Chương 2
CÁC KHÁI NIỆM CỦA BLOCKCHAIN

2.1. KHÁI NIỆM

2.1.1. Khái niệm

Blockchain là một công nghệ cơ sở dữ liệu phân tán, hoạt động như một sổ cái kỹ thuật số được bảo mật bằng mật mã, cho phép lưu trữ thông tin một cách minh bạch, an toàn và không thể thay đổi. Các thông tin này được tổ chức thành các khối (block), liên kết với nhau theo thứ tự thời gian thông qua các hàm băm (hash), tạo thành một chuỗi (chain). Chúng ta cùng tìm hiểu những khái niệm cơ bản về công nghệ này.

Blockchain cho đến nay chưa phải là một từ thông dụng trong gia đình, như đám mây hay Internet vạn vật. Nó chưa phải là một sáng kiến mà bạn có thể nhìn thấy và chạm vào dễ dàng như điện thoại thông minh hay một gói hàng từ Amazon. Nhưng trong một thế giới mà bất kỳ ai cũng có thể chỉnh sửa một mục trên Wikipedia, hay những thông tin trên các mạng xã hội,.. blockchain chính là câu trả lời cho một câu hỏi mà chúng ta đã đặt ra từ buổi bình minh của kỷ nguyên internet: Làm thế nào chúng ta có thể cùng nhau tin tưởng vào những gì xảy ra trực tuyến trên môi trường internet?

Mỗi năm, chúng ta xử lý công việc nhiều hơn cuộc sống của mình - nhiều chức năng cốt lõi của chính phủ, nền kinh tế và xã hội - trên internet. Chúng ta thực hiện nhiều giao dịch ngân hàng trực tuyến. Chúng ta mua sắm trực tuyến. Chúng ta đăng nhập vào các ứng dụng và dịch vụ tạo nên bản ghi thông tin kỹ thuật số của mình và gửi thông tin qua lại trên môi trường internet. Hãy nghĩ về blockchain như một cấu trúc lịch sử bên dưới ghi lại mọi thứ xảy ra - mọi giao dịch kỹ thuật số; trao đổi giá trị, hàng hóa và dịch vụ; hoặc dữ liệu riêng tư - chính xác như cách nó xảy ra.

Blockchain như một cơ sở dữ liệu phân tán duy trì danh sách các bản ghi và được chia sẻ trên môi trường internet. Các bản ghi này được gọi là khối và mỗi khối mã được mã hóa chứa lịch sử của mọi khối trước nó với dữ liệu giao dịch được ghi dấu thời gian xuống đến từng giây, các chuỗi khối liên kết lại với nhau gọi là chuỗi khối (blockchain) và sau đó chúng được phân tán trên một mạng lưới máy tính trên toàn cầu tạo nên blockchain hoàn chỉnh nơi mà các bên thứ ba không thể thay đổi được dữ liệu.

Blockchain được tạo thành từ hai thành phần chính: một mạng lưới phi tập trung tạo điều kiện và xác minh các giao dịch và sổ cái bất biến mà mạng lưới này duy trì. Mọi người trong mạng lưới đều có thể thấy sổ cái giao dịch được chia sẻ này, nhưng không có điểm lỗi nào mà từ đó hồ sơ hoặc tài sản kỹ thuật số có thể bị hack hoặc làm hỏng. Do sự tin tưởng phi tập trung đó, cũng không có tổ chức nào kiểm

soát dữ liệu đó, dù là một ngân hàng lớn hay một gã khổng lồ công nghệ như Facebook hay Google. Không có bên thứ ba nào đóng vai trò là người kiểm soát của internet. Sức mạnh của công nghệ sổ cái phân tán có ứng dụng trên mọi loại hồ sơ và giao dịch kỹ thuật số, và chúng ta đang bắt đầu chứng kiến các ngành công nghiệp lớn chuyển đổi theo xu hướng này.

Đầu tiên phải kể đến các ngân hàng lớn và các gã khổng lồ công nghệ. Doanh nghiệp lớn luôn dẫn đầu đổi mới, sự phát triển của các hợp đồng thông minh dựa trên blockchain đã đưa blockchain thành một trung gian thực hiện các giao dịch kinh doanh phức tạp, những thỏa thuận pháp lý và trao đổi dữ liệu tự động. Các công ty như Microsoft hay IBM đang tận dụng hạ tầng đám mây của họ để xây dựng blockchain tùy chỉnh cho khách hàng và thử nghiệm các ứng dụng của riêng mình, chẳng hạn như phát triển một mạng lưới an toàn thực phẩm toàn cầu kết nối nhà sản xuất và nhà bán lẻ. Về phía học thuật, các nhà nghiên cứu đang khám phá các ứng dụng blockchain trong các dự án từ nhận diện kỹ thuật số đến hồ sơ y tế và bảo hiểm v.v…

Đồng thời, hàng chục công ty khởi nghiệp đang sử dụng công nghệ này cho mọi thứ, từ thanh toán toàn cầu đến chia sẻ nhạc, từ theo dõi doanh số bán bán hàng đến việc theo dõi chuỗi cung ứng v.v... Đó là lý do tại sao tiềm năng của blockchain lại lớn đến vậy. Khi nói đến tài sản và giao dịch kỹ thuật số, bạn có thể đưa bất cứ thứ gì vào blockchain. Một loạt các rào cản về kinh tế, pháp lý, quy định và công nghệ phải được mở rộng trước khi chúng ta thấy công nghệ blockchain được áp dụng rộng rãi, nhưng những người đi đầu đang có những bước tiến đáng kinh ngạc. Trong vài năm tới, phần lớn cuộc sống kỹ thuật số của bạn có thể bắt đầu chạy trên nền tảng blockchain - và bạn thậm chí có thể không nhận ra điều đó.

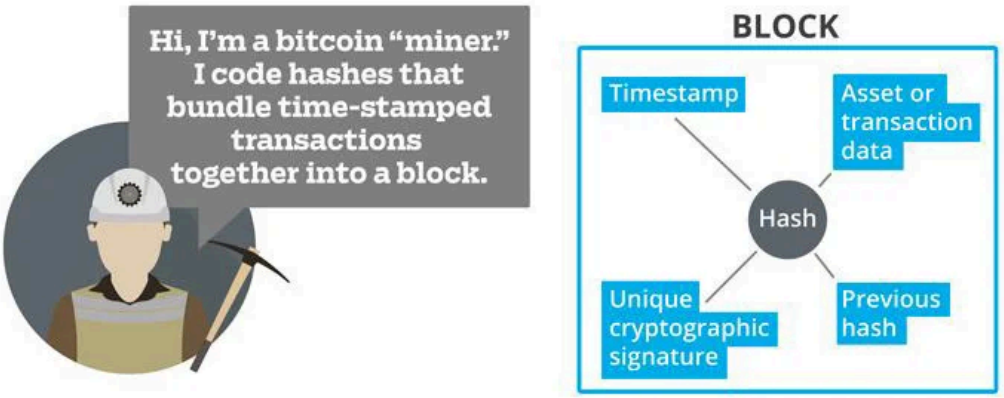
Blockchain là cấu trúc dữ liệu cho phép Bitcoin (BTC) và các loại tiền mã hóa thế hệ mới như Ether (ETH), Cardano (ADA),… phát triển mạnh mẽ thông qua sự kết hợp giữa mã hóa phi tập trung, tính ẩn danh, tính bất biến và quy mô toàn cầu. Đây là vũ khí không quá bí mật đằng sau sự trỗi dậy của tiền mã hóa và để giải thích cách thức blockchain ra đời, chúng ta phải bắt đầu một cách ngắn gọn với di sản của Bitcoin được giới thiệu ở phần tiếp theo của chương này.

Mọi người thường sa lầy vào sự phức tạp của công nghệ khi cố gắng hiểu blockchain, nhưng khái niệm cơ bản là một khái niệm đơn giản và phổ quát. Chúng ta có những sự kiện và thông tin mà chúng ta không muốn bị truy cập, sao chép hoặc giả mạo, nhưng trên internet khả năng chúng có thể bị hack hoặc sửa đổi. Blockchain cung cấp cho chúng ta một nguyên lý - một nền tảng mà chúng ta biết sẽ không thay đổi sau khi chúng ta đưa thứ gì đó vào nền tảng này, nơi một giao dịch sẽ chỉ được xác minh nếu nó tuân theo các quy tắc của nền tảng này.

Sách trắng Nakamoto giải thích những điều cơ bản về "khai thác" dữ liệu thành một khối, sau đó sử dụng hàm băm (liên kết có dấu thời gian) để xâu chuỗi các khối đó lại với nhau trên một mạng lưới phi tập trung gồm các "nút" xác minh từng giao dịch. Một cải tiến quan trọng khác trong sách trắng là sử dụng cái được gọi là mô hình bằng chứng công việc (PoW) để tạo ra sự đồng thuận "không cần tin cậy" phân

tán và giải quyết vấn đề chi tiêu gấp đôi (đảm bảo tiền mã hóa không được chi tiêu nhiều hơn một lần).

"Hệ thống không cần tin cậy" không có nghĩa là bạn không thể tin tưởng vào hệ thống. Hoàn toàn ngược lại, bởi vì blockchain xác minh từng giao dịch thông qua PoW, điều này có nghĩa là không cần sự tin tưởng giữa những người tham gia vào giao dịch. Bằng chứng công việc đến từ đâu? Những người khai thác. Một mạng lưới P2P của "người khai thác" Bitcoin tạo ra PoW khi họ băm các khối lại với nhau, xác minh các giao dịch sau đó được đưa vào sổ cái.



Hình 2.1. Khối (Block)

Trong cuốn sách Blockchain Revolution: How the Technology Behind Bitcoin Is Changing Money, Business, and the World xuất bản năm 2016, tác giả Don và Alex Tapscott đã giải thích mô hình Bitcoin của Nakamoto một cách ngắn gọn nhất có thể:

> *"Bitcoin hay các loại tiền kỹ thuật số khác không được lưu trong một tệp nào đó; nó được thể hiện bằng các giao dịch được ghi lại trong một blockchain - giống như một bảng tính hoặc sổ cái toàn cầu, tận dụng các nguồn lực của một mạng P2P lớn để xác minh và chấp thuận từng giao dịch Bitcoin. Mỗi blockchain, giống như [blockchain Bitcoin] được phân phối: nó chạy trên các máy tính do các tình nguyện viên trên khắp thế giới cung cấp. Không có cơ sở dữ liệu trung tâm nào để hack. Blockchain là công khai: bất kỳ ai cũng có thể xem nó bất kỳ lúc nào vì nó nằm trên mạng... và blockchain được mã hóa... nó sử dụng khóa công khai và riêng tư (giống như hệ thống hai khóa để truy cập vào hộp ký gửi an toàn) để duy trì bảo mật ảo."*

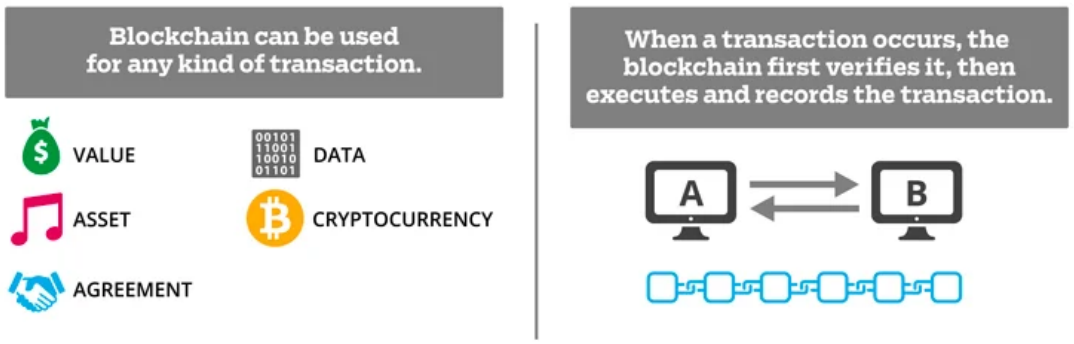
Xin lưu ý rằng không có gì là hoàn toàn không thể hack được, đặc biệt là khi bạn không sử dụng nó theo đúng mục đích. Tính bảo mật của Blockchain không chỉ hiệu quả vì nó được mã hóa mà còn vì nó phi tập trung. Các nạn nhân của các vụ vi phạm blockchain và trộm tiền mã hóa lớn nhất (**Mt. Gox** năm 2014 và **Bitfinex** năm 2016) đã bị nhắm mục tiêu và bị đánh cắp vì họ đã cố gắng tập trung hóa một hệ thống phi tập trung. **Ethereum** cũng đã chứng kiến một số vụ hack và sự cố bảo mật. Vụ hack DAO năm 2016 là một trong những sự kiện nổi bật trong lịch sử blockchain. Cụ thể, nó liên quan đến lỗ hổng trong các hợp đồng thông minh được

viết trên blockchain Ethereum. Gần đây, sàn giao dịch Ethereum lớn nhất tại Hàn Quốc đã bị tấn công, và một đợt chào bán tiền mã hóa đầu tiên (ICO) của một công ty khởi nghiệp Israel đã gặp sự cố khi trang web của họ bị xâm nhập.

Tất cả các vấn đề này đều xuất phát từ lỗ hổng trong các hệ thống kết nối với blockchain, chứ không phải từ chính blockchain. Mô hình bảo mật và mã hóa cơ bản của blockchain vẫn được coi là hợp lý, nhưng cách thực thi bảo mật đó lại là một vấn đề khác.

Chúng tôi đã giải thích cách mạng lưới hoạt động và cách bảo mật được thực hiện, nhưng các khối thực sự kết nối với nhau như thế nào? Tại sao blockchain càng mạnh thì tốc độ xử lý càng chậm? Tính bất biến xuất hiện ở đâu? Giải thích của Tapscotts tiếp tục như sau:

"Mỗi mười phút, giống như nhịp đập của mạng Bitcoin, tất cả các giao dịch được thực hiện đều được xác minh, xóa khỏi hàng đợi và lưu trữ trong một khối liên kết với khối trước đó, từ đó hình thành một chuỗi khối. Để có hiệu lực, mỗi khối phải tham chiếu đến khối trước đó. Cấu trúc này không chỉ đóng dấu thời gian vĩnh viễn mà còn lưu trữ các giao dịch giá trị, ngăn chặn bất kỳ ai thay đổi sổ cái. Vì vậy, blockchain là một sổ cái phân tán, đại diện cho sự đồng thuận của mạng lưới về mọi giao dịch đã diễn ra. Tương tự như World Wide Web là một mạng lưới thông tin toàn cầu, blockchain là 'World Wide Ledger' của giá trị. Sổ cái kỹ thuật số mới này có thể được lập trình để ghi lại hầu như mọi thứ quan trọng và có giá trị đối với nhân loại: từ giấy khai sinh, giấy chứng tử, giấy phép kết hôn, chứng thư và quyền sở hữu, bằng cấp giáo dục, tài khoản tài chính, thủ tục y tế, yêu cầu bảo hiểm, phiếu bầu, đến nguồn gốc thực phẩm hoặc bất kỳ thứ gì có thể được thể hiện bằng mã."



