

## CHƯƠNG 3

# MỘT SỐ NỀN TẢNG BLOCKCHAIN

Cho đến nay, Blockchain đã trải qua một hành trình phát triển đầy ấn tượng tạm chia thành ba thế hệ, với mỗi bước tiến là một sự cải thiện đáng kể về chức năng, hiệu suất và ứng dụng thực tế. Nay chúng ta cùng điểm qua sự tiến hóa và những khác biệt nổi bật của từng thế hệ blockchain.

### Thế hệ đầu tiên: Bitcoin – Nền tảng của Blockchain

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 không có tính năng lập trình.

### 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, Ethereum cũng kế thừa nhiều hạn chế của Bitcoin, bao gồm việc sử dụng bằng chứng công việc 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

<b>Phương pháp tiếp cận phát triển</b>	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
<b>Quản trị On-chain</b>	Không	Không	Có

### 3.1. Thế hệ đầu tiên: Bitcoin – Nền tảng của Blockchain

#### 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.

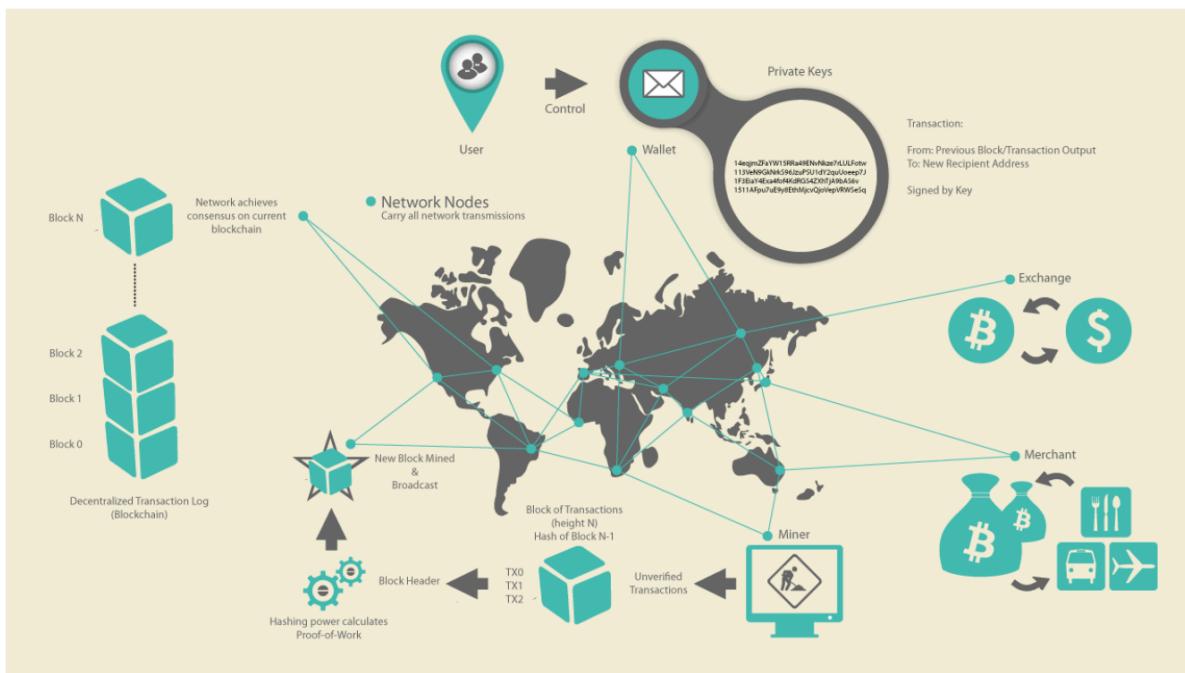
### 3.1.2. Nguyên lý hoạt động và cơ chế giao dịch của Bitcoin

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.

#### 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.

## 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.

## Đầu vào và đầu ra của giao dịch

Giao dịch Bitcoin có thể được hình dung như các dòng trong một sổ kê 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.

Transaction as Double-Entry Bookkeeping			
Inputs	Value	Outputs	Value
Input 1	0.10 BTC	Output 1	0.10 BTC
Input 2	0.20 BTC	Output 2	0.20 BTC
Input 3	0.10 BTC	Output 3	0.20 BTC
Input 4	0.15 BTC		
Total Inputs:	0.55 BTC	Total Outputs:	0.50 BTC
<hr/>			
-			
<u>Inputs</u>	<u>0.55 BTC</u>		
<u>Outputs</u>	<u>0.50 BTC</u>		
<u>Difference</u>	<u>0.05 BTC (implied transaction fee)</u>		

Hình 3-2. Giao dịch như sổ kê toán kép

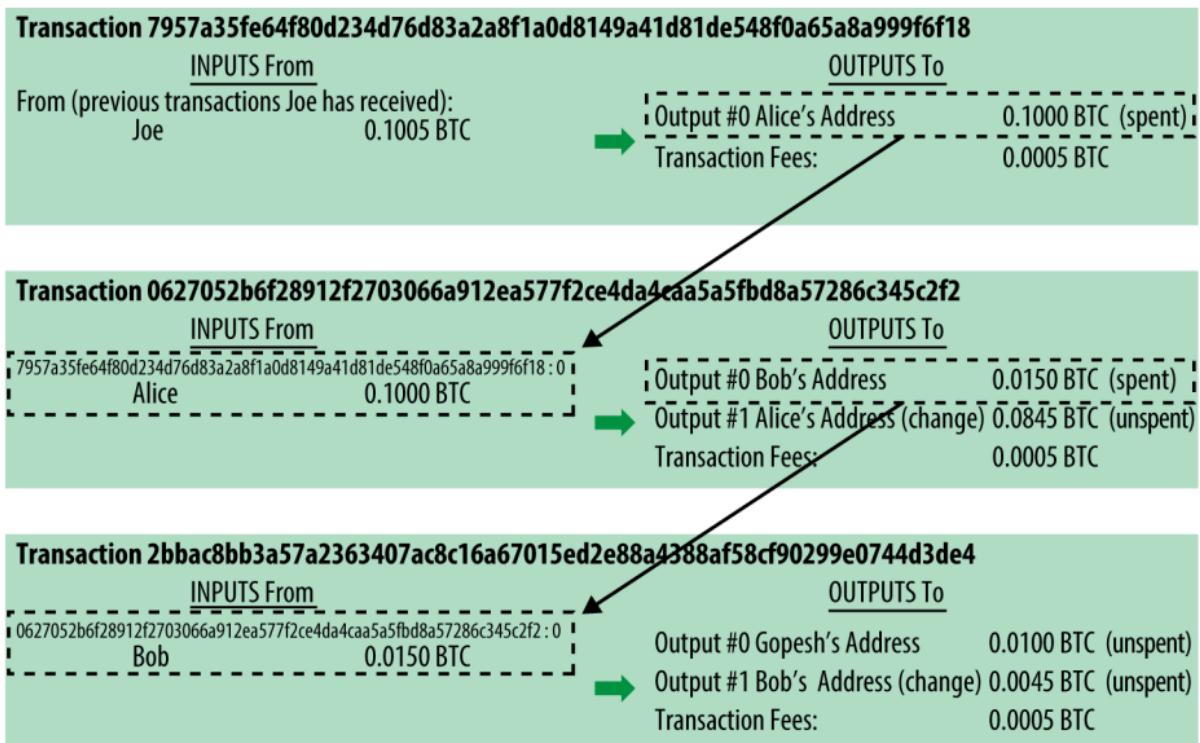
### Chuỗi giao dịch (Transaction Chains)

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 chẽ

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

### Thêm Giao Dịch vào Sô 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 khôi mới, sau khi được thêm vào blockchain, dần dần nhận được sự tin cậy ngày càng tăng từ mạng lưới khi có thêm nhiều khôi mới được bổ sung.

