với quyền sở hữu tài sản (ADA), tăng cường tính bảo mật.

Các cặp Khóa vận hành Node (Operator/Operational Key)

- Các cặp Khóa vận hành Node là các cặp khóa offline của người vận hành Node, nó liên kết các khóa KES, và VRF lại với nhau.
- Trách nhiệm của người vận hành là quản lý các khóa nóng (online) và khóa lạnh (offline) cho pool.

- Khóa lạnh phải được bảo mật tối đa và không được lưu trữ trên thiết bị có kết nối Internet. Nên tạo nhiều bản sao lưu của khóa lạnh.

Cặp khóa KES (Key Evolving Signature)

- KES được sử dụng để tạo chứng chỉ vận hành cho node sản xuất block, xác minh danh tính của người sử dụng.
- Khóa KES có thể tiến hóa trong một số chu kỳ nhất định, sau đó trở nên vô dụng.
- Điều này ngăn chặn việc tấn công lại lịch sử, ngay cả khi khóa bị lộ. Sau khi chu kỳ hết hạn, người vận hành node phải tạo khóa KES mới, cấp chứng chỉ node vận hành mới và khởi động lại node.

Khóa VRF (Verifiable Random Function)

- Khóa VRF được sử dụng trong giao thức Ouroboros Praos để tăng cường bảo mật cho việc sản xuất block.
- Khác với các giao thức khác như Ouroboros Classic, lịch trình slot leader trong Praos được giữ bí mật. Khi slot leader được chọn, khóa VRF chứng minh quyền tạo block.
- Khóa VRF được lưu trong chứng chỉ vận hành và xác minh rằng node có quyền tạo block trong slot đó.

Khóa địa chỉ

Khóa địa chỉ đại diện cho các chức năng của địa chỉ được dẫn xuất từ khóa, dùng để xác định tài sản trên blockchain. Các khóa bao gồm:

- **Khóa thanh toán (Payment key):** Cặp khóa địa chỉ đơn thường được sử dụng để tạo địa chỉ UTXO.
- **Khóa staking (Staking key):** Cặp khóa địa chỉ stake/phần thưởng thường được sử dụng để tạo địa chỉ tài khoản/phần thưởng.

Địa chỉ thanh toán và stake

Bạn có thể có nhiều địa chỉ với tiền ADA trong ví của mình. Nếu bạn tạo chứng chỉ stake và gửi nó tới blockchain Cardano, tất cả token sẽ được ủy quyền cho pool bạn đã chọn. Ví dụ, điều này cũng ứng dụng cho các địa chỉ mới được tạo mà bạn gửi ADA từ sàn giao dịch. Ngay khi snapshot tiếp theo xảy ra trong mạng Cardano, các token ADA mới nhận cũng sẽ được kích hoạt sử dụng để stake.

Để đạt được các khả năng được mô tả ở trên, *cần phải tách biệt riêng* việc theo dõi các giao dịch của tiền ADA và việc ủy quyền của chúng. Chỉ trong một địa chỉ ví duy nhất, Cardano có cấu trúc địa chỉ phân biệt giữa địa chỉ thanh toán và địa chỉ stake (đôi khi được gọi là địa chỉ phần thưởng). Địa chỉ thanh toán nhằm mục đích giữ tiền có thể được chi tiêu. Địa chỉ stake xác định nếu và cách tiền từ địa chỉ thanh toán được sử dụng trong stake.

Trong hình 3-16, bạn có thể thấy địa chỉ thanh toán Shelley, bao gồm một phần dành cho quản lý tài sản (thông tin xác thực thanh toán) và tham chiếu đến địa chỉ stake (khóa stake).

Hình 3-16: Địa chỉ của ví trên Blockchain cardano

Token ADA luôn thuộc về địa chỉ thanh toán (không bao giờ là địa chỉ stake). Mỗi địa chỉ thanh toán có thể tùy chọn tham chiếu đến một địa chỉ stake. Quyền stake của tất cả các token ADA tại địa chỉ thanh toán được liên kết với địa chỉ stake.

Token tại địa chỉ thanh toán đại diện cho quyền stake. Địa chỉ stake xác định cách xử lý quyền này. Việc ủy thác tiền ADA cho một pool được thực hiện theo hai bước. Thứ nhất, địa chỉ thanh toán phải tham chiếu đến địa chỉ stake. Sau đó, địa chỉ stake phải được ủy quyền cho pool.

Trong ví, người dùng chọn pool mà anh ấy muốn ủy quyền và xác nhận giao dịch, giao dịch này sẽ được gửi đến blockchain. Chứng chỉ stake được tạo ngầm, chứng chỉ này ủy quyền tiền cho pool đã chọn thông qua địa chỉ stake. Trong quá trình ủy quyền, một tài khoản phần thưởng được tạo trong đó hệ thống tích lũy phần thưởng stake.

Lưu ý rằng địa chỉ stake đã được đăng ký, không phải (các) địa chỉ thanh toán. Do đó, có thể thực hiện một lần đăng ký cho tất cả các địa chỉ thanh toán được tạo trong tương lai. Ngoài ra, hãy lưu ý rằng tiền vẫn nằm trên địa chỉ thanh toán (do chủ sở hữu kiểm soát hoàn toàn) và có thể được chi tiêu.

Bạn có thể dễ dàng phân biệt các địa chỉ với nhau bằng tiền tố. Địa chỉ thanh toán có tiền tố “addr”. Địa chỉ stake có tiền tố “stake”. Hãy nói thêm rằng các địa chỉ Byron không có tiền tố và được mã hóa bởi Base58. Địa chỉ thanh toán Shelley và địa chỉ stake đều được mã hóa bởi bech32.

Byron address:

37ctjaVyb4KDXBNC4haBVPCvro8AQPHwvCMp3RFhiSVWwfFmZ6iazSK6JK1hY6wHNmtrp1f1kdbva8TCneM2YsiXT7mrVr21EacHntXz5YyUdj84pe

Payment address:

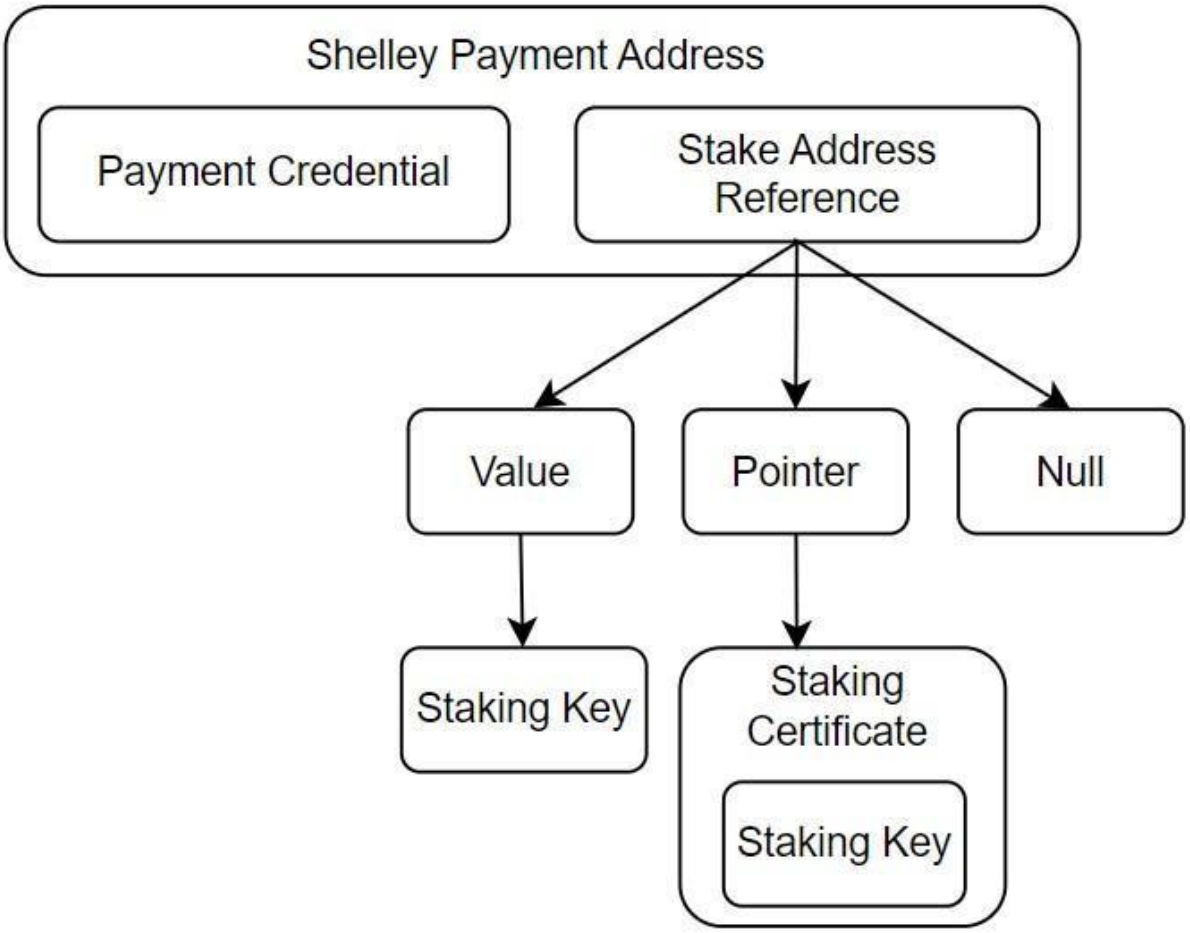
addr1vpu5vlrf4xkxv2qpwngf6cjhtw542ayty80v8dyr49rf5eg0yu80w

Stake address:

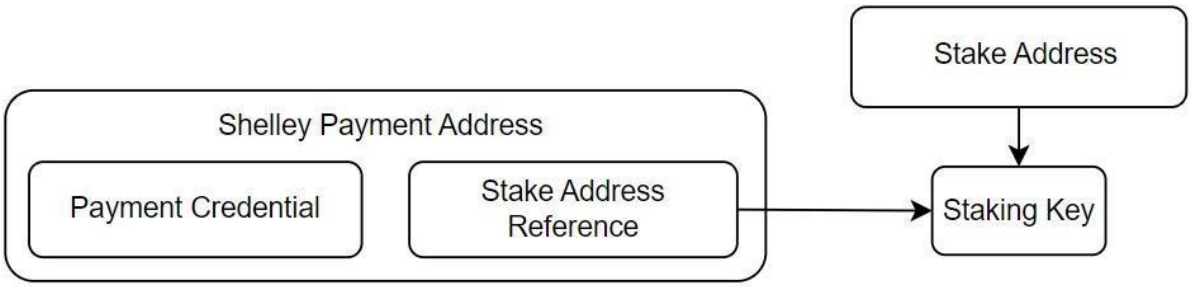
stake1vpu5vlrf4xkxv2qpwngf6cjhtw542ayty80v8dyr49rf5egfu2p0u

Tham chiếu địa chỉ stake (Stake Address Reference)

Có ba tùy chọn cho nội dung có thể xuất hiện trong tham chiếu địa chỉ stake của địa chỉ thanh toán Shelley. Dựa trên nội dung của tài liệu tham khảo, chúng tôi có thể chia địa chỉ thanh toán Shelley thành nhiều loại.



Tham chiếu (Stake Address Reference) có thể chứa gọi là Giá trị (Value), tức là chỉ hàm băm của khóa xác minh (staking key) hoặc tập lệnh xác thực. Những địa chỉ này được gọi là địa chỉ cơ sở (base addresses).

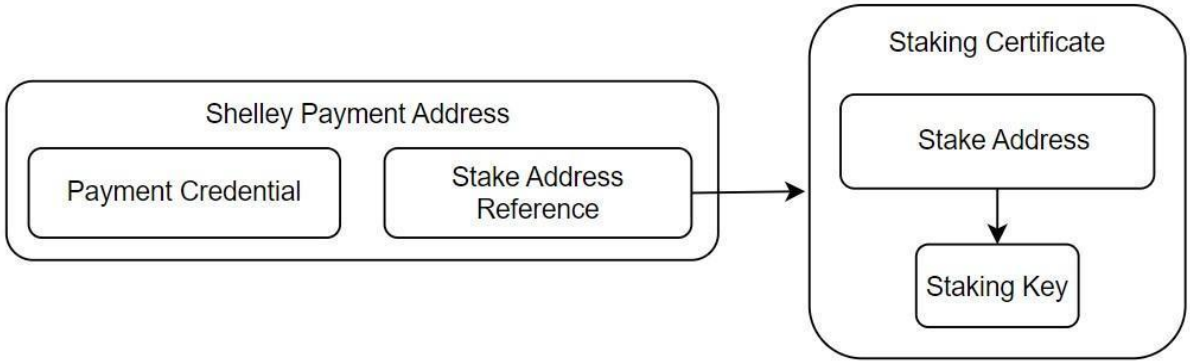


Hãy nói thêm rằng thay vì khóa stake, tham chiếu có thể đề cập đến hàm băm của tập lệnh (nghĩa là hàm băm của tập lệnh sẽ được sử dụng để chi tiêu).

Khóa stake được sử dụng để kiểm soát quyền stake đối với tất cả các địa chỉ thanh toán được liên kết. Khóa stake thường được sở hữu bởi cùng một thực thể sở hữu các địa chỉ thanh toán, nhưng điều này không phải lúc nào cũng đúng. Có thể một người nào đó không phải là chủ sở hữu của địa chỉ thanh toán có quyền kiểm soát quyền stake (ví dụ: hợp đồng thông minh). Những địa chỉ này được gọi là địa chỉ lai. Lưu ý rằng cần có một khóa khác để chi tiền cho các địa chỉ thanh toán.

Hơn nữa, tham chiếu có thể chứa cái gọi là Pointer. Các địa chỉ này được gọi là địa chỉ Pointer.

Trong trường hợp này, khóa stake được tham chiếu gián tiếp thông qua một Pointer. Tham chiếu trỏ đến vị trí trong blockchain nơi lưu trữ chứng chỉ stake. Khóa stake được lưu trữ trong chứng chỉ. Pointer chiếm một kích thước nhỏ hơn so với stake key. Chỉ cần 3 số để tìm thấy nó: chỉ mục vị trí (slot index), chỉ mục giao dịch (transaction index) trong khối và chỉ mục chứng chỉ (certificate index) trong giao dịch.



Cuối cùng, tham chiếu có thể không chứa bất kỳ thứ gì, chỉ có giá trị được gọi là Null. Những địa chỉ này được gọi là địa chỉ địa chỉ thương mại (enterprise addresses).

Trong trường hợp này, tiền trong địa chỉ thanh toán (payment addresses) không thể được liên kết với quyền stake. Nói cách khác, tiền ADA không thể được sử dụng để stake. Tùy chọn này phù hợp, chẳng hạn như đối với các sàn giao dịch hoặc các tổ chức khác muốn làm rõ rằng họ sẽ không stake ADA.

Có một loại địa chỉ nữa mà bạn nên biết. Điều này không dựa trên nội dung trong tài liệu tham khảo. Đó là một địa chỉ tài khoản phần thưởng (rewards account address).

Địa chỉ phần thưởng là giá trị băm của khóa stake công khai của địa chỉ. Chúng được sử dụng để phân phối phần thưởng stake. Không giống như địa chỉ thanh toán dựa trên mô hình UTxO, tài khoản phần thưởng dựa trên mô hình dựa trên tài khoản. Thanh toán phần thưởng thường xuyên sẽ chỉ làm tăng số dư tài khoản. Ngay sau khi người dùng rút phần thưởng thông qua một giao dịch, một UTxO mới sẽ được tạo từ số dư.

3.3.5. Hợp đồng thông minh trên Cardano

Giới thiệu hợp đồng thông minh trên Cardano

Hợp đồng thông minh trên Cardano có cách hoạt động khác biệt so với các blockchain khác. Để hiểu rõ về hợp đồng thông minh, trước tiên cần nắm vững mô hình eUTxO.

Hợp đồng thông minh thực chất là một đoạn mã được viết để xác thực việc di chuyển UTXO bị khóa tại địa chỉ hợp đồng. Khi bạn khóa UTXO tại địa chỉ của một tập lệnh, UTXO đó chỉ có thể được chi tiêu hoặc di chuyển nếu tập lệnh xác nhận và cho phép giao dịch thực hiện điều này.

Tổng quan về cấu trúc hợp đồng thông minh

Hợp đồng thông minh bao gồm hai thành phần chính:

1. **Thành phần On-Chain (trên chuỗi):**
   Đây là mã xác thực (validator script) được sử dụng để đảm bảo rằng mọi giao dịch liên quan đến giá trị bị khóa tại địa chỉ của hợp đồng đều tuân theo các quy tắc của hợp đồng. Việc tạo mã xác thực yêu cầu các công cụ và ngôn ngữ lập trình chuyên biệt.
2. **Thành phần Off-Chain (ngoài chuỗi):**
   Đây là mã hoặc ứng dụng dùng để tạo ra các giao dịch phù hợp với quy tắc của hợp đồng. Thành phần này có thể được viết bằng hầu hết các ngôn ngữ lập trình phổ biến.

Hợp đồng thông minh thường sử dụng dữ liệu **datum** được gắn vào UTXO để duy trì "trạng thái" của hợp đồng. Nếu một UTXO không có dữ liệu **datum**, nó có thể bị khóa vĩnh viễn trên địa chỉ của hợp đồng.

Thành phần On-Chain (Mã xác thực)

Mã xác thực (validator script) tự động được thực thi khi một UTXO tại địa chỉ của hợp đồng bị di chuyển thông qua giao dịch. Mã này sẽ nhận thông tin từ giao dịch làm đầu vào và trả về giá trị **true** (đúng) hoặc **false** (sai), quyết định giao dịch có hợp lệ hay không theo các quy tắc đã định.

- Mỗi UTXO được di chuyển sẽ kích hoạt mã xác thực riêng.
- Quá trình thực thi mã xác thực diễn ra trên node Cardano đang xác thực giao dịch đó.

Để kích hoạt mã xác thực, giao dịch đầu tiên cần chuyển một UTXO đến địa chỉ của hợp đồng, địa chỉ này được tạo toán học từ mã hợp đồng. Quá trình này được xem là khởi tạo một phiên bản hợp đồng.

Thành phần Off-Chain

Thành phần off-chain chịu trách nhiệm:

- Tìm các UTXO bị khóa trong hợp đồng.
- Tạo các giao dịch hợp lệ để di chuyển các UTXO này.

Trong các hợp đồng yêu cầu nhiều bước thực hiện, trạng thái của hợp đồng được mã hóa trong **datum** và được đính kèm vào mỗi giao dịch. Mỗi bước trong hợp đồng sẽ thay đổi **datum** để phản ánh trạng thái mới.

Cấu trúc đầu vào của mã xác thực (Redeemer):

Hợp đồng thông minh trên Cardano rất đơn giản về mặt kỹ thuật, chủ yếu dựa trên các mã xác thực (validator script). Các mã này cho phép bạn tạo ra các quy tắc hoặc logic để node Cardano thực thi khi xác nhận giao dịch.

- **Datum:** Dữ liệu gắn với UTXO bị khóa, thường được sử dụng để lưu trữ trạng thái.
- **Redeemer:** Dữ liệu từ giao dịch, cung cấp thông tin cho mã xác thực.
- **Context:** Thông tin về giao dịch, như danh sách chữ ký, giá trị giao dịch, và thời gian hợp lệ.

Mã xác thực sử dụng các thông tin trên để quyết định giao dịch có hợp lệ hay không.

Bảng 3-1: Thông tin có trong Context

Tham số	**Mô tả**
inputs	Các đầu vào để chi tiêu.
reference inputs	Sử dụng các đầu vào làm tham chiếu.
outputs	Tạo các đâu ra mới bằng giao dịch.
fees	Phí giao dịch.
minted value	Giá trị Minted hoặc Burned.
certificates	Các chứng chỉ có trong giao dịch.

withdrawals	Người dùng có thể rút phần thưởng khi ủy thác
valid range	Vùng thời gian có hiệu lực của giao dịch.
signatories	Danh sách chữ ký.
redeemers	Dữ liệu được sử dụng để cung cấp thông tin đầu vào cho tập lệnh từ người chi tiêu.
info data	Mã hàm băm của datum.
id	ID giao dịch.

Quy trình cơ bản của hợp đồng

Lưu ý: Đây chỉ là một ví dụ! Bộ xác thực không nhất thiết phải dựa vào hàm băm - bạn có thể triển khai bất kỳ logic nào bạn muốn.

1. **Thành phần trên chuỗi:**
   Bạn tạo một tập lệnh xác thực (validator-script) để so sánh giá trị datum trong UTXO được di chuyển từ địa chỉ của hợp đồng với giá trị băm của redeemer được sử dụng trong giao dịch đó.
2. **Thành phần ngoài chuỗi:**
   Bạn tạo một tập lệnh, sử dụng ngôn ngữ lập trình mà bạn chọn, để tạo giao dịch chuyển một lượng ADA hoặc tài sản khác đến địa chỉ của tập lệnh xác thực. Khi tạo giao dịch, bạn chỉ định giá trị datum là Hash("secret"), đảm bảo rằng chỉ có giá trị băm của từ "secret" được lưu trữ trên chuỗi.
3. **Ký và gửi giao dịch:**
   Bạn ký và gửi giao dịch này đến một node Cardano, trực tiếp hoặc thông qua một trong nhiều API có sẵn như Blockfrost hoặc Dandelion. Lúc này, lượng ADA bạn gửi vào hợp đồng sẽ bị khóa bởi tập lệnh xác thực.
4. **Quy tắc chi tiêu UTxO trên:**
   Cách duy nhất để chi tiêu UTxO vừa tạo ở bước 3 (di chuyển lượng ADA bị khóa

này) là tạo một giao dịch với từ "secret" làm redeemer, vì UTxO đã bị khóa trong tập lệnh, tập lệnh này sẽ thực thi quy tắc bạn tạo ra, yêu cầu giá trị băm của redeemer phải khớp với Hash("secret").

Thông thường, giá trị datum sẽ phức tạp hơn nhiều, và người sử dụng hợp đồng có thể không biết cách hoạt động cụ thể của nó. Vì vậy, họ sẽ dựa vào thành phần ngoài chuỗi của bạn để tạo giao dịch - điều này thường được bạn cung cấp dưới dạng một API.

Ngôn ngữ lập trình hợp đồng thông minh trên Cardano

Cardano đã giới thiệu hợp đồng thông minh vào năm 2021 và hiện hỗ trợ phát triển và triển khai hợp đồng thông minh bằng nhiều ngôn ngữ khác nhau bao gồm:

1. **Marlowe:**
   Một ngôn ngữ miền chuyên biệt (DSL) tập trung vào hợp đồng tài chính, giúp người dùng dễ dàng tạo các hợp đồng tài chính phức tạp mà không cần kỹ năng lập trình sâu.
2. **Aiken:**
   Ngôn ngữ tối ưu hóa cho việc tạo mã xác thực on-chain, chú trọng trải nghiệm của nhà phát triển.
3. **Opshin:**
   Ngôn ngữ lập trình hợp đồng thông minh dựa trên Python, thân thiện với các nhà phát triển đã quen thuộc với Python.
4. **Plutus:**
   Nền tảng mạnh mẽ cho phép tạo các ứng dụng tương tác với blockchain Cardano.
5. **Plu-ts:**
   Một ngôn ngữ lập trình nhúng trong TypeScript, đồng thời là thư viện hỗ trợ tạo giao dịch.

Để viết một hợp đồng thông minh được thiết kế tốt, trước tiên bạn cần hiểu rõ cách hoạt động của Cardano nói chung. Sau đó, bạn có thể học cách triển khai hợp đồng thông minh bằng các ngôn ngữ được hỗ trợ như đã đề cập.

3.3.6 Quản trị On-Chain trên Cardano

Cardano đang hướng tới mô hình quản trị phi tập trung, khuyến khích sự tham gia của cộng đồng và đảm bảo quá trình ra quyết định hiệu quả. Mô hình này được chi tiết trong CIP-1694, dựa trên cấu trúc ba bên và bảy loại hành động quản trị khác nhau.

Các vai trò chính trong quản trị:

1. **Người nắm giữ ADA:**
    - **Ủy quyền quyền biểu quyết:** Có thể ủy quyền quyền biểu quyết cho các Đại diện Ủy quyền (DReps).
    - **Đăng ký làm DRep:** Có thể đăng ký làm DRep bằng cách khóa một khoản đặt cọc (dRepDeposit).
    - **Đề xuất hành động quản trị:** Cần đặt cọc một khoản (govActionDeposit) để đề xuất các hành động quản trị.
2. **Đại diện Ủy quyền (DReps):**
    - Đề xuất, thảo luận, và biểu quyết các thay đổi giao thức.
    - Quyền biểu quyết dựa trên lượng stake được ủy quyền.
3. **Nhà vận hành Stake Pool (SPOs):**
    - Duy trì hạ tầng mạng và tham gia thảo luận, biểu quyết các thay đổi.
    - Quyền biểu quyết dựa trên lượng stake đang hoạt động.
4. **Ủy ban Hiến pháp (CC):**
    - Đảm bảo các hành động quản trị tuân thủ Hiến pháp Cardano.
    - Cung cấp cân bằng quyền lực và giám sát tính minh bạch, công bằng.