Hình 2.2. *World Wide Ledger*

Tính bất biến có lẽ là khái niệm quan trọng nhất để hiểu về blockchain và lý do tại sao nó lại có giá trị. Trong thế giới kỹ thuật số, việc tạo ra một đối tượng không thể thay đổi sau khi hình thành mang lại giá trị vô hạn, bởi nó đảm bảo tính toàn vẹn và độ tin cậy của dữ liệu.

Quay lại nguyên tắc 'sức mạnh của số lượng', blockchain càng được phân phối trên nhiều nút thì càng mạnh và đáng tin cậy. Đây là quá trình xác minh chồng xác

minh, kéo dài đến vô tận. Một bài blog của Garzik nhấn mạnh rằng hiệu ứng mạng của blockchain chính là chìa khóa cho tính bất biến của nó, và cũng là lý do tại sao blockchain công khai của Bitcoin vẫn là hệ thống phổ biến và đáng tin cậy nhất hiện nay.

"Garzik giải thích: Tính bất biến phụ thuộc rất nhiều vào hiệu ứng mạng. Điều này được thể hiện rõ ràng với Bitcoin. Chi phí tạo ra một tài sản kỹ thuật số mới gần như bằng không. Vì vậy, để thuyết phục ai đó rời khỏi blockchain Bitcoin, bạn cần chứng minh được giá trị vượt trội nhằm vượt qua hiệu ứng mạng vốn có. Không chỉ là thành tích đáng tin cậy, Bitcoin còn có giá trị bảo mật cao từ góc độ kỹ thuật. Bảo mật và tính bất biến của một blockchain là kết quả trực tiếp của nền kinh tế đằng sau nó – bao gồm mức độ đầu tư vào hệ sinh thái và số lượng người đang sử dụng hệ thống này."

2.1.2. Một số đặc điểm quan trọng của blockchain

Blockchain là một công nghệ nổi bật trong lĩnh vực tiền mã hóa, nhưng nó cũng có rất nhiều ứng dụng khác ngoài tiền tệ. Dưới đây là một số đặc điểm quan trọng của blockchain:

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

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

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

4. Bảo mật cao: Blockchain sử dụng mã hóa mạnh mẽ để bảo vệ dữ liệu và đảm bảo rằng chỉ những người có quyền truy cập mới có thể thay đổi thông tin. Điều này làm cho blockchain trở thành một nền tảng cực kỳ bảo mật.

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

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

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

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

2.1.3. Các thành phần cơ bản của blockchain

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

1. Blocs (Khối):

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

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

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

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

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

2. Sổ cái phân tán (Distributed Ledger):

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

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

3. Nút mạng (Node):

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

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

4. Mã hash (Hash):

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

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

5. Thuật toán đồng thuận (Consensus Algorithm):

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

Các thuật toán phổ biến bao gồm:

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

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

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

6. Hợp đồng thông minh (Smart Contract):

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

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

7. Kênh giao tiếp (P2P Network):

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

8. Cơ chế mã hóa (Cryptography):

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

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

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

2.1.4. Quy trình hoạt động của blockchain

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

1. Tạo giao dịch

Quá trình bắt đầu khi người dùng (hoặc các hệ thống) tạo ra một giao dịch. Giao dịch có thể là chuyển tiền, chuyển nhượng quyền sở hữu tài sản, hoặc thực hiện các hành động khác tùy theo ứng dụng của blockchain.

Giao dịch này sẽ được mã hóa và bao gồm thông tin như người gửi, người nhận, số tiền, và các thông tin liên quan.

2. Xác nhận giao dịch

Giao dịch sau khi tạo ra sẽ được phát tán đến mạng lưới các nút (nodes) trong blockchain.

Các nút trong mạng sẽ kiểm tra tính hợp lệ của giao dịch (ví dụ, xác minh rằng người gửi có đủ số dư để thực hiện giao dịch).

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

3. Tạo khối mới (Block)

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

Mỗi khối sẽ có các thành phần chính:

- Dữ liệu giao dịch: Các giao dịch đã được xác nhận.
- Mã hash của khối trước: Liên kết khối này với khối trước đó trong chuỗi.
- Mã hash của khối hiện tại: Đảm bảo tính toàn vẹn của khối.
- Timestamp: Thời gian khi khối được tạo ra.
- Thực thi hợp đồng thông minh (nếu có).

4. Xác thực khối thông qua thuật toán đồng thuận

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

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

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

5. Thêm khối vào blockchain

Khi một khối được xác nhận, nó sẽ được thêm vào chuỗi blockchain vĩnh viễn.

Khối mới sẽ chứa mã hash của khối trước đó, tạo thành một chuỗi liên kết không thể thay đổi. Điều này đảm bảo rằng một khi thông tin đã được ghi vào blockchain, nó không thể bị thay đổi hoặc xóa bỏ mà không làm thay đổi tất cả các khối sau đó, điều này rất khó khăn và tốn kém.

6. Phân phối bản sao sổ cái

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

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

7. Giao dịch hoàn tất

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

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

8. Quy trình tiếp tục

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

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

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

2.2. LỊCH SỬ RA ĐỜI CỦA BLOCKCHAIN

2.2.1. Sơ lược về lịch sử công nghệ blockchain

Ý tưởng cốt lõi về công nghệ blockchain đã bắt đầu xuất hiện từ cuối những năm 1980 và đầu những năm 1990. Vào năm 1989, Leslie Lamport phát triển giao thức Paxos; và vào năm 1990, ông đã nộp bài báo *The Part-Time Parliament* cho tạp chí *ACM Transactions on Computer Systems*. Bài báo này cuối cùng được xuất bản vào năm 1998, mô tả một mô hình đồng thuận giúp đạt được sự thống nhất trong một mạng máy tính, ngay cả khi các máy tính hoặc mạng đó có thể không hoàn toàn đáng tin cậy.

Vào năm 1991, một chuỗi thông tin được ký điện tử đã được sử dụng như một sổ cái điện tử để ký tài liệu số hóa, giúp chứng minh rằng không có tài liệu nào trong sổ cái bị thay đổi. Những ý tưởng này sau đó được kết hợp và ứng dụng vào tiền mã hóa; vào năm 2008, chúng được mô tả trong bài báo *Bitcoin: A Peer-to-Peer Electronic Cash System*, được xuất bản dưới bút danh Satoshi Nakamoto. Đến năm 2009, mạng blockchain của Bitcoin chính thức được thiết lập. Bài báo của Nakamoto đã đưa ra một thiết kế nền tảng mà hầu hết các hệ thống tiền mã hóa hiện đại đều dựa vào, dù có sự biến đổi và cải tiến. Bitcoin là ứng dụng blockchain đầu tiên, mở đường cho nhiều ứng dụng khác dựa trên công nghệ blockchain.

Trước Bitcoin, đã có nhiều hệ thống tiền điện tử khác như **ecash** và **NetCash**, nhưng không hệ thống nào đạt được sự phổ biến rộng rãi. Blockchain cho phép Bitcoin hoạt động dưới dạng phân tán, không có ai kiểm soát hoàn toàn hệ thống và không có điểm lỗi tập trung, điều này đã thúc đẩy sự chấp nhận của nó. Lợi ích chính của Bitcoin là cho phép giao dịch trực tiếp giữa các người dùng mà không cần bên trung gian đáng tin cậy. Hơn nữa, blockchain hỗ trợ việc phát hành tiền mã hóa mới theo cách được xác định sẵn cho những người tham gia duy trì mạng và cập nhật sổ cái, được gọi là *'thợ đào'* trong Bitcoin. Việc thanh toán tự động cho các thợ đào giúp quản lý hệ thống theo kiểu phân tán mà không cần tổ chức phức tạp. Blockchain và cơ chế đồng thuận đã tạo ra một hệ thống tự vận hành, đảm bảo rằng chỉ những giao dịch và khối hợp lệ mới được thêm vào blockchain.

Trong Bitcoin, blockchain cho phép người dùng ẩn danh một phần. Điều này có nghĩa là người dùng không bị nhận diện trực tiếp, nhưng mã định danh tài khoản của họ thì có thể được theo dõi. Hơn nữa, tất cả các giao dịch đều được công khai trên blockchain. Tính ẩn danh này giúp Bitcoin cung cấp mức độ bảo mật tương đối, vì tài khoản có thể được tạo mà không cần trải qua quy trình xác minh hoặc cấp phép, điều mà thường được yêu cầu theo luật *Know-Your-Customer (KYC)*.

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

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

Blockchain chính thức được giới thiệu vào năm 2009 với sự ra mắt của ứng dụng đầu tiên, tiền điện tử Bitcoin. Tuy nhiên, nguồn gốc của công nghệ này đã có từ nhiều thập kỷ trước. Nhiều công nghệ nền tảng của blockchain ngày nay đã được phát triển từ lâu trước khi Bitcoin xuất hiện.

Tuy nhiên, blockchain thường gắn liền với Bitcoin, dù theo hướng tích cực hay tiêu cực. Trong những năm hỗn loạn và ồn ào sau khi Bitcoin ra mắt, blockchain đã trở thành một công nghệ có tiếng tăm, giống như miền Tây hoang dã. Kiến trúc phân tán ngang hàng (P2P) của nó cho phép hầu như bất kỳ ai cũng có thể tham gia vào quy trình, khiến nó trở nên quá rủi ro đối với việc ứng dụng trong kinh doanh. Tuy nhiên, điều này bắt đầu thay đổi vào năm 2016, khi một cộng đồng nguồn mở đang phát triển bắt đầu xây dựng các nền tảng doanh nghiệp hoàn chỉnh.

Kể từ đó, công nghệ blockchain đã phát triển một cuộc sống riêng, thu hút sự quan tâm từ nhiều phía, bất chấp những tiêu đề đôi khi đáng sợ liên quan đến tiền điện tử. Các chính phủ, doanh nghiệp và các tổ chức khác đang nghiên cứu và triển khai công nghệ blockchain để phục vụ các nhu cầu không liên quan đến tiền kỹ thuật số. Trong bối cảnh các mối đe dọa mạng gia tăng và các quy định về quyền riêng tư dữ liệu của chính phủ, blockchain cung cấp tính bảo mật, tính bất biến, khả năng truy

xuất nguồn gốc và tính minh bạch trên toàn bộ mạng phân tán, giúp giải quyết những vấn đề mà cơ sở hạ tầng truyền thống khó có thể hỗ trợ và bảo vệ.

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

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

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

Vào năm 1979, một trong những công nghệ tiền blockchain đầu tiên, cây Merkle, được đặt theo tên nhà khoa học máy tính và nhà toán học Ralph Merkle. Ông đã mô tả một phương pháp phân phối khóa công khai và chữ ký số gọi là xác thực cây trong luận án tiến sĩ của mình tại Đại học Stanford. Sau đó, Merkle đã cấp bằng sáng chế cho ý tưởng này như một phương pháp cung cấp chữ ký số. Cây Merkle cung cấp một cấu trúc dữ liệu để xác minh các bản ghi riêng lẻ.

Vào năm 1992, trong luận án Tiến sĩ của mình tại Đại học California, Berkeley, David Chaum đã mô tả một hệ thống két để thiết lập, duy trì và tạo dựng lòng tin giữa các hệ thống máy tính của các nhóm nghi ngờ lẫn nhau. Hệ thống này bao gồm nhiều yếu tố tạo nên một blockchain. Chaum cũng được ghi nhận là người phát minh ra tiền kỹ thuật số, và vào năm 1989, ông đã thành lập công ty DigiCash.

Vào năm 1991, Stuart Haber và W. Scott Stornetta đã xuất bản một bài viết mô tả cách đóng dấu thời gian cho các tài liệu kỹ thuật số để ngăn người dùng thay đổi ngày tháng của các tài liệu điện tử. Mục tiêu là duy trì quyền riêng tư hoàn toàn của

tài liệu mà không cần phải lưu giữ hồ sơ của dịch vụ đóng dấu thời gian. Haber và Stornetta sau đó đã cập nhật thiết kế của mình để kết hợp cây Merkle, cho phép nhiều chứng chỉ tài liệu tồn tại trên một khối duy nhất.

Vào năm 1993, khái niệm ban đầu của **PoW** (Proof of Work) đã được công bố trong một bài báo của Cynthia Dwork và Moni Naor, nhằm cung cấp "*một kỹ thuật tính toán để chống thư rác nói riêng và kiểm soát quyền truy cập vào các tài nguyên được chia sẻ nói chung.*"

Vào năm 1997, Adam Black đã giới thiệu **hashcash**, một thuật toán PoW nhằm cung cấp các biện pháp đối phó với tình trạng từ chối dịch vụ (DoS).

Vào năm 1999, Markus Jakobsson và Ari Juels đã công bố thuật ngữ **bằng chứng công việc** (Proof of Work). Cùng năm, mạng **P2P** đã được phổ biến nhờ ứng dụng chia sẻ tệp ngang hàng **Napster**, mặc dù hiện nay ứng dụng này không còn tồn tại. Một số người cho rằng Napster không phải là mạng P2P thực sự vì nó sử dụng máy chủ tập trung. Tuy nhiên, dịch vụ này đã góp phần làm nổi bật khái niệm mạng P2P, giúp xây dựng các hệ thống phân tán có thể tận dụng sức mạnh tính toán và dung lượng lưu trữ từ hàng nghìn máy tính.

Vào năm 2000, Stefan Konst đã giới thiệu khái niệm về *chuỗi được bảo mật bằng mật mã* trong bài báo "Tệp nhật ký bảo mật dựa trên các mục được nối bằng mật mã." Mô hình của ông cho thấy các mục trong chuỗi có thể được truy ngược lại từ khối Genesis để chứng minh tính xác thực, và chính điều này đã trở thành cơ sở cho các mô hình blockchain ngày nay.

Vào năm 2004, Hal Finney đã giới thiệu PoW có thể tái sử dụng, một cơ chế để nhận một mã thông báo hashcash không thể trao đổi - hoặc không thể thay thế - để đổi lấy một mã thông báo được ký bằng RSA. Phương pháp PoW ngày nay đóng vai trò quan trọng trong việc khai thác Bitcoin. Các loại tiền điện tử như Bitcoin và Litecoin sử dụng PoW, trong khi Ethereum đã chuyển sang giao thức bằng chứng cổ phần (Proof of Stake) để bảo mật mạng với một phần năng lượng mà PoW sử dụng.