### 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.

## 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.

## 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,

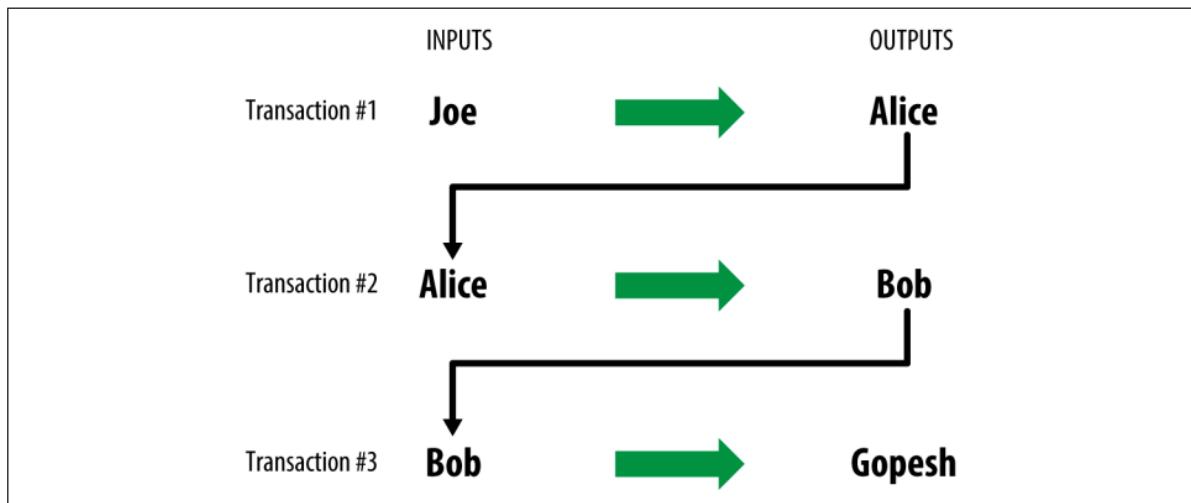
có hàng ngàn hàng và cột. Nếu bạn đưa ra một bảng hoàn chỉnh, người khác có thể kiểm tra rất nhanh. Tuy nhiên, nếu bảng chỉ có vài ô được điền, phần còn lại trống, thì cần rất nhiều công sức để giải! Độ khó của sudoku có thể được điều chỉnh bằng cách thay đổi kích thước của nó, nhưng vẫn dễ dàng xác minh ngay cả khi bảng rất lớn.

### 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.

## Mật mã Khóa Công khai

Mật mã khóa công khai được phát minh vào những năm 1970, đặt nền tảng toán học cho bảo mật máy tính và thông tin. Kể từ đó, nhiều hàm toán học phù hợp như lũy thừa số nguyên tố và phép nhân đường cong elliptic đã được khám phá. Các hàm này hầu như không thể đảo ngược, nghĩa là dễ tính toán theo một hướng nhưng rất khó tính toán ngược lại. Dựa trên các hàm này, mật mã học cho phép tạo ra các bí mật số và chữ ký số không thể giả mạo. Bitcoin sử dụng phép nhân đường cong elliptic làm cơ sở cho hệ mật mã của mình.

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.

Mỗi 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.

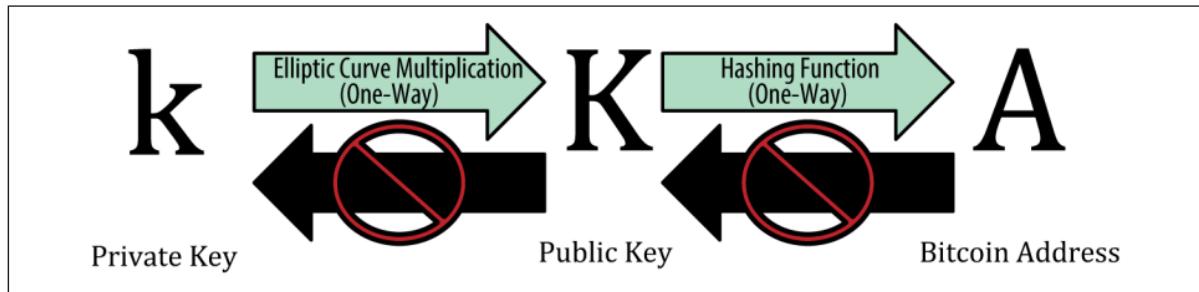
Trong hầu hết các ví Bitcoin, khóa bí mật và khóa công khai được lưu trữ cùng nhau dưới dạng cặp khóa để tiện lợi. Tuy nhiên, vì khóa công khai có thể được tính toán từ khóa bí mật, nên cũng có thể chỉ cần lưu trữ khóa bí mật.

## Khóa Bí Mật và Khóa Công Khai

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). Mỗi 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