Quy trình ra quyết định:

- **Thảo luận ngoài chuỗi:** Xây dựng đồng thuận trước khi gửi hành động quản trị lên blockchain.
- **Biểu quyết:** Các hành động quản trị được quyết định thông qua biểu quyết của DReps, SPOs, và CC.
- **Thực thi:** Các hành động được thực thi tại ranh giới epoch sau khi được phê duyệt.

Mô hình quản trị này đảm bảo sự minh bạch, công bằng và tính đại diện cao, đồng thời duy trì sự ổn định và phát triển bền vững cho hệ sinh thái Cardano.

Các loại hình quản trị trên Cardano

1. **Bất tín nhiệm:**
    - Đề xuất tạo trạng thái bất tín nhiệm đối với Ủy ban Hiến pháp hiện tại.
2. **Ủy ban Hiến pháp mới và/hoặc Ngưỡng và/hoặc Điều khoản:**

- Thay đổi thành viên Ủy ban Hiến pháp, ngưỡng chữ ký, hoặc các điều khoản liên quan.

3. **Cập nhật Hiến pháp hoặc Chính sách Đề xuất:**
   - Chỉnh sửa Hiến pháp hoặc chính sách đề xuất, được lưu trữ dưới dạng hash trên chuỗi.
4. **Khởi tạo Hard Fork:**
   - Kích hoạt nâng cấp không tương thích ngược của mạng, yêu cầu nâng cấp phần mềm trước đó.
5. **Thay đổi Tham số Giao thức:**
   - Thay đổi các tham số giao thức có thể cập nhật, ngoại trừ thay đổi phiên bản giao thức chính ("hard forks").
6. **Rút Quỹ Ngân Khố:**
   - Rút tiền từ ngân khố Cardano trên chuỗi.
7. **Thông tin:**
   - Ghi nhận thông tin lên chuỗi mà không gây ra bất kỳ tác động trực tiếp nào lên chuỗi.

Các loại hành động này đảm bảo tính linh hoạt và hiệu quả trong việc quản trị hệ sinh thái Cardano.

3.4 Tóm tắt chương và So sánh các thế hệ Blockchain

Thế hệ đầu tiên: Bitcoin – Blockchain đầu tiên

Bitcoin, ra đời vào năm 2009, được coi là thế hệ đầu tiên của công nghệ blockchain. Là hệ thống phi tập trung đầu tiên, Bitcoin sử dụng cơ chế đồng thuận bằng chứng công việc (Proof of Work - PoW) để đảm bảo tính bảo mật và minh bạch trong giao dịch. Tuy nhiên, PoW đòi hỏi một lượng năng lượng khổng lồ để giải quyết các thuật toán phức tạp, dẫn đến chi phí cao và tiêu thụ tài nguyên lớn. Bitcoin chủ yếu tập trung vào việc lưu trữ giá trị và giao dịch tài chính, với khả năng mở rộng hạn chế và năng lập trình hạn chế.

Thế hệ thứ hai: Ethereum – Sức mạnh từ hợp đồng thông minh

Ethereum, ra mắt năm 2015, đánh dấu thế hệ thứ hai của blockchain với khả năng lập trình và hỗ trợ hợp đồng thông minh. Nền tảng này cho phép các nhà phát triển tạo ra các ứng dụng phi tập trung (DApps) trên blockchain, mở rộng tiềm năng ứng dụng ngoài lĩnh vực tài chính. Tuy nhiên, còn có nhiều hạn chế của Bitcoin mà Etherum chưa giải quyết được như, việc sử dụng bằng chứng công việc (Etherum1.0) gây tiêu tốn năng lượng và khả năng mở rộng kém. Khi số lượng giao dịch tăng lên, mạng Ethereum trở nên chậm chạp, với phí giao dịch (gas) cao và trải nghiệm người dùng không ổn định.

Vào tháng 9 năm 2022, Ethereum đã chuyển sang cơ chế bằng chứng cổ phần (Proof of Stake - PoS) như một phần trong lộ trình Ethereum 2.0. Mặc dù đây là một bước tiến quan trọng, Ethereum vẫn đối mặt với nhiều thách thức, như phí gas cao và cơ chế stake phức tạp, điển hình là tính năng cắt giảm (slashing) và sự không chắc chắn về thời gian khóa stake.

Thế hệ thứ ba: Cardano – Xây dựng từ nghiên cứu học thuật

Cardano đại diện cho thế hệ thứ ba của blockchain, được thiết kế để giải quyết những hạn chế của các nền tảng trước đó. Cardano sử dụng bằng chứng cổ phần từ đầu, giúp tiết kiệm năng lượng đáng kể so với PoW. Hệ thống của Cardano được xây dựng dựa trên nghiên cứu học thuật và các bài toán chứng minh toán học, đảm bảo tính bảo mật, khả năng mở rộng và sự bền vững.

Không chỉ khắc phục điểm yếu về năng lượng, Cardano còn được thiết kế với khả năng mở rộng vượt trội và tính tương tác với các blockchain khác. Hơn nữa, Cardano tích hợp sẵn cơ chế quản trị phi tập trung và quỹ ngân sách, tạo điều kiện cho việc phát triển liên tục và thích nghi với các yêu cầu mới trong tương lai. Đây là bước tiến quan trọng giúp Cardano không chỉ lấp đầy những lỗ hổng của Ethereum mà còn đặt nền tảng vững chắc cho sự phát triển của hệ sinh thái blockchain toàn cầu.

So sánh một số đặc điểm của các nền tảng

Đặc điểm	**Bitcoin**	**Ethereum**	**Cardano**
Cơ chế đồng thuận	PoW	PoS (Ethereum 2.0)	PoS (Ouroboros)
Trạng thái Token Stake	Không	Khóa Token	Không khóa Token
Mô hình sổ cái	UTxO	Accounting	EUTxO
Tốc độ giao dịch	7 TPS	~20 TPS	250+ TPS
Thời gian Block	10 phút	12 giây	20 giây

Chi phí giao dịch	Cao, thay đổi	Phí gas cao hơn, thay đổi	Phí thấp hơn, có thể dự đoán được
Hợp đồng thông minh	Không có	Trưởng thành, được áp dụng rộng rãi	Mới phát triển, tập trung vào bảo mật
Hệ sinh thái phát triển	Đơn giản	Lớn, đa dạng	Đang phát triển, tập trung vào các ứng dụng thực tế
Phương pháp tiếp cận phát triển	Phát triển bảo thủ tập trung vào an ninh	Phát triển năng động với các nâng cấp liên tục	Đánh giá ngang hàng và phát triển dựa trên nghiên cứu
Quản trị On-chain	Không	Không	Có

Câu hỏi và bài tập

1. Bitcoin được tạo ra bởi ai và mục tiêu ban đầu của nó là gì?
2. Giao dịch Bitcoin được xác thực và thêm vào blockchain như thế nào?
3. Điều gì đảm bảo rằng giao dịch Bitcoin là không thể thay đổi và minh bạch?
4. Sự khác biệt giữa khóa công khai và khóa bí mật là gì? Vai trò của chúng trong bảo mật giao dịch Bitcoin?
5. Địa chỉ Bitcoin được tạo ra như thế nào từ khóa công khai?
6. Ví Bitcoin là gì, và có những loại ví nào? Ưu và nhược điểm của từng loại?
7. Vai trò của các node và thợ đào trong mạng lưới Bitcoin là gì?
8. Bitcoin đã thay đổi cách chúng ta nhìn nhận tiền tệ và giao dịch tài chính như thế nào?
9. Những thách thức chính mà Bitcoin phải đối mặt là gì? (ví dụ: tiêu thụ năng lượng, khả năng mở rộng)
10. Bitcoin khác biệt như thế nào so với các hệ thống tài chính truyền thống về tính minh bạch, bảo mật, và phân quyền?
11. Cardano ra đời trong bối cảnh nào, và những vấn đề nào của blockchain thế hệ trước mà nó muốn giải quyết?
12. Giai đoạn khởi động (2015-2017) của Cardano đã đạt được những cột mốc quan trọng nào?
13. Lộ trình phát triển của Cardano được chia thành những giai đoạn nào, và mục tiêu chính của mỗi giai đoạn là gì?
14. Tầm nhìn tương lai của Cardano là gì, và nó có tác động như thế nào đến hệ sinh thái blockchain?
15. Kiến trúc của Blockchain Cardano được chia thành những lớp nào, và vai trò của từng lớp là gì?
16. Cơ chế đồng thuận Ouroboros của Cardano hoạt động như thế nào để đảm bảo tính bảo mật và phân quyền?
17. Mô hình UTxO khác biệt như thế nào so với mô hình dựa trên tài khoản?
18. Lợi ích chính của mô hình EUTxO của Cardano là gì, và tại sao nó phù hợp cho hợp đồng thông minh?
19. Các thành phần cơ bản của EUTxO bao gồm những gì, và vai trò của chúng trong giao dịch?
20. Khóa trong Cardano được sử dụng như thế nào để đảm bảo tính bảo mật và xác thực giao dịch?

21. Địa chỉ thanh toán và địa chỉ stake khác nhau như thế nào, và vai trò của chúng trong hệ sinh thái Cardano?
22. Hợp đồng thông minh trên Cardano hoạt động như thế nào trong mô hình EUTxO?
23. Những điểm khác biệt chính giữa hợp đồng thông minh trên Cardano và các blockchain khác là gì?
24. Các vai trò chính trong quản trị On-Chain của Cardano là gì, và mỗi vai trò có trách nhiệm gì?
25. Quy trình ra quyết định trong quản trị On-Chain của Cardano diễn ra như thế nào?
26. Các loại hành động quản trị trên Cardano bao gồm những gì, và mỗi loại có mục đích gì?

CHƯƠNG 4: CÁC THUẬT TOÁN ĐỒNG THUẬN BLOCKCHAIN

4.1. THUẬT TOÁN ĐỒNG THUẬN

4.1.1. Khái niệm

Thuật toán đồng thuận blockchain là tập hợp các quy tắc và cơ chế mà các nút trong mạng blockchain sử dụng để xác nhận và thống nhất về tính hợp lệ của các giao dịch/khối mới, là cơ chế giúp đảm bảo tất cả các nút trong mạng đồng ý với trạng thái hiện tại của sổ cái kỹ thuật số, từ đó đảm bảo tính toàn vẹn và độ tin cậy cũng như duy trì sự ổn định và an toàn cho hệ thống phân tán blockchain mà không cần đến bất kỳ một bên trung gian nào.

4.1.2. Cơ chế hoạt động của thuật toán đồng thuận

Cơ chế đồng thuận trong blockchain hoạt động dựa trên nguyên tắc đồng thuận giữa các nút (nodes) trong mạng. Các nút trong mạng thực hiện các công việc cụ thể như xác minh giao dịch, đề xuất khối mới, và bỏ phiếu, nhằm mục đích chính là đảm bảo tất cả các nút đồng ý với trạng thái hiện tại của sổ cái (ledger) và xác nhận tính hợp lệ của các giao dịch mới trước khi chúng được thêm vào blockchain. Cách thức hoạt động của cơ chế đồng thuận gồm các công việc sau:

- Gửi giao dịch: Khi một giao dịch được tạo ra, nó được gửi đến mạng blockchain thông qua một nút mạng nào đó, từ đó lan truyền giao dịch này đến toàn bộ mạng.

- Xác nhận giao dịch: Các nút trong mạng (miners hoặc validator) ghi nhận giao dịch và bắt đầu quá trình xác nhận. Hệ thống sẽ kiểm tra xem giao dịch có hợp lệ không? Chẳng hạn như người gửi có đủ số dư không, giao dịch có đúng định dạng không, ...

- Đồng thuận: Để đạt được đồng thuận giữa các nút trong mạng, một mạng blockchain sử dụng một thuật toán cụ thể. Mỗi blockchain có thể sử dụng một thuật toán khác nhau. Một số thuật toán thường sử dụng như:

- Bằng chứng công việc (PoW - Proof of Work)
- Bằng chứng cổ phần (PoS - Proof of Stake)
- Bằng chứng cổ phần được ủy quyền (DPoS - Delegated Proof-of-Stake)
- Bằng chứng về trọng số (PoWeight - Proof-of-Weight)
- Bằng chứng lịch sử (PoH - Proof of History)
- Bằng chứng về quyền hạn (PoA - Proof-of-Authority)
- Bằng chứng dung lượng (PoC - Proof of Capacity)

…

- Thêm khối vào blockchain: Khi giao dịch đã được xác nhận và đồng thuận, khối mới chứa giao dịch đó được thêm vào chuỗi. Khối này liên kết với khối trước đó thông qua một chuỗi mã hash, tạo thành một chuỗi liên tục không thể thay đổi.

- Cập nhật và phát tán: Sau khi khối mới được thêm vào, thông tin được cập nhật và phát tán đến tất cả các nút trong mạng. Điều này đảm bảo rằng mọi nút đều có bản sao giống nhau của blockchain, duy trì tính nhất quán và đảm bảo tính minh bạch.

4.1.3. Các yêu cầu của một thuật toán đồng thuận Blockchain

Thuật toán đồng thuận trong blockchain được sử dụng để xác nhận và thống nhất về tính hợp lệ của các giao dịch hoặc khối mới. Thuật toán đồng thuận trong blockchain phải đáp ứng các yêu cầu cơ bản để đảm bảo mạng lưới hoạt động ổn định, an toàn, bảo mật và hiệu quả. Do đó nó phải đạt được một số yêu cầu chính sau đây:

1. *Tính nhất quán (Consistency):* Tất cả các nút trong mạng phải đồng ý về trạng thái của blockchain. Dữ liệu trong blockchain phải nhất quán trên toàn bộ mạng lưới.

2. *Tính toàn vẹn (Integrity)*: Chỉ các giao dịch hợp lệ mới được thêm vào blockchain. Mỗi khối phải tuân thủ các quy tắc đã được định nghĩa bởi giao thức. Giao dịch không thể bị chỉnh sửa hoặc thêm lại sau khi đã được ghi vào blockchain.

3. *Tính phi tập trung (Decentralization):* Quy trình đồng thuận không phụ thuộc vào một thực thể trung tâm. Bất kỳ nút nào cũng có thể tham gia xác thực mà không cần xin phép. Điều này đảm bảo tính minh bạch và loại bỏ các rủi ro từ một điểm thất bại duy nhất (single point of failure).

4. *Khả năng chịu lỗi Byzantine (Byzantine Fault Tolerance - BFT):* Hệ thống phải hoạt động chính xác ngay cả khi một số nút trong mạng gặp lỗi hoặc có hành vi gian lận. Thuật toán đồng thuận cần có khả năng đối phó với các tấn công từ các nút không trung thực.

Vấn đề này xuất phát từ một tình huống trong quân đội thời La mã, tướng Byzantine chỉ quy một nhóm tướng lĩnh của quân đội, các tướng lĩnh này chỉ huy các đội quân đóng ở các vị trí khác nhau xung quanh một thành phố của kẻ thù. Họ giao tiếp với nhau thông qua người đưa tin, các tướng lĩnh phải đồng thuận về một kế hoạch chiến đấu chung. Tuy nhiên, một hoặc nhiều tướng lĩnh có thể là những kẻ phản bội, cố gắng gây nhầm lẫn cho những người khác về kế hoạch chung. Vấn đề đặt ra là tìm một thuật toán đảm bảo rằng các tướng lĩnh trung thành có thể đạt được sự đồng thuận.

5. *Tính bảo mật (Security):* Blockchain phải được bảo vệ khỏi các cuộc tấn công như:

- Double-spending: Chi tiêu một lượng Tokehai lần,
- 51% Attack: Khi một thực thể kiểm soát hơn 50% sức mạnh mạng.

Thuật toán đồng thuận phải đảm bảo rằng không kẻ tấn công nào có thể sửa đổi chuỗi khối hoặc thay đổi trạng thái giao dịch.

6. *Hiệu suất (Performance):* Thuật toán đồng thuận phải có khả năng xử lý nhanh chóng và hiệu quả với số lượng lớn giao dịch. Thời gian xác nhận giao dịch và tạo khối phải được tối ưu để đảm bảo trải nghiệm người dùng.

7. *Khả năng mở rộng (Scalability)*: Hệ thống cần hỗ trợ số lượng nút tham gia ngày càng lớn mà không ảnh hưởng đến hiệu suất. Blockchain phải xử lý khối lượng giao dịch tăng dần mà vẫn duy trì tốc độ và bảo mật.

8. *Tính công bằng (Fairness)*: Mỗi nút phải có cơ hội công bằng để tham gia vào quá trình xác thực và thêm khối mới. Các nút không bị loại trừ hoặc ưu ái dựa trên vị trí địa lý hoặc tài nguyên sở hữu (trừ khi được quy định rõ ràng như PoS).

9. *Tính không thể đảo ngược (Finality)*: Một khi giao dịch đã được xác nhận, nó không thể bị hoàn tác hoặc thay đổi. Điều này đảm bảo tính toàn vẹn và bảo mật của blockchain.

10. *Tiết kiệm năng lượng (Energy Efficiency)*: Đặc biệt quan trọng đối với các thuật toán đồng thuận thế hệ mới (PoS, PoC). Thuật toán nên giảm thiểu tiêu thụ năng lượng mà vẫn đảm bảo tính bảo mật và hiệu quả.

Như vậy: *Một thuật toán đồng thuận trong blockchain cần đảm bảo: tính nhất quán, bảo mật, phi tập trung, hiệu suất cao, khả năng mở rộng, và khả năng chịu lỗi Byzantine. Tùy thuộc vào ứng dụng và mục tiêu, các blockchain có thể ưu tiên một số yếu tố nhất định để tối ưu hóa hiệu quả hoạt động*.

4.2. HỆ THỐNG CHỊU LỖI BYZANTINE (BFT)

Cũng giống như hầu hết các hệ thống tính toán phân tán, những người tham gia mạng lưới tiền điện tử cần phải đồng ý về trạng thái hiện tại của blockchain, và đó là cái mà chúng ta gọi là sự đồng thuận. Tuy nhiên, việc đạt được sự đồng thuận trên mạng lưới phân tán một cách an toàn và đáng tin cậy không phải là một điều dễ dàng. Vậy thì làm thế nào một mạng lưới phân tán gồm các nút máy tính đạt được sự đồng thuận khi xử lý một quyết định, nếu một số nút trong đó có khả năng là nút không đáng tin? Đây là câu hỏi cơ bản của vấn đề được gọi là bài toán các vị tướng Byzantine, từ đó sinh ra khái niệm về hệ thống chịu lỗi Byzantine.

Bài toán các vị tướng Byzantine được các nhà khoa học máy tính Leslie Lamport, Robert Shostak và Marshall Pease đề xuất trong một bài báo khoa học mang tên "The Byzantine Generals Problem" vào năm 1982 [3]. Bài toán này mô tả vấn đề đạt được **sự đồng thuận** trong một hệ thống phân tán, ngay cả khi một số thành phần trong hệ thống không hoạt động đúng hoặc cố tình đưa ra thông tin sai lệch. Trong [3] các tác giả đã chỉ ra rằng để giải quyết Bài toán các vị tướng Byzantine trong đó có m tướng phản bội, muốn đạt được đồng thuận thì toàn bộ quân đội cần phải có ít nhất $3m + 1$ vị tướng bao gồm cả trung thành và phản bội. Hay nói cách khác là phải có ít nhất $\frac{2}{3}$ số tướng trung thành.

Bài toán được diễn đạt một cách ẩn dụ bằng tình huống của một đội quân Byzantine (quân đội đế quốc La Mã), tiến hành vây hãm một thành phố. Các vị tướng cần trao đổi để đạt được đến một thoả thuận về một kế hoạch. Trong trường hợp đơn giản nhất, họ thoả thuận về kế hoạch **tấn công** hay **rút lui**.

Vấn đề tấn công hay rút lui không quan trọng mà là sự đồng thuận của tất cả các tướng, tức là, đồng thuận về một quyết định chung để cùng phối hợp thực hiện. Do đó, chúng ta có thể xem xét các mục tiêu sau:

- Mỗi tướng phải quyết định: tấn công hoặc rút lui (có hay không);
- Không thể thay đổi quyết định sau khi đưa ra;
- Tất cả tướng phải nhất trí về một quyết định giống nhau và tiến hành đồng bộ với nhau.

Các vấn đề liên lạc như đề cập ở trên liên quan đến thực tế là một tướng chỉ có thể giao tiếp với các tướng khác thông qua các thông điệp được chuyển đi bởi lính đưa tin. Vấn đề trọng tâm của bài toán các vị tướng Byzantine ở đây là các thông điệp có thể bị chậm, hủy hoặc mất. Ngoài ra, ngay cả khi thông điệp được gửi thành công, vẫn còn khả năng xảy ra một hoặc nhiều tướng có thể chọn thực hiện hành động gây hại và gửi đi một thông điệp sai để gây nhiễu tới các tướng khác, dẫn đến một thất bại hoàn toàn.

Nếu chúng ta áp dụng bài toán này vào trường hợp có sự xuất hiện của blockchain, mỗi tướng sẽ đại diện cho một nút mạng và các nút cần đạt được sự đồng thuận về trạng thái hiện tại của hệ thống. Nói cách khác, phần lớn những người tham gia trong một mạng lưới phân tán phải đồng ý và thực hiện cùng một hành động để tránh một thất bại hoàn toàn.

Cơ chế hoạt động của hệ thống chịu lỗi Byzantine

Cơ chế hoạt động của BFT là dựa trên sự đồng thuận và phân tách thông tin. Khi và chỉ khi các phần tử trong hệ thống đều đạt được sự đồng thuận thì một giao dịch hay một quyết định mới được thực hiện. Và để đạt được sự đồng thuận không phải là một câu chuyện dễ dàng. BFT phải sử dụng một số thuật toán phức tạp hơn, điều này nhằm đảm bảo tất cả các thành phần trong cùng một hệ thống sẽ thống nhất được thông tin chính xác nhất trước khi đưa ra kết quả cuối cùng.

Điểm quan trọng ở đây là sự phân tách thông tin trong hệ thống. Hệ thống không cần phải đạt được tất cả sự đồng thuận mà chỉ cần một phần nào đó là được. Mục đích của hành động này cũng nhằm ngăn chặn các sự gian lận của một số phần tử. Một khía cạnh quan trọng khác trong cơ chế hoạt động của BFT là việc phân bổ công việc và trách nhiệm cho các nút. Mỗi nút trong mạng lưới có thể được giao một phần công việc cụ thể để đảm bảo rằng không có nút nào có quyền kiểm soát quá nhiều thông tin hoặc ảnh hưởng quá lớn đến quyết định

chung. Sự phân bổ này giúp giảm thiểu rủi ro từ các nút độc hại và đảm bảo rằng ngay cả khi một số nút bị chiếm quyền điều khiển.

BFT cung cấp một lớp bảo mật và độ tin cậy cao, do đó việc triển khai và duy trì các hệ thống chịu lỗi này có nhiều thách thức. Những thách thức này đòi hỏi sự cân nhắc kỹ lưỡng và sự phát triển liên tục để đảm bảo rằng các hệ thống BFT có thể đáp ứng được yêu cầu của môi trường hoạt động thực tế.

Mô hình BFT là một trong những nền tảng cốt lõi để xây dựng các hệ thống blockchain an toàn và phi tập trung. Nhiều dự án blockchain hiện đại đã tích hợp hoặc phát triển các biến thể của mô hình này nhằm đảm bảo tính toàn vẹn, bảo mật và hiệu suất cao hơn.

Nói tóm lại, hệ thống chịu lỗi Byzantine là hệ thống có thể giải quyết được vấn đề của bài toán các vị tướng Byzantine. Điều này có nghĩa là hệ thống BFT có thể tiếp tục hoạt động ngay cả khi một số nút bị lỗi hoặc thực hiện hành động gây hại. Có nhiều giải pháp khả thi cho vấn đề của bài toán các vị tướng Byzantine. Do đó, có nhiều cách để xây dựng một hệ thống BFT. Tương tự như vậy, có nhiều cách khác nhau để một blockchain đạt được hệ thống chịu lỗi Byzantine và điều mà chúng ta có ở đây chính là các thuật toán đồng thuận. Trong các phần tiếp theo trình bày một số thuật toán đồng thuận đã được triển khai trong thực tế trong các mạng blockchain.

4.3. THUẬT TOÁN BẰNG CHỨNG CÔNG VIỆC

Thuật toán Bằng chứng công việc (Proof of Work - PoW), nguyên tắc chính của thuật toán này là các nút mạng phải giải một bài toán mật mã phức tạp để tìm ra một hàm băm hợp lệ thỏa mãn điều kiện đã cho. Nó đòi hỏi các nút phải mất chi phí tính toán (làm việc - work) rất lớn. Một số mạng sử dụng thuật toán này như là Bitcoin, Ethereum 1.0, …

4.3.1. Lịch sử phát triển của thuật toán bằng chứng công việc

Vào năm 1999, trong [4] Markus Jakobsson và Ari Juels đề xuất sáng kiến Bằng chứng công việc, đánh dấu một bước ngoặt quan trọng trong lĩnh vực tiền điện tử. Đây là một cách thức mới để xác thực giao dịch trên mạng lưới blockchain phi tập trung. Ý tưởng ban đầu được thực hiện để xây dựng một hệ thống hoạt động trên nền tảng mạng P2P vốn có. Jakobsson và Juels đã sử dụng kết hợp phương pháp băm (hashing) và Bằng chứng công việc để đạt được sự đồng thuận phi tập trung giữa các nút về thứ tự giao dịch. Hệ thống này được gọi là "Bằng chứng công việc". Ý tưởng này xuất phát từ mong muốn phi tập trung hóa quá trình xác thực giao dịch một cách tối đa. Điều này có nghĩa là mọi người tham gia đều có thể xác nhận giao dịch một cách hiệu quả mà không cần truy cập bất kỳ cơ sở dữ liệu trung tâm nào. Ý tưởng sau đó được tinh chỉnh và triển khai trên mạng Bitcoin. Trên mạng lưới Bitcoin, thợ đào cần giải một bài toán toán học phức tạp trước khi thêm giao dịch vào blockchain và nhận phần thưởng. Bài toán được thiết kế để tốn rất nhiều sức mạnh tính toán, khiến cho việc một cá nhân đơn độc

kiểm soát quá trình đào coin trở nên rất khó khăn. Điều này ngăn chặn một cá nhân chiếm đa số sức mạnh và kiểm soát giao dịch.