Vào năm 2008, Satoshi Nakamoto, được cho là bút danh của một cá nhân hoặc một nhóm cá nhân, đã xuất bản một sách trắng giới thiệu khái niệm về tiền mã hóa và blockchain, đồng thời phát triển phần mềm Bitcoin đầu tiên. Theo sách trắng, cơ sở hạ tầng blockchain sẽ hỗ trợ các giao dịch P2P an toàn mà không cần bên thứ ba đáng tin cậy như ngân hàng hoặc chính phủ. Danh tính thực sự của Nakamoto vẫn là một bí ẩn, nhưng không thiếu các giả thuyết.

Kiến trúc Bitcoin/blockchain được giới thiệu và xây dựng dựa trên các công nghệ và khái niệm phát triển từ ba thập kỷ trước. Thiết kế của Nakamoto cũng trình bày khái niệm về "chuỗi khối", cho phép thêm khối mà không cần sự xác nhận của bên thứ ba đáng tin cậy. Nakamoto định nghĩa đồng tiền mã hóa là "chuỗi chữ ký số", trong đó mỗi chủ sở hữu chuyển đồng tiền cho chủ sở hữu tiếp theo bằng cách "ký kỹ thuật số lên hàm băm của giao dịch trước đó và khóa công khai của chủ sở hữu tiếp theo, sau đó thêm chúng vào cuối đồng tiền".

Vào năm 2009, Bitcoin được ra mắt trong thời kỳ Đại suy thoái, khi các chính phủ đang bơm một lượng tiền lớn vào nền kinh tế. Lúc đó, giá trị của Bitcoin chưa đến một xu. Nakamoto đã khai thác khối Bitcoin đầu tiên, xác thực khái niệm blockchain. Khối này chứa 50 bitcoin và được gọi là khối Genesis, hay còn gọi là khối 0. Nakamoto đã phát hành Bitcoin v0.1 cho dịch vụ web SourceForge dưới dạng phần mềm nguồn mở. Hiện nay, Bitcoin có mặt trên GitHub.

Giao dịch Bitcoin đầu tiên diễn ra khi Nakamoto gửi cho Hal Finney 10 bitcoin trong khối 170. Kênh Bitcoin-dev được tạo ra trên hệ thống nhắn tin tức thời dựa trên văn bản Internet Relay Chat (IRC) dành cho các nhà phát triển Bitcoin. Sàn giao dịch Bitcoin đầu tiên - Bitcoin Market - được thành lập, cho phép mọi người đổi tiền giấy lấy bitcoin. Nakamoto đã ra mắt diễn đàn Bitcoin Talk để chia sẻ tin tức và thông tin liên quan đến Bitcoin.

Theo tinh thần coi tiền mã hóa là loại tiền có nguồn cung cố định, Nakamoto đã thiết lập một hệ thống để đảm bảo rằng số lượng bitcoin được khai thác sẽ không bao giờ vượt quá 21 triệu.

Vào ngày 22 tháng 5 năm 2010, Bitcoin đã đi vào lịch sử khi một lập trình viên Laszlo Hanyecz đã trả 10.000 bitcoin cho hai chiếc pizza Papa John's được giao. Hai chiếc pizza khi đó có giá trị khoảng 40 đô la, nhưng nếu tính theo mức giá Bitcoin hiện nay, giao dịch này sẽ có giá trị hơn 260 triệu đô la.

Một thời gian ngắn sau đó, Jed McCaleb, một lập trình viên, đã ra mắt Mt. Gox, một sàn giao dịch Bitcoin có trụ sở tại Tokyo. Mt. Gox là viết tắt của Magic: The Gathering Online eXchange, được lấy cảm hứng từ một trò chơi bài kỳ ảo. Vào thời kỳ đỉnh cao, Mt. Gox xử lý hơn 70% tổng số giao dịch Bitcoin. Tuy nhiên, vào tháng 8, một hacker đã khai thác một lỗ hổng trong mã của blockchain, tạo ra hơn 184 tỷ bitcoin trong khối 74.638, làm ảnh hưởng nghiêm trọng đến uy tín của Bitcoin. Nakamoto đã phát hành một phiên bản mới của phần mềm Bitcoin để khắc phục sự cố, nhưng đến cuối năm, anh ta đã hoàn toàn biến mất khỏi bối cảnh Bitcoin.

Năm 2011, một phần tư trong tổng số 21 triệu bitcoin đã được khai thác. Đến đầu tháng 2, giá trị của một bitcoin đã ngang bằng với đô la Mỹ. Ngay sau đó, McCaleb đã bán Mt. Gox cho Mark Karpelès. Bitcoin cũng đạt mức ngang bằng với đồng euro và bảng Anh. WikiLeaks bắt đầu chấp nhận quyên góp bằng bitcoin. Tuy nhiên, Mt. Gox đã bị hack và bitcoin đã bị đánh cắp, gây ra sự sụt giảm giá trị nhân tạo và dẫn đến việc đình chỉ giao dịch. Litecoin được phát hành vào tháng 10, là một sản phẩm phụ của Bitcoin và được coi là loại tiền điện tử thay thế đầu tiên.

Năm 2012, sự quan tâm đến tiền điện tử đã trở nên vững chắc. Giá Bitcoin dao động quanh mức 5 đô la trong hầu hết cả năm với một số biến động. Đầu năm đó, Mihai Alisie và người sáng lập Ethereum, Vitalik Buterin, đã ra mắt Tạp chí Bitcoin và xuất bản số đầu tiên vào tháng 5. Vài tháng sau, Quỹ Bitcoin được thành lập để quảng bá Bitcoin và khôi phục nhận thức công chúng về tiền điện tử sau một số vụ bê bối. McCaleb và Chris Larsen đã thành lập OpenCoin, dẫn đến sự phát triển của giao thức giao dịch Ripple cho các giao dịch tiền tệ và thanh toán theo thời gian thực. Coinbase đã huy động được hơn 600.000 đô la trong vòng gọi vốn đầu tiên và được

tài trợ bởi cộng đồng trên con đường trở thành một trong những sàn giao dịch Bitcoin hàng đầu.

Năm 2013, quỹ đạo đi lên của Bitcoin tiếp tục. Vào tháng 2, Coinbase báo cáo đã bán được 1 triệu đô la bitcoin chỉ trong một tháng, với giá hơn 22 đô la mỗi bitcoin. Đến cuối tháng 3, với 11 triệu bitcoin đang lưu hành, tổng giá trị của đồng tiền này đã vượt quá 1 tỷ đô la. Và vào tháng 10, máy ATM bitcoin đầu tiên được báo cáo đã ra mắt tại một quán cà phê ở Vancouver, BC.

Tuy nhiên, không phải tất cả đều là tin tốt cho tiền kỹ thuật số. Cả Thái Lan và Trung Quốc đều cấm tiền điện tử. Tòa án Liên bang Hoa Kỳ đã tịch thu tiền của Mt. Gox tại Hoa Kỳ vì chuyển tiền mà không có giấy phép. FBI cũng đã đóng cửa chợ đen Silk Road, tịch thu khoảng 144.000 bitcoin trị giá hơn 1 tỷ đô la, và kết quả là chủ sở hữu Ross Ulbricht bị kết án tù chung thân vì một loạt tội danh, bao gồm buôn bán ma túy, hack máy tính và rửa tiền.

Năm 2014, bất chấp những trở ngại, một trong những cột mốc quan trọng trong lịch sử blockchain đã diễn ra khi nhà đồng sáng lập Tạp chí Bitcoin, Vitalik Buterin, công bố một báo cáo đề xuất một nền tảng ứng dụng phi tập trung. Báo cáo này đã dẫn đến việc tạo ra Ethereum và Ethereum Foundation. Ethereum đã mở đường cho công nghệ blockchain được sử dụng cho các ứng dụng ngoài tiền điện tử. Nó giới thiệu các hợp đồng thông minh (smart contracts) và cung cấp cho các nhà phát triển một nền tảng để xây dựng các ứng dụng phi tập trung (dApps). Ethereum mang lại một cú hích lớn cho sự phát triển của blockchain, mở ra nhiều cơ hội ứng dụng trong các lĩnh vực như tài chính, quản lý chuỗi cung ứng, và nhiều lĩnh vực khác.

Các tổ chức tài chính và các ngành công nghiệp khác đã bắt đầu nhận ra và khai thác tiềm năng của công nghệ blockchain, chuyển trọng tâm từ tiền kỹ thuật số sang phát triển các ứng dụng blockchain. Tuy nhiên, Bitcoin vẫn là tâm điểm chú ý, cả tích cực lẫn tiêu cực. Sàn giao dịch Bitcoin Mt. Gox đã nộp đơn xin phá sản, và Phó Chủ tịch của Bitcoin Foundation bị bắt vì tội rửa tiền. Cùng lúc, cơ quan thuế Anh phân loại Bitcoin là tiền tư nhân. Dẫu vậy, một số công ty lớn như Chicago Sun-Times, Overstock.com, Microsoft, PayPal, và Expedia đã bắt đầu chấp nhận Bitcoin vào cuối năm. Sự chấp nhận này càng làm tăng sức nóng cho blockchain.

Năm 2015, mạng lưới Ethereum Frontier chính thức ra mắt, mở ra khả năng cho các nhà phát triển viết hợp đồng thông minh và xây dựng các ứng dụng phi tập trung trên một mạng lưới trực tiếp. Ethereum nhanh chóng trở thành một trong những ứng dụng nổi bật nhất của công nghệ blockchain, thu hút một cộng đồng nhà phát triển năng động và tiếp tục duy trì vị thế này cho đến ngày nay.Cùng năm, Nasdaq bắt đầu thử nghiệm công nghệ blockchain, trong khi Linux Foundation khởi xướng dự án Hyperledger nhằm thúc đẩy các ứng dụng blockchain doanh nghiệp. Đáng chú ý, chín ngân hàng đầu tư lớn đã hợp tác thành lập liên minh R3 để nghiên cứu cách blockchain có thể tối ưu hóa hoạt động của họ. Chỉ trong vòng sáu tháng, liên minh này đã mở rộng quy mô lên hơn 40 tổ chức tài chính trên toàn cầu.

Năm 2016 đánh dấu một bước ngoặt khi thuật ngữ "blockchain" chính thức được công nhận là một từ duy nhất, thay vì tách thành hai khái niệm riêng biệt như

trong bài báo gốc của Nakamoto. Trong năm này, Phòng Thương mại Kỹ thuật số và dự án Hyperledger đã thiết lập quan hệ đối tác nhằm thúc đẩy hoạt động vận động và giáo dục về công nghệ blockchain. Bên cạnh những bước tiến, năm 2016 cũng ghi nhận nhiều sự kiện đáng chú ý và thách thức. Một lỗ hổng trong mã của tổ chức tự trị phi tập trung Ethereum bị khai thác, buộc mạng Ethereum phải thực hiện một "hard fork" để giải quyết vấn đề. Đồng thời, sàn giao dịch tiền điện tử Bitfinex hứng chịu một vụ tấn công nghiêm trọng, dẫn đến việc mất cắp gần 120.000 bitcoin, tương đương khoảng 66 triệu USD vào thời điểm đó.

Năm 2017, Bitcoin đạt mức cao kỷ lục gần 20.000 USD, đánh dấu một cột mốc quan trọng trong lịch sử của tiền điện tử. Trong cùng năm, Nhật Bản chính thức công nhận Bitcoin là tiền tệ hợp pháp, tạo động lực lớn cho sự phát triển của thị trường này.

Bảy ngân hàng châu Âu đã hợp lực thành lập Digital Trade Chain Consortium, với mục tiêu phát triển một nền tảng tài chính thương mại dựa trên blockchain. Đồng thời, công ty phần mềm Block.one ra mắt hệ điều hành blockchain EOS, được xây dựng trên tiền điện tử EOS và thiết kế để hỗ trợ các ứng dụng phi tập trung cho mục đích thương mại.

Theo báo cáo, khoảng 15% các ngân hàng toàn cầu đã ứng dụng công nghệ blockchain ở một mức độ nào đó, minh chứng cho sự mở rộng nhanh chóng của công nghệ này trong lĩnh vực tài chính.

Năm 2018 đánh dấu cột mốc 10 năm kể từ khi Bitcoin ra đời, nhưng giá trị của nó lại giảm mạnh, khép lại năm với mức khoảng 3.800 USD. Trong bối cảnh này, công ty thanh toán trực tuyến Stripe đã ngừng chấp nhận thanh toán bằng Bitcoin, còn Google, Twitter và Facebook đồng loạt cấm quảng cáo tiền điện tử, gây thêm áp lực lên thị trường. Tuy nhiên, sự phát triển của công nghệ blockchain vẫn tiếp tục tiến lên. Hàn Quốc, dù cấm giao dịch tiền điện tử ẩn danh, đã cam kết đầu tư hàng triệu USD vào các sáng kiến blockchain. Ủy ban Châu Âu cũng ra mắt Đài quan sát và Diễn đàn Blockchain nhằm thúc đẩy sự phát triển của công nghệ này. Tại Trung Quốc, Baidu – gã khổng lồ công cụ tìm kiếm – đã giới thiệu nền tảng mở BaaS (Blockchain as a Service), khẳng định tầm quan trọng của blockchain trong các lĩnh vực công nghệ và kinh doanh.

Năm 2019 chứng kiến sự gia tăng đáng kể trong việc ứng dụng công nghệ blockchain vào các lĩnh vực thực tế. Walmart triển khai hệ thống chuỗi cung ứng dựa trên nền tảng Hyperledger, cải thiện đáng kể tính minh bạch và hiệu quả trong quản lý chuỗi cung ứng.

Amazon cũng gia nhập mạnh mẽ vào không gian blockchain với việc ra mắt dịch vụ Amazon Managed Blockchain trên nền tảng AWS. Dịch vụ này hỗ trợ người dùng xây dựng các ứng dụng Web 3.0 có khả năng phục hồi trên cả blockchain công khai lẫn riêng tư, mở ra nhiều tiềm năng mới cho doanh nghiệp.

Đồng thời, mạng Ethereum ghi nhận kỷ lục với hơn một triệu giao dịch mỗi ngày, phản ánh sự phát triển nhanh chóng của các ứng dụng phi tập trung (dApps). Trong bối cảnh đó, nghiên cứu và phát triển blockchain trở thành ưu tiên hàng đầu

khi các tổ chức trên toàn cầu tích cực áp dụng công nghệ này cho nhiều trường hợp sử dụng đa dạng, từ tài chính, y tế đến quản lý tài sản và chuỗi cung ứng.