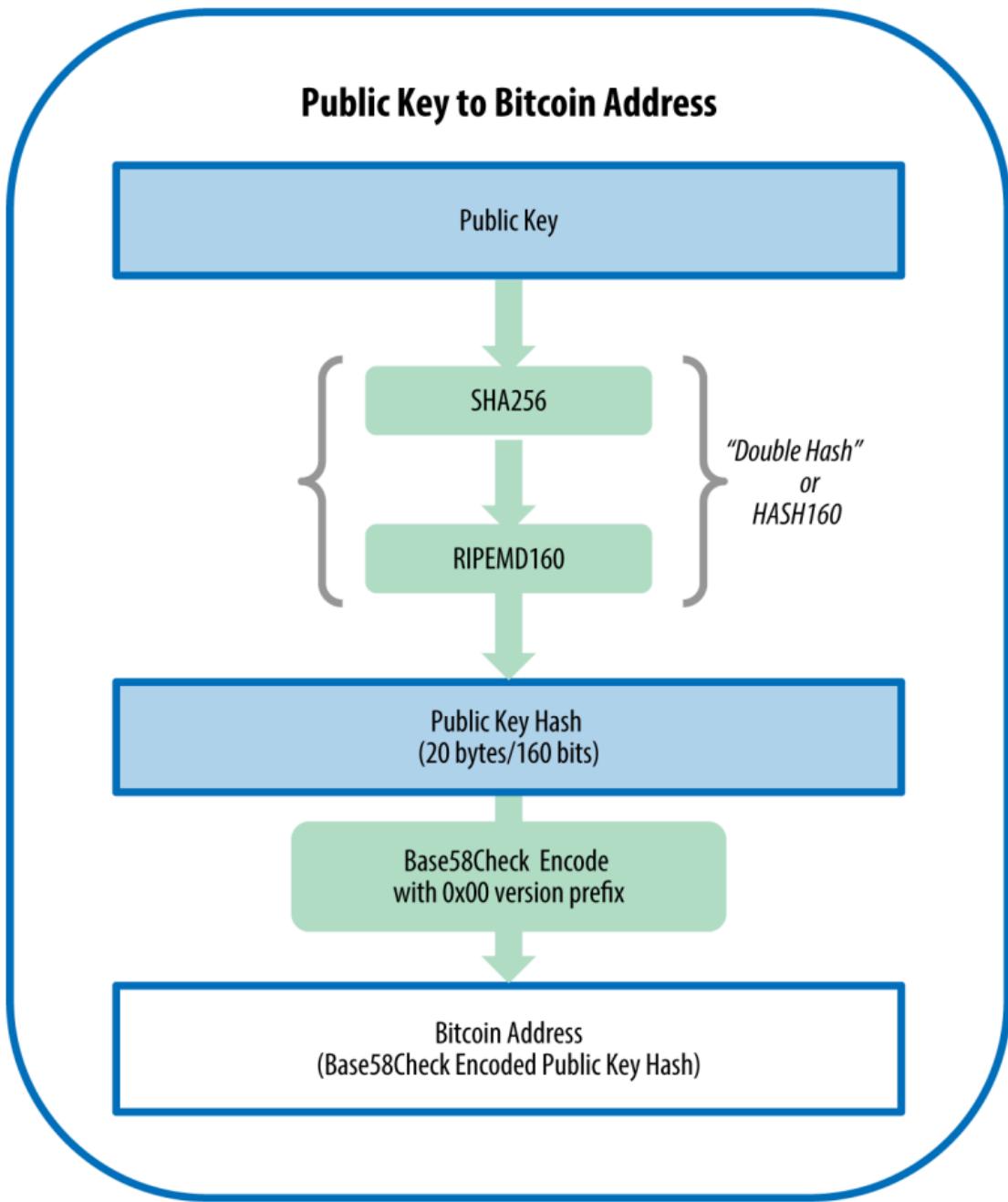
Địa chỉ Bitcoin là một chuỗi ký tự dùng để nhận tiền từ người khác. Được tạo ra từ khóa công khai, địa chỉ Bitcoin thường bắt đầu bằng số "1", Ví dụ về một địa chỉ Bitcoin: **1J7mdg5rbQyUHENYdx39WVWK7fsLpEoXZy** và có thể được so sánh với "người thụ hưởng" trong một tờ séc giấy. Nó đại diện cho nơi nhận 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

#### Kiến trúc Mạng Peer-to-Peer (P2P)

Bitcoin được xây dựng dựa trên kiến trúc mạng ngang hàng (peer-to-peer - P2P) hoạt động trên nền tảng internet. Thuật ngữ "peer-to-peer" có nghĩa là các máy tính tham gia mạng đều bình đẳng, không có nút nào "đặc biệt", và tất cả các nút cùng chia sẻ trách nhiệm cung cấp dịch vụ mạng. Các nút trong mạng được kết nối theo dạng lưới với cấu trúc "phẳng", không có máy chủ trung tâm, không có dịch vụ tập trung và không có phân cấp trong mạng.

Trong mạng P2P, các nút vừa cung cấp vừa sử dụng dịch vụ, với sự trao đổi qua lại đóng vai trò là động lực tham gia. Mạng P2P có tính chất bền vững, phi tập trung và mở. Một ví dụ tiêu biểu về kiến trúc mạng P2P chính là internet thuở ban đầu, nơi các nút trong mạng IP hoạt động bình đẳng. Mặc dù ngày nay kiến trúc internet có tính phân cấp hơn, giao thức IP vẫn giữ được bản chất cấu trúc phẳng của mình. Ngoài Bitcoin, ứng dụng thành công lớn nhất của công nghệ P2P là chia sẻ tệp, với Napster là người tiên phong và BitTorrent là phiên bản tiến hóa gần đây nhất.

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 phẳng, 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 cung 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

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 khôi, 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)**

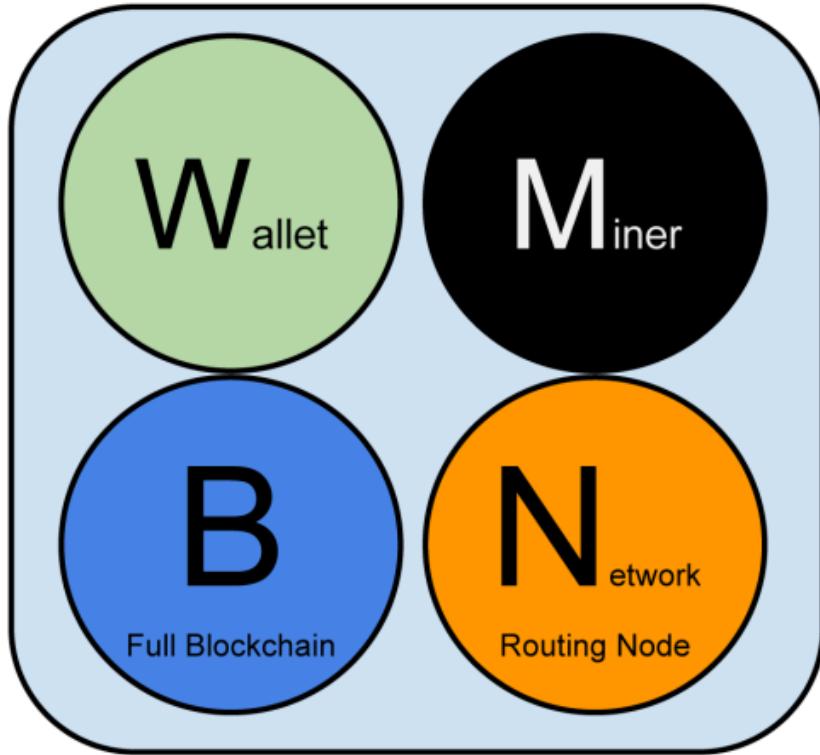
Các nút khai thác cạnh tranh để tạo ra các khối mới bằng cách chạy phần cứng chuyên dụng để giải thuật toán Proof-of-Work. Một số nút khai thác cũng là nút đầy đủ, duy trì bản sao đầy đủ của blockchain, trong khi một số khác là nút nhẹ tham gia khai thác nhóm (pool mining) và phụ thuộc vào máy chủ nhóm (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, khai thác (miner), cơ sở dữ liệu blockchain đầy đủ, và định tuyến mạng.