4.3.2. Cơ chế hoạt động của PoW

Bước 1: Tạo khối mới

Một nút trong mạng (thợ đào - miner) chuẩn bị một khối mới để thêm vào blockchain. Khối mới chứa các thành phần chính:

- Danh sách các giao dịch hợp lệ đã được xác thực.
- Mã hash của khối trước để liên kết với khối trước đó trong chuỗi.
- Nonce: Một số ngẫu nhiên sẽ được tìm kiếm để giải bài toán băm.
- Thông tin metadata: Bao gồm thời gian khối và thông tin khác.

Bước 2: Giải bài toán băm

Mỗi thợ đào thực hiện hàng triệu phép tính băm để tìm giá trị nonce sao cho hàm băm của khối thỏa mãn yêu cầu độ khó (số lượng chữ số 0 nhất định ở đầu chuỗi băm).

Ví dụ: Nếu độ khó là 4, hàm băm phải có dạng 0000abcd1234ef....

Đây là bước tiêu tốn tài nguyên tính toán vì cần thử nhiều giá trị nonce cho đến khi tìm được kết quả theo yêu cầu.

Bước 3: Phát tán kết quả

Thợ đào đầu tiên tìm được giá trị nonce hợp lệ sẽ gửi (broadcast) kết quả cho toàn bộ các nút trong mạng. Thông tin phát tán bao gồm:

- Dữ liệu của khối.
- Nonce đã tìm được.
- Kết quả hàm băm của khối.

Bước 4: Xác minh khối

Các nút khác trong mạng nhận thông tin và tiến hành kiểm tra tính hợp lệ của khối:

- Kiểm tra xem hàm băm có đúng định dạng yêu cầu (có đủ số chữ số 0 ở đầu) hay không.
- Kiểm tra tính đúng đắn của các giao dịch trong khối để đảm bảo không có gian lận như double-spending (chi tiêu hai lần).

Nếu khối hợp lệ, các nút sẽ thêm khối đó vào chuỗi blockchain của mình.

Bước 5: Thêm khối vào blockchain

Sau khi được xác minh, khối được thêm vào chuỗi blockchain. Chuỗi blockchain sẽ tiếp tục phát triển từ khối mới này như một phần mở rộng của chuỗi chính.

Bước 6: Nhận phần thưởng

Thợ đào giải thành công bài toán sẽ nhận được:

- Phần thưởng khối: Một lượng coin mới được sinh ra từ giao thức.
- Phí giao dịch: Tổng phí từ các giao dịch được chứa trong khối.

Bước 7: Điều chỉnh độ khó

Mạng blockchain tự động điều chỉnh độ khó để duy trì thời gian tạo khối trung bình ổn định.

Ví dụ: Trong mạng Bitcoin, độ khó được điều chỉnh sau mỗi 2016 khối (~2 tuần), nhằm duy trì thời gian tạo khối trung bình là 10 phút.

4.3.3. Cơ chế đồng thuận trong mạng Bitcoin

Bước 1: Tạo khối mới

Sau khi xác thực giao dịch, một nút bitcoin sẽ thêm chúng vào danh sách giao dịch (memory pool) các giao dịch này chờ cho đến khi chúng được đưa vào để tạo thành một khối (block). Giả sử hiện tại (thời điểm viết giáo trình này) một nút **X** đã lắp ráp được một chuỗi lên đến khối 878.903. Nút **X** đang lắng nghe các giao dịch, cố gắng khai thác một khối mới đồng thời lắng nghe các khối được các nút khác phát hiện. Khi nút của **X** đang khai thác thì nhận được khối 878.904 thông qua mạng bitcoin. Sự xuất hiện của khối này báo hiệu sự kết thúc của cuộc cạnh tranh cho khối 878.904 và bắt đầu của cuộc cạnh tranh để tạo ra khối 878.905.

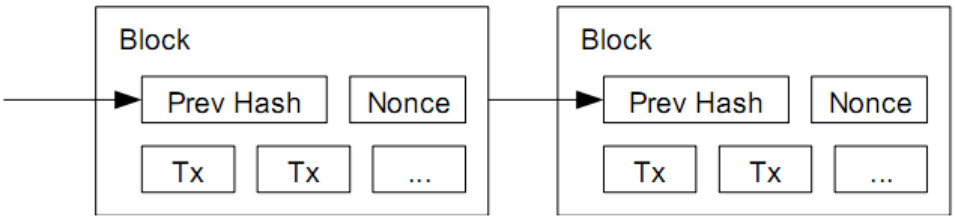
Trong 10 phút trước đó, khi nút **X** đang tìm kiếm giải pháp cho khối 878.904, nó đồng thời thu thập các giao dịch để chuẩn bị cho khối tiếp theo. Đến thời điểm này, nút đã thu thập được vài trăm giao dịch trong memory pool. Khi nhận được khối 878.904 và xác thực thành công, nút **X** sẽ so sánh các giao dịch trong khối đó với tất cả các giao dịch trong memory pool và loại bỏ những giao dịch đã được đưa vào khối 878.904. Những giao dịch còn lại trong memory pool là các giao dịch chưa được xác nhận và đang chờ được ghi vào một khối mới (khối thứ 878.905).

Nút **X** sẽ tạo một khối trống mới, khối thứ 878.905. Khối này được gọi là khối ứng viên (candidate block), vì nó chưa phải là khối hợp lệ do chưa có bằng chứng công việc hợp lệ. Khối này chỉ trở thành hợp lệ nếu thợ đào thành công trong việc tìm ra giải pháp cho thuật toán PoW.

Lưu ý giao dịch đầu tiên trong bất kỳ khối nào, là một giao dịch đặc biệt, được gọi là giao dịch coinbase. Giao dịch này được tạo bởi nút **X** và chứa phần thưởng cho người sở hữu nút **X** nếu khai thác khối thành công. Nút **X** tạo giao dịch coinbase như một khoản thanh toán

vào ví của người sở hữu **X**. Giao dịch này thực hiện chuyển đến địa chỉ ví của **X** số tiền bằng tiền thưởng (hiện tại là 3,125 BTC) + phí giao dịch.

Khác với các giao dịch thông thường, giao dịch coinbase không sử dụng UTXO (đầu ra chưa được chi tiêu) làm đầu vào. Thay vào đó, nó chỉ có một đầu vào duy nhất, gọi là coinbase, tạo ra bitcoin từ "Nothing". Giao dịch coinbase có một đầu ra, là khoản thanh toán đến địa chỉ ví bitcoin của thợ đào.



Hình 4.1. Minh họa cấu trúc các khối trong blockchain

Tạo Block Header

Một Block header sẽ không chứa giao dịch nào và có kích thước 80 bytes. Gồm các trường thông tin:

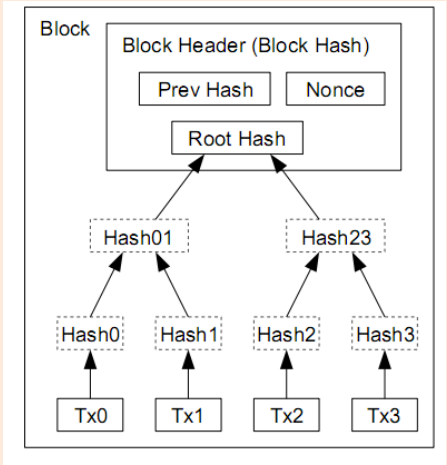
Kích thước	Trường	Mô tả
4 bytes	Phiên bản (Version)	Số phiên bản dùng để theo dõi các bản nâng cấp phần mềm/giao thức.
32 bytes	Mã hash khối trước (Previous Block Hash)	Tham chiếu đến mã hash của khối trước đó (khối cha) trong chuỗi.
32 bytes	Gốc cây Merkle (Merkle root)	Mã hash của gốc cây Merkle chứa các giao dịch của toàn bộ khối
4 bytes	Dấu thời gian (Timestamp)	Thời gian tạo khối (tính bằng giây kể từ Unix Epoch).
4 bytes	Độ khó (Target)	Mục tiêu của thuật toán PoW cho khối này.

4 bytes	Nonce	Bộ đếm được sử dụng trong thuật toán PoW

Trường đầu tiên mô tả số phiên bản của khối được lưu trong 4 bytes, tại thời điểm khối 878.903 được khai thác, số phiên bản của khối là 0x2710e000. Mô tả mã hash của khối trước đó bằng 32 bytes, mã hash của khối trước của khối 878.903 là:

00000000000000000001d043b2c9bd7f4bb4e41b1730381b87da0cae7b0343c2

Tiếp theo là 32 bytes mô tả mã hash của gốc cây Merkle. Cây Merkle là cây mô tả mã hash của các giao dịch trong khối. Cây Merkle được xây dựng như sau: lá của cây là các giao dịch, lưu ý giao dịch coinbase được liệt kê đầu tiên, tiếp theo là các giao dịch được thêm vào khối. Thực hiện tính mã hash của mỗi giao dịch (lá), được các nút cha của các lá, tiếp theo kết hợp 2 mã hash của 2 giao dịch liền kề để được mã hash cha của 2 mã hash đó, cứ làm như vậy cho đến khi ta thu được mã hash của nút gốc. Xem mô tả cây Merkle trong hình 4.2 dưới đây.



Hình 4.2. Cấu trúc cây Merkle

Dấu thời gian của nút được mô tả trong 4 bytes, được mã hóa dưới dạng thời gian epoch Unix, dựa trên số giây đã trôi qua kể từ nửa đêm ngày 1 tháng 1 năm 1970 theo giờ UTC/GMT. Độ khó (target) của thuật toán PoW được lưu trong 4 bytes và cuối cùng là số nonce, ban đầu được khởi tạo bằng 0. Sau khi tất cả các trường khác đã được điền đầy đủ, block header đã hoàn chỉnh và quá trình khai thác được bắt đầu. Mục tiêu lúc này là tìm một giá trị nonce sao cho mã hash của block header nhỏ hơn giá trị mục tiêu (target). Nút khai thác thực hiện bước 2.

Bước 2: Giải bài toán băm (khai thác)

Sau khi khối ứng viên được tạo bởi nút **X**, nó sẽ thực hiện khai thác khối này nhằm tìm ra lời giải cho thuật toán PoW để làm cho khối trở nên hợp lệ. Tức là lúc này này nút **X** phải đi tìm một giá trị nonce sao cho mã hash của block header nhỏ hơn giá trị mục tiêu.

Nói một cách đơn giản, khai thác là quá trình băm đi băm lại block header, với sự thay đổi một tham số duy nhất đó là số nonce cho đến khi giá trị mã hash kết quả thỏa mãn mục tiêu đã đề ra. Kết quả của hàm băm không thể được xác định trước, cũng như không thể tạo ra một mẫu có thể sinh ra một giá trị hash cụ thể. Tính chất này của hàm băm dẫn tới cách duy nhất là để tạo ra một kết quả mã hash khớp với mục tiêu thì chúng ta phải thử đi thử lại nhiều lần bằng cách thay đổi ngẫu nhiên đầu vào cho đến khi tìm được mã hash mong muốn.

Một thuật toán băm nhận dữ liệu đầu vào tùy ý và tạo ra một kết quả đầu ra có độ dài cố định. Thuật toán băm như vậy được gọi là **dấu vân tay số** của dữ liệu đầu vào. Đối với một đầu vào cụ thể, kết quả băm sẽ luôn giống nhau và có thể dễ dàng tính toán cũng như xác minh bởi bất kỳ ai sử dụng cùng thuật toán băm. Với thuật toán băm SHA256, đầu ra luôn có độ dài 256 bit, bất kể kích thước của dữ liệu đầu vào.

Trong mạng bitcoin sử dụng hàm băm SHA256 để tìm giá trị mã hash của Block header nhỏ hơn mục tiêu được thiết lập của mạng. Quá trình tìm giá trị nonce để tạo ra mã hash của Block header thỏa mãn sẽ mất rất nhiều công sức. Do đó, nó được gọi là bằng chứng công việc (PoW).

Như vậy PoW phải tạo ra một giá trị hash nhỏ hơn mục tiêu. Mục tiêu càng cao thì việc tìm một giá trị hash nhỏ hơn mục tiêu càng dễ dàng. Ngược lại, mục tiêu càng nhỏ thì việc tìm một giá trị hash nhỏ hơn mục tiêu càng khó.

Bước 3: Phát tán kết quả

Khi giá trị nonce được tìm thấy và được ghi vào block header, nó tạo ra giá trị hash của block header này. Ngay lập tức, nút **X** truyền khối này đến tất cả các nút ngang hàng của nó. Các nút đó nhận khối, xác thực, và sau đó tiếp tục lan truyền khối mới này tới các nút khác. Khi khối được lan truyền khắp mạng lưới, mỗi nút thêm khối vào bản sao blockchain của riêng mình, tăng chiều cao khối mới là 878.905. Khi các nút khai thác nhận và xác thực khối này, chúng sẽ từ bỏ việc tìm kiếm khối ở cùng chiều cao và ngay lập tức bắt đầu tính toán khối tiếp theo trong chuỗi bằng cách sử dụng khối được tạo ra bởi nút **X** làm "khối cha". Các thợ đào đưa khối của nút **X** đào được vào blockchain của mình là đã "bỏ phiếu" cho khối của **X** và chuỗi mà nó mở rộng.

Bước 4: Xác minh khối

Khi khối mới tìm được một nút trong mạng tìm được số nonce sao cho mã hash của của block header thỏa mãn độ khó nó được lan truyền qua mạng, mỗi nút nhận được khối này sẽ thực hiện một loạt các kiểm tra để xác thực khối đó trước khi tiếp tục lan truyền đến các nút khác. Điều này đảm bảo rằng chỉ các khối hợp lệ mới được lan truyền trong mạng lưới.

Việc xác thực độc lập này đảm bảo rằng các thợ đào hành động trung thực thì các khối của họ sẽ được thêm vào blockchain, từ đó nhận được phần thưởng. Ngược lại, những thợ đào hành động không trung thực khối của họ sẽ bị từ chối và không chỉ mất phần thưởng mà còn

lãng phí công sức và chi phí điện năng đã bỏ ra để tìm kiếm lời giải cho PoW mà không được bù đắp.

Khi một nút nhận được một khối mới, nó sẽ xác thực khối đó bằng cách kiểm tra dựa trên một danh sách các tiêu chí cần phải đáp ứng; nếu không, khối sẽ bị từ chối. Các tiêu chí này có thể được xem trong mã nguồn của **Bitcoin Core Client** qua các hàm CheckBlock và CheckBlockHeader, bao gồm:

- Cấu trúc dữ liệu của khối phải hợp lệ về mặt cú pháp.
- Giá trị hash của block header phải nhỏ hơn mục tiêu.
- Dấu thời gian của khối không được vượt quá 2 giờ so với thời gian hiện tại.
- Kích thước của khối phải nằm trong giới hạn cho phép.
- Giao dịch đầu tiên (và chỉ giao dịch đầu tiên) phải là giao dịch coinbase.
- Tất cả các giao dịch trong khối phải hợp lệ.

Việc xác thực độc lập mỗi khối mới bởi tất cả các nút trong mạng lưới đảm bảo rằng thợ đào không thể gian lận. Trong các phần trước, chúng ta đã thấy rằng thợ đào có quyền tạo một giao dịch để nhận phần thưởng bitcoin mới được tạo ra trong khối đồng thời thu phí giao dịch.

Vậy tại sao thợ đào không tự tạo cho mình một giao dịch với phần thưởng lên đến một nghìn bitcoin thay vì phần thưởng đúng quy định? Bởi vì mọi nút trong mạng đều xác thực các khối theo cùng một quy tắc chung. Một giao dịch coinbase không hợp lệ sẽ khiến toàn bộ khối trở nên không hợp lệ, dẫn đến khối đó sẽ bị từ chối và giao dịch sẽ không bao giờ được ghi vào blockchain. Thợ đào buộc phải xây dựng một khối hoàn hảo dựa trên các quy tắc chung mà tất cả các nút phải tuân theo và khai thác khối đó với một lời giải PoW hợp lệ. Để làm được điều này, họ phải tiêu tốn rất nhiều điện năng trong quá trình khai thác. Nếu gian lận, tất cả công sức và chi phí điện năng sẽ bị lãng phí. Đó là lý do tại sao quá trình xác thực độc lập là một thành phần quan trọng trong cơ chế đồng thuận phi tập trung.

Bước 5: Thêm khối vào blockchain

Bước cuối cùng trong cơ chế đồng thuận phi tập trung của Bitcoin là lắp ráp các khối thành chuỗi.

Mỗi nút trong mạng Bitcoin duy trì ba tập hợp khối:

1. Các khối được kết nối với nhau tạo thành chuỗi chính (main blockchain).
2. Các khối tạo thành các nhánh rẽ (fork) ra từ chuỗi chính (secondary chains).
3. Các khối không có "khối cha" đã biết trong các chuỗi hiện tại (orphans – khối mồ côi hoặc stale block - khối lạc).

Khi một nút nhận được một khối mới và nó đã xác thực thành công, nó sẽ cố gắng lắp ráp vào **chuỗi chính,** tức là chuỗi có tổng công sức PoW lớn nhất. Trong hầu hết các trường hợp, đây là chuỗi có nhiều khối nhất (dài nhất tính theo số khối), trừ khi có hai chuỗi dài bằng nhau nhưng một chuỗi có tổng công sức PoW lớn hơn.

Tổng công sức PoW của một chuỗi là tổng lượng công việc (work) mà các thợ đào đã bỏ ra để tạo ra tất cả các khối trong chuỗi đó, được đo bằng tổng độ khó (cumulative difficulty) của các khối.

Độ khó của mỗi khối bằng tỉ lệ giữa mục tiêu lớn nhất so với mục tiêu hiện tại. Khối genesis có độ khó thấp nhất là 1. Độ khó của một khối bất kỳ được tính như sau:

$$Diffilculty = \frac{Target_{max}}{Target_{current}}$$

Tổng công sức PoW của một chuỗi sẽ là:

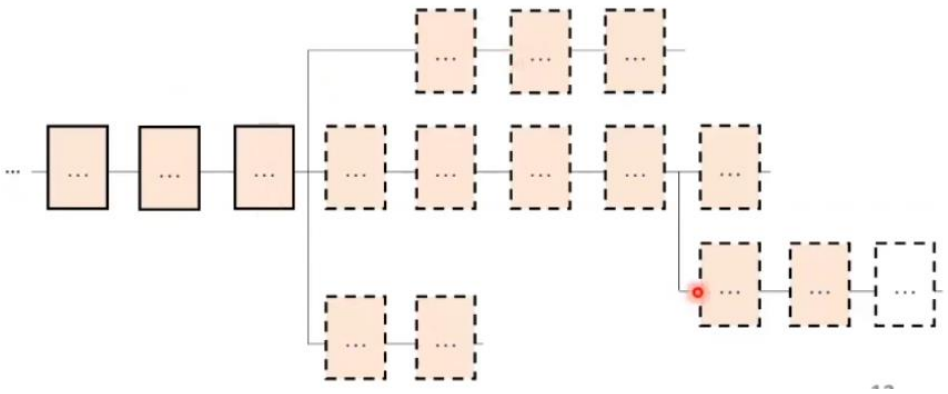
$$Total\ work = \sum_{i=1}^{N} 2^{Difficulty_i}$$

Trong đó:

N là số lượng khối trong chuỗi.

Difficulty$_i$ là độ khó của khối thứ *i*.

$2^{Difficulty_i}$thể hiện lượng công sức tính toán cần thiết để tìm ra khối đó.



Hình 4.3. Minh họa các chuỗi khối trong một nút của mạng blockchain

Một vấn đề xảy khi một nút nhận được 2 khối hợp lệ do các thợ đào tìm ra đồng thời khi đó chuỗi trên nút này tạm thời phân nhánh tức là chia thành nhiều chuỗi. Đây là hiện tượng tự nhiên trong hệ thống phân tán khi không có trung tâm điều phối. Mạng Bitcoin giải quyết vấn đề này qua cơ chế đồng thuận PoW và nguyên tắc chuỗi dài nhất (longest chain rule).

Nguyên nhân của phân nhánh là do:

- Hai thợ đào (hoặc nhóm thợ đào) tìm ra giải pháp cho khối thứ *N* của chuỗi cùng một lúc.
- Độ trễ mạng (network latency) khiến các nút khác nhau nhận được các khối khác nhau trước.

Giải quyết vấn đề phân nhánh:

Khi phân nhánh xảy ra, các nút trong mạng sẽ tạm thời chia thành các nhóm, mỗi nhóm ủng hộ một chuỗi khác nhau (ví dụ: chuỗi A và chuỗi B).

Các thợ đào tiếp tục đào trên chuỗi mà họ nhận được đầu tiên hoặc chuỗi họ cho là "chuỗi chính ". Điều này dẫn đến cuộc đua giữa các chuỗi.

Khối 800,000A và 800,000B được đào cùng lúc. Một nửa mạng theo A, nửa còn lại theo B.

Ví dụ: Nếu chuỗi A được thêm một khối mới (trở thành 800,001) trước chuỗi B, các nút sẽ chuyển sang chuỗi A vì nó dài hơn. Chuỗi B bị bỏ rơi, và khối của nó trở thành **khối lạc** hay **mồ côi**.

Sau một hoặc hai khối tiếp theo, mạng thường đạt được sự thống nhất vì xác suất hai chuỗi tiếp tục kéo dài song song giảm rất nhanh (do tính ngẫu nhiên của PoW).

Các nút sẽ tự động tái tổ chức (reorganize) blockchain của mình để theo chuỗi dài nhất, loại bỏ các khối từ chuỗi ngắn hơn.

Vậy xử lý khối lạc như thế nào?

Mỗi nút trong mạng Bitcoin duy trì một mempool riêng, chứa các giao dịch mà nó đã nhận được từ người dùng nhưng chưa được đưa vào blockchain. Mempool là nơi lưu trữ tạm thời các giao dịch chưa được xác nhận trong mạng Bitcoin. Khi một khối lạc bị loại bỏ, mempool đóng vai trò quan trọng để đảm bảo giao dịch không bị mất.

Thợ đào chọn giao dịch từ mempool để tạo khối mới, thường ưu tiên những giao dịch có phí cao hơn.

Khi khối lạc bị loại: Các giao dịch trong khối lạc không trùng với các giao dịch trong khối được chấp nhận trên chuỗi chính. Những giao dịch này được trả lại mempool của các nút, miễn là chúng vẫn hợp lệ (tức là chưa bị chi tiêu kép hoặc hết thời gian chờ).

Quá trình tái sử dụng:

Thợ đào sẽ lấy các giao dịch từ mempool để đưa vào khối tiếp theo trên chuỗi chính. Ví dụ, nếu giao dịch X nằm trong khối lạc 800,000B, nó có thể được thêm vào khối 800,001A

hoặc sau đó. Nếu giao dịch đã quá cũ hoặc không cạnh tranh được về phí, nó có thể bị xóa khỏi mempool sau một thời gian (thường là 14 ngày trong Bitcoin Core)

Bước 6: Nhận phần thưởng

Để tạo giao dịch coinbase, nút **X** trước tiên tính tổng số phí giao dịch bằng cách cộng tất cả các đầu vào và đầu ra của các giao dịch được thêm vào khối. Phí giao dịch được tính theo công thức:

Tổng phí = Tổng (Đầu vào) - Tổng (Đầu ra)

Tiếp theo, nút **X** tính phần thưởng cho người khai thác được khối mới. Ban đầu phần thưởng được thiết lập là 50 BTC khi khai thác được một khối mới, sau mỗi 210.000 khối thì phần thưởng sẽ giảm đi một nửa. Như vậy với việc đào được khối thứ 878.905 thì nút **X** sẽ nhận được phần thưởng là 3,125 BTC.

Số lần giảm một nửa tối đa được phép là 64, vì vậy nếu vượt quá 64 lần giảm, phần thưởng sẽ bị đặt về 0. Khi đó thợ đào chỉ nhận được phí giao dịch khi đào được khối mới.

Bước 7: Điều chỉnh độ khó

Khi tạo ra một khối mời, nhiệm vụ của các nút là tìm ra số nonce để làm cho giá trị hash của block header nhỏ hơn mục tiêu. Với độ khó hiện tại trên mạng Bitcoin, thợ đào phải thử hàng hàng **triệu tỷ** lần trước khi tìm được một số nonce để tạo ra giá trị hash của block header đủ nhỏ để thỏa mãn mục tiêu. Chúng ta có thể thấy, việc tăng độ khó thêm 1 bit sẽ làm tăng không gian tìm kiếm lời giải tăng gấp đôi.