Năm 2020, blockchain tiếp tục đóng vai trò chiến lược quan trọng, với 40% doanh nghiệp triển khai vào sản xuất và 55% coi là ưu tiên hàng đầu, theo khảo sát của Deloitte. Ethereum ra mắt Beacon Chain, chuẩn bị cho Ethereum 2.0 nhằm cải thiện khả năng mở rộng và bảo mật. Stablecoin phát triển mạnh mẽ nhờ tính ổn định so với tiền điện tử truyền thống. Đồng thời, sự kết hợp giữa blockchain và AI thu hút sự chú ý, tập trung vào tối ưu hóa quy trình kinh doanh và khai thác dữ liệu phi tập trung.

Năm 2021, blockchain và tiền điện tử đạt những cột mốc quan trọng. Bitcoin chạm mức cao kỷ lục 68.789,63 USD, với vốn hóa thị trường vượt 3 nghìn tỷ USD. Coinbase thực hiện đợt niêm yết lớn trên sàn chứng khoán Hoa Kỳ, trong khi thị trường DeFi tăng trưởng 600%, đạt giá trị 200 tỷ USD. Tác phẩm nghệ thuật NFT được bán với giá 69 triệu USD, khẳng định sự bùng nổ của lĩnh vực này.

Nhiều nhân vật nổi tiếng, như Elon Musk và Aaron Rogers, tham gia vào thị trường, với Musk cho phép thanh toán bằng Bitcoin cho xe Tesla (dù sau đó hủy bỏ) và Rogers nhận lương NFL bằng Bitcoin.

Blockchain không chỉ còn gắn liền với tiền điện tử mà còn được áp dụng rộng rãi trong các lĩnh vực như bỏ phiếu, bất động sản, theo dõi sức khỏe, sở hữu trí tuệ, IoT và phân phối vắc-xin trong đại dịch COVID-19. Các nhà cung cấp dịch vụ đám mây mở rộng dịch vụ blockchain, và nhu cầu về nhà phát triển blockchain tăng cao.

Theo Statista, thị trường blockchain toàn cầu được định giá gần 6 tỷ USD trong năm 2021 và dự báo sẽ vượt qua 1 nghìn tỷ USD vào năm 2030, cho thấy tiềm năng phát triển mạnh mẽ của công nghệ này trong tương lai.

Năm 2022, NFT tiếp tục tăng trưởng, mạng lưới blockchain thân thiện với môi trường xuất hiện và các ứng dụng blockchain tăng lên trong các công ty. Hoạt động khai thác Bitcoin tiến gần hơn đến giới hạn 21 triệu coin của Nakamoto, đạt 19 triệu và chỉ còn chưa đến 10% bitcoin có thể khai thác.

Giá của Bitcoin và các loại tiền điện tử khác đã giảm mạnh vào mùa xuân sau khi đạt mức cao nhất mọi thời đại, do lo ngại từ các nhà đầu tư về lạm phát và sự xuất hiện của biến thể Omicron của COVID-19. Một số sàn giao dịch tiền điện tử đã tuyên bố phá sản. Sự sụp đổ của sàn giao dịch FTX và vụ bắt giữ CEO Sam Bankman-Fried đã làm dấy lên lo ngại về rủi ro trong ngành tiền điện tử. Nền tảng blockchain nguồn mở Terra cũng đã sụp đổ. Sự suy đoán về các quy định mới của chính phủ Hoa Kỳ đối với tiền điện tử đã làm gia tăng sự không chắc chắn, nhưng cũng được cho là sẽ giúp hợp pháp hóa ngành công nghiệp này.

Trên toàn cầu, công ty vận chuyển Đan Mạch Maersk đã thông báo đóng cửa sổ cái kỹ thuật số TradeLens, dựa trên blockchain, mà họ đồng phát triển với IBM, do thiếu sự tham gia từ các bên tham gia. Đồng thời, Sở giao dịch chứng khoán Úc đã hủy bỏ kế hoạch kéo dài bảy năm để chuyển nền tảng giao dịch của mình sang blockchain. Theo Statista, hơn 100 quốc gia đã tham gia vào việc phát triển tiền kỹ

thuật số của ngân hàng trung ương (CBDC). CBDC là phiên bản kỹ thuật số của tiền pháp định trong thế giới thực, nhằm tăng tốc các giao dịch bán lẻ xuyên biên giới trên blockchain, trái ngược với tốc độ chậm và sự biến động giá của tiền điện tử.

Những tuyên bố về tính bất khả xâm phạm của blockchain đã bị tấn công, không chỉ theo nghĩa bóng. Công ty phân tích blockchain Chainalysis đã xác định gần 200 vụ hack tiền điện tử hoặc blockchain, gây thiệt hại lên đến 3,8 tỷ đô la. Sự cố đáng chú ý nhất xảy ra khi blockchain của trò chơi điện tử Ronin Network báo cáo vụ trộm 625 triệu đô la Ether và stablecoin USDC. Bộ Tài chính Hoa Kỳ đã đổ lỗi cho một nhóm tin tặc từ Triều Tiên về vụ tấn công này.

Năm 2023, ngành tiền điện tử tiếp tục đối mặt với những thách thức lớn khi Ủy ban Chứng khoán và Giao dịch Hoa Kỳ (SEC) truy tố các giám đốc điều hành của hai sàn giao dịch lớn, Coinbase và Binance. Đồng thời, SEC cũng đệ đơn kiện doanh nhân Justin Sun và ba công ty do ông sở hữu hoàn toàn với cáo buộc thực hiện hành vi chào bán và bán chứng khoán tiền điện tử chưa đăng ký.

Các doanh nghiệp vẫn tiếp tục triển khai công nghệ blockchain, nhưng với sự thận trọng hơn trước. Hiện tại, blockchain được ứng dụng chủ yếu trong lĩnh vực tài chính và ngân hàng, nhưng các lĩnh vực tiềm năng khác cũng đang dần được khám phá, bao gồm trò chơi, truyền thông và giải trí, bất động sản, chăm sóc sức khỏe, an ninh mạng, hợp đồng thông minh, NFT, IoT, vận tải, quản lý chuỗi cung ứng và quản trị công. Đặc biệt, Web 3.0 – phiên bản mới nhất của internet – với khả năng cung cấp tính phi tập trung và bảo mật dữ liệu, đang được xem là động lực lớn nhất thúc đẩy sự phát triển của công nghệ blockchain.

Bitcoin hiện đã ổn định ở mức giá tương đối vững chắc trong khoảng từ 25.000 đến 30.000 USD. Theo thiết kế ban đầu của Satoshi Nakamoto, hoạt động khai thác Bitcoin sẽ dần tiến tới giới hạn tối đa 21 triệu đồng, dự kiến đạt được vào khoảng năm 2140.

Sau năm 2023, một số xu hướng dự kiến sẽ đóng góp đáng kể vào việc đạt được mức định giá nghìn tỷ đô la của công nghệ blockchain, bao gồm:

- Mở rộng ứng dụng DeFi (Tài chính phi tập trung): Các giao thức DeFi tiếp tục phát triển, mang lại giải pháp tài chính minh bạch và phi tập trung cho người dùng toàn cầu.

- Sự phát triển của Web 3.0: Internet phi tập trung, với các ứng dụng dựa trên blockchain, sẽ mở ra tiềm năng to lớn trong việc bảo mật dữ liệu và quyền riêng tư.

- Tích hợp blockchain vào quản lý chuỗi cung ứng: Đảm bảo tính minh bạch và truy xuất nguồn gốc trong chuỗi cung ứng toàn cầu.

- NFT và tài sản kỹ thuật số: Sự phát triển của NFT tiếp tục định hình cách thức sở hữu và giao dịch tài sản kỹ thuật số trong các lĩnh vực như nghệ thuật, giải trí và thể thao.

- Ứng dụng trong lĩnh vực IoT: Kết hợp blockchain với Internet vạn vật (IoT) để cải thiện khả năng bảo mật và quản lý thiết bị.

- Hợp đồng thông minh nâng cao: Sử dụng các hợp đồng tự thực thi ngày càng phổ biến trong các lĩnh vực pháp lý, bất động sản và chăm sóc sức khỏe.

- Chuyển đổi kỹ thuật số trong chính phủ: Blockchain có tiềm năng cách mạng hóa quản lý dữ liệu, bầu cử và dịch vụ công tại nhiều quốc gia.

2.3. CÁC LOẠI MẠNG BLOCKCHAIN

Có bốn loại mạng blockchain chính: blockchain công khai, blockchain riêng tư, blockchain liên minh và blockchain lai. Mỗi loại mạng này có đặc điểm riêng, với các lợi ích, nhược điểm và ứng dụng lý tưởng khác nhau. Chúng ta sẽ cùng khám phá chi tiết về từng nền tảng.

2.3.1. Blockchain công khai

Cách thức hoạt động: Blockchain công khai là nơi tiền điện tử như Bitcoin ra đời, giúp phổ biến công nghệ sổ cái phân tán (Distributed Ledger Technology - DLT). Công nghệ này giải quyết các vấn đề của tập trung hóa, bao gồm bảo mật và minh bạch kém. DLT không lưu trữ thông tin ở một địa điểm duy nhất, mà phân phối thông tin trên một mạng ngang hàng (peer-to-peer). Bản chất phi tập trung của blockchain yêu cầu sử dụng các phương pháp xác minh tính xác thực của dữ liệu. Một trong những phương pháp này là thuật toán đồng thuận, giúp các thành viên trong mạng blockchain đạt được sự thỏa thuận về trạng thái hiện tại của sổ cái. Hai phương pháp đồng thuận phổ biến nhất là Bằng chứng công việc (Proof of Work - PoW) và Bằng chứng cổ phần (Proof of Stake - PoS).

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

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

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

Trường hợp sử dụng: Trường hợp sử dụng phổ biến nhất của blockchain công khai là khai thác và trao đổi tiền điện tử như Bitcoin. Tuy nhiên, nó cũng có thể được

áp dụng để tạo ra các hồ sơ cố định với chuỗi lưu ký có thể kiểm toán, ví dụ như công chứng điện tử các bản tuyên thệ hoặc tạo hồ sơ công khai về quyền sở hữu tài sản.

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

2.3.2. Blockchain riêng tư

Cách thức hoạt động: Một blockchain riêng tư hoạt động trong một môi trường hạn chế, như một mạng lưới khép kín hoặc dưới sự kiểm soát của một thực thể duy nhất. Mặc dù sử dụng các kết nối ngang hàng và phi tập trung giống như blockchain công khai, nhưng blockchain riêng tư có quy mô nhỏ hơn nhiều. Thay vì cho phép bất kỳ ai tham gia và cung cấp sức mạnh tính toán, blockchain riêng tư thường được vận hành trên một mạng lưới nhỏ trong nội bộ một công ty hoặc tổ chức. Loại blockchain này còn được gọi là blockchain được cấp phép hoặc blockchain doanh nghiệp.

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

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

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

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

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

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

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

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

2.3.3. Blockchain lai

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

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

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

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

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

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

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

2.3.4. Blockchain liên kết

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

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

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

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

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

2.4. TIỀN MÃ HÓA VÀ TOKENOMICS

2.4.1. Tiền mã hóa

2.4.1.1. Khái niệm

Tiền mã hóa hay tiền điện tử là một loại tiền kỹ thuật số được thiết kế để hoạt động thông qua một mạng máy tính, không phụ thuộc bất kỳ cơ quan trung ương nào, chẳng hạn như chính phủ hoặc ngân hàng …

Tiền mã hóa là một dạng tiền tệ kỹ thuật số sử dụng mật mã để bảo mật các quy trình liên quan đến việc tạo đơn vị, thực hiện giao dịch và xác minh việc trao đổi quyền sở hữu tiền tệ.

Hầu hết các loại tiền tệ hiện đại thường được gọi là tiền tệ "**fiat**", được quản lý và sản xuất bởi một thực thể chính phủ. Ví dụ, đồng đô la Mỹ là một loại tiền tệ fiat. Ngược lại, tiền điện tử không được phát hành bởi bất kỳ cơ quan chính phủ nào. Nó thường không được quản lý trực tiếp bởi một cơ quan duy nhất mà hoạt động theo phương pháp tiếp cận đồng thuận phân tán.

Tiền mã hóa có tên gọi này từ sự kết hợp của "mật mã" và "tiền tệ". Trọng tâm của tất cả các loại tiền mã hóa là một thuật toán mật mã với mã hóa phức tạp . Tiền mã hóa được tạo ra bằng cách giải một phần của thuật toán băm mật mã trong một

chuỗi dài. Nó không phải là một đơn vị vật lý, như một đồng xu hoặc một tờ đô la, mà là một phép tính toán học. Tài sản tiền mã hóa thường được lưu trữ trong một ví kỹ thuật số để theo dõi tiền mã hóa.

Một sổ cái phân tán, phi tập trung giám sát tất cả các giao dịch tiền mã hóa trên toàn thế giới. Một trong những loại tiền mã hóa nổi tiếng nhất là Bitcoin, được giới thiệu vào năm 2009. Kể từ đó, tiền mã hóa đã trở nên cực kỳ phổ biến. Theo một số ước tính, có hơn 10.000 loại tiền kỹ thuật số đang lưu hành trên toàn thế giới.

Không giống như tiền tệ truyền thống, được một quốc gia chấp thuận là tiền tệ hợp pháp và được quản lý bởi chính phủ quốc gia và ngân hàng trung ương, tiền mã hóa phần lớn không được quản lý và không có một thực thể tài chính bao quát nào giám sát việc sử dụng nó.

Tiền mã hóa là gì?

Tiền mã hóa là loại tiền kỹ thuật số được bảo vệ bằng mật mã, giúp đảm bảo tính bảo mật và xác thực của giao dịch. Đây là một tài sản kỹ thuật số thường được sử dụng làm phương tiện trao đổi trong các giao dịch. Tiền mã hóa có thể hoạt động trên toàn cầu, không bị giới hạn bởi múi giờ, và hoạt động 24/7. Đặc biệt, tiền mã hóa độc lập với các trung gian như ngân hàng và đơn vị xử lý thanh toán, giúp giảm thiểu chi phí giao dịch và thời gian xử lý.

Bản chất phi tập trung của tiền mã hoá hỗ trợ giao dịch trực tiếp giữa cá nhân với cá nhân (P2P). Vì vậy, thay vì sử dụng ví cứng và tài khoản ngân hàng, mọi người truy cập tiền mã hóa thông qua các ví tiền mã hóa hoặc sàn giao dịch tiền mã hoá độc đáo như Binance, Remitano, BitMart, …

Đồng tiền mã hóa đầu tiên?