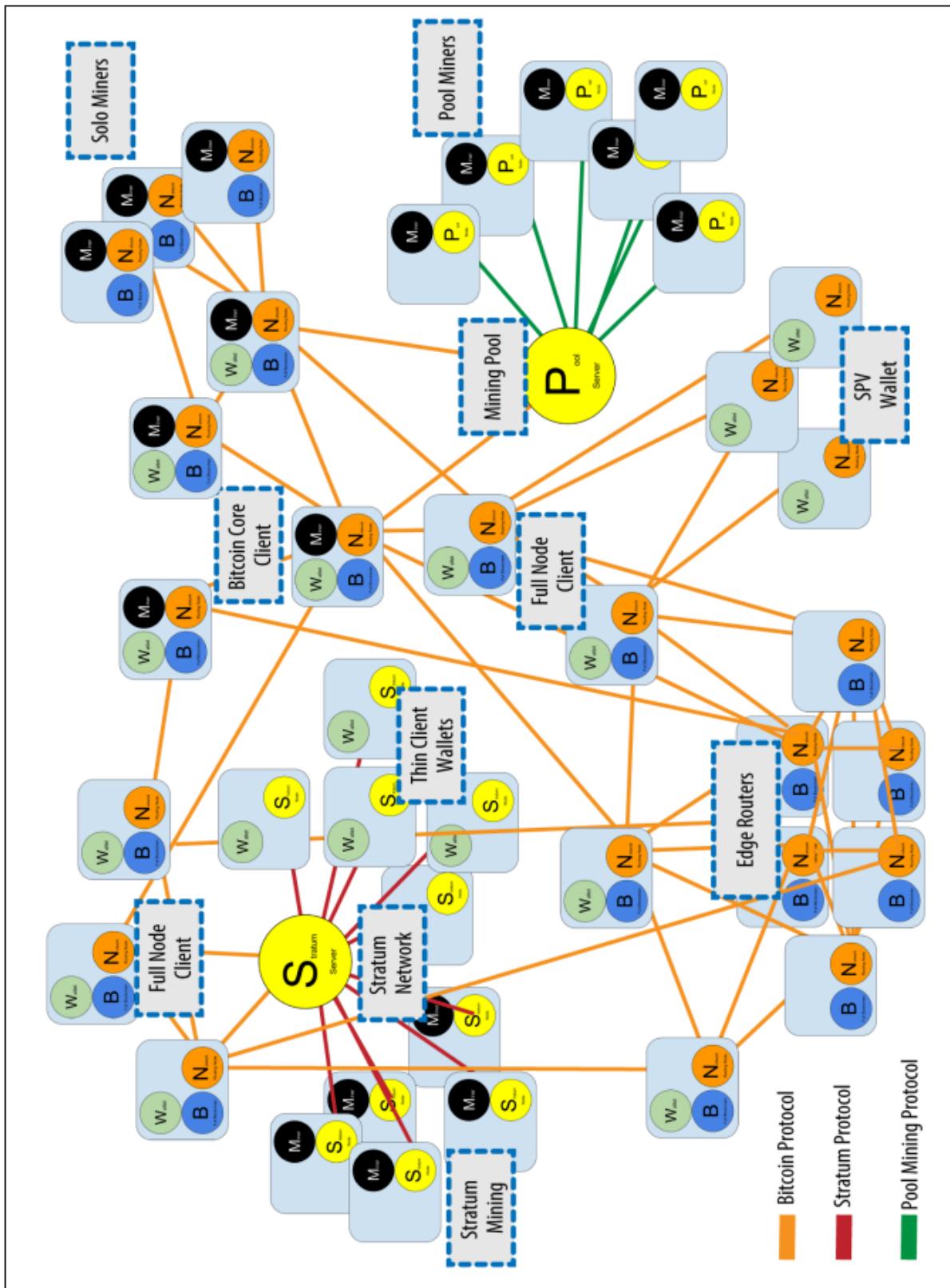
### Mạng Bitcoin Mở Rộng

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 công, 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 chuyên 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). Tâm 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 không 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 Metacoin, phần lớn là chỉ có 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

chiều dài 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://bezale1.tuxen.de/articles/accidentally\\_turing\\_complete.html](http://bezale1.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 cần 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 ràng, 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:

- Gửi giao dịch:** Người dùng tạo và gửi giao dịch đến mạng Ethereum thông qua ví điện tử của họ (ví dụ: MetaMask, MyEtherWallet).
- 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.
- 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.
- 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.
- 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 ( $1 \text{ gwei} = 10^{-9} \text{ ether}$ ).

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:

- o Truy cập Remix IDE tại địa chỉ <https://remix.ethereum.org/>
- o Tạo một file mới (ví dụ: Test.sol).
- o Dán đoạn mã trên vào file.

The screenshot shows the Remix IDE interface. In the top right, there's a code editor tab for 'Test.sol' with the following content:

```
1 pragma solidity ^0.8.18;
2 contract chao{
3     string public chaomung="Hello World!!!!";
4 }
```

In the bottom left, the 'FILE EXPLORER' sidebar shows the project structure:

- WORKSPACES: default\_workspace
- .states
- contracts
- artifacts
- build-info
- 1.Storage.sol
- 2\_Owner.sol
- 3\_Ballot.sol
- Test.sol
- scripts
- tests
- Ballot\_test.sol
- storage.test.js
- .prettierc.json
- README.txt

### 2. Biên dịch (Compile):

- o Chọn tab "Compiler" trong Remix.
- o Chọn phiên bản Solidity phù hợp và nhấn "Compile Test.sol".

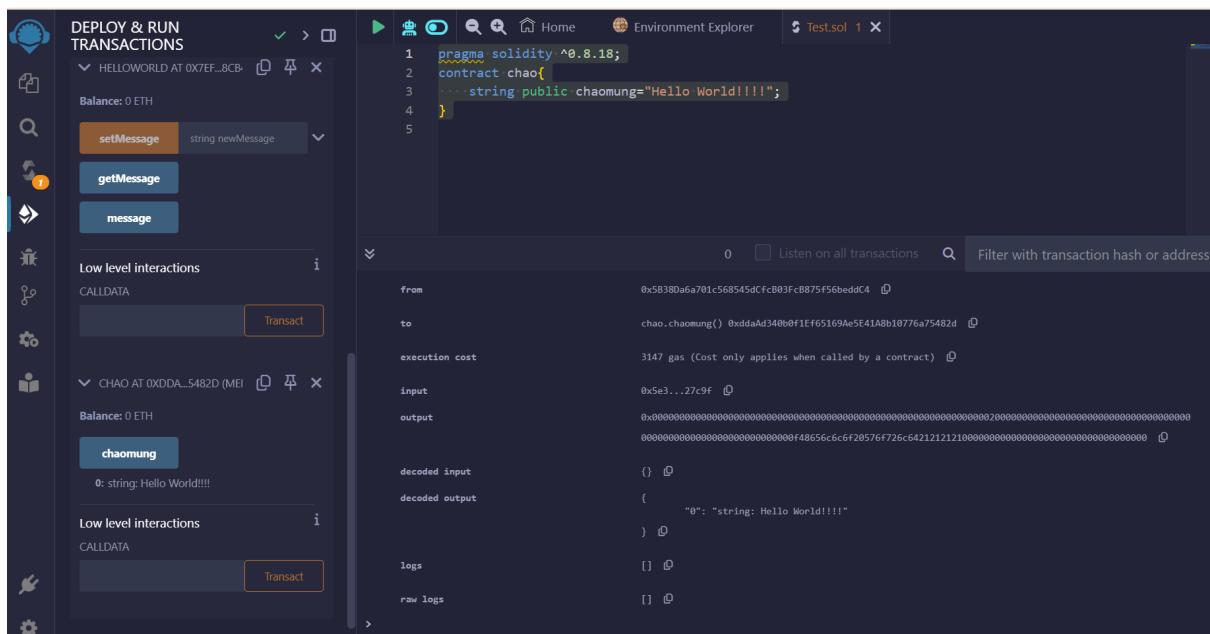
### 3. Triển khai (Deploy):

- o Chuyển sang tab "Deploy & Run Transactions".