Trung bình, mạng lưới cần thực hiện hơn 1,8 septa-hashes (tức hàng **nghìn tỷ tỷ tỷ** phép tính băm) mỗi giây để tìm ra khối tiếp theo. Điều này có vẻ là một nhiệm vụ bất khả thi, nhưng may mắn thay, mạng lưới hiện có sức mạnh xử lý lên đến 3 exa-hashes mỗi giây (EH/s, tương đương 3 tỷ tỷ phép tính băm mỗi giây), cho phép tìm ra một khối trong khoảng 10 phút trung bình.

Như chúng ta đã thấy, mục tiêu quyết định độ khó và do đó ảnh hưởng đến thời gian tìm ra giải pháp cho thuật toán PoW. Điều này dẫn đến các câu hỏi hiển nhiên là: Tại sao độ khó cần được điều chỉnh, ai điều chỉnh nó và điều chỉnh như thế nào?

Các khối của Bitcoin được tạo ra trung bình mỗi 10 phút. Đây được coi như "nhịp đập" của hệ thống Bitcoin, hỗ trợ tần suất phát hành tiền tệ và tốc độ xử lý giao dịch. Tần suất này cần phải được duy trì ổn định không chỉ trong ngắn hạn mà còn trong suốt hàng thập kỷ. Trong khoảng thời gian dài đó, công suất tính toán dự kiến sẽ tiếp tục tăng với tốc độ nhanh chóng. Hơn nữa, số lượng người tham gia khai thác và hệ thống máy tính họ sử dụng cũng sẽ liên tục

thay đổi. Để giữ thời gian tạo khối ở mức trung bình 10 phút**,** độ khó khai thác phải được điều chỉnh để bù đắp cho những thay đổi này.

Với mạng Bitcoin, việc điều chỉnh độ khó (retargeting) diễn ra một cách tự động và độc lập trên mỗi nút mạng. Cứ sau 2016 khối, tất cả các nút sẽ điều chỉnh lại PoW. Phương trình điều chỉnh đo thời gian thực tế cần để tìm ra 2016 khối cuối cùng và so sánh với thời gian mong đợi là 20160 phút. Tỷ lệ giữa thời gian thực tế và thời gian mong đợi được tính toán, và từ đó thực hiện điều chỉnh mục tiêu (tăng hoặc giảm) một cách tương ứng.

- Nếu mạng lưới tìm ra các khối nhanh hơn 10 phút/khối, độ khó sẽ tăng lên (giá trị mục tiêu giảm xuống).
- Nếu tốc độ tìm khối chậm hơn mong đợi, độ khó sẽ giảm xuống (giá trị mục tiêu tăng lên).

Công thức điều chỉnh có thể được tóm tắt như sau:

$$Target_{new} = Target_{current} \times \left(\frac{Số\ phút\ thực\ tế\ đào\ 2016\ khối}{20160\ (phút)} \right)$$

Để tránh sự biến động quá lớn trong độ khó, việc điều chỉnh độ khó phải nhỏ hơn hoặc bằng hệ số 4 cho mỗi chu kỳ điều chỉnh. Nếu cần điều chỉnh mục tiêu vượt quá hệ số 4, thì nó sẽ bị giới hạn ở mức hệ số 4 và không cao hơn.

Bất kỳ sự điều chỉnh thêm nào sẽ được thực hiện trong chu kỳ điều chỉnh tiếp theo, vì sự mất cân bằng sẽ tiếp tục tồn tại qua 2016 khối tiếp theo. Do đó, sự chênh lệch lớn giữa sức mạnh tính toán và độ khó có thể cần đến vài chu kỳ 2016 khối để được cân bằng hoàn toàn.

Độ khó của việc khai thác một khối bitcoin được thiết lập sao cho toàn bộ mạng lưới mất khoảng 10 phút để xử lý một khối, dựa trên thời gian khai thác 2016 khối trước đó và được điều chỉnh sau mỗi 2016 khối. Điều này đạt được bằng cách giảm hoặc tăng mục tiêu.

Lưu ý rằng mục tiêu không phụ thuộc vào số lượng giao dịch hoặc giá trị của các giao dịch. Điều này có nghĩa là lượng sức mạnh tính toán, và do đó lượng điện năng tiêu tốn để bảo vệ mạng lưới Bitcoin, hoàn toàn độc lập với số lượng giao dịch.

4.3.4. Ưu nhược điểm của thuật toán đồng thuận PoW

4.3.4.1. Ưu điểm của PoW

- Bảo mật cao: PoW yêu cầu các thợ đào phải giải các bài toán mật mã rất khó, nhưng dễ dàng kiểm tra. Việc thay đổi dữ liệu trong một khối sẽ làm thay đổi toàn bộ chuỗi mã hash liên kết, khiến kẻ tấn công phải giải lại toàn bộ chuỗi, điều này đòi hỏi sức mạnh tính toán cực kỳ lớn. Tấn công 51% về lý thuyết có thể xảy ra nhưng thực tế rất khó khăn với các mạng blockchain lớn như Bitcoin.

- Tính phi tập trung: PoW giúp đảm bảo rằng không có thực thể trung tâm nào kiểm soát mạng lưới. Bất kỳ ai có thiết bị tính toán đều có thể tham gia mạng lưới và trở thành thợ đào mà không cần sự cho phép từ một bên thứ ba.

- Chống gian lận và double-spending: PoW đảm bảo rằng các giao dịch không thể bị ghi đè hoặc sửa đổi sau khi đã được thêm vào blockchain. Ngăn chặn hành vi chi tiêu hai lần (double-spending) vì các giao dịch đã được xác nhận trở thành một phần vĩnh viễn của chuỗi khối.

- Khả năng bất biến và minh bạch: Một khi dữ liệu được ghi vào blockchain thông qua PoW, nó gần như không thể thay đổi hoặc bị xóa. Blockchain PoW công khai tất cả các khối, cho phép người dùng kiểm tra và xác minh một cách minh bạch.

- Đơn giản trong cơ chế hoạt động: PoW chỉ yêu cầu việc giải các phép tính băm mật mã (trong mạng Bitcoin là SHA-256), giúp các nút tham gia có thể dễ dàng kiểm tra tính hợp lệ mà không cần cơ chế phức tạp.

4.3.4.2. Nhược điểm của PoW

- Tiêu tốn năng lượng: Việc giải bài toán băm đòi hỏi sức mạnh tính toán khổng lồ và tiêu tốn rất nhiều điện năng.

- Yêu cầu phần cứng mạnh: Các thợ đào cần sử dụng các thiết bị chuyên dụng như ASIC để cạnh tranh trong việc tìm giá trị nonce, khiến chi phí đầu tư phần cứng rất cao. Người dùng thông thường khó tham gia khai thác do không đủ điều kiện phần cứng và tài nguyên, dẫn đến sự tập trung vào các mỏ đào lớn (mining pools).

- Khả năng tập trung hóa: Các mỏ đào lớn có thể tập trung sức mạnh tính toán và chi phối mạng. Các pool đào (mining pools) – nơi nhiều thợ đào hợp tác để chia sẻ phần thưởng – có thể làm giảm tính phi tập trung của mạng. Các mỏ đào lớn có thể chiếm phần lớn sức mạnh tính toán, gây nguy cơ tập trung hóa.

- Tốc độ xử lý giao dịch thấp: Do thời gian tạo khối cố định (trung bình 10 phút/khối trong Bitcoin), số lượng giao dịch có thể xử lý trong một giây (TPS) bị giới hạn. Bitcoin chỉ có thể xử lý khoảng 7 giao dịch/giây (TPS), trong khi các hệ thống thanh toán tập trung như Visa có thể xử lý hàng chục nghìn giao dịch mỗi giây.

4.4. THUẬT TOÁN BẰNG CHỨNG CỔ PHẦN (POS)

- Thay vì sử dụng sức mạnh tính toán như PoW, Bằng chứng cổ phần (PoS - Proof of Stake) chọn người xác thực (validators) dựa trên số lượng coin (hoặc token) họ đặt cọc trong mạng lưới. Người nắm giữ nhiều coin hơn (hoặc đặt cọc lâu hơn) có cơ hội cao hơn để được chọn tạo khối mới. Một số mạng sử dung thuật toán này như là Ethereum 2.0, Cardano, Solana, Algorand, …

4.4.1. Lịch sử phát triển của thuật toán bằng chứng cổ phần

Một trong những vấn đề chính mà chúng ta cần quan tâm đến các giao thức của các blockchain dựa trên PoW là năng lượng cần thiết để thực thi chúng. Hiên nay lượng điện tiêu thụ để duy trì mạng blockchain Bitcoin có thể so sánh với một quốc gia nhỏ. Thực trạng này đã thúc đẩy việc nghiên cứu các giao thức mới thay thế, nhằm loại bỏ sự phụ thuộc vào PoW bằng cách thay thế một cơ chế khác hiệu quả hơn về năng lượng nhưng vẫn đảm bảo chức năng tương tự.

Khái niệm về PoS đã được thảo luận rộng rãi trên diễn đàn Bitcoin. Các thiết kế blockchain dựa trên bằng chứng cổ phần đã được nghiên cứu một cách chính thức bởi Bentov và cộng sự, cả khi kết hợp với bằng chứng công việc (PoW) và khi PoS là cơ chế duy nhất cho một giao thức blockchain [5]. Mặc dù Bentov và cộng sự đã chỉ ra rằng các giao thức của họ an toàn trước một số loại tấn công nhất định, nhưng họ không cung cấp một mô hình chính thức để phân tích các giao thức dựa trên PoS hoặc các chứng minh bảo mật dựa trên các định nghĩa chính xác. Nhiều giao thức blockchain dựa trên PoS đã được đề xuất (và triển khai) cho một số loại tiền điện tử, tuy nhiên vì dựa trên các lập luận bảo mật có tính chất kinh nghiệm, các loại tiền điện tử này thường được phát hiện có những thiếu sót từ góc độ bảo mật.

Ý tưởng về PoS lần đầu tiên được đề xuất trên diễn đàn Bitcointalk vào năm 2011 bởi một số nhà phát triển trong cộng đồng Bitcoin như QuantumMechanic. Mục tiêu ban đầu của PoS là làm giảm thiểu tiêu tốn năng lượng do khai thác PoW và tạo ra một hệ thống đồng thuận không phụ thuộc vào sức mạnh tính toán. Tuy nhiên, vào thời điểm đó, ý tưởng này chỉ mới ở mức lý thuyết và chưa được triển khai thực tế. Lần đầu tiên PoS được áp dụng trong mạng blockchain Peercoin (PPC). Đây là mạng blockchain do Sunny King và Scott Nadal phát triển lần đầu năm 2012. Peercoin sử dụng một cơ chế hybrid (kết hợp) giữa PoW và PoS để đảm bảo tính bảo mật ban đầu và dần chuyển sang PoS hoàn toàn. Năm 2014 mạng blockchain Blackcoin ra đời và là blockchain đầu tiên chuyển hoàn toàn sang PoS mà không sử dụng PoW sau khối khởi tạo (genesis block). Giai đoạn 2015-2018 sự ra đời của mạng blockchain Ethereum do Vitalik Buterin phát triển. Năm 2015, Ethereum ra mắt như một blockchain sử dụng cơ chế đồng thuận PoW nhưng đã lên kế hoạch chuyển đổi sang PoS ngay từ những phiên bản đầu tiên. Năm 2017, Ethereum giới thiệu kế hoạch nâng cấp Casper, một thuật toán PoS nhằm thay thế cơ chế PoW trong mạng Ethereum và cũng trong năm 2017 ra đời của mạng blockchain Cardano, Cardano được phát triển bởi Charles Hoskinson, người đồng sáng lập Ethereum. Đây là mạng blockchain sử dụng PoS ngay từ đầu với thuật toán đồng thuận Ouroboros, được thiết kế để tăng cường bảo mật và hiệu suất cao mà vẫn tiết kiệm năng lượng. Năm 2022 mạng Ethereum chính thức chuyển hoàn toàn từ PoW sang PoS với sự kiện "The Merge". Đây là cột mốc quan trọng, biến Ethereum trở thành mạng PoS lớn nhất thế giới. Với việc chuyển sang PoS đã làm giảm hơn 99% lượng năng lượng tiêu thụ của mạng lưới. Mở đường cho các nâng cấp khác như Sharding để tăng khả năng mở rộng. Giải đoạn 2020 đến nay là giai đoạn bùng nổ của các mạng blockchain PoS hiện đại. Các blockchain mới như

Polkadot, Tezos, Solana, Avalanche đã áp dụng các biến thể của PoS ngay từ đầu, mang lại tốc độ xử lý nhanh và phí giao dịch thấp. Các nền tảng PoS hiện đại kết hợp các tính năng như Bằng chứng cổ phần được ủy quyền (Delegated Proof of Stake - DPoS), Bằng chứng lịch sử (Proof of History - PoH) để tăng hiệu suất mà vẫn đảm bảo tính phi tập trung và bảo mật.

4.4.2. Cơ chế hoạt động của PoS

Bước 1: Đặt cọc tài sản (Staking)

Người dùng muốn trở thành validator phải đặt cọc một số lượng token nhất định vào mạng blockchain. Số token này đóng vai trò như một cam kết và "thế chấp" để tham gia quá trình xác thực.

Tùy vào mạng lưới, số lượng token đặt cọc yêu cầu có thể khác nhau (ví dụ: Ethereum 2.0 yêu cầu tối thiểu 32 ETH).

Bước 2: Chọn người xác thực khối (Validator Selection)

Hệ thống chọn validator để xác thực khối mới dựa trên các tiêu chí sau:

- Số lượng coin đặt cọc: Validator có nhiều token đặt cọc hơn có xác suất được chọn cao hơn.
- Thời gian đặt cọc: Validator đặt cọc càng lâu có khả năng được chọn càng lớn.
- Ngẫu nhiên hóa: Một số giao thức PoS áp dụng yếu tố ngẫu nhiên để đảm bảo tính công bằng trong việc lựa chọn.

Trong PoS, xác suất một validator được chọn tỷ lệ thuận với tỷ lệ cổ phần của họ trong hệ thống. Công thức cơ bản được định nghĩa như sau:

$$P_i = \frac{S_i}{S_{Total}}$$

Trong đó:

- S_i: Số token được validator *i* stake.
- S_{total}: Tổng số coin được stake trong toàn mạng.
- $P_i \in [0, 1]$ biểu thị xác suất ngẫu nhiên validator *i* được chọn tạo khôi.
- Điều kiện chuẩn hóa: $\sum_{i=1}^{N} P_i = 1$ với *N* là tổng số validator.

Quy trình ngẫu nhiên hóa

Để lựa chọn validator, hệ thống thường sử dụng một hàm ngẫu nhiên có trọng số. Một số hàm thường sử dụng như hàm băm, hàm ngẫu nhiên có thể xác minh.

- **Hàm băm kết hợp với giá trị cổ phần:**

Lấy giá trị băm $H(B_{prev} \| t \| i)$ của khối trước (B_{prev}), thời gian hiện tại (t), và i là định danh của validator (public key hoặc index), || là phép nối chuỗi.

So sánh với ngưỡng tỷ lệ cổ phần:

$$r = H(B_{prev} \| t \| i) < P_i \cdot 2^k$$

Trong đó k là độ dài bít của hàm băm (ví dụ, k=256 cho SHA-256). Validator đầu tiên thỏa mãn điều kiện này được chọn.

- **Hàm ngẫu nhiên có thể xác minh (VRF)**

VRF (Verifiable Random Function) là một hàm mật mã tạo ra giá trị ngẫu nhiên r từ đầu vào công khai (public input) và khóa bí mật (secret key), đồng thời cung cấp bằng chứng (proof) để bất kỳ ai cũng có thể xác minh tính đúng đắn của r. Trong PoS, VRF được dùng để chọn validator một cách an toàn và không thể dự đoán. VRF thường dựa trên các hệ mật mã như ECDSA (Elliptic Curve Digital Signature Algorithm) hoặc BLS (Boneh-Lynn-Shacham)

Cho:

- sk_i: Khóa bí mật của validator i.
- pk_i: Khóa công khai tương ứng.
- x = (B_{prev}, t): Đầu vào công khai (khối trước và timestamp).

VRF bao gồm ba hàm:

- $r = VRF_{sk_i}(x)$: Tạo giá trị ngẫu nhiên r.
- $\pi = Prove_{sk_i}(x)$: Tạo bằng chứng π.
- $Verify_{pk_i}(x, r, \pi)$: Trả về *true* nếu r hợp lệ, *false* nếu không.

Validator i được chọn nếu:

$$r < \frac{S_i}{S_{Total}} \cdot 2^k$$

Dưới đây là mã giả cho một VRF đơn giản:

```
Function VRF(sk, x):
   // sk: khóa bí mật, x: đầu vào (B_prev || t)
   h = Hash(x)          // Hàm băm SHA-256, h ∈ [0, 2^256-1]
   r = ScalarMultiply(sk, h)// Nhân vô hướng trên đường cong elliptic
π = Sign(sk, h)         // Chữ ký làm bằng chứng
   Return (r, π)
```

```
Function Verify(pk, x, r, π):     // pk: khóa công khai
    h = Hash(x)
    If VerifySignature(pk, h, π) AND r == ScalarMultiply(π, h):
        Return True
    Else:
        Return False
```

Bước 3: Xác thực giao dịch và tạo khối (Block creation)

Validator được chọn sẽ xác minh các giao dịch trong khối mới và đảm bảo rằng tất cả các giao dịch hợp lệ, không vi phạm quy tắc của mạng (ví dụ: không có giao dịch chi tiêu hai lần). Nếu tất cả các điều kiện đều hợp lệ, validator sẽ thêm khối mới vào blockchain và phát broadcast khối đó đến các nút khác trong mạng.

Bước 4: Xác nhận và đồng thuận (Consensus verification)

Các nút khác trong mạng sẽ kiểm tra và xác nhận khối mới. Nếu khối được xác nhận là hợp lệ, khối sẽ được thêm vào blockchain chính thức.

Bước 5: Nhận phần thưởng và phí giao dịch (Reward distribution)

Validator tạo khối thành công sẽ nhận được phần thưởng là tổng phí giao dịch từ các giao dịch trong khối và tùy vào giao thức, validator có thể nhận thêm coin mới sinh ra.

Bước 6: Cơ chế phạt (Slashing)

Cơ chế phạt được áp dụng để ngăn hành vi xấu. Nếu một validator cố tình tạo khối sai hoặc gửi dữ liệu không hợp lệ, họ sẽ bị phạt thông qua cơ chế slashing. Validator tạo khối sai hoặc gửi dữ liệu không hợp lệ sẽ mất một phần hoặc toàn bộ số coin đặt cọc, có thể bị loại khỏi quá trình tham gia xác thực trong một khoảng thời gian. Điều này giúp đảm bảo rằng các validator sẽ luôn hành xử trung thực để tránh mất tài sản. Dưới đây là công thức thức cơ bản để tính số token bị mất L khi bị phạt, trong một số mạng sẽ có công thức cải tiến:

$$L_i = \alpha \,.S_i, \qquad 0 < \alpha \leq 1$$

α: Hệ số phạt, thường được thiết kế trước bởi giao thức (ví dụ: 0.05).

Trong Casper của Etherium:

$$L_i = max(\ S_i, (S_i,\ F)\ )$$

γ: Hệ số dựa trên tổng thiệt hại *F* (faulty stake).

4.4.3. Cơ chế đồng thuận của mạng Cardano

Cardano là một nền tảng blockchain công khai được xây dựng dựa trên nghiên cứu học thuật và phương pháp luận khoa học. Nó được tạo ra để giải quyết các hạn chế của Bitcoin và Ethereum 1.0 về khả năng mở rộng, khả năng tương tác và tính bền vững. Cardano được Charles Hoskinson bắt đầu phát triển vào năm 2015, ông là một trong những người đồng sáng lập của Ethereum. Công nghệ cốt lõi của Cardano là sử dụng giao thức đồng thuận PoS tiên tiến được gọi là Ouroboros và được công bố năm 2017. Nó được phát triển bằng ngôn ngữ lập trình Haskell, một ngôn ngữ lập trình cho phép Cardano đạt được tính bảo mật và ổn định cao. Ouroboros là tên một biểu tượng cổ đại, một con rắn tự ăn đuôi của chính nó, tượng trưng cho sự tái tạo và tuần hoàn vĩnh cửu. Cơ chế đồng thuận Ouroboros cho phép mạng Cardano đạt được sự đồng thuận một cách an toàn và hiệu quả về trạng thái của sổ cái phân tán. Ouroboros đã và được phát triển qua phiên bản.

Hình 4.4. Các phiên bản cơ chế đồng thuận Ouroboros

1. Ouroboros Classic (2017)

Đây là phiên bản đầu tiên của Ouroboros, được công bố vào năm 2017. Nó là một trong những thuật toán PoS đầu tiên được nghiên cứu và chứng minh lý thuyết về tính bảo mật và khả năng phân tán. Ouroboros Classic thiết lập cơ chế đồng thuận bằng cách chia mạng thành các chu kỳ thời gian (epochs) và các slot nhỏ hơn (slots), trong đó các "slot leaders" được chọn ngẫu nhiên từ những người sở hữu cổ phần ADA (stakeholders). Ouroboros cung cấp mức bảo mật tương đương với PoW nhưng tiết kiệm năng lượng hơn; validator nắm giữ nhiều tocken ADA hơn sẽ có xác suất cao hơn được chọn làm slot leader. Phiên bản này có một số hạn chế là chưa thực sự hỗ trợ tính phi tập trung hoàn toàn; chưa tối ưu cho các trường hợp tấn công mạng và bảo mật danh tính.

2. Ouroboros BFT (Byzantine Fault Tolerance) (2018)

Phiên bản Ouroboros BFT được sử dụng trong kỷ nguyên Shelley. Đặc điểm chính của nó là chỉ cần 2/3 số nút trung thực để đảm bảo an toàn; tốc độ xử lý nhanh hơn do không cần

nhiều nút xác thực; dễ dàng nâng cấp mạng lưới Cardano từ kỷ nguyên Byron sang kỷ nguyên Shelley. Hạn chế không phải là một hệ thống phi tập trung hoàn toàn vì chỉ một số lượng nhỏ node được ủy quyền xác thực giao dịch.

3. Ouroboros Praos (2018)

Đây là một phiên bản nâng cấp từ Ouroboros Classic, giúp tăng cường bảo mật và hỗ trợ phi tập trung hoàn toàn. Cải tiến chính lựa chọn slot leader trong bí mật, tránh bị tấn công DoS hoặc tấn công Sybil; hỗ trợ mạng lưới phi tập trung với nhiều stake pool tham gia xác thực giao dịch; cho phép các nút hoạt động trong điều kiện kết nối mạng không ổn định. Lợi ích đem lại an toàn hơn trước các cuộc tấn công trên mạng blockchain; giảm thiểu rủi ro khi một slot leader bị lộ danh tính.

4. Ouroboros Genesis (2018)

Giải quyết một vấn đề quan trọng trong PoS đó là cách một nút mới tham gia mạng mà không cần tin tưởng vào bất kỳ ai. Đặc điểm chính của nó là cho phép các nút mới xác minh toàn bộ lịch sử chuỗi khối mà không cần sự tin cậy bên ngoài; cải thiện khả năng phục hồi của blockchain trong trường hợp sự cố mạng; tăng độ tin cậy và giúp quá trình đồng bộ hóa mạng nhanh hơn. Lợi ích không cần phải dựa vào bên thứ ba khi một nút mới tham gia; nâng cao tính phi tập trung của Cardano.

5. Ouroboros Crypsinous (2019)

Phiên bản Ouroboros tích hợp với công nghệ zero-knowledge proofs để cải thiện quyền riêng tư. Đặc điểm chính của nó là cung cấp khả năng xác minh giao dịch mà không tiết lộ dữ liệu cụ thể; hỗ trợ các hợp đồng thông minh bảo mật. Cải tiến này nhằm đem lại cải thiện quyền riêng tư trên Cardano; hỗ trợ các ứng dụng cần ẩn danh hoặc bảo mật cao.

6. Ouroboros Chronos (2020)

Mục tiêu của Chronos là cải thiện đồng bộ hóa thời gian trong blockchain mà không cần dựa vào đồng hồ hệ thống. Đặc điểm chính mạng blockchain có thể xác minh thời gian một cách an toàn mà không cần một nguồn thời gian bên ngoài đáng tin cậy; tăng khả năng chống giả mạo thời gian trên blockchain. Cải tiến này nhằm đảm bảo tính nhất quán về thời gian giữa các nút trong mạng; tăng cường độ an toàn và tránh bị tấn công bằng cách giả mạo thời gian.

7. Ouroboros Leios (Đang phát triển - 2023+)

Phiên bản này được thiết kế để giúp Cardano đạt hàng triệu TPS (giao dịch mỗi giây) bằng cải tiến chính là hỗ trợ xử lý giao dịch song song, giúp tốc độ mạng tăng lên đáng kể. Mục tiêu là cải thiện khả năng mở rộng của Cardano lên hàng triệu TPS; hỗ trợ ứng dụng phi tập trung và DeFi.