Bitcoin là đồng tiền mã hóa đầu tiên và nổi tiếng nhất. Bitcoin được một người hoặc một nhóm người lấy tên là "Satoshi Nakamoto" tạo ra vào năm 2009. Kể từ đó, hàng nghìn loại tiền mã hóa ra đời, mỗi loại lại có những đặc điểm và mục đích riêng.

Giống như tiền pháp định truyền thống, tiền mã hóa có thể được sử dụng làm phương tiện trao đổi. Tuy nhiên, công dụng của tiền mã hoá đã phát triển đáng kể trong những năm qua và hiện bao gồm nhiều ứng dụng trong nhiều ngành chẳng hạn như tài chính phi tập trung (DeFi), trí tuệ nhân tạo, game, quản trị, chăm sóc sức khỏe, đồ sưu tầm kỹ thuật số cùng nhiều ngành khác.

2.4.1.2. Những đặc điểm chính của tiền mã hóa?

- Tiền mã hóa là loại tiền kỹ thuật số được bảo vệ bằng mật mã. Tiền mã hóa được hỗ trợ bởi công nghệ blockchain, cho phép người dùng gửi và nhận tài sản thông qua mạng lưới ngang hàng (P2P) phi tập trung.
- Bitcoin, ETH, BNB, USDT và SOL là ví dụ về các đồng tiền mã hoá hàng đầu tính theo vốn hóa thị trường.

- Người dùng truy cập tiền mã hóa thông qua ví tiền mã hóa hoặc sàn giao dịch. Mặc dù mọi người thường nói rằng tiền mã hóa được "lưu trữ" trong ví nhưng thực tế số dư được ghi lại trên blockchain.

Tiền mã hóa hoạt động như thế nào?

Mạng lưới blockchain

Hầu hết các loại tiền mã hoá đều phi tập trung, nghĩa là chúng sử dụng mạng lưới máy tính phân tán (node) để quản lý và ghi lại các giao dịch trong một sổ cái công khai được gọi là blockchain.

Vì vậy, bất cứ khi nào bạn gửi bitcoin cho bạn bè, giao dịch của bạn phải được các node của mạng lưới cùng xác minh và xác thực.

Mỗi node máy tính phải duy trì một bản sao cục bộ của blockchain và cập nhật bản sao đó mỗi khi có dữ liệu mới được thêm vào sổ cái. Sau khi được xác thực và xác nhận, các giao dịch tiền mã hóa sẽ được ghi lại vĩnh viễn trong cơ sở dữ liệu blockchain.

Kiến trúc phân tán này làm tăng tính bảo mật của mạng lưới vì không có điểm lỗi duy nhất nào để đối tượng xấu khai thác. Nếu một node cố gắng xác thực các giao dịch không hợp lệ hoặc hoạt động không đúng cách, node đó sẽ nhanh chóng bị trục xuất khỏi mạng lưới.

Mật mã học

Tiền mã hóa sử dụng mật mã để bảo mật giao dịch, duy trì tính toàn vẹn dữ liệu và kiểm soát việc tạo ra các đơn vị bổ sung. Khi bạn mở ví và thực hiện giao dịch tiền mã hoá, về cơ bản bạn đang sử dụng khóa riêng tư của mình để tạo chữ ký số. Sau đó, mạng lưới sẽ kiểm tra chữ ký của bạn. Nếu mọi thứ đều ổn, giao dịch của bạn sẽ được thêm vào một block mới.

Blockchain là một chuỗi các block được liên kết với nhau, do đó bạn có thể coi mỗi block là một trong nhiều trang trên sổ cái blockchain. Mỗi block chứa một danh sách duy nhất các giao dịch tiền mã hoá, cùng với những thông tin khác.

2.4.1.3 Phân loại tiền mã hóa?

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

Bitcoin

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

Bitcoin sử dụng cơ chế đồng thuận gọi là **proof-of-work (PoW)**, trong đó các thợ đào cạnh tranh với nhau để xác thực giao dịch và nhận phần thưởng dưới dạng block. Quá trình này đòi hỏi sức mạnh tính toán để giải các bài toán phức tạp, giúp đảm bảo tính bảo mật của mạng lưới.

Ngoài ra, với nguồn cung hạn chế chỉ **21 triệu coin**, Bitcoin trở nên tương đối khan hiếm và thường được coi là "vàng kỹ thuật số", bởi vì tính khan hiếm này làm tăng giá trị và sự hấp dẫn của nó như một tài sản đầu tư dài hạn.

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

Một số đồng tiền mã hóa altcoin phổ biến:

Ether (ETH)

Ether (ETH) là đồng coin gốc của blockchain Ethereum. Được tạo ra bởi Vitalik Buterin, Ethereum cung cấp một mạng lưới phi tập trung để nhà phát triển có thể xây dựng DApp bằng hợp đồng thông minh.

Ban đầu, Ethereum sử dụng cơ chế đồng thuận proof-of-work nhưng sau đó đã chuyển sang proof-of-stake (PoS) để tăng hiệu quả và giảm mức tiêu thụ năng lượng. Sự thay đổi này cho phép người dùng xác thực giao dịch và bảo mật mạng lưới bằng cách stake ETH thay vì thông qua các node sử dụng công suất tính toán.

Cardano (ADA)

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

Cardano (ADA) là nền tảng blockchain mã nguồn mở được sáng lập bởi Charles Hoskinson, nhằm cung cấp một hệ thống an toàn và bền vững cho các ứng dụng phân tán và hợp đồng thông minh. Cardano sử dụng cơ chế đồng thuận Proof of Stake (PoS) với tên gọi Ouroboros, giúp tiết kiệm năng lượng và tăng khả năng mở rộng. Nó có kiến trúc phân tách thành hai tầng: Settlement Layer (SL) cho giao dịch và Computation Layer (CL) cho hợp đồng thông minh. Cardano hỗ trợ hợp đồng thông minh qua ngôn ngữ Plutus, với mục tiêu cung cấp khả năng tương tác giữa các blockchain khác nhau và phát triển bền vững. Token ADA là đồng tiền chính, được dùng trong các giao dịch và staking.

BNB

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

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

BNB có nhiều công dụng, bao gồm staking, thanh toán phí giao dịch trên BNB Chain và sàn Binance, cũng như tham gia các đợt mở bán token trên Launchpool. Ngoài ra, cơ chế tự động đốt BNB giúp giảm nguồn cung và tạo ra sự khan hiếm, góp phần duy trì giá trị của đồng coin này.

Tether (USDT)

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

Trong trường hợp của USDT, mỗi token được đảm bảo bằng một lượng tài sản tương đương nắm giữ trong khoản dự trữ của công ty. Các stablecoin như USDT giúp loại bỏ chi phí bổ sung và sự chậm trễ thường thấy khi chuyển qua lại giữa tiền mã hoá và tiền pháp định.

Litecoin

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

Solana (SOL)

SOL là đồng tiền mã hoá gốc của blockchain Solana. Solana là một blockchain PoS thế hệ thứ ba ra mắt vào năm 2020. Solana đã thực hiện nhiều cải tiến độc đáo để mang lại thông lượng cao, tốc độ giao dịch nhanh và phí thấp.

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

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

Dịch vụ chuyển tiền

Một trong những ứng dụng lớn nhất của các loại tiền mã hoá (đặc biệt là các loại tiền mã hoá Litecoin- LTC, Stellar Lumen- XLM và Bitcoin Cash- BCH) là khả năng thực hiện các giao dịch quy mô lớn trong thời gian ngắn và chi phí thấp dựa trên nền tảng công nghệ chuỗi khối của các đồng tiền mã hoá. Chẳng hạn, một giao dịch chuyển tiền bằng LTC trị giá 99 triệu USD đã được thực hiện trong vòng 2,5 phút và chỉ tiêu tốn của người gửi 0,4 USD phí giao dịch (Lielacher, 2018). Quy trình chuyển tiền, bao gồm cả thời gian và chi phí được đánh giá có ưu thế vượt trội so với chi phí dịch vụ chuyển tiền tại các định chế tài chính.

Thanh toán

Tiền mã hoá cũng được một số tổ chức, đơn vị chấp nhận sử dụng trong việc thanh toán cho giao dịch hoặc trả thưởng nhân viên, thành viên tham gia. Chẳng hạn,

nền tảng kết nối xã hội và nhật ký trực tuyến (blog) hàng đầu thế giới, trang Steemit (https:// steemit.com/) thưởng bằng tiền mã hoá cho các thành viên có bài đăng trên trang và những thành viên chịu trách nhiệm quản lý nội dung bài đăng trên trang nhằm khuyến khích các thành viên của trang web gia tăng chất lượng nội dung đăng tải trên trang (Lielacher, 2018). Thống kê của Statista (2020) cũng cho thấy số lượng tài khoản ví điện tử Blockchain trên thế giới tăng gần 5 lần, từ 8,95 triệu ví ở quý 3/2016 lên gần 44,7 triệu ví tính đến cuối quý 4/2019 (Hình 4).

Một số công ty du lịch như CheapAir và Destinia cũng chấp nhận Bitcoin trong thanh toán tiền vé máy bay, dịch vụ thuê phương tiện đi lại, dịch vụ khách sạn (Lielacher, 2018). Việc thanh toán khi đi du lịch cũng trở nên dễ dàng hơn với những cá nhân, tổ chức có sở hữu tiền mã hoá khi thị trường các ATM Bitcoin ngày càng trở nên phổ biến trên thế giới, nghĩa là người dùng có thể đổi tiền mã hoá sang tiền pháp định địa phương ở nhiều thành phố du lịch lớn trên thế giới. Thống kê của coinmap biểu thị trong Hình 1 ở trên cũng đã cho thấy mức độ ứng dụng và chấp nhận rộng rãi của các chủ thể tham gia nền kinh tế đối với Bitcoin nói riêng và tiền mã hoá nói chung trong lĩnh vực thanh toán.

Huy động vốn và Đầu tư

Huy động vốn thông qua các đợt phát hành tiền mã hoá (ICOs-Initial coin offerings) đang ngày càng trở nên phổ biến và có ý nghĩa quan trọng đối với các doanh nghiệp khởi nghiệp hoạt động trong lĩnh vực công nghệ chuỗi khối, đặc biệt là các doanh nghiệp có quy mô nhỏ và khó có khả năng tiếp cận các nguồn tài trợ vốn truyền thống từ phía các định chế tài chính hay thông qua huy động vốn trên TTCK.

Về mặt thuật ngữ, "tiền mã hoá" trong tên gọi Phương án phát hành tiền mã hoáICOs- hàm ý nói tới các token phát hành theo các dự án hoặc tổ chức phát hành cụ thể, chứ không phải các đồng tiền mã hoá được tạo lập với công nghệ chuỗi khối riêng biệt như Bitcoin, Eutherem… Loại tài sản số như "token" và "tiền mã hoá" ("coin") thường bị sử dụng một cách nhầm lẫn, lẫn nhau về mặt thuật ngữ mặc dù về mặt tính chất, đặc điểm là khác nhau hoàn toàn.

Để huy động vốn thông qua các đợt phát hành tiền mã hoá, các tổ chức phát hành (doanh nghiệp khởi nghiệp blockchain) thường phải có hệ thống tiền tệ riêng (là các loại tiền mã hoá- tài sản kỹ thuật số tư nhân, thường được gọi "token" mã hoá). Các token này sẽ được định giá bởi tổ chức phát hành và được bán cho nhà đầu tư bằng tiền mã hoá. Sau đó nhà đầu tư có thể nắm giữ token hoặc bán token trên thị trường thứ cấp để đổi lấy tiền mã hoá. Tuy nhiên, thị trường thứ cấp của các token tương đốikém thanh khoản (Lipush, 2018).

Khác với phát hành chứng khoán phải tuân thủ quy định chặt chẽ của Bộ Tài chính, việc phát hành tiền mã hoá để huy động vốn phần lớn không chịu sự quản lý của cơ quan chức năng. Tổ chức phát hành chỉ cần có ý tưởng kinh doanh, sách trắng (bản báo cáo thông tin phát hành và mục đích sử dụng vốn, thay vì phải có Bản cáo bạch trong hồ sơ phát hành theo yêu cầu của một phương án phát hành chứng khoán) là có thể tổ chức huy động vốn bằng tiền mã hoá.

2.4.2. Tokenomics

2.4.2.1. Khái niệm

Trong nền kinh tế học truyền thống, quá trình sản xuất, phân phối và tiêu thụ hàng hóa thường đi kèm với các phương tiện trao đổi như tiền tệ và hàng hóa. Tiền tệ là phương tiện trao đổi phổ biến nhất, giúp đơn giản hóa việc mua bán và định giá hàng hóa, dịch vụ. Trước khi tiền tệ ra đời, trao đổi hàng hóa trực tiếp (barter) là hình thức phổ biến, trong đó một loại hàng hóa được đổi lấy một loại hàng hóa khác có giá trị tương đương. Tương tự, trong hệ sinh thái blockchain, phương thức trao đổi, quản lý và lưu hành là các token kỹ thuật số (hay còn gọi là tokenomics). Tokenomics đề cập đến các yếu tố kinh tế liên quan đến sự phát triển, phân phối và sử dụng các token trong blockchain, đóng vai trò tương tự như tiền tệ trong nền kinh tế truyền thống.

Hiểu về tokenomics là điều tối quan trọng đối với bất kỳ ai tham gia hoặc quan tâm đến thế giới tiền mã hóa, vì nó ảnh hưởng trực tiếp đến giá trị, tiện ích và tiềm năng của một tài sản kỹ thuật số. Hãy tìm hiểu sâu hơn để nắm bắt các khái niệm cơ bản và khám phá lý do tại sao tokenomics lại đóng vai trò then chốt đối với tương lai của tài chính phi tập trung, và của nền kinh tế số tương lai.

Tokenomics là gì?

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

Chúng ta hãy cùng xem xét crypto token là gì . Đây là đơn vị tiền tệ kỹ thuật số được các dự án crypto xây dựng trên blockchain hiện có. Giống như bất kỳ loại tiền tệ thông thường nào, crypto token giữ một giá trị nhất định và có thể trao đổi được.

Về kinh tế, việc tìm hiểu xem kinh tế token khác với kinh tế truyền thống như thế nào là điều rất quan trọng. Bất kể thời đại nào trong lịch sử, các chính phủ đều tạo ra thêm tiền mà không dựa trên bất kỳ cơ sở thực tế nào. Từ việc xung đột chiến tranh hoặc giải quyết hạn hán có thể rất tốn kém. Để giải quyết vấn đề này, tăng doanh thu không phải lúc nào cũng là một lựa chọn và các nhà chức trách thấy rằng đúc tiền là một giải pháp thay thế đơn giản hơn. Việc tạo ra thêm tiền cuối cùng sẽ làm giảm giá trị của đồng tiền hiện có.