- o Chọn môi trường là "JavaScript VM (London)" để thử nghiệm trên mạng giả lập.
  - o Nhấn nút "Deploy" để triển khai contract.

#### 4. Tương tác:

- o Sau khi triển khai, bạn sẽ thấy các nút và trường liên quan đến contract trong Remix.
  - o 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**
  - o 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.
  - o 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**
  - o Bản chất của DApp trên chuỗi khối cho phép mọi người kiểm tra mã nguồn để hiểu rõ hơn về cách hoạt động.
  - o Mọi tương tác với DApp được lưu giữ vĩnh viễn trên blockchain.
3. **Khả năng chống kiểm duyệt**
  - o 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.
  - o 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

- o 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

- o 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.
- o 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. Thể 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. Ngày nay, 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 Đầu (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 số 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 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.

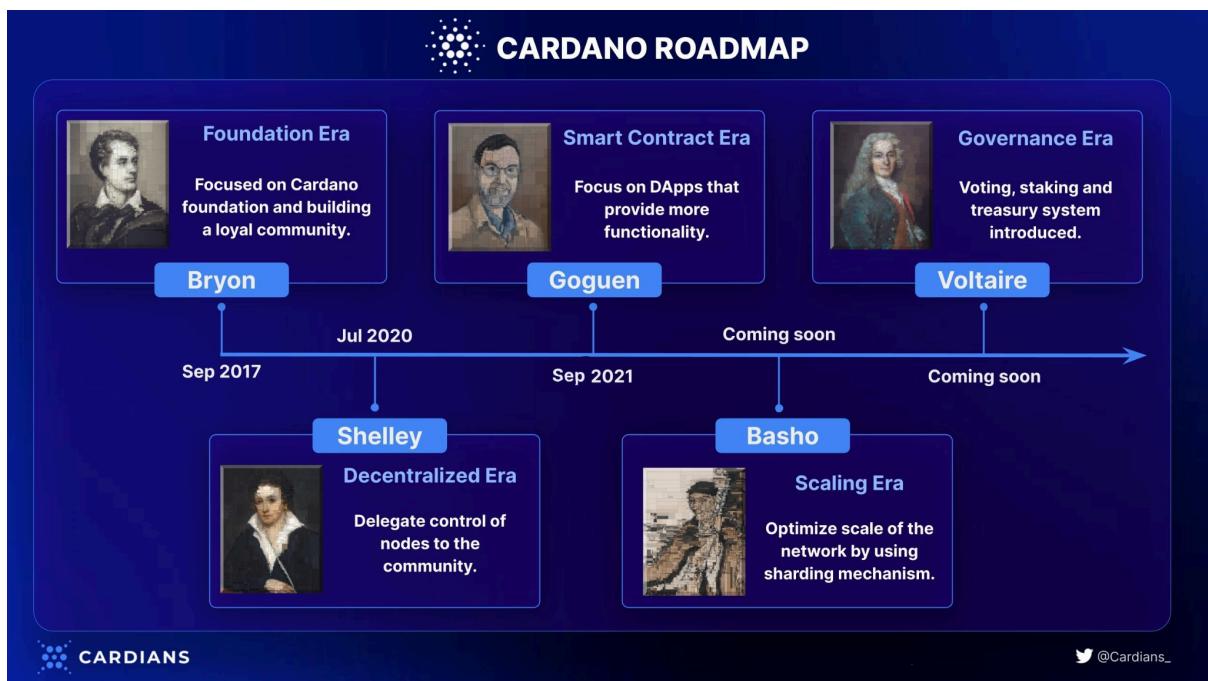
### 3.3.1.3. Lộ trình phát triển của Cardano

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-xx: 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**

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 Lai**

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.

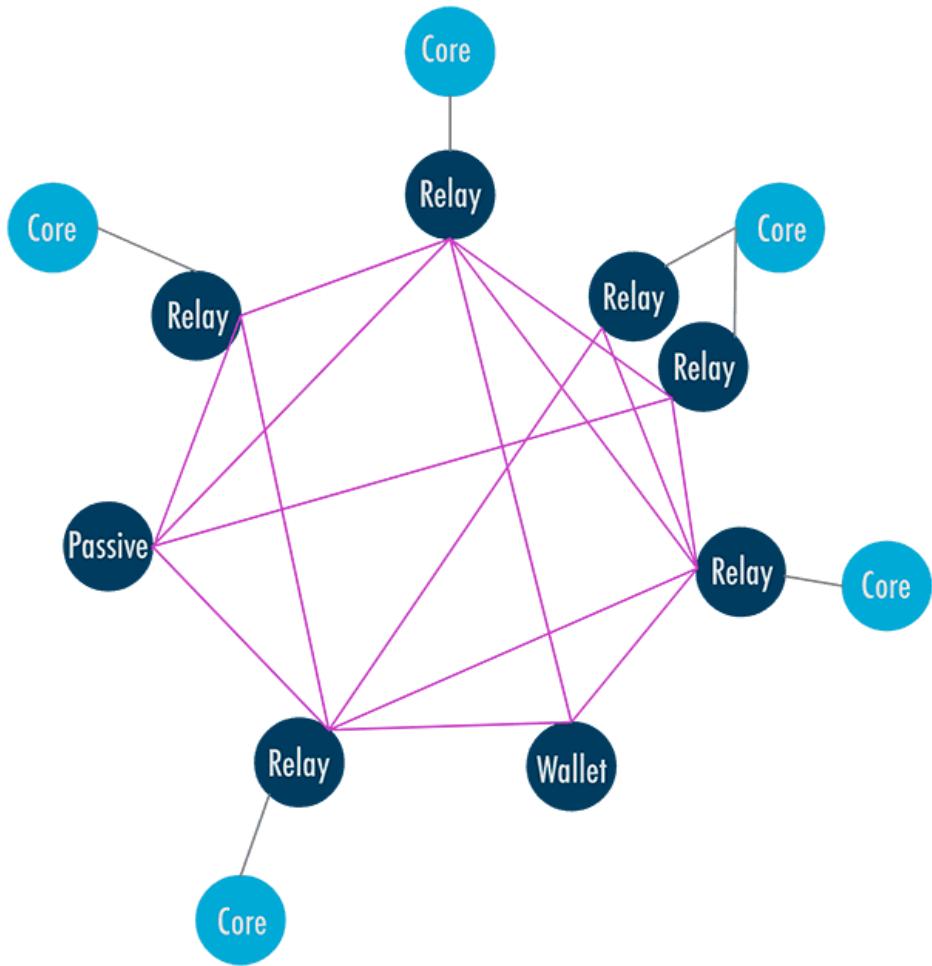
**Ứng dụng thực tiễn:** Cardano sẽ tập trung vào việc tạo ra các giải pháp blockchain thực tế, giúp giải quyết các vấn đề toàn cầu như nhận dạng số, quản lý tài nguyên, và minh bạch trong quản trị.