8. Ouroboros Omega (Định hướng tương lai)

Ouroboros Omega là phiên bản hợp nhất tất cả các cải tiến trước đây của Ouroboros để tạo ra một giao thức PoS tối ưu nhất. Mục tiêu là bảo mật cao nhất với mọi loại tấn công; tối ưu tốc độ nhưng vẫn duy trì tính phi tập trung; hỗ trợ ứng dụng blockchain quy mô toàn cầu. Dự kiến cải tiến kết hợp ưu điểm của Hydra, Leios, Chronos, Crypsinous; mở rộng khả năng xử lý giao dịch trong cả môi trường on-chain và off-chain.

4.4.3.1. Một số khái niệm chính của Ouroboros

- **Epoch (Kỷ nguyên):** Thời gian được chia thành các epoch, mỗi epoch kéo dài một khoảng thời gian nhất định, trong mạng Cardano là 5 ngày.
- **Slot (Khe thời gian):** Mỗi epoch được chia thành các slot ngắn hơn. Trong mạng Cardano mỗi slot là một giây, như vậy trong một Epoch sẽ có 432.000 slots.
- **Slot leader (Người đứng đầu khe thời gian):** Trong mỗi slot, một nút mạng *i* được chọn ngẫu nhiên với xác xuất $p_i = \frac{s_i}{\sum_{j=1}^{n} s_j}$ để trở thành slot leader. Slot leader có trách nhiệm (quyền) tạo ra một khối mới. Trong đó *n* là số nút trong mạng, s_i số ADA mà nút mạng thứ *i* đặt cược.

  Ouroboros sử dụng hàm ngẫu nhiên có thể xác minh (VRF) để chọn slot leader:

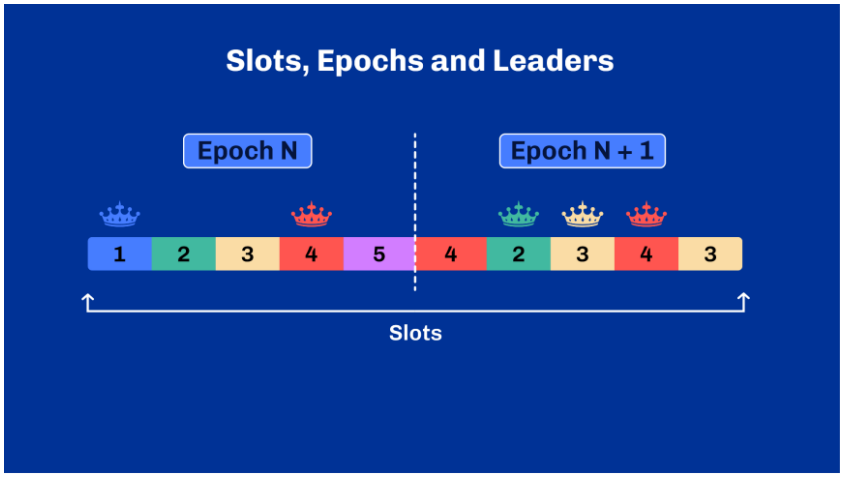
  $$r = VRF_{ski}(seed_{epoch})$$

  - sk_i : Khóa bí mật của validator
  - $seed_{epoch}$: Hạt giống ngẫu nhiên của epoch, tạo từ các cam kết của validator ở epoch trước và được tính như sau:

  $$seed_{epoch} = \bigoplus H(r_i^{epoch-1})$$

    - $r_i^{epoch-1}$: Giá trị ngẫu nhiên do validator *i* đóng góp ở epoch trước.
    - H: Hàm băm (SHA-256).
    - $\bigoplus$: Phép XOR.

  Nếu r < $P_i \cdot 2^k$ (với *k* là độ dài bit của *VRF*), *i* được chọn.



Hình 4.5. Minh họa các khái niệm epoch, slot, Slot leader

- **Stake (Cổ phần):** Các chủ sở hữu ADA có thể đặt cược token của họ để tham gia vào quá trình đồng thuận. Khả năng một nút được chọn làm slot leader tỷ lệ thuận với số lượng ADA mà nó đã stake hoặc được ủy quyền stake.

4.4.3.2. Cách Ouroboros hoạt động

Bước 1. Stake pool (Nhóm cổ phần): Người dùng có thể stake ADA của họ trực tiếp hoặc ủy quyền cho các stake pool. Stake pool là các nút vận hành bởi các nhà điều hành pool, họ chịu trách nhiệm duy trì hoạt động của nút và thay mặt cho những người ủy quyền nhận phần thưởng.

Bước 2. Lựa chọn slot leader: Vào đầu mỗi epoch, một quá trình lựa chọn ngẫu nhiên diễn ra để xác định slot leader cho mỗi slot trong epoch đó. Xác suất một nút được chọn phụ thuộc vào tổng số ADA được stake của nút đó hoặc stake pool mà nó vận hành.

Bước 3. Tạo khối: Slot leader được chọn có quyền tạo một khối mới trong slot của mình. Khối này chứa các giao dịch đã được xác minh. Một giao dịch Cardano bao gồm các thành phần sau:

Đầu vào (Inputs): Bao gồm các UTXO hiện có mà người gửi muốn chi tiêu. Mỗi đầu vào chỉ định một UTXO cụ thể từ các giao dịch trước đó.

Đầu ra (Outputs): Bao gồm các UTXO mới được tạo ra bởi giao dịch. Mỗi đầu ra chỉ định một địa chỉ nhận và một giá trị ADA được chuyển đến địa chỉ đó. Ngoài ra, nó có thể chứa dữ liệu script.

Phí giao dịch (Transaction Fee): Một khoản phí nhỏ được trả cho mạng để xử lý giao dịch. Phí này được tính toán dựa trên kích thước của giao dịch và độ tắc nghẽn của mạng.

Chữ ký (Witness): Chữ ký số của người gửi được sử dụng để xác minh tính hợp lệ của giao dịch và đảm bảo rằng chỉ người sở hữu khóa riêng tư tương ứng mới có thể chi tiêu các UTXO đầu vào.

Bước 4. Xác nhận khối và động thuận: Slot leader phát tán khối mới được tạo tới các nút trong mạng. Các nút trong mạng xác minh tính hợp lệ của khối được tạo bởi slot leader.

Một giao dịch hợp lệ trong Cardano là giao dịch đáp ứng các điều kiện sau:

Tính hợp lệ của đầu vào: Tất cả các UTXO đầu vào phải tồn tại và chưa được chi tiêu. Người gửi phải chứng minh quyền sở hữu của mình đối với các UTXO này bằng cách cung cấp chữ ký số hợp lệ.

Tính hợp lệ của đầu ra: Tổng giá trị của các đầu ra cộng với phí giao dịch phải nhỏ hơn hoặc bằng tổng giá trị của các đầu vào. Điều này đảm bảo rằng không có ADA mới được tạo ra từ các giao dịch.

Kiểm tra Script (nếu có): Nếu bất kỳ UTXO đầu ra nào chứa dữ liệu script, script đó phải được thực thi thành công. Điều này đảm bảo rằng các điều kiện được quy định trong script được đáp ứng.

Chữ ký hợp lệ: Tất cả các chữ ký được cung cấp phải hợp lệ và tương ứng với các khóa riêng tư của người gửi.

Kiểm tra tuân thủ giao thức: Nút kiểm tra xem khối có tuân thủ các quy tắc của giao thức Ouroboros hay không, ví dụ như: số lượng giao dịch tối đa trong một khối, kích thước khối tối đa, thông tin metadata của khối.

Đồng thuận: Nếu khối vượt qua tất cả các kiểm tra trên, nút sẽ coi nó là hợp lệ và thêm nó vào bản sao cục bộ của blockchain. Quá trình này được lặp lại bởi tất cả các nút trong mạng, tạo ra sự đồng thuận về trạng thái của blockchain.

Sau khi được xác thực bởi phần lớn các nút, khối mới sẽ được chính thức thêm vào blockchain, kéo dài chuỗi và ghi lại vĩnh viễn các giao dịch trong khối đó.

Bước 5. Nhận phần thưởng: Các slot leader và các stake pool nhận được phần thưởng ADA cho việc tạo và xác nhận khối. Phần thưởng này được chia sẻ với những người đã ủy quyền stake cho pool.

4.4.4. Ưu nhược điểm của của PoS

4.4.4.1. Ưu điểm của PoS

- Tiết kiệm năng lượng: Một trong những ưu điểm lớn nhất của PoS là nó tiêu tốn ít năng lượng hơn so với PoW. PoW yêu cầu các thợ đào giải các bài toán tính toán phức tạp, tiêu tốn năng lượng rất lớn. Ngược lại, PoS không yêu cầu tính toán phức tạp mà thay vào đó, lựa

chọn người tạo khối (validator) dựa trên cổ phần họ nắm giữ. Điều này làm cho PoS trở thành một lựa chọn bền vững và thân thiện với môi trường.

- Khả năng mở rộng cao: PoS có thể xử lý giao dịch nhanh hơn và hiệu quả hơn khi số lượng người tham gia tăng lên, do không yêu cầu giải bài toán tính toán phức tạp. Điều này giúp cải thiện khả năng mở rộng của blockchain, làm cho PoS trở thành một lựa chọn tốt cho các mạng lưới blockchain với khối lượng giao dịch lớn.

- Chi phí thấp: Việc không cần đến phần cứng mạnh mẽ như trong PoW giúp giảm chi phí tham gia mạng cho các validator. Điều này khiến PoS dễ tiếp cận hơn đối với nhiều người tham gia và có thể làm giảm sự tập trung vào một nhóm nhỏ các thợ đào hoặc nhà đầu tư.

- An toàn và bảo mật: PoS có cơ chế bảo mật mạnh mẽ, vì các validator cần đặt cược tài sản của mình (stake) để tham gia vào việc tạo khối và xác minh giao dịch. Nếu validator hành động không trung thực, họ sẽ mất một phần hoặc toàn bộ tài sản đã đặt cược. Điều này giúp giảm thiểu các cuộc tấn công vào mạng, vì chi phí tấn công mạng PoS sẽ tốn kém và khó thực hiện.

- Khả năng kháng tấn công 51%: Trong PoS, để chiếm ưu thế trong mạng và thực hiện một cuộc tấn công 51% (tức là kiểm soát hơn 50% sức mạnh đồng thuận), kẻ tấn công cần phải sở hữu hơn 50% tổng số cổ phần của mạng. Điều này cực kỳ khó thực hiện và đắt đỏ, đặc biệt trong các mạng lưới PoS lớn.

4.4.4.2. Nhược điểm của PoS

- Tập trung hóa (Centralization): Một trong những vấn đề lớn nhất của PoS là sự tập trung vào những người sở hữu nhiều cổ phần. Những người sở hữu lượng lớn token có nhiều cơ hội hơn để trở thành các validator và tạo ra khối, dẫn đến việc mạng có thể trở nên tập trung vào một số ít cá nhân hoặc tổ chức có tài sản lớn. Điều này có thể làm giảm tính phân quyền của mạng blockchain, mục tiêu chính của các hệ thống như Bitcoin.

- Người giàu càng giàu hơn: Trong PoS, những người sở hữu nhiều token có cơ hội cao hơn để kiếm phần thưởng từ việc xác minh giao dịch và tạo khối. Điều này có thể dẫn đến sự gia tăng sự giàu có của các nhà đầu tư lớn và làm giảm cơ hội cho những người tham gia nhỏ lẻ. Đây là một vấn đề tiềm ẩn trong việc duy trì sự công bằng trong mạng blockchain.

- Tính ngẫu nhiên và rủi ro lựa chọn Validator: Mặc dù PoS có cơ chế ngẫu nhiên để chọn các validator, nhưng việc lựa chọn người tạo khối dựa trên cổ phần có thể dẫn đến việc một số người tham gia không được lựa chọn trong một thời gian dài, điều này có thể làm giảm động lực tham gia. Hơn nữa, một số phương pháp lựa chọn validator có thể dẫn đến những quyết định không công bằng hoặc có sự thiên lệch.

- Cần lượng cổ phần lớn để tham gia: Để có cơ hội trở thành một validator và tạo ra khối, người tham gia cần phải có một lượng cổ phần đáng kể. Điều này có thể tạo ra một rào cản đối với những người mới tham gia hoặc những người có tài sản nhỏ hơn. Một số mạng PoS

yêu cầu người tham gia phải đặt cược một số lượng token lớn để tham gia vào quá trình đồng thuận, điều này có thể khiến cho mạng lưới bị hạn chế về số lượng người tham gia.

- Rủi ro phân mảnh và tấn công: PoS có thể đối mặt với các vấn đề về phân mảnh mạng, đặc biệt nếu không có sự phân bổ công bằng về cổ phần. Nếu có quá ít validator hoặc nếu quá nhiều cổ phần được tập trung vào một số ít người, có thể gây ra các vấn đề về sự đồng thuận và hiệu quả của mạng. Hơn nữa, PoS cũng có thể gặp phải các cuộc tấn công Sybil, tức là kẻ tấn công tạo ra nhiều nút giả để tăng cổ phần của mình và có thể làm thay đổi quá trình đồng thuận.

4.5. CÁC BIẾN THỂ CỦA THUẬT TOÁN BẰNG CHỨNG CỔ PHẦN

4.5.1. Thuật toán Bằng chứng ủy cổ phần được ủy quyền (DPoS)

- Bằng chứng cổ phần được ủy quyền (DPoS - Delegated Proof-of-Stake) là một biến thể của PoS trong đó người dùng ủy quyền quyền xác thực của mình cho một nhóm đại diện (Delegates). Các đại diện được lựa chọn thông qua cơ chế bỏ phiếu, với quyền biểu quyết tỷ lệ thuận với lượng coin mà người dùng nắm giữ. Một số mạng sử dung thuật toán này như là EOS, TRON, Tezos, …

4.5.1.1. Cơ chế hoạt động của DPoS

Bỏ phiếu: Những người nắm giữ token sử dụng cổ phần của họ để bỏ phiếu cho các đại biểu mà họ tin tưởng. Số lượng phiếu bầu của mỗi người tỷ lệ thuận với số lượng token mà họ nắm giữ.

Lựa chọn Đại biểu: Một số lượng nhất định các đại biểu được bầu chọn dựa trên số phiếu bầu mà họ nhận được. Số lượng này được xác định bởi giao thức của blockchain.

Xác thực và tạo khối: Các đại biểu được bầu chọn sẽ luân phiên nhau xác thực giao dịch và tạo ra các khối mới. Thứ tự này thường được xác định bởi một lịch trình được xác định trước hoặc một thuật toán ngẫu nhiên.

Phần thưởng: Các đại biểu nhận được phần thưởng cho việc tạo ra các khối mới. Phần thưởng này có thể được chia sẻ với những người đã bỏ phiếu cho họ, tùy thuộc vào cách giao thức được thiết lập.

4.5.1.2. Ưu điểm của DPoS

Khả năng mở rộng: DPoS có khả năng xử lý số lượng giao dịch lớn hơn so với PoS truyền thống do số lượng người xác thực được giới hạn.

Tốc độ giao dịch nhanh: Thời gian tạo khối thường nhanh hơn so với PoS, dẫn đến tốc độ giao dịch nhanh hơn.

Hiệu quả năng lượng: Tương tự như PoS, DPoS tiết kiệm năng lượng hơn so với Bằng chứng công việc (PoW).

4.5.1.3. Nhược điểm của DPoS

Tập trung hóa: Do số lượng đại biểu được giới hạn, DPoS có thể dẫn đến sự tập trung quyền lực vào một nhóm nhỏ người, làm giảm tính phi tập trung của blockchain.

Khả năng bị thao túng: Nếu một nhóm người nắm giữ một lượng lớn token có thể kiểm soát quá trình bầu chọn và bầu ra các đại biểu thân cận với họ, họ có thể thao túng mạng lưới.

4.5.2. Thuật toán Bằng chứng trọng số (PoWeight)

Bằng chứng về trọng số (Proof of Weight - PoWeight) là một cơ chế đồng thuận được sử dụng trong công nghệ blockchain để bảo mật mạng lưới và xác thực giao dịch. Không giống như PoW truyền thống, dựa trên việc giải các bài toán mật mã phức tạp, PoWeight dựa trên sự đồng thuận của nó vào số lượng "trọng lượng" hoặc cổ phần mà những người tham gia nắm giữ trong mạng lưới. Trọng lượng này thường tương quan với số lượng token hoặc tài sản do người tham gia kiểm soát, ảnh hưởng đến khả năng tạo khối mới và xác thực giao dịch của họ.

PoWeight được ra mắt vào năm 2017 như một thuật toán đồng thuận trên nền tảng blockchain Filecoin và là bản nâng cấp lớn của cơ chế PoS nhằm mục đích loại bỏ bản chất thiên vị của PoS. PoWeight không phải là một thuật toán đồng thuận duy nhất. Thay vào đó, nó là một thuật ngữ chung cho toàn bộ một loạt các thuật toán đồng thuận phần lớn dựa trên mô hình đồng thuận Algorand do các nhà nghiên cứu tại Phòng thí nghiệm Khoa học máy tính và Trí tuệ nhân tạo MIT phát triển, trong đó Algorand là một giao thức xác nhận giao dịch rất nhanh.

4.5.2.1. Cơ chế hoạt động của PoWeight

Xác định trọng số: Người tham gia được chỉ định trọng số dựa trên số lượng token hoặc tài sản họ nắm giữ và sẵn sàng khóa làm tài sản thế chấp. Người tham gia có trọng số càng lớn thì họ càng có nhiều ảnh hưởng trong mạng lưới.

Tạo và xác thực khối: Những người tham gia có trọng số đáng kể có thể đề xuất các khối mới để thêm vào blockchain. Cơ hội được chọn để tạo khối của họ tỷ lệ thuận với trọng số của họ. Những người tham gia mạng khác xác thực các khối được đề xuất. Vì quy trình này dựa trên trọng số không phải công việc tính toán, nên nó tập trung vào việc xác minh tính hợp lệ dựa trên cổ phần của người tham gia.

Đạt được sự đồng thuận: Khi một khối được đề xuất và xác thực, nó sẽ được thêm vào blockchain nếu nó đáp ứng các quy tắc đồng thuận của mạng. Hệ thống đạt được sự đồng thuận dựa trên trọng số của những người tham gia vào quá trình tạo và xác thực khối.

Phần thưởng và khuyến khích: Những người tham gia tạo và xác thực khối thành công sẽ được thưởng token hoặc phí. Phần thưởng thường tỷ lệ thuận với số lượng token họ nắm giữ, khuyến khích họ hành động trung thực và tham gia tích cực.

4.5.2.2. Ưu điểm của PoWeight

Khả năng mở rộng: Ưu điểm chính của cơ chế đồng thuận bằng chứng trọng số là nó có khả năng tùy chỉnh cao và có khả năng mở rộng cho nhiều người dùng. Hệ thống Bằng chứng trọng số cho phép tạo ra các ủy ban bao gồm những người dùng mạng ngẫu nhiên được chỉ định 'trọng số' theo giao thức đồng thuận.

Bảo mật: PoWeight cũng cung cấp một số mức độ tập trung giúp duy trì mạng lưới phi tập trung toàn diện và an toàn.

Rủi ro phân nhánh: Cơ chế bằng chứng trọng số cố gắng đạt được sự đồng thuận mà không có bất kỳ rủi ro phân nhánh mới nào vì nó xem xét giá trị có trọng số tương đối dựa trên bất kỳ yếu tố có trọng số nào chứ không chỉ dựa trên số tiền mà nút nắm giữ.

Giảm mức tiêu thụ năng lượng: Không giống như PoW, đòi hỏi sức mạnh tính toán và năng lượng đáng kể, PoWeight dựa vào tiền cược thay vì các phép tính mở rộng, dẫn đến mức tiêu thụ năng lượng thấp hơn.

Chi phí vận hành thấp hơn: Với nhu cầu năng lượng và nhu cầu tính toán giảm, việc vận hành và duy trì mạng blockchain theo PoWeight thường tiết kiệm chi phí hơn.

Phần thưởng dựa trên cổ phần: Người tham gia được thưởng dựa trên số lượng trọng số hoặc cổ phần họ nắm giữ. Động lực tài chính này khuyến khích sự tham gia tích cực và trung thực, vì cá nhân có lợi ích kinh tế trực tiếp trong việc duy trì tính toàn vẹn của mạng lưới.

4.5.2.2. Một số nhược điểm của PoWeight

Thiết lập và quản lý: Việc triển khai PoWeight đòi hỏi phải thiết kế và quản lý cẩn thận việc phân phối tiền cược và tính toán trọng lượng. Điều này có thể phức tạp và có thể yêu cầu các hệ thống tinh vi để xử lý tiền cược và trọng lượng một cách chính xác.

Phân phối Token: Việc phân phối token hoặc tài sản ban đầu có thể ảnh hưởng đến tính công bằng của cơ chế đồng thuận. Nếu việc phân bổ ban đầu không đồng đều, có thể dẫn đến sự bất bình đẳng trong việc kiểm soát và ảnh hưởng của mạng lưới.

Rủi ro về Staking: Tính bảo mật của mạng phụ thuộc vào giá trị kinh tế của các stake do người tham gia nắm giữ. Trong trường hợp cực đoan, nếu một phần đáng kể stake của mạng bị xâm phạm hoặc bị đánh cắp, điều này có thể ảnh hưởng đến tính bảo mật của mạng.

Thách thức pháp lý: Bối cảnh pháp lý cho PoWeight và các cơ chế tương tự vẫn đang trong quá trình phát triển. Sự không chắc chắn về mặt pháp lý và các vấn đề tuân thủ có thể gây ra thách thức cho việc áp dụng và vận hành.

Tải mạng: Mặc dù PoWeight cải thiện khả năng mở rộng so với PoW, nhưng nó vẫn có thể gặp phải các vấn đề về khả năng mở rộng khi khối lượng giao dịch hoặc quy mô mạng cực lớn, tùy thuộc vào cách triển khai.

4.5.3 Một số thuật toán khác.

4.5.3.1. Thuật toán PoH

Bằng chứng lịch sử (PoH - Proof of History) là một cơ chế đồng thuận kết hợp với các thuật toán khác (thường là PoS) để tăng tốc độ xác nhận giao dịch trong mạng blockchain. PoH tạo ra một chuỗi thời gian mã hóa, cho phép các nút xác minh thứ tự các sự kiện (giao dịch) một cách độc lập mà không cần đồng bộ hóa thời gian với nhau, thời gian và thứ tự các giao dịch được ghi lại trước khi đưa vào khối. Một số mạng sử dung thuật toán này như là Solana một nền tảng blockchain hiệu suất cao, Pipelined blockchain.

PoH là một cơ chế đồng thuận được phát triển bởi Anatoly Yakovenko, người sáng lập Solana Labs. Ý tưởng cốt lõi của PoH là thứ tự của các sự kiện trong mạng Blockchain cũng quan trọng như chính các sự kiện đó, và khả năng chứng minh được thứ tự này là yếu tố cần thiết để duy trì tính toàn vẹn của mạng.

Để đạt được điều này, PoH sử dụng một Hàm trì hoãn có thể xác minh (Verifiable Delay Function - VDF) để tạo ra một dấu thời gian (timestamp) cho mỗi khối trong Blockchain. VDF được thiết kế để khó bị thao túng, nhờ tính "kháng trì hoãn" và "kháng bộ nhớ," khiến cho các kẻ tấn công không dễ dàng thao túng các dấu thời gian. Dấu thời gian do VDF tạo ra được tích hợp vào mỗi khối trên Blockchain, cung cấp một bản ghi thứ tự giao dịch bất biến và có thể xác minh được. Nhờ PoH, Solana đạt được khả năng chốt giao dịch nhanh (fast finality), nghĩa là khi một khối được thêm vào Blockchain, nó được xem như đã hoàn tất và không thể bị thay đổi.

PoH chủ yếu được sử dụng trong mạng Blockchain Solana, với thiết kế xử lý được hàng nghìn giao dịch mỗi giây. PoH giúp giảm thiểu yêu cầu về lưu trữ và băng thông để duy trì mạng Blockchain, đồng thời cải thiện hiệu quả và tốc độ của hệ thống, trong khi vẫn đảm bảo tính bảo mật và khả năng xác minh giao dịch.

Cách hoạt động của PoH

1. Ghi Dấu Thời Gian Mật Mã (Cryptographic Timestamping)

PoH sử dụng một hàm băm có tính liên tiếp và kháng tiền hình ảnh (pre-image resistant). Hàm băm này nhận một đầu vào (bao gồm trạng thái hiện tại của Blockchain và một seed ngẫu nhiên) và tạo ra một đầu ra duy nhất, không thể đảo ngược, gọi là hash. Hash này là dấu thời gian có thể xác minh được.

2. Tạo chuỗi hash (Generating a Hash Chain)

Solana tạo ra một chuỗi hash bằng cách áp dụng hàm băm liên tục lên đầu ra của hash trước đó. Mỗi bước trong chuỗi đại diện cho một "tick" (nhịp thời gian), với số lượng hash được tính toán biểu thị khoảng thời gian đã trôi qua. Kết quả là một bản ghi thời gian liên tục, có thể xác minh được, dùng để sắp xếp các giao dịch.

3. Ghi nhận giao dịch

Khi một giao dịch được thực hiện, nó được gắn với hash gần nhất trong chuỗi PoH. Các validator (người xác thực) kiểm tra tính hợp lệ và thời gian của giao dịch bằng cách đảm bảo rằng nó tham chiếu đến một hash trong chuỗi PoH hiện tại.