Tuy nhiên, các dự án tiền điện tử đã xác định trước và tạo lịch phát hành theo thuật toán cho các token. Chúng ta có thể dự đoán chính xác số lượng coin đang lưu hành tại một thời điểm cụ thể. Việc phân phối coin giữa các bên liên quan khác nhau cũng được cân nhắc trước. Mặc dù về mặt kỹ thuật có thể thay đổi lịch phát hành và kế hoạch phân phối, nhưng quá trình này rất khó thực hiện.

Ví dụ: Bitcoin cho thấy cách thiết kế tokenomics của một đồng token khá đơn giản và khéo léo. Tổng nguồn cung của Bitcoin được lập trình trước với số lượng tối đa là 21 triệu token. Bitcoin được tạo ra và phát hành thông qua quá trình đào tạo,

trong đó các miners (thợ đào) được thưởng bằng một số lượng Bitcoin khi khối được khai thác khoảng mỗi 10 phút một lần.

Phần thưởng này, còn được gọi là block subsidy, sẽ giảm một nửa mỗi khi 210.000 block được khai thác. Theo lịch trình này, mỗi lần giảm một nửa sẽ diễn ra sau mỗi bốn năm. Dựa trên các quy tắc này, ta có thể dễ dàng tính toán được số Bitcoin được khai thác hàng năm và dự đoán rằng Bitcoin cuối cùng sẽ được khai thác vào khoảng năm 2140.

Tokenomics của Bitcoin cũng bao gồm thiết kế phí giao dịch, mà các miners nhận được khi khối mới được xác nhận. Phí này được thiết kế để tăng lên khi kích thước giao dịch và tắc nghẽn mạng tăng. Nó giúp ngăn chặn các giao dịch spam và khuyến khích miners tiếp tục xác nhận giao dịch ngay cả khi block subsidy giảm dần.

Tóm lại, tokenomics của Bitcoin rất đơn giản và khéo léo, tất cả đều minh bạch và dự đoán được. Các động lực xung quanh Bitcoin giúp các thành viên tham gia được bồi thường để giữ cho mạng lưới vững mạnh và đóng góp vào giá trị của nó như một loại token.

2.4.2.2. Phân loại

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

a) Phân loại theo mục đích sử dụng

Utility Token (Token tiện ích):

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

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

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

Security Tokens:

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

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

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

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

Governance Token (Token quản trị):

Cung cấp quyền biểu quyết cho người nắm giữ trong các quyết định liên quan đến phát triển hoặc quản lý dự án.

Token quản trị là token mà các nhà phát triển tạo ra để cho phép người nắm giữ token giúp định hình tương lai của một giao thức. Người nắm giữ token quản trị có thể tác động đến các quyết định liên quan đến dự án như đề xuất hoặc quyết định về các đề xuất tính năng mới và thậm chí thay đổi chính hệ thống quản trị.

Trong nhiều trường hợp, các thay đổi được đề xuất, thẩm định và sau đó bỏ phiếu thông qua quản trị trên chuỗi được truy cập bằng cách sử dụng mã thông báo quản trị được áp dụng tự động do hợp đồng thông minh. Trong các trường hợp khác, nhóm duy trì dự án được giao nhiệm vụ áp dụng các thay đổi hoặc thuê người sẽ thực hiện.

Những người ủng hộ hệ thống sử dụng token quản trị tin rằng chúng cho phép người dùng kiểm soát, điều này đúng với lý tưởng ban đầu của tiền điện tử về phi tập trung và dân chủ hóa. Trong hầu hết các trường hợp, các tổ chức cho phép người dùng kiểm soát sự phát triển của hệ thống của họ được gọi là các tổ chức tự trị phi tập trung (DAO).

Một ví dụ nổi tiếng về token quản trị là Maker (MKR). Token này cho phép người nắm giữ bỏ phiếu cho các quyết định liên quan đến giao thức tài chính phi tập trung (DeFi) mà stablecoin phi tập trung DAI chạy trên đó.

Mỗi token quản trị mà một người nắm giữ thường tương đương với một phiếu bầu cho các đề xuất sắp tới, nhưng có những phương pháp khác. Những người có token quản trị có thể sử dụng chúng để chấp nhận hoặc từ chối các thay đổi đối với một ứng dụng phi tập trung (dApp) hoặc blockchain trong các giai đoạn bỏ phiếu theo lịch trình. Nhiều dApp cũng cho phép mọi người sử dụng token quản trị của họ để tạo ra các sáng kiến và đưa chúng ra để bỏ phiếu.

Payment Tokens (Token thanh toán):

Token thanh toán được sử dụng như một phương tiện thanh toán và trao đổi thay thế. Không giống như các loại tiền tệ fiat như Đô la Mỹ, Euro hoặc Yên Nhật, token thanh toán như Bitcoin không phải là tiền tệ hợp pháp và không được chính phủ hỗ trợ. Thay vào đó, mục tiêu chính của chúng là trở thành một công cụ phi tập trung để mua và bán hàng hóa và dịch vụ mà không cần trung gian truyền thống và không có chức năng nào khác (hoặc chỉ có chức năng hạn chế).

Ví dụ, trong một bài báo tham vấn được công bố vào tháng 1 năm 2019, FCA của Vương quốc Anh đã xác nhận rằng các token Thanh toán hoặc Trao đổi - như

FCA gọi chúng - "hiện nằm ngoài phạm vi quản lý. Điều này có nghĩa là việc chuyển nhượng, mua và bán các token này, bao gồm cả hoạt động thương mại của các sàn giao dịch tiền điện tử để lấy token trao đổi, là các hoạt động hiện không được FCA quản lý".

Cơ quan quản lý FINMA của Thụy Sĩ cũng không coi token thanh toán là chứng khoán nhưng nhấn mạnh rằng nếu chúng được phân loại là chứng khoán thông qua luật lệ hoặc văn bản pháp lý mới, FINMA sẽ sửa đổi hoạt động của mình.

Hơn nữa, điều đáng chú ý là với bản sửa đổi sắp tới của chỉ thị về rửa tiền của EU ("AMLD 5") cần được thực hiện tại mỗi quốc gia thành viên trước ngày 10 tháng 1 năm 2020, các quy tắc AML chặt chẽ hơn sẽ được áp dụng cho các thực thể thực hiện các hoạt động như trao đổi giữa tài sản tiền mã hóa và tiền pháp định, giữa một hoặc nhiều hình thức tài sản tiền mã hóa khác, chuyển giao tài sản tiền mã hóa, lưu giữ hoặc quản lý tài sản tiền mã hóa hoặc các công cụ cho phép kiểm soát tài sản tiền mã hóa, tham gia và cung cấp các dịch vụ tài chính liên quan đến ưu đãi của bên phát hành hoặc bán tài sản tiền mã hóa.

Stablecoin (Token ổn định giá):

Stablecoin giá trị gắn liền với một tài sản ổn định như tiền pháp định (USD, EUR) hoặc vàng; Ví dụ: Tether (USDT), USD Coin (USDC).

Stablecoin là một loại tiền điện tử tìm cách duy trì giá trị ổn định bằng cách gắn giá trị thị trường của chúng với một tham chiếu bên ngoài. Tham chiếu này có thể là một loại tiền tệ fiat như đô la Mỹ, một loại hàng hóa như vàng hoặc một công cụ tài chính khác. Mục tiêu chính của stablecoin là cung cấp một giải pháp thay thế cho tính biến động cao của các loại tiền điện tử phổ biến như Bitcoin (BTC), điều này có thể khiến các tài sản kỹ thuật số này ít phù hợp hơn cho các giao dịch thông thường.

Stablecoin đóng vai trò quan trọng trong hệ sinh thái tiền điện tử do tính ổn định của chúng. Các loại tiền điện tử như Bitcoin và Ether mang lại nhiều lợi ích, chẳng hạn như không cần tin tưởng vào một tổ chức trung gian để gửi thanh toán đến bất kỳ đâu và cho bất kỳ ai. Tuy nhiên, giá của chúng không thể đoán trước và có thể dao động mạnh, khiến chúng trở nên khó sử dụng hàng ngày. Stablecoin hướng đến mục tiêu giải quyết những biến động giá này bằng cách gắn giá trị của tiền điện tử với các tài sản ổn định hơn, thường là tiền pháp định. Tính ổn định này nhằm mục đích duy trì giá trị của chúng theo thời gian và khuyến khích việc áp dụng chúng trong các giao dịch thường xuyên.

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

Inflationary Token (Token lạm phát):

Lạm phát token (Token Inflation) là sự gia tăng số lượng token lưu thông theo thời gian. Khi lạm phát token xảy ra, giá trị của từng token sẽ giảm và giá trị tài sản của các nhà đầu tư cũng sẽ bị ảnh hưởng nếu như cung vượt quá cầu.

Một số yếu tố có thể dẫn đến lạm phát token:

- Gia tăng số lượng token trong lưu thông do các hoạt động unlock mở khoá token theo lộ trình roadmap.
- Dự án bị tấn công, hacker tạo ra nhiều token để đưa vào lưu thông.
- Các hoạt động của dự án khuyến khích user khoá (lock), staking giúp giảm 1 lượng token lưu thông tạm thời. Nếu các chính sách này kém hấp dẫn, lượng token mới đưa vào lưu thông lớn hơn lượng token được khoá, cũng dẫn tới lạm phát.

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

Deflationary Token (Token giảm phát):

Token giảm phát là sự gia tăng giá trị nội tại của một loại tiền điện tử theo thời gian khi nguồn cung giảm hoặc không đổi.

Token giảm phát có cách tiếp cận khác, vì chúng được thiết kế để giảm nguồn cung token. Dù nhu cầu ổn định, việc giảm số lượng coin mới ít nhất cũng sẽ duy trì được giá trị của chúng.

Thiết kế của một loại tiền mã hóa giảm phát nhằm đạt được sự khan hiếm token bằng cách giảm nguồn cung và tăng giá trị của token theo thời gian. Quá trình này hy vọng sẽ dần dần giảm số lượng token và duy trì tính hữu dụng thực tế mà không làm xáo trộn cân bằng hoặc gây ra sự biến động thị trường.

Các token giảm phát, không giống như các loại token lạm phát, không có tỷ lệ giảm phát cố định trong giao thức của chúng. Thay vào đó, giao thức quy định các điều kiện để loại bỏ token khỏi lưu thông, thường thông qua quy trình đốt token. Cơ chế này làm giảm nguồn cung theo thời gian, nhưng tốc độ giảm không được ấn định cho một khoảng thời gian cụ thể mà thay đổi tùy theo hoạt động của mạng lưới. Ví dụ, một token có tỷ lệ giảm phát 2% sẽ giảm tổng nguồn cung token của nó xuống 2% mỗi năm. Một token giảm phát có thể có giới hạn nguồn cung cố định hoặc biến đổi, giới hạn số lượng token được phát hành.

Những người tạo ra các token giảm phát có thể sử dụng các cơ chế trực tiếp hoặc gián tiếp để tiêu hủy các đồng tiền đang lưu thông. Một cách phổ biến để giảm nguồn cung là sử dụng cơ chế đốt token, một quy trình loại bỏ vĩnh viễn một phần token khỏi lưu thông. Ngoài ra, họ cũng có thể đốt một số token dưới dạng phí gas cho các giao dịch trên blockchain.

Một ví dụ về tiền mã hóa giảm phát là Binance Coin (BNB). Mỗi quý, Binance tổ chức sự kiện đốt coin để loại bỏ lượng BNB dư thừa. Ngoài ra, Binance còn đốt một phần BNB dưới dạng phí giao dịch. Binance cam kết sẽ đốt 50% tổng nguồn cung của BNB.

Fixed Supply Token (Token có cung cố định):

Một số loại tiền điện tử, như Bitcoin, tuân theo mô hình cung cấp token cố định. Điều này có nghĩa là tổng số token sẽ tồn tại được xác định trước và không thể thay đổi. Ví dụ, Bitcoin có nguồn cung cố định là 21 triệu coin và khi tất cả chúng được khai thác, sẽ không có Bitcoin mới nào được tạo ra. Nguồn cung token cố định tạo ra sự khan hiếm, vì số lượng token có sẵn bị hạn chế, dẫn đến giá trị tiềm năng tăng theo thời gian khi nhu cầu tăng lên.

Sự khan hiếm này thường được coi là một trong những lý do đằng sau giá trị của Bitcoin, vì nó phản ánh các đặc tính của kim loại quý như vàng, vốn cũng có nguồn cung hạn chế. Các nhà đầu tư và những người đam mê tin rằng sự khan hiếm này góp phần vào tiềm năng của Bitcoin như một kho lưu trữ giá trị và một hàng rào chống lại lạm phát trong các loại tiền tệ fiat truyền thống.

c) Phân loại theo phương thức phát hành

Pre-Mined Token:

Toàn bộ token được phát hành trước khi dự án khởi chạy; ví dụ Ripple (XRP), ADA,...

Trong khi Bitcoin giải phóng tiền mới vào lưu thông thông qua khai thác, một số loại tiền điện tử, chẳng hạn như Ripple, Cardano và Stellar, được "đào trước", nghĩa là một phần tiền đã được khai thác và phân phối trước ngày ra mắt chính thức của dự án.

Khi một loại tiền mã hóa được phát hành trước, điều đó chỉ có nghĩa là một phần tiền xu hoặc token của loại tiền tệ đó đã được tạo ra - và trong một số trường hợp, được phân phối - trước khi ra mắt chính thức loại tiền mã hóa đó. Trái ngược với Bitcoin, phát hành tiền xu mới khi khai thác diễn ra, một số dự án tiền mã hóa được tạo trước các đơn vị tiền tệ của họ trước khi ra mắt chính thức.

Đối với các loại tiền mã hóa được khai thác trước (pre-mined), một phần nguồn cung coin được tạo ra ngay khi ra mắt trong khối đầu tiên của giao thức và được phân phối cho các nhà đầu tư ICO, nhà phát triển và thành viên nhóm. Chẳng hạn, Ripple (XRP) được tạo ra như một loại tiền mã hóa cho hệ thống thanh toán tập trung, cho phép chuyển tiền nhanh chóng và tiết kiệm chi phí khi hợp tác với các ngân hàng. Tuy nhiên, phần lớn lượng tiền XRP vẫn do Ripple nắm giữ và công ty này kiểm soát tập trung việc phát hành đồng tiền. Không giống như các loại tiền mã hóa có thể khai thác được như Bitcoin hay Litecoin, các đồng coin hoặc token được khai thác trước thường được phát hành bởi một tổ chức tập trung.

Trước khi chuyển sang Proof-of-Stake (PoS), Ethereum vừa là một token được khai thác trước, vừa được khai thác trong cùng một thời gian. Ether đầu tiên được cung cấp như một phần thưởng khai thác trước cho những người đã tài trợ cho dự án Ethereum trong đợt chào bán coin lần đầu (ICO) vào tháng 7 và tháng 8 năm 2014.