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. Cơ chế hoạt động 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 khoa học. Trong 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-xx: 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 kỹ 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 kỹ 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
- ...

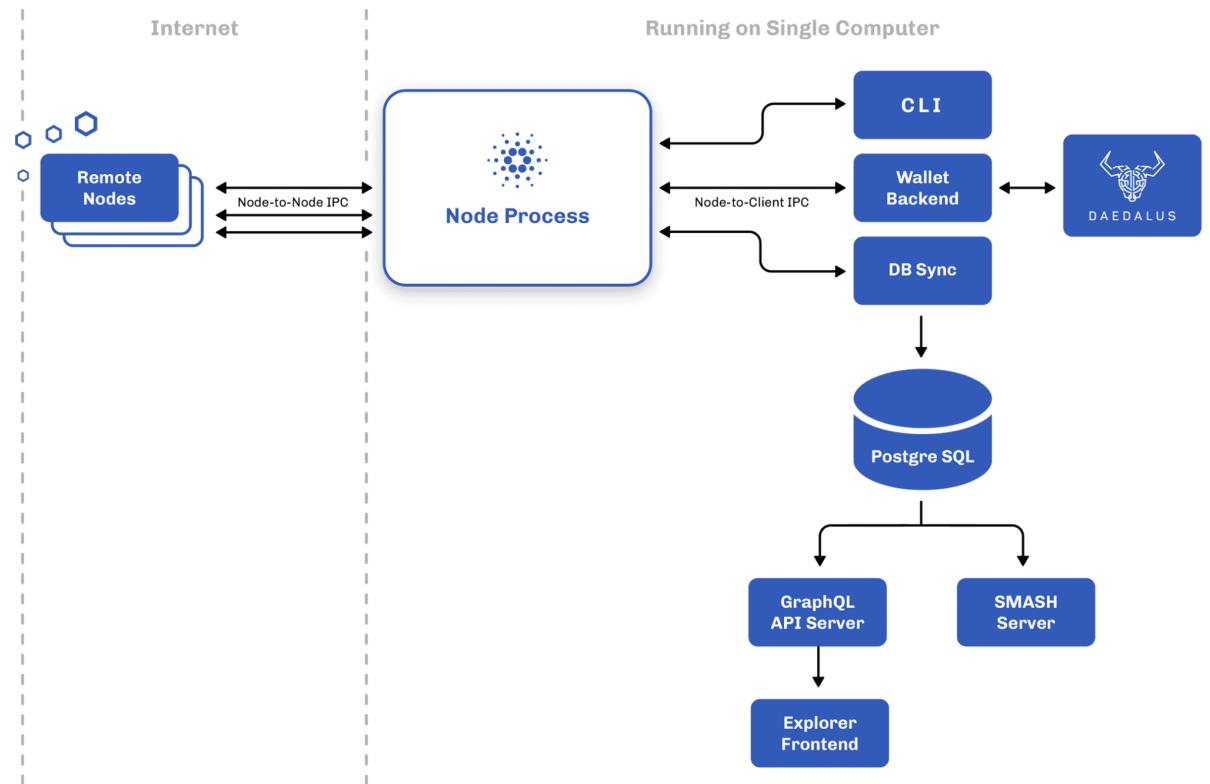
Bằng cách chọn một khối cụ thể, bạn có thể khám phá khối đó chi tiết hơn để xem ID, kích thước, Epoch và thông tin chi tiết về khối, số lượng giao dịch.

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-xx: 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](#)
- ❖ [Guarda](#)
- ❖ [Tangem](#)

- ❖ SimpleHold Wallet
- ❖ Coin Wallet
- ❖ NuFi
- ❖ NOW 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

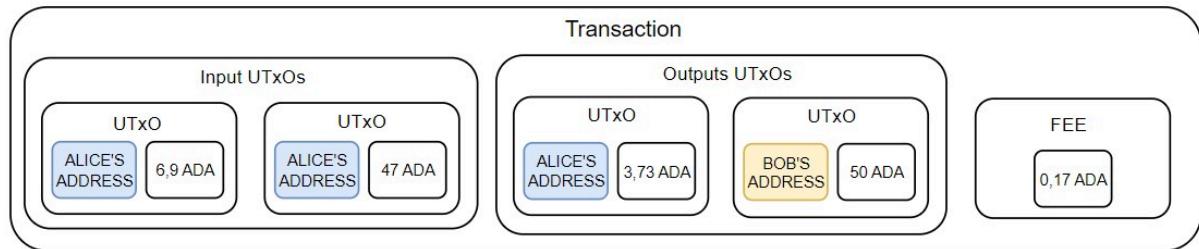
#### **Thông tin cơ bản về UTXO**

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.

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. Vì 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.



### Sự khác biệt giữa UTxO 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.

### Mô hình UTXO mở rộng của Cardano

Cardano sử dụng mô hình kế toán 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 UTxO. Mục đích là giải thích chi tiết cách người dùng chi tiêu UTxO.



Mô hình EUTxO 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 một ví thành nhiều ví con.

## Các thành phần cơ bản của EUTxO



- **Hợp đồng thông minh (Contract):** Dùng để khóa UTxO, 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 1 tham số.
- **Ngữ cảnh (Context):** Thông tin như siêu dữ liệu về giao dịch đang được xác thực.