4. Đồng thuận

Các giao dịch được gắn dấu thời gian bởi PoH sau đó được xử lý thông qua cơ chế đồng thuận dựa trên Proof of Stake (PoS), cụ thể là Tower BFT trong mạng Solana. Các validator đặt cọc token SOL để tham gia, nhận phần thưởng khi bảo vệ mạng và xác nhận giao dịch. Nhờ sự hỗ trợ từ cơ chế ghi thời gian của PoH, Tower BFT đạt được đồng thuận nhanh chóng, cho phép Solana xử lý hàng nghìn giao dịch mỗi giây.

5. Hàm trì hoãn có thể xác minh (VDF)

VDF đảm bảo rằng các nhà sản xuất khối phải đi qua nó để có quyền tạo khối. Solana kết hợp hash của dữ liệu từ trạng thái đã được tạo trước đó trong chuỗi giao dịch, tạo ra dấu thời gian có thể xác minh được mà không thể tái tạo hoặc thay đổi.

Ưu điểm của PoH

- Khả năng mở rộng cao: PoH cho phép Solana xử lý hàng chục nghìn giao dịch mỗi giây.
- Độ trễ thấp: Thời gian chờ giao dịch được giảm thiểu đáng kể nhờ khả năng xác minh nhanh chóng.
- Bảo mật cao: Chuỗi hash liên tục đảm bảo rằng thứ tự giao dịch không thể bị thao túng.
- Hiệu quả năng lượng: Không yêu cầu các phép tính phức tạp hoặc tiêu tốn năng lượng như trong PoW.
- Loại bỏ đồng hồ tập trung: PoH tích hợp thời gian trực tiếp vào Blockchain, loại bỏ nhu cầu về một hệ thống đồng hồ tập trung.

Nhược điểm của PoH

- Yêu cầu phần cứng Cao: Do cần xử lý khối lượng lớn dữ liệu, các nút phải có phần cứng mạnh mẽ, có thể làm giảm tính phi tập trung.
- Tập trung hóa: Các yêu cầu về hiệu suất phần cứng có thể dẫn đến sự tập trung hóa trong số ít các node lớn.
- Phức tạp kỹ thuật: Việc triển khai PoH đòi hỏi sự tích hợp chặt chẽ giữa phần cứng và phần mềm, tăng độ phức tạp vận hành.

4.5.3.2. Thuật toán Bằng chứng thẩm quyền (PoA)

Bằng chứng thẩm quyền (Proof of Authority - PoA) là một thuật toán đồng thuận dựa trên uy tín, cung cấp giải pháp khả thi và hiệu quả cho các mạng lưới blockchain, đặc biệt là các mạng lưới blockchain riêng tư (private blockchain). Thuật ngữ này được đề xuất vào năm 2017 bởi Gavin Wood, đồng sáng lập và cựu CTO của Ethereum.

Thuật toán đồng thuận PoA tận dụng giá trị của danh tính, thay vì để các node xác thực đặt cược tiền mã hóa (như trong PoS), họ đặt cược uy tín của chính mình. Do đó, các blockchain PoA được bảo vệ bởi các node xác thực được chọn lựa cẩn thận và được xem là các thực thể đáng tin cậy.

Thuật toán đồng thuận PoA rất linh hoạt và được coi là một lựa chọn giá trị cho các ứng dụng trong lĩnh vực hậu cần. Đối với chuỗi cung ứng, chẳng hạn, PoA được xem là một giải pháp hiệu quả và hợp lý. Mô hình PoA cho phép các doanh nghiệp duy trì tính riêng tư của mình trong khi vẫn tận dụng được những lợi ích của công nghệ blockchain.

Microsoft Azure là một ví dụ khác về một công ty áp dụng PoA. Nền tảng Azure cung cấp các giải pháp cho các mạng riêng tư mà không yêu cầu một loại tiền tệ nội bộ, chẳng hạn như "gas" trong ether, vì quá trình khai thác là không cần thiết.

PoA là một hệ thống có khả năng mở rộng cao vì nó dựa vào số lượng nhỏ các validator. Hệ thống này được điều hành bởi những người tham gia đã được phê duyệt trước, chịu trách nhiệm xác minh các khối và giao dịch. Một số mạng sử dung thuật toán này như là Binance Smart Chain, VeChain, Microsoft Azure Blockchain, …

Cách hoạt động của PoA

PoA là một cơ chế đồng thuận dựa vào việc xác thực các giao dịch blockchain bởi các thực thể được ủy quyền. So với PoS, PoA được thiết kế để cung cấp một giải pháp mở rộng và hiệu quả hơn cho việc xây dựng các mạng blockchain riêng tư.

Xác thực dựa trên danh tính: Không giống như PoW và PoS phụ thuộc vào năng lực tính toán hoặc số lượng tiền đặt cọc, PoA sử dụng danh tính của các validator làm điều kiện xác thực chính. Đây là một cơ chế đồng thuận hiệu quả, nhấn mạnh vào sự tin cậy và công nhận danh tiếng.

Lựa chọn Validator: Validator hay "authority" phải có danh tính rõ ràng và được xác minh bởi toàn bộ mạng lưới. Khi nhận được đề xuất giao dịch mới, tất cả các validator sẽ độc lập xác minh giao dịch dựa trên các quy tắc của mạng. Nếu đa số đồng ý, giao dịch sẽ được thêm vào khối mới.

Xác thực khối: Một thuật toán đồng thuận như chọn ngẫu nhiên có trọng số hoặc vòng tuần tự được sử dụng để chọn validator tạo khối. Sau khi khối được tạo, nó sẽ được phát đến

tất cả các node trong mạng. Các nút sẽ kiểm tra tính hợp lệ của khối, bao gồm các giao dịch và liên kết với khối trước đó. Khi đa số đồng thuận, khối sẽ được thêm vào blockchain.

Ưu điểm của PoA

- Hiệu quả: Không yêu cầu khai thác (mining) tiêu tốn năng lượng như PoW hay đặt cọc vốn lớn như PoS.
- Tốc độ: Quá trình xác thực nhanh, độ trễ thấp do danh sách validator cố định.
- Bảo mật: Danh tiếng và danh tính rõ ràng của validator giúp chống lại các cuộc tấn công Sybil và các hoạt động độc hại khác.
- Quản trị: Thích hợp cho các mạng blockchain riêng hoặc liên minh, nơi quản trị tập trung là cần thiết.
- Khả năng mở rộng: Dễ dàng mở rộng do không bị giới hạn bởi tài nguyên như PoW hoặc PoS.

Nhược điểm của PoA

- Tập trung hóa: Validator là những thực thể được chọn trước, dẫn đến lo ngại về khả năng cấu kết hoặc tập trung quyền lực.
- Giới hạn phân quyền: PoA không đạt mức độ phân quyền cao như PoW hay PoS.
- Rủi ro tấn công Validator: Nếu một thực thể độc hại kiểm soát được đa số validator, mạng có thể bị xâm phạm.

4.5.3.3. Thuật toán PoC

- Bằng chứng dung lượng (PoC - Proof of Capacity) là một thuật toán đồng thuận trong blockchain, dựa trên dung lượng lưu trữ ổ cứng thay vì sức mạnh tính toán hoặc tài sản đặt cọc. Trong PoC, người tham gia sử dụng dung lượng lưu trữ để khai thác và xác thực giao dịch. PoC còn được gọi là Bằng chứng không gian (Proof of Space) hoặc Bằng chứng lưu trữ (Proof of Storage). Một số mạng sử dung thuật toán này như là Burstcoin, Chia Network, Signum, …

Trong PoC, các thợ đào sử dụng dung lượng ổ cứng của họ để giải quyết các bài toán toán học và tạo ra các khối mới. Dung lượng lưu trữ càng lớn, cơ hội của thợ đào để tạo ra một khối mới càng cao. Khác với PoW, nơi các thợ đào phải giải quyết các bài toán toán học phức tạp, PoC sử dụng một thuật toán băm đơn giản hơn, yêu cầu ít năng lực tính toán hơn. Điều này giúp PoC dễ tiếp cận hơn với các thợ đào quy mô nhỏ, những người không có điều kiện sở hữu các thiết bị khai thác đắt tiền.

Những điểm chính của PoC:

1. Dung lượng lưu trữ

Trong PoC, dung lượng lưu trữ là tài nguyên quan trọng nhất. Thợ đào càng có nhiều không gian lưu trữ, họ càng có cơ hội cao hơn để tạo ra các khối mới. Tuy nhiên, điều này không có nghĩa là cần phải sở hữu dung lượng lớn để tham gia mạng lưới. Ngay cả với một dung lượng nhỏ, thợ đào vẫn có thể nhận được phần thưởng.

2. Quá trình "plotting"

Plotting là quá trình tính toán trước các hàm băm để tăng tốc độ khai thác. Thợ đào sử dụng không gian lưu trữ của mình để tạo ra các tệp plot chứa tất cả các hàm băm cần thiết cho việc khai thác. Các tệp này sau đó được sử dụng để khai thác các khối mới. Quá trình plotting có thể mất nhiều thời gian và tài nguyên, nhưng một khi hoàn thành, việc khai thác sẽ trở nên nhanh chóng và hiệu quả hơn.

3. Khai thác (Mining)

Khai thác trong PoC liên quan đến việc đọc tệp plot và tìm kiếm câu trả lời chính xác cho bài toán toán học. Khi câu trả lời chính xác được tìm thấy, thợ đào có thể tạo ra một khối mới và nhận phần thưởng. Khai thác trong PoC tiêu tốn ít năng lượng hơn so với PoW, giúp nó trở thành một giải pháp bền vững hơn.

4. Phần thưởng

Các thợ đào trong PoC nhận được phần thưởng khi tạo ra các khối mới. Phần thưởng thường ở dạng tiền mã hóa. Số lượng phần thưởng phụ thuộc vào kích thước của khối và giá trị thị trường hiện tại của loại tiền mã hóa đó.

Ưu điểm của PoC:

- Bền vững và thân thiện với môi trường: PoC tiêu tốn ít năng lượng hơn, góp phần giảm tác động tiêu cực đến môi trường.
- Dễ tiếp cận: Không yêu cầu thiết bị khai thác đắt tiền, cho phép nhiều người tham gia hơn.
- Hỗ trợ thợ đào nhỏ: Ngay cả những người có dung lượng lưu trữ hạn chế cũng có thể tham gia và nhận phần thưởng.

PoC là một giải pháp thay thế bền vững và dễ tiếp cận hơn so với các thuật toán đồng thuận truyền thống. Bằng cách sử dụng dung lượng lưu trữ làm tài nguyên chính, PoC góp phần xây dựng một mạng lưới blockchain hiệu quả về năng lượng và thân thiện với môi trường. Khi ngành công nghiệp blockchain tiếp tục phát triển, chúng ta có thể kỳ vọng nhiều thuật toán đồng thuận sáng tạo như PoC sẽ ra đời.

Câu hỏi và bài tập

1 Thuật toán đồng thuận blockchain là gì, và vai trò của nó trong việc duy trì tính an toàn và ổn định của hệ thống phân tán?

2 Nêu các bước chính trong cơ chế hoạt động của một thuật toán đồng thuận blockchain.

3 Tại sao tính phi tập trung (decentralization) lại là yêu cầu quan trọng đối với một thuật toán đồng thuận?

4 Mô tả bài toán các vị tướng Byzantine và sự liên quan của nó đến hệ thống chịu lỗi Byzantine (BFT).

5 So sánh các ưu, nhược điểm của thuật toán Proof of Work (PoW) và Proof of Stake (PoS).

6 Giải thích cách hoạt động của thuật toán Proof of History (PoH) trong mạng Solana và vai trò của nó trong việc tăng tốc độ xử lý giao dịch.

7 Thuật toán Proof of Authority (PoA) hoạt động như thế nào, và tại sao nó phù hợp với các mạng blockchain riêng tư (private blockchain)?

8 Mô tả cơ chế chọn Slot Leader trong thuật toán Ouroboros của Cardano.

9 Thuật toán Proof of Capacity (PoC) giúp giảm tiêu thụ năng lượng như thế nào, và nó khác gì so với PoW?

10 Bằng chứng cổ phần được ủy quyền (DPoS) giải quyết vấn đề tập trung hóa như thế nào so với PoS?

11 Hãy giải thích cách hệ thống chịu lỗi Byzantine (BFT) đảm bảo tính ổn định của mạng lưới blockchain ngay cả khi một số nút không trung thực.

12 Một thợ đào sử dụng thuật toán PoC có 5 TB dung lượng lưu trữ, trong khi người khác có 10 TB. Tính xác suất tương đối của mỗi người trong việc tạo khối mới.

13 Lập bảng so sánh ưu, nhược điểm của PoW, PoS và PoC. Đề xuất tình huống ứng dụng phù hợp cho từng thuật toán.

14 Mô phỏng cách tạo và xác thực khối bằng thuật toán PoW. Mô tả các bước từ tạo khối ứng viên đến xác nhận khối hợp lệ.

15 Nếu bạn phải xây dựng một blockchain cho một ứng dụng tài chính với yêu cầu cao về tốc độ và bảo mật, bạn sẽ chọn thuật toán nào trong số PoW, PoS, PoH hoặc PoA? Giải thích lý do.

CHƯƠNG 5: THÁCH THỨC VÀ XU HƯỚNG MỚI

5.1. Các thách thức của Blockchain

Để Bitcoin có thể trở thành *"tài sản số kiểu mới"* như (và có thể là hơn) cách mà vàng đã từng làm được trong thế giới thực, hay Ethereum đóng vai trò *máy tính của thế giới* (Vitalik Buterin, đồng sáng lập Ethereum), hoặc Cardano là *nền tảng Blockchain công cộng phục vụ hàng tỷ người* (Charles Hoskinson, nhà sáng lập Cardano) ... các nền tảng Blockchain cần vượt qua một loạt các thách thức. Chương này sẽ phân tích từ những thách thức kỹ thuật cơ bản, được gọi là "bộ ba tam giác bất khả thi" (Blockchain Trilemmas), đến các thách thức liên quan đến ứng dụng đại trà của các nền tảng Blockchain trong cuộc sống.

"Bộ ba tam giác bất khả thi" lần đầu được đề cập đến trong một bài viết của Vitalik Buterin năm 2017, đề cập đến ba yếu tố quan trọng mà bất kỳ nền tảng Blockchain nào cũng phải cân bằng: sự phân tán (decentralization), mức độ bảo mật (security), và khả năng mở rộng (scalability). Theo lý thuyết, rất khó để một Blockchain tối ưu hóa cả ba yếu tố này cùng lúc. Ví dụ, nếu tập trung vào khả năng mở rộng để xử lý nhiều giao dịch hơn trong thời gian ngắn, nền tảng có thể phải hy sinh một phần mức độ phân tán hoặc bảo mật. Ngược lại, khi ưu tiên bảo mật hoặc phân tán, khả năng mở rộng thường bị giảm đi. Thách thức này buộc các nhà phát triển phải đưa ra những giải pháp sáng tạo để đạt được sự cân bằng hợp lý giữa các yếu tố mà không làm suy giảm mục tiêu cốt lõi của Blockchain.

Ngoài các thách thức về mặt kỹ thuật, các nền tảng Blockchain cũng phải đối mặt với nhiều vấn đề khác. Thách thức pháp lý là một trong số đó, xuất phát từ tính mới mẻ của công nghệ và việc một số cá nhân hoặc tổ chức lợi dụng Blockchain để thực hiện các hành vi bất hợp pháp như rửa tiền, lừa đảo, hoặc kinh doanh đa cấp. Những vấn đề này không chỉ làm giảm lòng tin của công chúng mà còn khiến các cơ quan quản lý phải ban hành nhiều chính sách kiểm soát chặt chẽ hơn, đôi khi làm chậm lại quá trình phát triển của ngành.

Bên cạnh đó, độ phức tạp của các ứng dụng Blockchain cũng là một rào cản lớn. Việc hiểu và sử dụng công nghệ này đòi hỏi một mức độ kiến thức nhất định, khiến nó khó tiếp cận với đại đa số người dùng. Nhận thức của xã hội về Blockchain vẫn còn hạn chế, và nhiều người thậm chí vẫn coi đây là một công nghệ không thực tế hoặc mang tính đầu cơ cao. Hơn nữa, sự thiếu hụt các chuyên gia có kinh nghiệm trong lĩnh vực này cũng cản trở khả năng ứng dụng Blockchain vào các lĩnh vực thực tiễn, làm giảm tốc độ mà công nghệ này có thể tích hợp vào cuộc sống hàng ngày.

Chúng ta sẽ cùng nhau tìm hiểu về các thách thức trong phần dưới đây

5.1.1. Thách thức về mặt kỹ thuật

5.1.1.1. Khả năng mở rộng (Scalability)

Một trong những thách thức lớn nhất của blockchain là khả năng mở rộng. Vấn đề này thể hiện qua các khía cạnh sau:

• **Giới hạn kích thước block**: Mỗi block trên blockchain có kích thước cố định, giới hạn số lượng giao dịch có thể xử lý trong một thời gian nhất định. Ví dụ, Bitcoin với giới hạn block 1 MB thường gặp tắc nghẽn khi số lượng giao dịch tăng cao, khiến thời gian xác nhận kéo dài. Ethereum cũng gặp vấn đề tương tự trong quá khứ do phụ thuộc vào gas limit cho mỗi block, đặc biệt khi có nhiều ứng dụng phi tập trung (dApps) hoạt động trên nền tảng này.

• **Thời gian xử lý giao dịch**: Với các cơ chế đồng thuận như đã nêu ở chương trước, thời gian xác nhận giao dịch có thể kéo dài từ vài phút đến hàng giờ trong thời điểm mạng tắc nghẽn. Ví dụ, Bitcoin sử dụng cơ chế Proof of Work (PoW), khiến thời gian trung bình để thêm một block mới mất khoảng 10 phút. Trong khi đó, Ethereum, sau khi chuyển sang cơ chế Proof of Stake (PoS) vào năm 2022 thông qua sự kiện "The Merge," đã cải thiện hiệu suất và giảm mức tiêu thụ năng lượng. Tuy nhiên, thời gian chờ xử lý giao dịch vẫn có thể kéo dài trong các giai đoạn cao điểm.

• **Chi phí giao dịch**: Khi lưu lượng tăng cao, cả Bitcoin và Ethereum đều từng chứng kiến chi phí giao dịch tăng vọt. Trên Ethereum, chi phí gas đã giảm nhờ các giải pháp Layer-2 như Optimistic Rollup và zk-Rollups, nhưng tình trạng phí tăng đột biến vẫn có thể xảy ra khi có nhiều hợp đồng thông minh hoặc dApps hoạt động đồng thời.

Để giải quyết các vấn đề về khả năng mở rộng, nhiều phương án đã được triển khai và tiếp tục phát triển:

1. **Chuyển đổi cơ chế đồng thuận**: Ethereum đã hoàn tất chuyển đổi từ cơ chế Proof of Work (PoW) – chậm chạp và tốn kém năng lượng - sang Proof of Stake (PoS) – nhanh chóng và giảm tối đa năng lượng tiêu thụ- vào năm 2022 thông qua sự kiện lịch sử "The Merge." Đây là bước quan trọng trong lộ trình Ethereum 2.0 nhằm nâng cao khả năng mở rộng và giảm tác động môi trường. Trước "The Merge," mạng Ethereum vận hành song song hai chuỗi: chuỗi chính (Mainnet) dựa trên PoW và Beacon Chain dựa trên PoS. Khi "The Merge" xảy ra, hai chuỗi này được hợp nhất, loại bỏ PoW hoàn toàn và Ethereum chính thức hoạt động hoàn toàn dựa trên PoS. Sau khi chuyển sang POS, mạng Ethreum đã đạt được những kết quả ấn tượng ban đầu:
    - **Hiệu quả năng lượng**: PoS giảm tới 99.95% lượng năng lượng tiêu thụ so với PoW.
    - **Bảo mật cao hơn**: PoS yêu cầu người xác thực khóa một lượng lớn ETH để tham gia, làm tăng chi phí tấn công mạng.

- **Nền tảng cho các cải tiến tiếp theo**: Việc chuyển sang PoS mở đường cho các giải pháp mở rộng như sharding.

2. **Sharding**: Đây là một trong những giải pháp quan trọng trong lộ trình phát triển của Ethereum. Sharding chia mạng lưới blockchain thành nhiều phân đoạn nhỏ hơn, gọi là "shards." Mỗi shard có thể xử lý các giao dịch và hợp đồng thông minh một cách độc lập, giúp mạng lưới xử lý nhiều giao dịch song song thay vì tuần tự trên một chuỗi duy nhất. Ví dụ, một ngân hàng phải xử lý 1.000 giao dịch cùng lúc. Nếu ngân hàng có 10 chi nhánh (tương tự như các shard), mỗi chi nhánh chỉ cần xử lý 100 giao dịch thay vì toàn bộ 1.000 giao dịch. Điều này giúp tiết kiệm thời gian và giảm tải cho hệ thống chính. Trên Ethereum, sharding sẽ làm giảm áp lực lên mạng lưới chính (Layer-1), giúp tăng tốc độ giao dịch và giảm chi phí.

   Tính đến 2025, sharding vẫn đang trong giai đoạn triển khai, dự kiến sẽ trở thành một phần quan trọng của Ethereum trong các năm tới với những cải tiến phù hợp. Đây là bước tiếp theo sau sự kiện "The Merge," giúp Ethereum đạt được mục tiêu khả năng mở rộng và tương thích tốt hơn với các ứng dụng phi tập trung.

3. **Layer-2**: Các giải pháp Layer-2 như Lightning Network cho Bitcoin, Optimistic Rollup, zk-Rollups, và Polygon trên Ethereum đã được áp dụng rộng rãi. Chúng giúp giảm tải mạng lưới chính (Layer-1) và cải thiện tốc độ xử lý cũng như giảm chi phí giao dịch.

4. **Blockchain thế hệ mới**: Các dự án như Solana, Avalanche, Cardano, Sui, Aptos… đã đưa ra các cải tiến mới về khả năng mở rộng và tương tác giữa các blockchain. Solana nổi bật với tốc độ xử lý giao dịch cao, trong khi Aptos và Sui tập trung vào hiệu quả lập trình và khả năng xử lý dữ liệu song song.

Nhờ những cải tiến này, hệ sinh thái blockchain đã dần khắc phục được nhiều hạn chế về khả năng mở rộng, tạo nền tảng cho sự phát triển bền vững và mở rộng ứng dụng trong thực tế.

5.1.1.2 Vấn đề về bảo mật

Mặc dù blockchain được thiết kế với tính bảo mật cao nhờ các cơ chế mã hóa và phi tập trung, vẫn tồn tại một số điểm yếu tiềm tàng mà nếu không được quản lý tốt, có thể gây ảnh hưởng nghiêm trọng đến hệ thống.

- **Tấn công 51%**: Đây là một trong những rủi ro lớn nhất đối với các blockchain sử dụng cơ chế đồng thuận Proof of Work (PoW). Một cuộc tấn công 51% xảy ra khi một thực

thể hoặc nhóm kiểm soát hơn 50% sức mạnh tính toán (hash power) của toàn bộ mạng. Với quyền lực này, kẻ tấn công có thể thao túng mạng lưới bằng cách tạo ra các khối giả mạo, đảo ngược giao dịch đã xác nhận, hoặc ngăn chặn các giao dịch mới. Điều này làm mất đi tính toàn vẹn và đáng tin cậy của mạng blockchain. Tuy nhiên, tấn công này thường khó xảy ra với các blockchain lớn như Bitcoin do chi phí và tài nguyên cần thiết là rất lớn.

- **Lỗ hổng trong hợp đồng thông minh**: Smart Contract là những đoạn mã tự động hóa các quy tắc và giao dịch trên blockchain, nhưng chúng không tránh khỏi lỗi lập trình hoặc thiết kế. Các lỗ hổng trong mã nguồn có thể bị khai thác bởi các hacker để trộm tiền hoặc phá hủy dữ liệu. Một ví dụ điển hình là vụ tấn công DAO trên Ethereum vào năm 2016, khi hacker tận dụng lỗi trong mã hợp đồng thông minh để rút hàng triệu đô la từ quỹ. Vì vậy, việc kiểm tra và kiểm toán mã nguồn (auditing) kỹ lưỡng là cực kỳ quan trọng để giảm thiểu rủi ro này.
- **Nguy cơ từ máy tính lượng tử**: Với sức mạnh tính toán vượt trội, máy tính lượng tử có thể đe dọa phá vỡ các thuật toán mã hóa hiện tại của blockchain như SHA-256 (Bitcoin) hoặc ECDSA (Ethereum). Các thuật toán này vốn được thiết kế để chống lại các cuộc tấn công từ máy tính cổ điển, nhưng không đủ khả năng chống lại sự tiến bộ của máy tính lượng tử. Nếu các thuật toán mã hóa bị phá vỡ, toàn bộ dữ liệu trên blockchain có thể bị giải mã, dẫn đến nguy cơ mất an toàn thông tin và tài sản. Chúng ta tạm thời yên tâm rằng ở thời điểm hiện tại, các nhà nghiên cứu và nhà phát triển đang tích cực làm việc để tạo ra các thuật toán mã hóa kháng lượng tử nhằm bảo vệ blockchain trong tương lai.

Những điểm yếu này nhấn mạnh rằng, mặc dù blockchain là một công nghệ tiên tiến và bảo mật cao, nó không phải là bất khả xâm phạm. Việc nâng cấp liên tục, kết hợp với các biện pháp bảo vệ như kiểm toán mã nguồn, tăng cường phi tập trung, và nghiên cứu công nghệ kháng lượng tử, là cần thiết để duy trì sự an toàn và phát triển bền vững của blockchain.