Ưu và nhược điểm của tiền mã hóa được phát hành trước (pre-mining):

Ở thời điểm hiện tại, việc phát hành trước (pre-mining) nhìn chung đã được cộng đồng tiền mã hóa chấp nhận rộng rãi, bởi nhiều đồng tiền và token được phân phối theo cách này thông qua các đợt ICO và các hình thức chào bán token khác.

Một số người cho rằng việc khai thác trước các loại tiền mã hóa là hợp lý để thưởng cho các nhà phát triển đã tham gia vào quá trình tạo ra nó và thực hiện các công việc cần thiết để mang lại động lực ban đầu cho đồng tiền mã hóa. Các đồng tiền được khai thác trước và phân phối cho các thành viên trong nhóm phát triển có thể đóng vai trò như một phần thưởng khuyến khích dành cho nhân viên và những người dùng đầu tiên.

Phát hành trước (pre-mine) cũng là một bằng chứng cho các nhà đầu tư rằng đồng tiền hoặc token đã được tạo ra thực sự hoạt động. Một đồng tiền được phát hành trước có thể được sử dụng như một nguyên mẫu để trình bày cho các bên quan tâm.

Mặt khác, các nhà phê bình cho rằng việc phát hành trước (pre-mining) chủ yếu phục vụ các startup ICO để thực hiện hành vi "bơm và xả" (pump and dump) đồng tiền mã hóa của họ. "Bơm và xả" là một hình thức gian lận đầu tư, trong đó giá trị của một tài sản được mua ở mức giá thấp bị thổi phồng một cách giả tạo để bán ra ở mức giá cao hơn.

Minted Token:

Token được phát hành dần dần trong quá trình vận hành của mạng lưới. Ví dụ: Bitcoint (BTC) thông qua cơ chế Proof-of-Work, Ethereum (ETH) thông qua cơ chế Proof-of-Stake.

Minting là quá trình phát hành các tài sản số mới trong hệ sinh thái tiền mã hóa. Phương pháp này đưa các đồng tiền hoặc token mới vào lưu thông, cho phép chúng được giao dịch hoặc sử dụng trong hệ sinh thái. Theo nhiều cách, minting tương tự như mining. Tuy nhiên, có một vài điểm khác biệt quan trọng.

Các hệ thống Proof of Stake (PoS) sử dụng phương pháp minting (đúc) để đưa các đồng tiền mới vào lưu thông. Hệ thống này dựa vào validators (người xác thực) hoặc stakers (người đặt cọc) để xác minh giao dịch và thêm các khối mới vào blockchain.

Mặt khác, mining (khai thác) gắn liền với cơ chế Proof of Work (PoW). Trong các hệ thống này, miners (thợ đào) sử dụng phần cứng chuyên dụng để giải quyết các bài toán mật mã phức tạp nhằm tạo ra các khối mới trên blockchain.

Trong khi mining (khai thác) là một quá trình tiêu tốn năng lượng lớn, minting lại thân thiện với môi trường hơn rất nhiều. Không giống như việc minting chỉ diễn ra một lần khi tạo ra token mới, mining là một hoạt động liên tục. Nó duy trì trong suốt thời gian mạng blockchain hoạt động, liên tục xác minh giao dịch và củng cố tính bảo mật của mạng lưới.

Ngoài các đơn vị tiền mã hóa thông thường, minting (đúc) cũng là một quá trình không thể thiếu để tạo ra Non-Fungible Tokens (NFTs). Thông thường, quá trình đúc một NFT bao gồm các bước sau:

Bước 1: Tạo hoặc chọn tài sản kỹ thuật số

Tài sản này có thể là hình ảnh, video, âm nhạc, hoặc bất kỳ loại tệp kỹ thuật số nào mà người tạo muốn biến thành NFT.

Bước 2: Chọn nền tảng và blockchain

Người tạo chọn nền tảng minting NFT (ví dụ: OpenSea, Rarible, Mintable) và blockchain mà NFT sẽ tồn tại (ví dụ: Ethereum, Binance Smart Chain, Solana).

Bước 3: Tạo hợp đồng thông minh (Smart Contract)

Hợp đồng thông minh sẽ xác định các thông số của NFT, bao gồm quyền sở hữu, chuyển nhượng và các điều kiện khác.

Bước 4: Đúc NFT

Quá trình minting bắt đầu khi tài sản được tải lên nền tảng và hợp đồng thông minh được kích hoạt. Điều này tạo ra một token duy nhất trên blockchain, xác nhận quyền sở hữu và tính độc nhất của tài sản.

Bước 5: Thanh toán phí gas (nếu có)

Phí gas là chi phí thanh toán cho các giao dịch trên blockchain, và trong trường hợp của Ethereum, phí này có thể khá cao. Người tạo phải thanh toán phí gas để hoàn tất quá trình minting.

Bước 6: Bán hoặc chuyển nhượng NFT

Sau khi NFT được đúc, người tạo có thể bán nó trên các thị trường NFT hoặc chuyển nhượng cho người khác.

Airdrop Token:

Phát hành miễn phí cho người dùng nhằm khuyến khích tham gia hoặc quảng bá dự án.

Airdrop tiền điện tử là việc một dự án phân phối các token hoặc coin mới cho nhiều cá nhân trong cộng đồng tiền điện tử.

Các nhóm đứng sau những dự án này thường sử dụng airdrop để nâng cao nhận thức về dự án của họ và khuyến khích mọi người trở thành người dùng hoặc nhà đầu tư. Các tài sản được airdrop được tặng miễn phí, nhưng một số airdrop yêu cầu người dùng hoàn thành các nhiệm vụ cụ thể trước khi họ có thể yêu cầu token của mình. Các airdrop tiền điện tử trở nên phổ biến trong thời kỳ bùng nổ của đợt chào bán tiền xu ban đầu (ICO) năm 2017, nhưng vẫn được nhiều dự án tiền điện tử sử dụng cho đến ngày nay.

Khi một dự án thông báo về airdrop, dự án đó thường cũng đặt ra các tiêu chí hoặc yêu cầu cụ thể mà người tham gia phải đáp ứng để đủ điều kiện. Các yêu cầu này có thể bao gồm tham gia một nhóm Telegram cụ thể, theo dõi dự án trên phương tiện truyền thông xã hội, đăng ký nhận bản tin hoặc nắm giữ một số lượng tối thiểu của một loại tiền cụ thể trong ví. Các airdrop cũng chỉ có thể được trao cho các ví đã tương tác với nền tảng của dự án trước một ngày đã định.

Tuy nhiên, các tiêu chí này không phải lúc nào cũng được công bố trước. Một số đợt airdrop nổi tiếng đã khiến người dùng tích cực của nền tảng ngạc nhiên khi airdrop token mới trước khi tiết lộ tiêu chí airdrop. Không có quy tắc nào cho airdrop và mỗi dự án có thể có phương pháp và kế hoạch riêng.

"Tại sao các dự án tiền điện tử lại thực hiện Airdrop?"

Các dự án tiền điện tử thường sử dụng airdrop như một phần trong chiến lược ra mắt token của họ nhằm nâng cao nhận thức trong cộng đồng tiền điện tử và khuyến khích người nhận sử dụng token của họ. Airdrop cũng có thể được sử dụng để phân phối token cho người dùng hoặc nhà đầu tư tiềm năng một cách công bằng bằng cách đảm bảo rằng nguồn cung ban đầu được phân bổ cho nhiều người, thay vì tập trung vào tay một số ít nhà đầu tư ban đầu. Mô hình phân phối này có thể góp phần tạo nên một hệ sinh thái cân bằng và phi tập trung hơn.

Airdrop cũng được khởi xướng như một phần của chiến lược tiếp thị của dự án để tạo tiếng vang và thu hút sự chú ý đến dự án. Người nhận có thể tò mò về dự án và khám phá thêm hoặc thảo luận về dự án trên phương tiện truyền thông xã hội. Sự tiếp xúc gia tăng này có thể dẫn đến một nhóm người dùng, nhà đầu tư và quan hệ đối tác tiềm năng lớn hơn.

Airdrop cũng có thể cải thiện việc người dùng chấp nhận vì các token miễn phí khuyến khích mọi người trải nghiệm trực tiếp lợi ích của tiền điện tử của họ. Điều này có thể khuyến khích người dùng tham gia vào dự án và cung cấp phản hồi có giá trị. Điều này có thể giúp cải thiện nền tảng theo thời gian.

d) Phân loại theo giá trị kinh tế

Asset-Backed Token (Token được đảm bảo tài sản):

Asset-backed tokens (Token được đảm bảo bởi tài sản) là các yêu cầu số hóa đối với một tài sản vật lý và được đảm bảo bởi tài sản đó. Vàng, dầu thô, bất động sản, cổ phiếu, đậu nành hoặc hầu hết bất kỳ tài sản vật lý thực tế nào khác đều có thể được mã hóa và trở thành token hỗ trợ bởi tài sản.

Asset-backed tokens là một sự tiến hóa được tạo ra nhờ vào công nghệ blockchain. Bitcoin, tất nhiên, là token đầu tiên, nhưng đồng tiền mã hóa này không được đảm bảo bởi bất kỳ tài sản vật lý nào. Kể từ khi có Bitcoin, nhiều thứ đã thay đổi và hiện nay có hàng nghìn loại tiền mã hóa khác nhau, từ những đồng tiền kỹ thuật số mới đến stablecoin gắn với tiền pháp định. Tuy nhiên, cuộc cách mạng tiền mã hóa và sự biến động của nó đã thúc đẩy các sáng tạo ra các tài sản token hóa ổn định hơn, được thiết kế để lưu trữ giá trị và có thể trao đổi giữa các bên mà không cần sự trung gian của tổ chức tài chính.

Phiên bản tiếp theo của các đổi mới trong lĩnh vực tiền mã hóa mang giao diện này vào lĩnh vực thực tế và vật lý, với các asset-backed tokens (Token được đảm bảo bởi tài sản) đại diện cho các tài sản trong thế giới thực. Giá trị của một token hỗ trợ bởi tài sản bị ảnh hưởng trực tiếp bởi giá trị của tài sản cơ sở của nó, và thường được phân loại là một chứng khoán theo các cơ quan quản lý tài chính.

Quyền sở hữu token thường đại diện cho quyền sở hữu đối với tài sản và tùy thuộc vào tài sản, có thể đi kèm với kỳ vọng về lợi nhuận trong tương lai khi tài sản tăng giá trị. Khi bản thân tài sản tăng giá trị, token cũng vậy.

Sự phát triển của các mã thông báo này cũng có nghĩa là một cá nhân, công ty hoặc tổ chức khác có thể tìm kiếm khoản đầu tư để đổi lấy mã thông báo và huy động vốn thông qua hệ thống dựa trên blockchain, được thực hiện bằng cách phát hành mã thông báo được hỗ trợ bằng tài sản dưới dạng công cụ vốn chủ sở hữu mới, theo các quy định tài chính.

Ngoài ra, các doanh nghiệp có thể token hóa tài sản hiện có để bán. Các nhà đầu tư cá nhân, không chỉ những người giàu có, giờ đây có thể mua vào tài sản kinh doanh thực tế mà không cần lưu trữ hoặc trao đổi chúng. Điều này không chỉ làm giảm ma sát thương mại mà còn giảm chi phí hậu cần. Thông qua các token được hỗ trợ bằng tài sản, các giao dịch có thể diễn ra nhanh hơn và hiệu quả hơn.

Token được hỗ trợ bằng tài sản cũng có thể giải quyết các vấn đề do tiền tệ bị thổi phồng hoặc mất giá, cũng như thị trường chứng khoán không thể đoán trước, mang đến cho cá nhân một giải pháp thay thế tài chính mới hợp lý kết hợp thanh khoản kỹ thuật số với giá trị tài sản cứng khi cần. Chúng tôi đã quan sát thấy tiềm năng của token được hỗ trợ bằng tài sản khi chúng thu hút được nhiều ứng dụng hơn.

Các chính phủ đang gắn giá dầu thô với giá trị của các token kỹ thuật số chính thức và thị trường bất động sản đang dần chuyển sang quyền sở hữu phân đoạn được token hóa. Các token được hỗ trợ bằng tài sản đang cải thiện tính thanh khoản cho các thị trường trước đây không thanh khoản và cho phép các giao dịch hiệu quả về mặt chi phí mà không phụ thuộc vào một bên trung tâm, đồng thời thúc đẩy cả tính bảo mật và tính minh bạch. Điều này đang có tác động lớn đến cách chúng ta kinh doanh và suy nghĩ về quyền sở hữu và tạo ra của cải trong tương lai. (tác giả: *Johannes Schweifer)*

Non-Asset-Backed Token (Token không đảm bảo tài sản):

Giá trị dựa vào cung và cầu, không gắn liền với tài sản thực tế. Ví dụ: Dogecoin (DOGE).

Non-Asset-Backed Token (Token không hỗ trợ bởi tài sản) là những loại token không có sự đảm bảo hoặc giá trị từ một tài sản vật lý cụ thể nào. Giá trị của chúng chủ yếu phụ thuộc vào yếu tố thị trường, sự chấp nhận của cộng đồng hoặc các yếu tố kỹ thuật, thay vì được bảo đảm bởi tài sản như vàng, bất động sản hay cổ phiếu.

Ví dụ về Non-Asset-Backed Token:

- Bitcoin (BTC): Là một loại tiền mã hóa không hỗ trợ bởi bất kỳ tài sản vật lý nào. Giá trị của Bitcoin phụ thuộc vào cung cầu và sự tin tưởng của cộng đồng người dùng.

- Ethereum (ETH): Cũng không phải là token hỗ trợ bởi tài sản, mà có giá trị nhờ vào việc sử dụng của nó trong các ứng dụng phân tán (dApps) và hợp đồng thông minh.

- Cardano (ADA): ADA là đồng tiền mã hóa gốc của blockchain cardano. ADA không gắn với một tài sản vật lý hoặc tài chính như Stablecoin (USDT hay USDC); giá trị của ADA đến từ:

+ *Việc sử dụng của blockchain Cardano*: Blockchain này hỗ trợ hợp đồng thông minh, ứng dụng phi tập trung (DApp), và nhiều dự án khác.

+ *Niềm tin cộng đồng*: Cardano được xem là một blockchain thế hệ mới với công nghệ dựa trên bằng chứng cổ phần (Proof of Stake - PoS), giúp tiết kiệm năng lượng và cải thiện khả năng mở rộng.

+ *Các tính năng kỹ thuật*: Cardano chú trọng vào nghiên cứu học thuật và xây dựng các giao thức blockchain bền vững.