### 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.

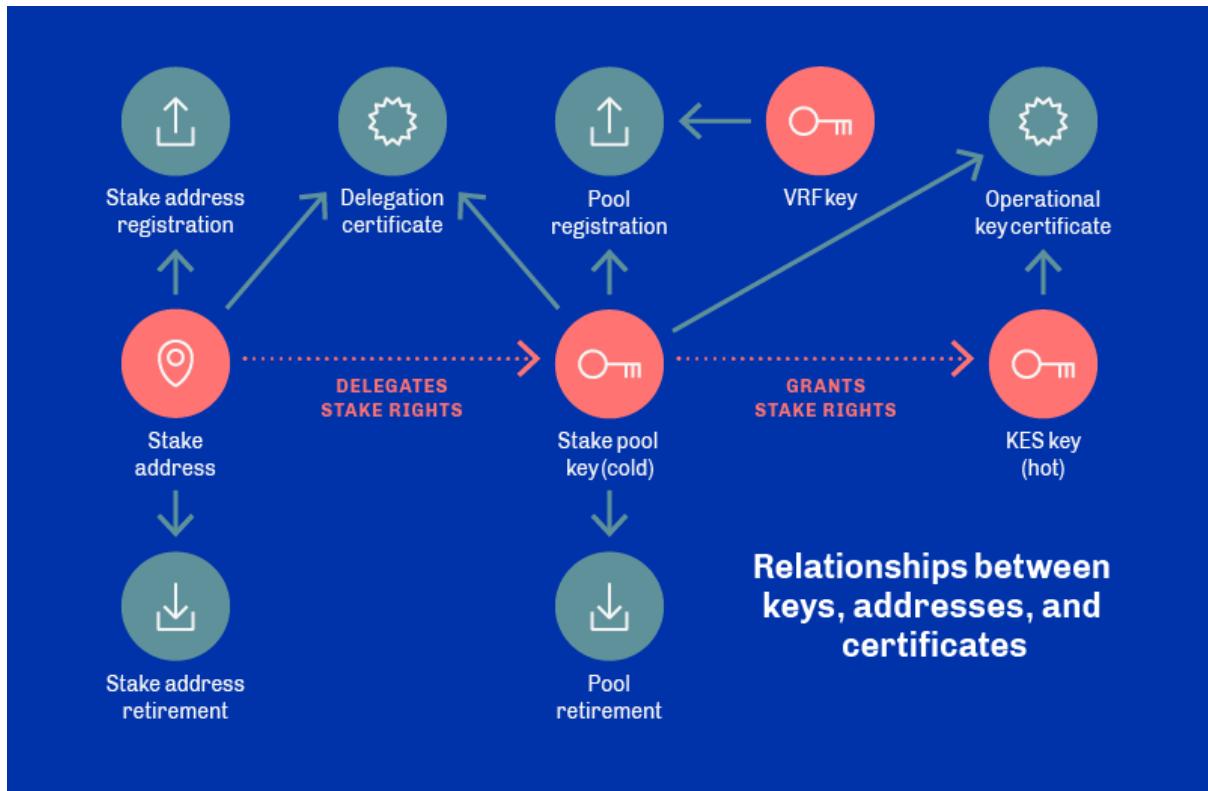
#### 3.3.4. Khóa, địa chỉ của Blockchain cardano.

## Khóa của Cardano

Khóa của Cardano là các cặp khóa mật mã bất đối xứng 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:



## Các loại khóa trong Cardano

Trong hệ sinh thái Cardano, có hai loại khóa chính:

- **Khóa node**
- **Khóa địa chỉ**

**Khóa node** đại diện cho tính bảo mật của blockchain và bao gồm các khóa sau:

### Khóa vận hành (Operator/Operational Key)

- Khóa vận hành là các cặp khóa offline của người vận hành node, bao gồm một bộ đếm chứng chỉ dùng để tạo chứng chỉ mới.
- 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:

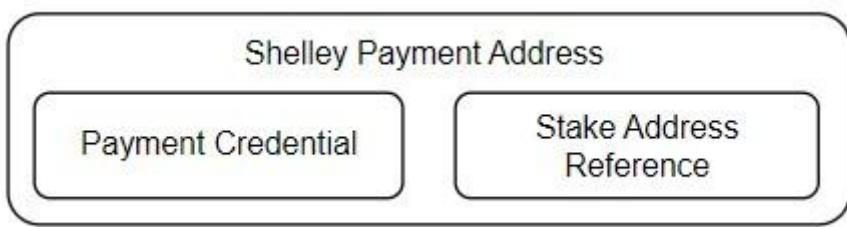
- Khóa thanh toán (Payment key):** Cặp khóa địa chỉ đơn thường được sử dụng để tạo địa chỉ UTXO.
- Khóa staking (Staking key):** Cặp khóa địa chỉ stake/phần thưởng thường được sử dụng để tạo địa chỉ tài khoản/phần thưởng.

### 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 ảnh bên dưới, bạn có thể thấy địa chỉ thanh toán Shelley, bao gồm một phần dành cho tiền (thông tin xác thực thanh toán) và tham chiếu đến địa chỉ stake (khóa stake).



Tiền 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.

Tiền 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.

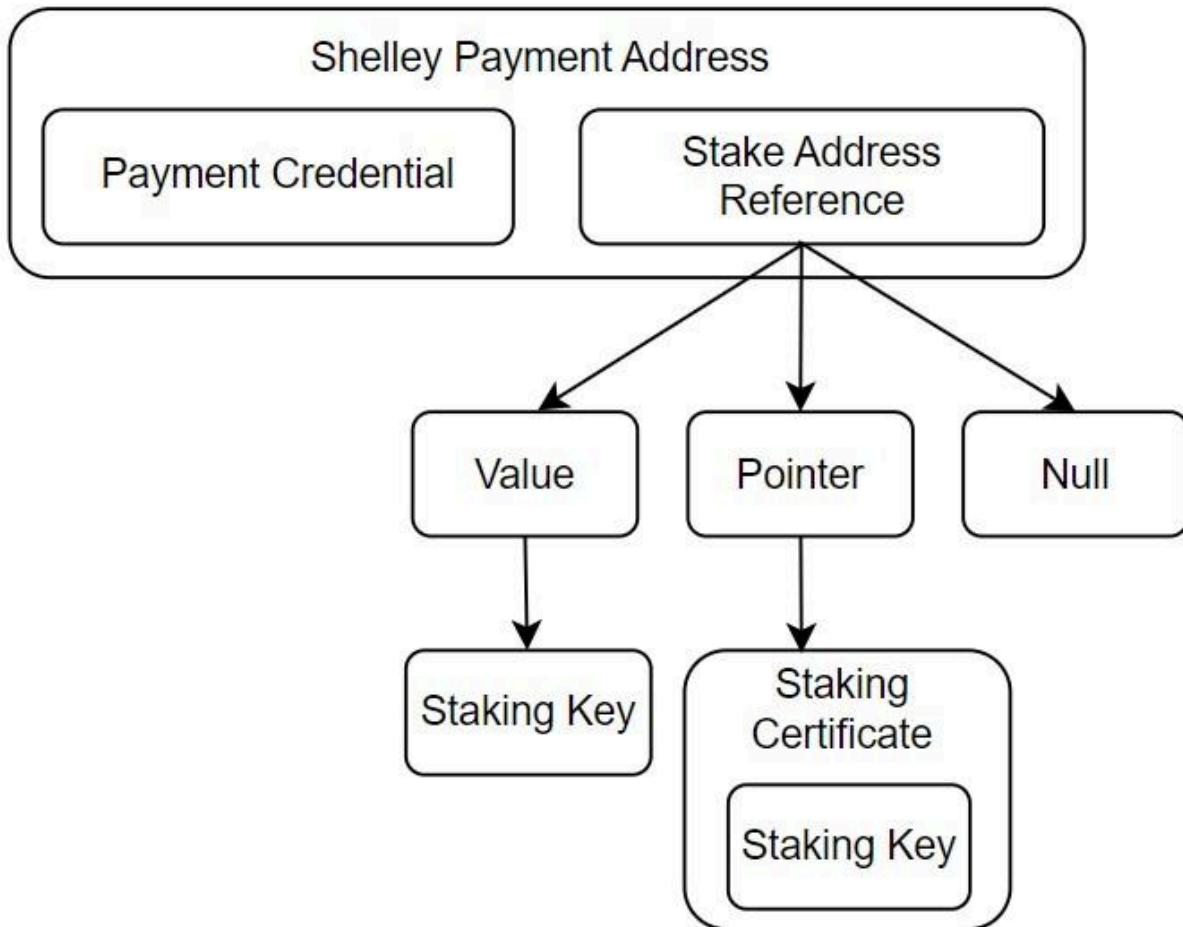
Lưu ý rằng địa chỉ stake đã được đăng ký, không phải (các) địa chỉ thanh toán. Do đó, có thể thực hiện một lần đăng ký cho tất cả các địa chỉ thanh toán được tạo trong tương lai. Ngoài ra, hãy lưu ý rằng tiền vẫn nằm trên địa chỉ thanh toán (do chủ sở hữu kiểm soát hoàn toàn) và có thể được chi tiêu.