5.1.1.3. Tiêu thụ năng lượng và tác động môi trường

Các mạng lưới blockchain, đặc biệt là những hệ thống sử dụng cơ chế đồng thuận Proof of Work (PoW) như Bitcoin và Ethereum trước khi chuyển đổi sang Proof of Stake (PoS), đã bị chỉ trích vì mức tiêu thụ năng lượng cao và tác động tiêu cực đến môi trường.

Tiêu thụ năng lượng của các mạng lưới Blockchain

PoW yêu cầu các "thợ đào" giải quyết các bài toán mật mã phức tạp để xác minh giao dịch và tạo ra khối mới. Quá trình này sử dụng một lượng lớn tài nguyên tính toán, dẫn đến mức tiêu thụ năng lượng khổng lồ. Theo các ước tính:

- Mạng lưới Bitcoin tiêu thụ khoảng 110 TWh mỗi năm (tương đương mức tiêu thụ của một quốc gia nhỏ như Hà Lan).
- Ethereum trước khi chuyển đổi sang PoS tiêu thụ khoảng 70 TWh/năm.

Việc tiêu thụ năng lượng chủ yếu đến từ các trung tâm dữ liệu và thiết bị chuyên dụng (ASIC, GPU), thường được vận hành 24/7 tại các quốc gia có giá điện thấp.

Tác động môi trường

Nguồn điện cho các mạng lưới blockchain thường đến từ năng lượng hóa thạch như than đá hoặc khí tự nhiên, dẫn đến lượng lớn khí CO2 thải vào môi trường. Các nghiên cứu chỉ ra rằng:

- Hoạt động khai thác Bitcoin thải ra khoảng 60-70 triệu tấn CO2 mỗi năm.
- Tình trạng nóng lên toàn cầu và cạn kiệt tài nguyên năng lượng là những hậu quả đáng kể.

Ngoài ra, việc sản xuất và vận hành các thiết bị đào cũng tạo ra chất thải điện tử khổng lồ, gây thêm áp lực lên môi trường.

Cách thức vận hành giảm tác động

Các giải pháp được đề xuất và triển khai nhằm giảm thiểu tác động môi trường của blockchain bao gồm:

- **Chuyển đổi sang Proof of Stake (PoS):** Ethereum đã thành công chuyển đổi sang PoS vào năm 2022, giảm mức tiêu thụ năng lượng xuống hơn 99,9%. PoS không yêu cầu các bài toán mật mã phức tạp, thay vào đó, các trình xác thực được chọn dựa trên số lượng tài sản nắm giữ.
- **Sử dụng năng lượng tái tạo:** Các trung tâm dữ liệu khai thác đang hướng đến việc sử dụng năng lượng mặt trời, gió và thủy điện để giảm lượng phát thải carbon. Ví dụ, tại Iceland và Canada, các công ty khai thác tận dụng nguồn năng lượng địa nhiệt và thủy điện dồi dào.

- **Off-chain và Layer 2:** Các giải pháp mở rộng như Lightning Network hoặc Optimistic Rollup giúp giảm tải giao dịch trực tiếp trên blockchain, từ đó giảm tiêu thụ năng lượng tổng thể.
- **Quy định và chính sách:** Một số quốc gia đang áp dụng các chính sách hạn chế khai thác PoW hoặc ưu tiên các dự án blockchain thân thiện với môi trường.

Ví dụ thực tế

Ethereum sau khi chuyển sang PoS đã trở thành một minh chứng rõ ràng về việc blockchain có thể duy trì tính phi tập trung và bảo mật mà không tiêu tốn quá nhiều năng lượng. Bên cạnh đó, các mạng lưới blockchain mới như Algorand, Cardano, và Polkadot cũng sử dụng các cơ chế đồng thuận tiết kiệm năng lượng ngay từ khi thiết kế, để tối ưu hóa hiệu suất và giảm tác động môi trường.

Tóm lại, mặc dù blockchain mang lại nhiều lợi ích cho xã hội và kinh tế, nhưng vấn đề năng lượng và môi trường vẫn cần được quản lý chặt chẽ để đảm bảo tính bền vững lâu dài

5.1.2. Thách thức về quản trị và khả năng tương tác

5.1.2.1. Thách thức về quản trị của các mạng lưới Blockchain

Quản trị blockchain đề cập đến cách thức các quyết định được đưa ra và thực thi trong hệ thống, bao gồm việc quản lý các cập nhật, thay đổi trong giao thức và cách giải quyết các tranh chấp. Các thách thức lớn về quản trị blockchain bao gồm:

a. Quyết định tập trung vs. phi tập trung

Mặc dù blockchain thường được thiết kế để phi tập trung, nhiều dự án lại gặp phải vấn đề về sự tập trung quyền lực trong tay một số ít người. Điều này xảy ra khi các nhóm phát triển, các "lãnh đạo" của dự án hoặc những người nắm giữ phần lớn token có thể kiểm soát các quyết định quan trọng, chẳng hạn như thay đổi giao thức hoặc cập nhật phần mềm.

Ví dụ, trong trường hợp của Bitcoin, sự kiểm soát của các thợ đào hoặc các tổ chức lớn về việc thay đổi giao thức hoặc nâng cấp mạng có thể gây ra sự chia rẽ trong cộng đồng, như đã xảy ra với việc chia tách thành Bitcoin và Bitcoin Cash vào năm 2017.

b. Thiếu sự đồng thuận trong cộng đồng

Mặc dù blockchain là hệ thống phân tán, nhưng việc đạt được sự đồng thuận giữa các bên liên quan trong cộng đồng lại rất khó khăn. Các thay đổi trong giao thức hoặc các nâng cấp mạng có thể gặp phải sự phản đối từ một bộ phận người dùng hoặc các nhà phát triển. Điều này có thể dẫn đến các phân mảnh mạng (hard forks) hoặc các vấn đề lớn trong việc duy trì

tính thống nhất của mạng. Ví dụ, việc nâng cấp Ethereum từ Proof of Work (PoW) sang Proof of Stake (PoS) đã gặp phải rất nhiều tranh cãi trước khi thành công.

c. Khả năng quyết định của cộng đồng

Một số blockchain, chẳng hạn như Ethereum, đã áp dụng cơ chế quản trị phi tập trung thông qua các DAO (Decentralized Autonomous Organizations), nơi các quyết định được đưa ra thông qua việc bỏ phiếu của cộng đồng. Tuy nhiên, việc này vẫn gặp phải nhiều vấn đề như sự tham gia của cộng đồng hạn chế, sự thiếu vắng các cơ chế kiểm soát và những rủi ro về việc bị thao túng bởi các nhóm có ảnh hưởng lớn.

5.1.2.2. Thách thức về khả năng tương tác của các mạng lưới Blockchain

Khả năng tương tác giữa các blockchain (cross-chain interoperability) là một trong những yếu tố quan trọng để tạo ra một hệ sinh thái blockchain toàn diện, nơi các mạng lưới có thể giao tiếp và trao đổi dữ liệu hoặc tài sản với nhau. Tuy nhiên, vấn đề này gặp phải một số thách thức lớn:

a. Thiếu tiêu chuẩn chung

Mỗi blockchain đều có các đặc điểm và giao thức riêng biệt, điều này tạo ra sự phân mảnh lớn trong không gian blockchain. Các mạng lưới khác nhau có thể sử dụng các hệ thống đồng thuận, cách thức mã hóa và mô hình kinh tế hoàn toàn khác nhau. Việc này làm cho việc kết nối và tương tác giữa các blockchain trở nên phức tạp và đòi hỏi sự phát triển các công nghệ và tiêu chuẩn chung. Hiện tại, không có một tiêu chuẩn chung duy nhất cho khả năng tương tác của các mạng blockchain.

b. Cầu nối và trung gian

Một trong những phương pháp hiện tại để giải quyết vấn đề tương tác giữa các blockchain là thông qua các cầu nối (bridges), cho phép chuyển tài sản và dữ liệu giữa các mạng lưới khác nhau. Tuy nhiên, cầu nối cũng mang lại những rủi ro, đặc biệt là vấn đề bảo mật. Các vụ tấn công nhằm vào các cầu nối blockchain, chẳng hạn như hack Poly Network năm 2021, đã làm lộ ra những lỗ hổng trong hệ thống, gây thiệt hại hàng trăm triệu đô la.

c. Các giải pháp Layer 2 và giao thức liên chuỗi

Các giải pháp Layer 2 như Lightning Network (cho Bitcoin) và các giao thức liên chuỗi như Polkadot, Cosmos, hay Avalanche được phát triển để giải quyết vấn đề khả năng tương tác. Các giải pháp này cho phép nhiều blockchain giao tiếp và tương tác với nhau mà không

cần phải thay đổi cấu trúc bên trong của từng mạng lưới. Tuy nhiên, các giải pháp này vẫn đang trong giai đoạn phát triển và không phải lúc nào cũng dễ dàng triển khai và duy trì.

5.1.2.3. Ví dụ thực tế

- **Ethereum và Bitcoin:** Mặc dù Ethereum và Bitcoin đều là hai blockchain lớn và phổ biến nhất, chúng không thể giao tiếp trực tiếp với nhau. Các giải pháp như wrapped Bitcoin (WBTC) trên Ethereum giúp giải quyết vấn đề này, nhưng vẫn có những hạn chế và không phải là một giải pháp tối ưu.
- **Polkadot:** Polkadot là một ví dụ về một blockchain được thiết kế từ đầu để hỗ trợ khả năng tương tác giữa các blockchain. Mạng Polkadot sử dụng một cơ chế gọi là parachains để kết nối các blockchain với nhau, giúp các ứng dụng và tài sản có thể chuyển giao giữa các mạng.

5.1.2.4. Tương lai của quản trị và khả năng tương tác

Mặc dù quản trị và khả năng tương tác của blockchain hiện tại còn nhiều thách thức, nhưng sự phát triển của các giao thức và nền tảng mới đang mở ra những cơ hội lớn. Các cơ chế quản trị phi tập trung đang ngày càng được hoàn thiện và phổ biến, đồng thời các giải pháp Layer 2 và giao thức liên chuỗi hứa hẹn sẽ giúp tạo ra một hệ sinh thái blockchain mạnh mẽ và liên kết chặt chẽ hơn trong tương lai.

Tóm lại, thách thức về quản trị và khả năng tương tác là những vấn đề quan trọng cần phải giải quyết để blockchain có thể trở thành một công nghệ thực sự phát triển và ứng dụng rộng rãi trong xã hội.

5.1.3. Thách thức về pháp lý và tuân thủ

5.1.3.1. Khung pháp lý chưa hoàn thiện

Một trong những thách thức lớn nhất trong việc áp dụng blockchain và cryptocurrency là khung pháp lý chưa hoàn thiện. Mặc dù blockchain đã tồn tại trong nhiều năm, các cơ quan pháp lý vẫn chưa hoàn thiện được các quy định cần thiết để điều chỉnh hoạt động của các mạng lưới này. Những vấn đề liên quan đến khung pháp lý bao gồm:

a. Thiếu các quy định rõ ràng về cryptocurrency và blockchain

Trong khi một số quốc gia đã bắt đầu xây dựng các quy định liên quan đến cryptocurrency và blockchain, phần lớn các quy định này còn thiếu rõ ràng và đầy đủ. Các quốc gia như Mỹ, Trung Quốc, và Liên minh Châu Âu đều đã bắt đầu thử nghiệm và đưa ra

một số quy định, nhưng nhiều khía cạnh vẫn chưa được giải quyết, như cách thức phân loại các cryptocurrency, thuế đối với các giao dịch blockchain, hoặc các quy định về bảo vệ người tiêu dùng.

Ví dụ, tại Mỹ, Cơ quan Chứng khoán và Giao dịch (SEC) chưa đưa ra một định nghĩa rõ ràng về cryptocurrency và đối tượng quản lý đối với từng loại tiền kỹ thuật số. Điều này dẫn đến sự bất ổn trong các giao dịch và các quyết định đầu tư liên quan đến cryptocurrency.

b. Khác biệt trong quy định giữa các quốc gia

Một thách thức lớn khác là sự khác biệt trong quy định giữa các quốc gia. Mỗi quốc gia có một cách tiếp cận khác nhau đối với blockchain và cryptocurrency, tạo ra một môi trường pháp lý phức tạp. Một số quốc gia như Nhật Bản và Thụy Sĩ đã chấp nhận cryptocurrency và blockchain, coi chúng như một phần của nền kinh tế chính thống, trong khi các quốc gia khác như Trung Quốc và Ấn Độ đã đưa ra các biện pháp cấm hoặc hạn chế nghiêm ngặt đối với các hoạt động liên quan đến blockchain và cryptocurrency.

Sự khác biệt này không chỉ tạo ra sự thiếu đồng bộ trong các quy định mà còn làm cho các doanh nghiệp và cá nhân gặp khó khăn trong việc hoạt động xuyên quốc gia. Việc không có một hệ thống pháp lý thống nhất có thể khiến các công ty blockchain gặp khó khăn trong việc mở rộng và tuân thủ các quy định quốc tế.

Điều đáng mừng là trong năm 2024, Việt Nam đã ban hành Quyết định số 1236/QĐ-TTg của Thủ tướng Chính phủ về Chiến lược quốc gia ứng dụng và phát triển công nghệ chuỗi khối (blockchain) đến năm 2025, định hướng đến năm 2030. Quyết định này xác định Blockchain là một công nghệ trọng tâm cần được ưu tiên phát triển, với tầm nhìn đưa Việt Nam trở thành quốc gia dẫn đầu khu vực và có vị thế quốc tế trong nghiên cứu, triển khai công nghệ Blockchain vào năm 2030. Đây là nền tảng pháp lý quan trọng, góp phần thúc đẩy chuyển đổi số toàn diện, đồng thời mở ra cơ hội phát triển mạnh mẽ cho công nghệ Blockchain tại Việt Nam hiện tại và trong tương lai.

c. Thách thức trong việc áp dụng luật hiện hành với công nghệ mới

Một trong những vấn đề lớn là việc áp dụng các luật hiện hành vào blockchain và cryptocurrency. Các luật hiện tại được thiết kế cho các hệ thống tài chính truyền thống và không phù hợp với các đặc điểm riêng biệt của blockchain như tính phi tập trung, sự ẩn danh và khả năng tự động hóa thông qua smart contracts. Điều này gây khó khăn cho các cơ quan quản lý trong việc điều chỉnh và áp dụng các quy định hiện hành đối với các công nghệ mới này.

5.1.3.2. Bảo vệ người dùng trong hệ sinh thái Blockchain

Một trong những yếu tố quan trọng cần được xem xét trong các mạng blockchain là bảo vệ người dùng. Mặc dù blockchain mang lại sự minh bạch và bảo mật, nhưng các vấn đề bảo vệ người dùng lại rất phức tạp, đặc biệt là trong môi trường phi tập trung và không có trung gian. Các thách thức lớn về bảo vệ người dùng bao gồm:

a. Thiếu cơ chế bảo vệ người dùng khi xảy ra sự cố

Trong hệ thống blockchain, các giao dịch là không thể thay đổi và không có một cơ chế rõ ràng để giải quyết khi có sự cố xảy ra, chẳng hạn như khi tài sản của người dùng bị đánh cắp hoặc mất. Việc thiếu các cơ chế pháp lý hoặc cơ chế bảo vệ người tiêu dùng khiến người dùng gặp nhiều rủi ro khi tham gia vào các mạng lưới blockchain.

Một ví dụ điển hình là các vụ hack các sàn giao dịch tiền mã hóa, nơi người dùng có thể mất tài sản mà không có cơ hội khôi phục hoặc bảo vệ quyền lợi của mình. Vì không có một cơ quan giám sát hoặc bảo vệ pháp lý như các ngân hàng truyền thống, việc yêu cầu bồi thường hoặc giải quyết tranh chấp trở nên khó khăn.

b. Khó khăn trong việc khôi phục tài sản số bị mất hoặc đánh cắp

Một vấn đề lớn khác trong blockchain là việc khôi phục tài sản số bị mất hoặc đánh cắp. Với tính chất phi tập trung và không có cơ chế giám sát trung gian, khi người dùng mất quyền truy cập vào ví của mình hoặc tài sản bị đánh cắp, rất khó để khôi phục hoặc có được sự hỗ trợ pháp lý. Các thợ đào hoặc hacker có thể lấy cắp tiền từ các ví điện tử mà không có cơ chế dễ dàng để lấy lại tài sản.

Một số sàn giao dịch hoặc dịch vụ ví điện tử cung cấp các giải pháp khôi phục mật khẩu hoặc tài khoản, nhưng chúng lại có hạn chế và không phải lúc nào cũng hiệu quả.

c. Vấn đề về quyền riêng tư và bảo mật thông tin

Blockchain cung cấp một mức độ bảo mật cao nhờ vào cơ chế mã hóa và phân tán, nhưng vấn đề bảo vệ quyền riêng tư vẫn là một thách thức. Các giao dịch trên blockchain, mặc dù được bảo vệ bởi các mã hóa phức tạp, vẫn có thể được theo dõi và phân tích nếu không sử dụng các biện pháp bảo vệ bổ sung như coin mixers hoặc các blockchain chuyên dụng cho quyền riêng tư như Monero và Zcash.

Ngoài ra, việc quản lý và bảo vệ dữ liệu cá nhân của người dùng trên các nền tảng blockchain vẫn chưa được quy định rõ ràng, đặc biệt khi blockchain là một công nghệ không

thay đổi và lưu trữ dữ liệu vĩnh viễn. Việc lưu trữ dữ liệu nhạy cảm trên blockchain mà không có cơ chế bảo mật hợp lý có thể tạo ra nguy cơ rò rỉ thông tin và vi phạm quyền riêng tư của người dùng.

5.1.3.3. Tương lai của pháp lý và bảo vệ người dùng trong Blockchain

Để giải quyết các thách thức pháp lý và bảo vệ người dùng, các quốc gia và tổ chức quốc tế cần hợp tác để xây dựng các khuôn khổ pháp lý rõ ràng và phù hợp với công nghệ blockchain. Điều này có thể bao gồm việc xây dựng các tiêu chuẩn toàn cầu cho việc bảo vệ người tiêu dùng, tăng cường các quy định về bảo mật và quyền riêng tư, và phát triển các cơ chế bảo vệ người dùng trong trường hợp xảy ra sự cố.

5.1.4. Thách thức về xã hội và chấp nhận

5.1.4.1. Rào cản về nhận thức

Mặc dù công nghệ blockchain có tiềm năng lớn trong nhiều lĩnh vực, nhưng vẫn còn một số rào cản về nhận thức mà các tổ chức và người dùng cần phải vượt qua. Dưới đây là những vấn đề quan trọng liên quan đến nhận thức xã hội về blockchain:

1. **Thiếu hiểu biết về công nghệ blockchain**: Một trong những rào cản lớn nhất trong việc áp dụng blockchain là sự thiếu hiểu biết chung về công nghệ này. Rất nhiều người và doanh nghiệp vẫn chưa hiểu rõ về cách blockchain hoạt động, cũng như các ứng dụng tiềm năng của nó. Việc thiếu thông tin và sự giáo dục về blockchain khiến cho nhiều người không dám thử nghiệm hoặc đầu tư vào công nghệ này, mặc dù nó có thể mang lại nhiều lợi ích.
2. **Lo ngại về tính bảo mật và độ tin cậy**: Mặc dù blockchain có thể mang lại sự bảo mật cao, nhưng các lỗ hổng trong phần mềm, các cuộc tấn công mạng và việc sử dụng không đúng cách có thể làm dấy lên lo ngại về tính bảo mật. Cộng đồng vẫn còn lo ngại về các vấn đề như gian lận, mất tiền, và các vụ hack đã xảy ra trước đây. Điều này gây ảnh hưởng đến lòng tin của người dùng vào blockchain, đặc biệt trong các ứng dụng như tiền điện tử và các hợp đồng thông minh.
3. **Thói quen sử dụng hệ thống truyền thống**: Người tiêu dùng và các tổ chức đã quen với các hệ thống tài chính truyền thống và các mô hình kinh doanh cũ. Việc chuyển sang các hệ thống phân quyền mới đòi hỏi thời gian và sự thay đổi trong tư duy. Việc thay đổi này không chỉ khó khăn về mặt kỹ thuật mà còn đụng phải các thói quen lâu dài trong việc sử dụng các dịch vụ tài chính, thanh toán, và quản lý dữ liệu.

5.1.4.2. Chi phí triển khai

Dù blockchain mang lại nhiều lợi ích, nhưng việc triển khai và áp dụng công nghệ này cũng đụng phải những vấn đề về chi phí, đặc biệt là đối với các doanh nghiệp vừa và nhỏ.

1. **Chi phí đầu tư ban đầu cao**: Để triển khai blockchain, các doanh nghiệp phải đối mặt với chi phí đầu tư ban đầu rất lớn. Điều này bao gồm việc xây dựng hạ tầng, tuyển dụng nhân lực chuyên môn, và phát triển các ứng dụng blockchain. Các chi phí này có thể khiến cho việc triển khai blockchain trở nên khó khăn đối với các doanh nghiệp có nguồn lực hạn chế.
2. **Thiếu nguồn nhân lực có chuyên môn**: Blockchain là một công nghệ mới, và việc tìm kiếm nhân lực có chuyên môn về blockchain hiện nay vẫn là một vấn đề lớn. Các kỹ sư blockchain và các chuyên gia trong lĩnh vực này rất hiếm và đắt đỏ, gây khó khăn cho các doanh nghiệp khi muốn triển khai các giải pháp blockchain. Bên cạnh đó, việc đào tạo nhân viên cũng đụng phải thách thức lớn vì kiến thức chuyên sâu về blockchain không được dạy phổ biến trong các trường đại học.
3. **Chi phí vận hành và bảo trì**: Sau khi triển khai, các doanh nghiệp còn phải đối mặt với chi phí vận hành và bảo trì. Các nền tảng blockchain yêu cầu bảo trì hệ thống, nâng cấp phần mềm, và giám sát bảo mật liên tục. Đặc biệt đối với các ứng dụng lớn, chi phí này có thể trở thành gánh nặng lâu dài.

5.2. Blockchain 3.0: Các Đột Phá Mới trong Công Nghệ Blockchain

Blockchain 3.0 đại diện cho sự tiến hóa của công nghệ blockchain, giải quyết những hạn chế và vấn đề tồn tại trong các phiên bản trước đó (Blockchain 1.0 và 2.0). Nó tập trung vào những yếu tố như hiệu suất, khả năng mở rộng, bảo mật, và đặc biệt là tính bền vững. Ba yếu tố nổi bật trong Blockchain 3.0 là **Blockchain xanh**, **Zero-Knowledge Proof (ZKP)**, và **Layer 2 và Rollups**.

1. Blockchain Xanh

Một trong những vấn đề lớn của các nền tảng blockchain hiện tại là tiêu thụ năng lượng cao, đặc biệt là các mạng lưới sử dụng cơ chế đồng thuận Proof of Work (PoW), như Bitcoin. Trong khi Blockchain 2.0 (Ethereum) đang chuyển sang Proof of Stake (PoS) để giảm tiêu thụ năng lượng, Blockchain 3.0 tiếp tục tiến xa hơn với khái niệm **Blockchain xanh**.

- **Blockchain xanh** là những hệ thống blockchain được thiết kế để giảm thiểu tác động đến môi trường. Các nền tảng này sử dụng các cơ chế đồng thuận tiết kiệm năng

lượng, như PoS, hoặc các công nghệ thay thế khác để giúp giảm lượng năng lượng cần thiết cho việc vận hành mạng lưới.

- Một ví dụ điển hình là **Algorand**, một nền tảng blockchain sử dụng PoS và cam kết duy trì một mức phát thải carbon cực thấp. Điều này giúp các blockchain xanh không chỉ có thể mở rộng và thực hiện các giao dịch nhanh chóng mà còn giảm thiểu tác động tiêu cực tới môi trường.
- **Cardano và Tezos** cũng là những ví dụ của các nền tảng chú trọng vào tính bền vững và hiệu quả năng lượng trong khi duy trì các tính năng bảo mật và khả năng mở rộng.

2. Zero-Knowledge Proof (ZKP)

Zero-Knowledge Proof (ZKP) là một trong những công nghệ quan trọng trong Blockchain 3.0 giúp nâng cao bảo mật và quyền riêng tư của người dùng mà không cần tiết lộ dữ liệu nhạy cảm. ZKP là một kỹ thuật trong đó một bên (người chứng minh) có thể chứng minh với một bên khác (người xác minh) rằng một tuyên bố là đúng mà không cần tiết lộ bất kỳ thông tin nào ngoài tính đúng đắn của tuyên bố đó.

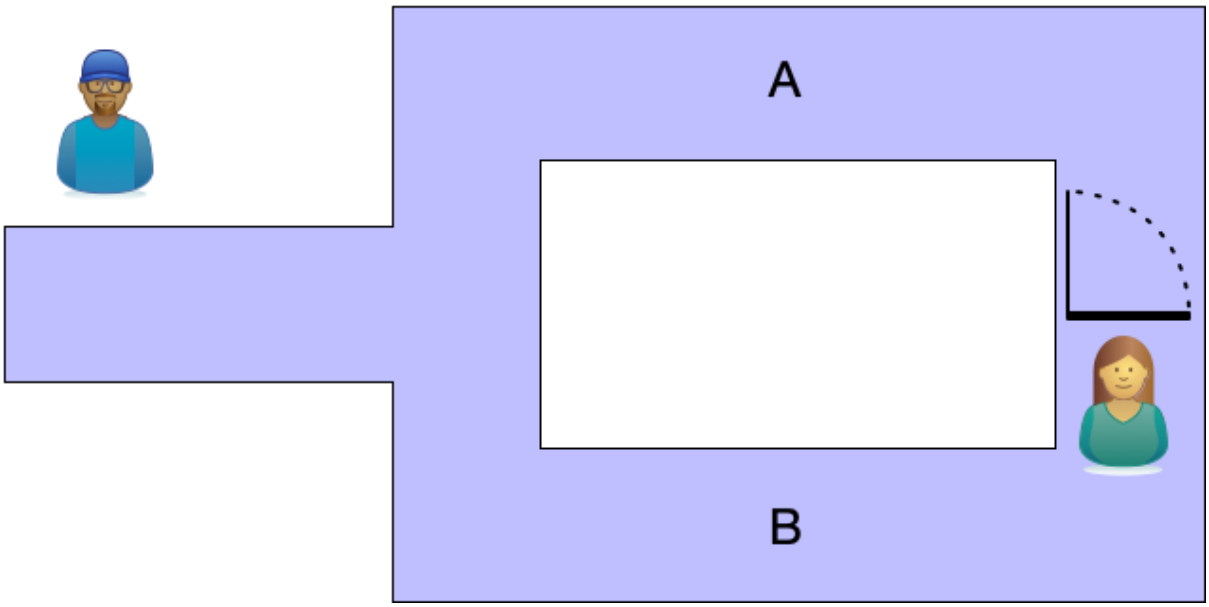
Giả sử Peggy cần chứng minh với Victor rằng cô ấy đang sở hữu một bí mật mà không tiết lộ bí mật đó. Cô ấy có thể làm vậy một cách thuyết phục Victor rằng cô ấy thực sự biết bí mật đó không? Đây là câu hỏi nằm ở trung tâm của một trong những quy trình mật mã mạnh mẽ nhất mà chúng ta có thể sử dụng trong các hệ thống nhận dạng: bằng chứng không có kiến thức (ZKP). Giả sử ví dụ rằng Peggy có một giấy phép lái xe kỹ thuật số và muốn chứng minh với Victor, người phục vụ tại quầy bar, rằng cô ấy trên 21 tuổi mà không cần đưa giấy phép lái xe của mình hoặc thậm chí không cần cho anh ta xem ngày sinh của cô. ZKPs cho phép Peggy chứng minh rằng giấy phép lái xe của cô nói rằng cô ấy ít nhất 21 tuổi mà không cần tiết lộ bất kỳ thông tin nào khác (tức là không có kiến thức dư thừa).

Vấn đề này lần đầu tiên được các nhà nghiên cứu MIT Shafi Goldwasser, Silvio Micali và Charles Rackoff khám phá vào những năm 1980 như một cách để chống lại sự rò rỉ thông tin. Mục tiêu là giảm bớt lượng thông tin thừa mà người xác minh, Victor, có thể biết về người chứng minh, Peggy.

Một cách để hiểu cách thức hoạt động của ZKP là câu chuyện về Hang động Alibaba, lần đầu tiên được các nhà mật mã học Quisquater, Guillou và Berson công bố. Sơ đồ sau đây cung cấp một minh họa.

Peggy và Victor trong "Hang động Alibaba"

Hang động Alibaba có hai lối đi, được đánh dấu là A và B, chia ra từ một hành lang duy nhất nối với cửa ra vào. Peggy sở hữu một mã bí mật cho phép cô mở khóa một cánh cửa nối A và B. Victor muốn mua mã này nhưng sẽ không trả tiền cho đến khi anh ấy chắc chắn rằng Peggy biết mã này. Peggy sẽ không chia sẻ nó với Victor cho đến khi anh ấy trả tiền.



Thuật toán để Peggy chứng minh rằng cô ấy biết mã tiến hành như sau:

1. Victor đứng ngoài hang động trong khi Peggy vào và chọn một trong các lối đi. Victor không được phép nhìn thấy lối đi nào mà Peggy chọn.
2. Victor vào hang và gọi ra "A" hoặc "B" một cách ngẫu nhiên.
3. Peggy xuất hiện từ đúng lối đi vì cô có thể dễ dàng mở cửa dù chọn lối đi nào khi vào.
4. Tất nhiên, Peggy có thể chỉ đoán đúng và may mắn, vì vậy Peggy và Victor sẽ thử lại thí nghiệm nhiều lần.
5. Nếu Peggy luôn có thể trở lại từ lối đi mà Victor chọn, thì xác suất Peggy thực sự biết mã sẽ tăng dần. Sau 20 lần thử, có ít hơn một cơ hội trong triệu lần rằng Peggy chỉ đơn giản là đoán đúng chữ mà Victor sẽ gọi. Đây là một bằng chứng xác suất cho thấy Peggy biết bí mật.

Thuật toán này không chỉ cho phép Peggy thuyết phục Victor rằng cô ấy biết mã mà còn làm điều đó theo cách đảm bảo Victor không thể thuyết phục ai khác rằng Peggy biết mã. Giả sử Victor ghi lại toàn bộ giao dịch. Điều duy nhất mà người quan sát thấy là Victor gọi các chữ cái và Peggy xuất hiện từ đúng đường hầm. Người quan sát không thể chắc chắn rằng Victor và Peggy không đã thỏa thuận trước một chuỗi các chữ cái để lừa người quan sát. Lưu ý rằng

tính chất này phụ thuộc vào việc thuật toán sử dụng một bộ sinh số giả ngẫu nhiên tốt với một hạt giống có độ ngẫu nhiên cao để Peggy và người quan sát thứ ba không thể dự đoán các lựa chọn của Victor.

Do đó, trong khi Peggy không thể từ chối với Victor rằng cô ấy biết bí mật, cô ấy có thể từ chối rằng cô ấy biết bí mật với những bên thứ ba khác. Điều này đảm bảo rằng bất cứ điều gì cô ấy chứng minh cho Victor sẽ chỉ giữa họ và Victor không thể tiết lộ nó - ít nhất là theo cách mật mã chứng minh rằng nó đến từ Peggy. Peggy giữ quyền kiểm soát cả bí mật của mình và việc cô ấy biết bí mật đó.

Khi chúng ta nói "không có kiến thức" và nói về việc Victor không học được gì ngoài tuyên bố đang được kiểm tra, điều đó không hoàn toàn chính xác. Trong hang động Alibaba, Peggy chứng minh trong không có kiến thức rằng cô ấy biết bí mật. Nhưng có rất nhiều điều khác mà Victor học về Peggy mà ZKP không thể làm gì được. Ví dụ, Victor biết rằng Peggy có thể nghe thấy anh ta, nói cùng ngôn ngữ, đi bộ, và hợp tác. Anh ta cũng có thể học được những điều về hang động, như mất bao lâu để mở cửa. Peggy học được những điều tương tự về Victor. Vì vậy, thực tế là bằng chứng là kiến thức gần như không có chứ không phải là hoàn toàn không có kiến thức.

Hệ thống ZKP

Ví dụ về Hang động Alibaba là một ứng dụng rất cụ thể của ZKPs, gọi là bằng chứng không có kiến thức về kiến thức (zero-knowledge proof of knowledge). Peggy đang chứng minh rằng cô ấy biết (hoặc sở hữu một thứ gì đó). Nói chung, Peggy có thể muốn chứng minh nhiều sự thật với Victor. Những sự thật này có thể bao gồm các mệnh đề hoặc thậm chí các giá trị. ZKP có thể làm được điều này.

Để hiểu cách chúng ta có thể chứng minh các mệnh đề trong không có kiến thức, hãy xem một ví dụ khác, đôi khi được gọi là Vấn đề Triệu phú Xã hội chủ nghĩa. Giả sử Peggy và Victor muốn biết liệu họ có được trả lương công bằng không. Cụ thể, họ muốn biết liệu họ có được trả cùng một mức lương hay không, nhưng không muốn tiết lộ mức lương cụ thể của mình cho nhau hoặc thậm chí cho một bên thứ ba đáng tin cậy. Trong trường hợp này, Peggy không chứng minh cô ấy biết một bí mật, mà cô ấy chứng minh một mệnh đề về sự bình đẳng (hoặc không bình đẳng).

Để đơn giản, giả sử Peggy và Victor được trả một trong các mức lương $10, $20, $30 hoặc $40 mỗi giờ. Thuật toán hoạt động như sau:

1. Peggy mua bốn hộp khóa và gắn nhãn $10, $20, $30, và $40.
2. Cô ấy vứt đi chìa khóa của mọi hộp trừ hộp có nhãn mức lương của cô.
3. Peggy đưa tất cả các hộp khóa cho Victor, người sẽ bí mật bỏ một mẩu giấy có dấu "+" vào khe trên hộp có mức lương của anh ta. Anh ấy sẽ bỏ mẩu giấy có dấu "-" vào tất cả các hộp còn lại.
4. Victor trả lại các hộp cho Peggy, người sẽ sử dụng chìa khóa của mình để mở hộp có mức lương của cô.
5. Nếu cô tìm thấy dấu "+", điều đó có nghĩa là họ có mức lương giống nhau. Nếu không, họ có mức lương khác nhau. Cô ấy có thể sử dụng điều này để chứng minh sự thật cho Victor.

Đây được gọi là chuyển giao không biết và chứng minh mệnh đề "VictorSalary = PeggySalary" là đúng hay sai trong không có kiến thức (tức là, mà không tiết lộ bất kỳ thông tin nào khác).

Để điều này hoạt động, Peggy và Victor phải tin tưởng vào việc đối phương sẽ minh bạch và khai báo mức lương thật của mình. Victor cần tin rằng Peggy sẽ vứt đi ba chìa khóa còn lại. Peggy phải tin rằng Victor sẽ chỉ bỏ một mẩu giấy có dấu "+" vào các hộp.

Cũng giống như chứng chỉ kỹ thuật số cần có một hệ thống PKI để tạo dựng sự tin tưởng vượt ra ngoài những gì có thể có chỉ với chứng chỉ tự phát hành, ZKPs mạnh mẽ hơn trong một hệ thống cho phép Peggy và Victor chứng minh các sự thật từ những điều mà người khác nói về họ, không chỉ từ những gì họ nói về chính họ. Ví dụ, thay vì Peggy và Victor tự khẳng định mức lương của họ, giả sử họ có thể dựa vào một tài liệu đã được ký từ phòng nhân sự để đưa ra khẳng định, để cả hai đều biết rằng người kia đang khai báo mức lương thật của mình. **Chứng chỉ có thể xác minh (Verifiable Credentials)** cung cấp một hệ thống để sử dụng ZKPs nhằm chứng minh nhiều sự thật khác nhau, riêng lẻ hoặc kết hợp, theo cách tạo ra sự tin tưởng vào phương pháp và niềm tin vào dữ liệu.

ZKP không tương tác (Non-Interactive ZKPs)

Trong các ví dụ trước, Peggy đã có thể chứng minh những điều cho Victor thông qua một loạt các tương tác. Để ZKP trở nên thực tế, các tương tác giữa người chứng minh và người xác minh nên được giảm thiểu tối đa. May mắn thay, một kỹ thuật gọi là SNARK cho phép chứng minh không có kiến thức không tương tác.

SNARKs có các đặc điểm sau (từ đó tên gọi của chúng được sinh ra):

- **Ngắn gọn**: kích thước của các thông điệp là nhỏ so với độ dài của chứng minh thực tế.

- **Không tương tác**: ngoài một số thiết lập ban đầu, người chứng minh chỉ gửi một thông điệp duy nhất tới người xác minh.
- **Lập luận**: đây thực sự là một lập luận cho rằng cái gì đó là đúng, không phải là một chứng minh như chúng ta hiểu về mặt toán học. Cụ thể, người chứng minh lý thuyết có thể chứng minh các phát biểu sai nếu có đủ sức mạnh tính toán. Vì vậy, SNARKs là "chắc chắn về mặt tính toán" thay vì "chắc chắn tuyệt đối".
- **Kiến thức**: người chứng minh biết sự thật đang được nói đến.

Thông thường, bạn sẽ thấy "zk" (từ viết tắt của zero-knowledge) được thêm vào phía trước để chỉ rằng trong quá trình này, người xác minh không học được gì ngoài các sự kiện được chứng minh.

Toán học cơ bản của zkSNARKs liên quan đến tính toán đồng hình trên các đa thức bậc cao. Tuy nhiên, chúng ta có thể hiểu cách thức hoạt động của zkSNARKs mà không cần biết toán học cơ sở đảm bảo rằng chúng là chắc chắn. Nếu bạn muốn tìm hiểu thêm chi tiết về toán học, tôi khuyên bạn nên tham khảo "zkSNARKs in a Nutshell" của Christian Reitwiessner.

Lấy một ví dụ đơn giản, giả sử Victor được cung cấp một giá trị băm sha256, H, của một giá trị nào đó. Peggy muốn chứng minh rằng cô ấy biết một giá trị s sao cho sha256(s) == H mà không tiết lộ s cho Victor. Chúng ta có thể định nghĩa một hàm C mô tả mối quan hệ này:

$$C(x, w) = (\text{sha256}(w) == x)$$

Vậy C(H, s) == true, trong khi các giá trị khác cho w sẽ trả về false.

Việc tính toán một zkSNARK yêu cầu ba hàm G, P và V. G là hàm tạo khóa nhận đầu vào một tham số bí mật gọi là lambda và hàm C, rồi tạo ra hai khóa công khai, khóa chứng minh pk và khóa xác minh vk. Chúng chỉ cần được tạo ra một lần cho một hàm C nhất định. Tham số lambda phải bị hủy sau bước này vì nó không còn cần thiết và bất kỳ ai có nó đều có thể tạo ra các chứng minh giả.

Hàm chứng minh P nhận đầu vào là khóa chứng minh pk, một giá trị công khai x, và một chứng cứ (bí mật) w. Kết quả của việc thực thi P(pk,x,w) là một chứng minh, prf, rằng người chứng minh biết giá trị w thỏa mãn C.

Hàm xác minh V tính toán V(vk, x, prf), và kết quả là true nếu chứng minh prf là đúng và false nếu không phải.

Trở lại với Peggy và Victor, Victor chọn một hàm C đại diện cho điều anh ta muốn Peggy chứng minh, tạo ra một số ngẫu nhiên lambda, và chạy G để tạo ra khóa chứng minh và khóa xác minh:

$$(pk, vk) = G(C, lambda)$$

Peggy không được phép biết giá trị của lambda. Victor chia sẻ C, pk và vk với Peggy.

Peggy muốn chứng minh cô ấy biết giá trị s thỏa mãn C cho x = H. Cô ấy chạy hàm chứng minh P sử dụng các giá trị này làm đầu vào:

$$prf = P(pk, H, s)$$

Peggy đưa chứng minh prf cho Victor, người chạy hàm xác minh:

$$V(vk, H, prf)$$

Nếu kết quả là true, Victor có thể yên tâm rằng Peggy biết giá trị s.

Hàm C không cần phải giới hạn chỉ là một băm như trong ví dụ này. Trong giới hạn của toán học cơ sở, C có thể rất phức tạp và liên quan đến bất kỳ số lượng giá trị nào mà Victor muốn Peggy chứng minh, tất cả trong một lần.

Ứng dụng ZKP trong blockchain giúp bảo vệ quyền riêng tư của người dùng, vì các thông tin giao dịch không cần phải công khai nhưng vẫn đảm bảo rằng giao dịch đó là hợp lệ. Điều này có thể giúp giải quyết các vấn đề về bảo mật và quyền riêng tư trên các mạng lưới blockchain công khai như Ethereum.

- **Zcash** là một ví dụ về đồng tiền điện tử sử dụng ZKP. Nó cho phép người dùng thực hiện giao dịch mà không tiết lộ số tiền hoặc người nhận, qua đó bảo vệ quyền riêng tư của họ.
- **zk-SNARKs** (Zero-Knowledge Succinct Non-Interactive Argument of Knowledge) là một dạng cụ thể của ZKP, đã được áp dụng trên Ethereum để cải thiện khả năng bảo mật và tối ưu hiệu suất các hợp đồng thông minh.

3. Layer 2 và Rollups

Trong bối cảnh Blockchain 3.0, **Layer 2** và **Rollups** là các giải pháp nâng cao khả năng mở rộng và hiệu suất của các blockchain, đặc biệt là Ethereum, mà không làm giảm tính bảo mật hoặc phi tập trung.

Layer 2

Layer 2 (L2) là một giải pháp giúp cải thiện khả năng mở rộng và hiệu suất của các mạng blockchain mà không làm giảm tính bảo mật hoặc phi tập trung. Để hiểu rõ hơn về Layer 2, hãy tưởng tượng blockchain giống như một con đường giao thông, nơi tất cả các giao dịch đều phải di chuyển qua con đường chính (Layer 1). Nếu con đường này quá đông đúc, việc giao dịch sẽ rất chậm và tốn kém. Layer 2 giống như việc xây dựng thêm những con đường phụ, giúp các giao dịch có thể di chuyển nhanh hơn mà không làm tắc nghẽn con đường chính.

Cách thực Layer 2 hoạt động?

Layer 2 hoạt động bằng cách xử lý các giao dịch ngoài chuỗi chính (Layer 1) và chỉ gửi dữ liệu quan trọng hoặc kết quả của giao dịch đó vào blockchain chính. Việc này giúp giảm tải cho Layer 1, tăng tốc độ giao dịch và giảm chi phí giao dịch mà không cần phải ghi tất cả mọi giao dịch vào blockchain chính.

Có hai loại giải pháp Layer 2 phổ biến:

1. **State Channels**:
    - Là một kênh giao tiếp giữa hai bên (hoặc nhiều bên) mà các giao dịch diễn ra bên ngoài blockchain chính. Sau khi các giao dịch hoàn tất, kết quả cuối cùng được ghi vào blockchain chính.
    - Ví dụ: Giả sử bạn và tôi muốn trao đổi tiền trong một khoảng thời gian dài. Thay vì mỗi lần trao đổi lại ghi vào blockchain (mất thời gian và chi phí), chúng ta có thể giao dịch ngoài chuỗi qua một state channel và chỉ ghi kết quả cuối cùng vào blockchain.
2. **Rollups**:
    - Rollups hoạt động bằng cách chuyển các giao dịch và tính toán ra ngoài blockchain chính (Layer 1), nhưng các kết quả này vẫn được xác minh và công nhận trên blockchain chính. Điều này giúp giảm thiểu sự tắc nghẽn và chi phí giao dịch của blockchain chính, đồng thời vẫn đảm bảo tính bảo mật và phi tập trung. Các giao dịch được thực hiện trên Layer 2 và sau đó "cuộn" lại thành một giao dịch duy nhất hoặc một nhóm giao dịch để ghi vào blockchain chính. Kết quả là chỉ có dữ liệu tổng hợp của các giao dịch mới được lưu trữ trên blockchain chính, không cần lưu trữ tất cả các giao dịch chi tiết. Có hai loại Rollups chính:

- **Optimistic Rollups**: Giả định rằng các giao dịch là hợp lệ và không kiểm tra ngay lập tức, nhưng có thể yêu cầu chứng minh nếu có nghi ngờ về tính hợp lệ của giao dịch.
- **zk-Rollups**: Sử dụng công nghệ Zero-Knowledge Proof (ZKP) để xác minh tính chính xác của các giao dịch mà không cần phải tiết lộ toàn bộ dữ liệu giao dịch, giúp tăng cường bảo mật và hiệu suất.

Lợi ích của Layer 2

- **Tăng tốc giao dịch**: Layer 2 giúp giao dịch diễn ra nhanh hơn vì nó giảm bớt sự tắc nghẽn trên blockchain chính.
- **Giảm chi phí**: Bằng cách xử lý các giao dịch ngoài chuỗi, chi phí giao dịch giảm đáng kể so với khi phải thực hiện tất cả trên blockchain chính.
- **Mở rộng quy mô**: Các giải pháp Layer 2 giúp blockchain có thể xử lý nhiều giao dịch hơn mà không gặp phải các vấn đề về tắc nghẽn hoặc chi phí cao.

Ví dụ về Layer 2

- **Lightning Network** trên Bitcoin là một ví dụ nổi bật về Layer 2. Nó cho phép người dùng thực hiện giao dịch nhanh chóng và rẻ hơn mà không cần phải ghi tất cả vào blockchain chính của Bitcoin.
- **Optimism và Arbitrum** trên Ethereum là hai giải pháp Layer 2 đang giúp Ethereum giải quyết vấn đề tắc nghẽn và chi phí giao dịch cao.

Layer 2 là một công nghệ quan trọng giúp blockchain có thể mở rộng và xử lý nhiều giao dịch hơn mà không làm giảm tính bảo mật hoặc phi tập trung. Các giải pháp như State Channels và Rollups sẽ giúp cải thiện hiệu suất của blockchain và giảm chi phí giao dịch, tạo ra một hệ sinh thái blockchain mạnh mẽ và hiệu quả hơn trong tương lai.

Như vậy, việc phát triển các giải pháp cho mạng lưới Blockchain thế hệ 3.0 và xa hơn nữa không chỉ đơn thuần là những cải tiến về công nghệ mà còn tập trung vào những yếu tố quan trọng như bảo mật, hiệu suất, khả năng mở rộng và tính bền vững. Những công nghệ mới như Blockchain xanh, Zero-Knowledge Proofs và Layer 2, Rollups là những yếu tố giúp blockchain giải quyết các vấn đề còn tồn tại trong các phiên bản trước đó, đồng thời mở ra nhiều cơ hội cho việc ứng dụng blockchain trong nhiều lĩnh vực khác nhau trong tương lai.

5.3. Tổng kết

Blockchain là một công nghệ đầy tiềm năng nhưng đang phải đối mặt với nhiều thách thức phức tạp. Việc giải quyết các thách thức này đòi hỏi sự nỗ lực của toàn bộ cộng đồng blockchain, từ các nhà phát triển, doanh nghiệp đến các cơ quan quản lý. Sự phát triển của công nghệ và các giải pháp mới đang dần giải quyết những thách thức này, mở ra triển vọng cho việc ứng dụng blockchain rộng rãi hơn trong tương lai.

Câu hỏi ôn tập

1. Phân tích các thách thức chính về khả năng mở rộng của blockchain và đề xuất giải pháp khắc phục.
2. Tại sao vấn đề tiêu thụ năng lượng lại là một thách thức lớn đối với blockchain? Các giải pháp nào đang được phát triển để giải quyết vấn đề này?
3. So sánh các thách thức về mặt kỹ thuật và thách thức về mặt quản trị trong việc triển khai blockchain.
4. Thảo luận về vai trò của khung pháp lý trong việc phát triển và ứng dụng công nghệ blockchain.
5. Đánh giá tác động của các thách thức xã hội đối với việc chấp nhận và áp dụng rộng rãi công nghệ blockchain.

TÀI LIỆU THAM KHẢO

[1] Andreas M. Antonopoulos, “Mastering Bitcoin”, Second edition, Oreilly (2017).

[2] Andreas M. Antonopoulos, Dr. Gavin Wood, “MasteringEthereum, Building Smart Contracts and DApps”, Oreilly (2019).

[3] The Byzantine Generals Problem, Leslie Lamport, Robert Shostak, and Marshall Pease, SRI International (1982).

[4] Markus Jakobsson, Proofs of work and bread pudding protocols (extended abstract), Information Sciences Research Center, Bell Labs, Murray Hili, New Jersey 07974, www.bell-Iabs.com/user (1999).

[5] Iddo Bentov, Charles Lee, Alex Mizrahi, and Meni Rosenfeld. Proof of activity: Extending bitcoin’s proof of work via proof of stake [extended abstract]y. SIGMETRICS Performance Evaluation Review, 42(3):34–37, 2014

[6] Aggelos Kiayias, Alexander Russell, Bernardo David, Roman Oliynykov, Ouroboros: A Provably Secure Proof-of-Stake Blockchain Protocol, July 20, 2019

[7] https://www.lcx.com/proof-of-authority-explained/

[8] https://academy.cardanofoundation.org/cbca

[9] https://ocw.mit.edu/courses/15-s12-blockchain-and-money-fall-018/pages/lecture-slides/

[10] https://iohk.io/en/research/library/papers/ouroboros-a-provably-secure-proof-of-stake-blockchain-protocol/

[11] Stallings, William. "Cryptography and Network Security: Principles and Practice" (7th Edition)

[12] Schneier, Bruce. "Applied Cryptography: Protocols, Algorithms, and Source Code in C" (2nd Edition)

[13] Stinson, Douglas R. "Cryptography: Theory and Practice"

[14] Katz, Jonathan; Lindell, Yehuda. "Introduction to Modern Cryptography"

[15] Menezes, Alfred; van Oorschot, Paul C.; Vanstone, Scott A. "Handbook of Applied Cryptography" (CRC Press, 1996)

[16] Schneier, Bruce. "Applied Cryptography: Protocols, Algorithms, and Source Code in C" (John Wiley & Sons, 2015)

[17] Coulouris, George; Dollimore, Jean; Kindberg, Tim; Blair, Gordon. "Distributed Systems: Concepts and Design" (5th Edition)

[18] Tanenbaum, Andrew S.; Van Steen, Maarten. "Distributed Systems: Principles and Paradigms" (2nd Edition)