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.

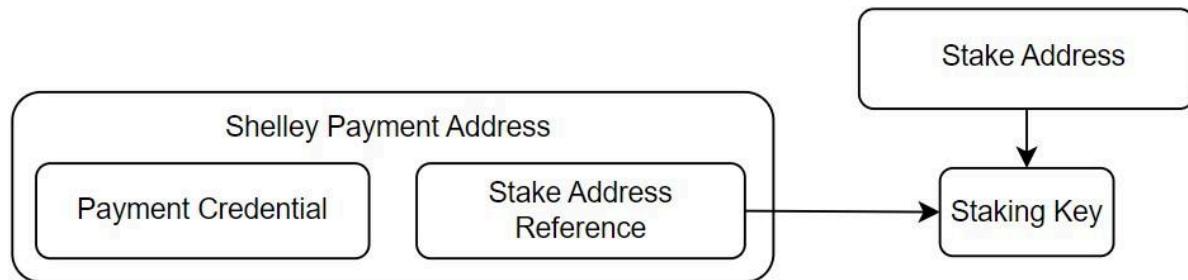
<b>Byron address:</b>
37ctjaVyb4KDXBNC4haBVPCvro8AQPHwvCMp3RFhiSVWwfFmZ6iazSK6JK1hY6wHNmtrp1f1kdbva8TCneM2YsiXT7mrVr21EacHntXz5YyUdj84pe
<b>Payment address:</b>
addr1vpu5vlrf4xkxv2qpwnfg6cjhtw542ayty80v8dyr49rf5eg0yu80w
<b>Stake address:</b>
stake1vpu5vlrf4xkxv2qpwnfg6cjhtw542ayty80v8dyr49rf5egfu2p0u

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 cái 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).

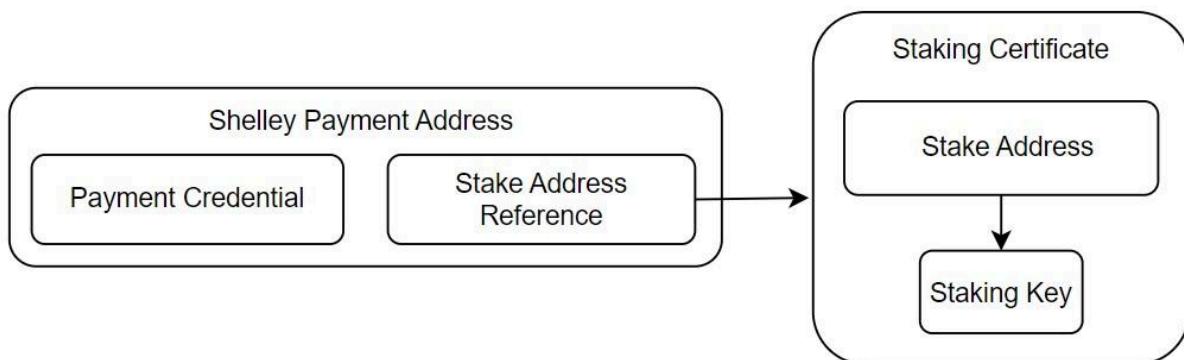


Hãy nói thêm rằng thay vì khóa stake, tham chiếu có thể đề cập đến hàm băm của tập lệnh (nghĩa là hàm băm của tập lệnh sẽ được sử dụng để chi tiêu).

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

## Hợp đồng thông minh là gì?

Hợp đồng thông minh (smart contracts) là các thỏa thuận kỹ thuật số được định nghĩa bằng mã lệnh, tự động hóa và thực thi các điều khoản mà không cần đến các bên trung gian. Điều này cho phép thực hiện các giao dịch minh bạch và an toàn trên blockchain. Dựa vào các điều kiện được thiết lập sẵn trong mã lệnh, trạng thái của hợp đồng chỉ có thể thay đổi theo cách tuân thủ các quy tắc đã định trước.

Trên blockchain Cardano, mã biên dịch của hợp đồng thông minh được lưu trữ và phân phối trên mạng lưới phi tập trung. Sau khi được triển khai, không thể thay đổi các quy tắc của hợp đồng, cũng như không thể dịch ngược mã biên dịch trở lại thành mã nguồn ban đầu.

## 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:

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 xx: 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 đầu 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 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 Hành Động 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 Nguõng và/hoặc Điều khoản:

- Thay đổi thành viên Ủy ban Hiến pháp, nguõng chữ ký, hoặc các điều khoản liên quan.

### 3. Cập nhật Hiến pháp hoặc Chính sách Đề xuất:

- Chính 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.

## 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?

Tài liệu tham khảo

Bitcoin

<https://learnmeabitcoin.com/>

[https://drive.google.com/file/d/1kG\\_oKReuoXi-yqhAda9rXPbL5T4KeEWJ/view?usp=drive\\_link](https://drive.google.com/file/d/1kG_oKReuoXi-yqhAda9rXPbL5T4KeEWJ/view?usp=drive_link)

<https://dl.ebooksworld.ir/motoman/Oreilly.Mastering.Bitcoin.Unlocking.Digital.Cryptocurrencies.www.EBooksWorld.ir.pdf>

ETH

[https://drive.google.com/file/d/1S9P5K4aeSNnvIletKVgPNmSfrSGwqN\\_y/view?usp=drive\\_link](https://drive.google.com/file/d/1S9P5K4aeSNnvIletKVgPNmSfrSGwqN_y/view?usp=drive_link)

Cardano

<https://docs.cardano.org/>

[https://drive.google.com/file/d/1Ci38r\\_r9MoAiELKiwjhtLb0txsRZpLF/view?usp=drive\\_link](https://drive.google.com/file/d/1Ci38r_r9MoAiELKiwjhtLb0txsRZpLF/view?usp=drive_link)

[https://drive.google.com/file/d/1\\_XcsxjDhRH1kND0V8dBjOTIMdSGFvTaQ/view?usp=drive\\_link](https://drive.google.com/file/d/1_XcsxjDhRH1kND0V8dBjOTIMdSGFvTaQ/view?usp=drive_link)

<https://cexplorer.io/article/understanding-cardano-addresses>

<https://cexplorer.io/article/understanding-utxo-spending-through-a-script>

<https://www.ledger.com/academy/library/topic/blockchain>

[https://aft.acm.org/wp-content/uploads/2019/10/Ouroboros\\_AFT19\\_Tutorial.pdf](https://aft.acm.org/wp-content/uploads/2019/10/Ouroboros_AFT19_Tutorial.pdf)