Giá trị của ADA từng dao động mạnh, phụ thuộc vào sự phát triển của dự án và điều kiện thị trường; Ví dụ: Trong đợt bull run năm 2021, ADA tăng giá đáng kể nhờ các bản cập nhật quan trọng như Alonzo Hard Fork, cho phép chạy hợp đồng thông minh trên Cardano.

Đặc điểm của Non-Asset-Backed Tokens:

- Không có tài sản vật lý bảo chứng: Chúng không đại diện cho tài sản thực tế nào mà có giá trị dựa vào sự chấp nhận và nhu cầu từ thị trường.

- Biến động giá cao: Vì không có tài sản cơ sở để bảo vệ giá trị, những token này có thể trải qua sự biến động giá lớn.

- Tính thanh khoản: Các token này có thể dễ dàng mua bán trên các sàn giao dịch tiền mã hóa.

Tóm lại, Non-Asset-Backed Tokens là các loại tiền mã hóa không có tài sản bảo chứng, mà có giá trị chủ yếu dựa vào sự sử dụng, nhu cầu thị trường và các yếu tố kỹ thuật.

2.4.2.3. Các yếu tố chính của một tokenomics

"Tokenomics" là một từ ghép của "token" (đồng token) và "economics" (kinh tế), được sử dụng để mô tả cấu trúc kinh tế xung quanh một đồng token trong một hệ thống blockchain hoặc mạng blockchain. Điều này bao gồm các yếu tố như cung và cầu, giá trị, phân phối, và cách mà token được sử dụng trong hệ thống.

a) Coin/token supply

- Tổng cung (Total supply): tổng số lượng coin/ token đang lưu thông trên thị trường cùng số lượng đang bị khóa trừ đi số lượng đã burn. Một số loại total supply: tổng cung cố định, tổng cung không cố định (tổng cung tăng dần, tổng cung giảm dần, tổng cung thay đổi liên tục).

- Cung lưu thông(Circulating supply): số lượng coin/ token đang được lưu thông trên thị trường.

- Cung tối đa (Max supply): số lượng coin/ token tối đa có thể tồn tại, bao gồm cả những token đã được khai thác hoặc sẵn có trong tương lai.

b) Token governance (Token quản trị)

Chủ yếu được chia thành 3 nhóm chính

- Decentralized (Token phi tập trung): coin/token được quản trị bởi toàn bộ quyết định của cộng đồng quyết định và không chịu bất kỳ sự can thiệp nào bởi bên thứ ba. Ví dụ như Bitcoin, Ethereum, Cardano…

- Centralized (Token Tập trung): coin/token được quản trị bởi một tổ chức đứng đầu quyết định, họ có quyền ảnh hưởng lên tính chất của coin/ token hay cả dự án mà token đó đại diện. Ví dụ như Tether, True USD, Ripple,…

- Từ centralized đến decentralized: coin/ token được xây dựng bởi một tổ chức nhưng sau đó sẽ phân quyền dần về cho cộng đồng, chuyển đổi từ tập trung sang phi tập trung. Ví dụ: Binance Coin lúc đầu hoàn toàn được quản trị bởi Binance. Thế nhưng, sau khi ra mắt Binance Smart Chain (BSC), Binance đã dần dần phân quyền BSC và BNB token cho cộng đồng kiểm soát.

c) Token allocation (Phân bổ token)

Phân bổ token là quá trình xác định cách thức phân phối và sử dụng tổng số token được phát hành trong một dự án blockchain. Đây là yếu tố quan trọng trong **tokenomics**, ảnh hưởng trực tiếp đến giá trị, tính bền vững, và niềm tin của cộng đồng đối với dự án.

**) Team (Đội ngũ phát triển):*

Số token này sẽ được phân cho đội ngũ phát triển của dự án bao gồm founder, co-founder, developer, marketer, advisor,…(những người đã có đóng góp quan trọng).

- **Tỷ lệ thường thấy**: 10% - 20%.

- **Mục đích**: Thưởng cho đội ngũ sáng lập và phát triển dự án.

- **Thời gian khóa (Vesting Period)**: Thường khóa từ 1-4 năm để tránh việc bán tháo token làm giảm giá trị.

- **Ví dụ**: Ethereum khóa token cho đội ngũ phát triển trong thời gian dài để đảm bảo cam kết lâu dài. ADA token allocation có tổng cung cố định là 45 tỷ và đội ngũ phát triển đã phân bổ nó thành ba phần với tỷ lệ như sau: 25,927,070,538 ADA (khoảng 57,6%) đã được bán ra thị trường qua ICO; 13,887,515,354 ADA (khoảng 30,9%) được dành cho các phần thưởng staking.

**) Liquidity mining (thanh khoản):*

Yếu tố này xuất hiện nhiều hơn vào thời gian gần đây, đặc biệt là sau giai đoạn tháng 9 năm 2020 khi các dự án DeFi bắt đầu phát triển mạnh mẽ. Đây là khoản token được trích ra như phần thưởng cho những nhà đầu tư tích cực cung cấp thanh khoản.

Người dùng gửi tài sản kỹ thuật số (crypto) vào các Liquidity Pool trên các giao thức DeFi. Các Liquidity Pool này thường được sử dụng trên các nền tảng DEX

như Uniswap, PancakeSwap, hoặc trên các blockchain như Cardano, Ethereum, hoặc Binance Smart Chain. Đổi lại, người dùng nhận được phần thưởng bằng các token gốc của nền tảng hoặc token khác (như ADA, ETH, hoặc token quản trị).

- Cách thức hoạt động:

+ Cung cấp thanh khoản: Người dùng gửi cặp token (ví dụ: ADA/USDT) vào một Liquidity Pool trên DEX.

+ Phí giao dịch: Các nhà cung cấp thanh khoản (Liquidity Providers - LPs) nhận phần trăm phí từ các giao dịch diễn ra trong pool.

+ Phần thưởng bổ sung: Ngoài phí giao dịch, họ thường nhận được phần thưởng dưới dạng token gốc của giao thức. Đây chính là cơ chế Liquidity Mining.

- Liquidity Mining trên các blockchain lớn:

+ Ethereum: Với các nền tảng nổi tiếng như Uniswap, Sushiswap, Curve.

+ Binance Smart Chain (BSC): PancakeSwap là một trong những nền tảng lớn nhất.

+ Cardano: Các nền tảng như Minswap, SundaeSwap.

+ Avalanche, Solana: Hỗ trợ các giao thức DeFi tập trung vào hiệu suất cao.

- Ví dụ về Liquidity Mining:

Giả sử bạn tham gia cung cấp thanh khoản cho một pool ADA/USDT trên Cardano:

+ Bạn gửi 1,000 ADA và số USDT tương đương vào pool.

+ Trong 30 ngày, bạn nhận được:

- Phí giao dịch**:** 0.3% từ khối lượng giao dịch.
- Token thưởng**:** 50 token quản trị từ giao thức.

+ Tổng lợi nhuận = Phí giao dịch + Giá trị token phần thưởng (đã tính giá thị trường).

**) Private/ Public sale (các hình thức bán token):*

Đây là thông số token dành cho các đợt mở bán để huy động vốn phát triển sản phẩm. Thông thường, một dự án sẽ có khoảng ba đợt mở bán là Seed sale, Private sale và Public sale.

- Seed Sale: là một giai đoạn đầu tiên trong quy trình huy động vốn của một dự án blockchain hoặc tiền mã hóa. Đây là hình thức bán token trước cả Private Sale và Public Sale, nhằm huy động vốn ban đầu để phát triển dự án.

+ Mục tiêu:

Huy động vốn ở giai đoạn rất sớm của dự án; Tài trợ cho các hoạt động nghiên cứu, phát triển sản phẩm, và xây dựng nền tảng cơ bản của dự án.

+ Đối tượng tham gia:

Các nhà đầu tư thiên thần (angel investors); Các quỹ đầu tư mạo hiểm (venture capital); Các đối tác chiến lược; Một số ít cá nhân có quan hệ gần gũi với đội ngũ phát triển.

+ Giá token:

Thường rất thấp, rẻ nhất trong các vòng huy động vốn; Thể hiện mức độ rủi ro cao nhất, nhưng cũng mang lại tiềm năng lợi nhuận lớn nếu dự án thành công.

+ Số lượng token bán ra:

Rất giới hạn, thường chiếm khoảng 5–10% tổng cung.

+ Điều khoản:

Thường đi kèm với các điều kiện khóa token (vesting period), nhằm tránh việc bán tháo sau khi dự án niêm yết token; Ví dụ: Token được phát hành dần trong 12–24 tháng.

- Private sale: là một giai đoạn huy động vốn của các dự án blockchain và tiền mã hóa, diễn ra trước giai đoạn Public Sale (Bán công khai). Đây là một trong những hình thức bán token phổ biến để tài trợ cho các hoạt động phát triển dự án.

+ Đối tượng tham gia:

Nhà đầu tư lớn (high-net-worth individuals), quỹ đầu tư mạo hiểm (VCs), hoặc đối tác chiến lược; Thường yêu cầu mức đầu tư tối thiểu cao và hạn chế số lượng người tham gia.

+ Mục tiêu:

Gọi vốn ở quy mô lớn hơn Seed Sale, giúp dự án mở rộng quy mô và chuẩn bị cho các giai đoạn tiếp theo như Public Sale hoặc niêm yết token trên sàn giao dịch.

+ Mức giá token:

Thường thấp hơn Public Sale, nhưng cao hơn Seed Sale; Giá ưu đãi nhằm thu hút các nhà đầu tư chiến lược.

+ Điều kiện:

Thường có các điều khoản khóa token (vesting period) để đảm bảo nhà đầu tư không bán tháo ngay sau khi token được niêm yết. Ví dụ: 20% token được mở khóa ngay khi niêm yết, phần còn lại mở dần trong 12–24 tháng.

+ Phân phối token:

Token bán trong Private Sale chiếm khoảng 10–20% tổng cung, tùy thuộc vào chiến lược của dự án.

- Public sale: Là giai đoạn bán token cuối cùng trong quá trình huy động vốn của một dự án blockchain. Đây là bước mở bán token cho công chúng, nơi bất kỳ nhà đầu tư nào cũng có thể tham gia (tuỳ thuộc vào quy định pháp lý và điều kiện của dự án). Giai đoạn này thường được thực hiện sau **Seed Sale** và **Private Sale**.

+ Đối tượng tham gia:

Mở cho công chúng, không giới hạn bởi mối quan hệ chiến lược hay mức đầu tư lớn; Phù hợp với nhà đầu tư nhỏ lẻ hoặc người mới tham gia vào thị trường tiền mã hóa.

+ Mục tiêu:

Huy động vốn mở rộng để hoàn thiện sản phẩm hoặc ra mắt chính thức; Tăng mức độ nhận diện dự án trong cộng đồng; Phân phối token một cách công bằng hơn so với các giai đoạn trước.s

+ Giá token:

Thường cao hơn giá của Seed Sale và Private Sale nhưng thấp hơn giá niêm yết trên sàn giao dịch; Phản ánh mức độ trưởng thành của dự án.

+ Phân phối token:

Phần lớn token dành cho cộng đồng, thường chiếm 20–30% tổng cung.

+ Hình thức:

Có thể diễn ra thông qua ICO (Initial Coin Offering), IEO (Initial Exchange Offering) , hoặc IDO(Initial DEX Offering) trên các nền tảng giao dịch tập trung hoặc phi tập trung.

**) Airdrop (tặng quà):*

Đây là hình thức phân phối miễn phí token hoặc tiền mã hóa đến các ví của người dùng nhằm tăng sự nhận diện, thu hút cộng đồng, hoặc khuyến khích sử dụng dự án blockchain. Đây là một chiến lược marketing phổ biến trong lĩnh vực tiền mã hóa.

- Mục tiêu của Airdrop:

+ Tăng nhận diện dự án: Giới thiệu token đến một lượng lớn người dùng, giúp dự án được biết đến nhiều hơn.

+ Xây dựng cộng đồng: Thu hút những người dùng mới tham gia vào hệ sinh thái dự án.

+ Thúc đẩy sử dụng: Khuyến khích người dùng trải nghiệm sản phẩm hoặc dịch vụ của dự án.

+ Phân phối token: Đảm bảo token được phân phối rộng rãi để tăng tính phi tập trung.

+ Tăng thanh khoản: Khi người dùng sở hữu token, họ có thể giao dịch, làm tăng thanh khoản trên thị trường.

- Các loại Airdrop phổ biến:

+ Standard Airdrop (Airdrop tiêu chuẩn): Người dùng nhận được token miễn phí chỉ cần thực hiện các bước đơn giản như đăng ký tài khoản, điền thông tin ví, hoặc theo dõi mạng xã hội.

+ Bounty Airdrop (Airdrop thưởng): Người dùng phải thực hiện các nhiệm vụ như chia sẻ bài viết, tham gia nhóm Telegram, đăng tweet, hoặc viết bài blog giới thiệu dự án; Thường áp dụng cho các chiến dịch marketing lớn.

+ Holder Airdrop (Airdrop cho người sở hữu) Phân phối token miễn phí cho những người đã nắm giữ một loại tiền mã hóa cụ thể (ví dụ: ETH, BTC); Thường dựa trên số dư ví của người dùng tại một thời điểm nhất định (snapshot).

+ Exclusive Airdrop (Airdrop độc quyền): Dành cho những người dùng đặc biệt như nhà đầu tư sớm, đối tác, hoặc người đóng góp lớn cho dự án.

+ Hard Fork Airdrop: Diễn ra khi một blockchain chia tách, và người dùng trên blockchain cũ nhận được token mới từ blockchain mới (ví dụ: Bitcoin Cash từ Bitcoin).

- Ví dụ thực tế về Airdrop

+ Stellar (XLM):

Stellar từng tổ chức một airdrop lớn, tặng miễn phí hàng triệu token XLM cho những người sở hữu Bitcoin.

+ Uniswap (UNI):

Phát hành token UNI miễn phí cho những người đã sử dụng sàn Uniswap trước một thời điểm cụ thể. Mỗi người nhận được ít nhất 400 UNI, trị giá hàng nghìn USD tại thời điểm đó.

+ ApeCoin (APE):

Người sở hữu NFT từ bộ sưu tập Bored Ape Yacht Club (BAYC) nhận được token APE miễn phí dựa trên số lượng NFT họ sở hữu.

- Cách Airdrop trên cardano blockchain

+ Token gốc của Cardano (Native Token):

Cardano hỗ trợ phát hành các token gốc (native token) mà không cần hợp đồng thông minh phức tạp; Điều này giúp việc phân phối airdrop trở nên nhanh chóng và tiết kiệm chi phí.

+ Ví Cardano:

Người dùng thường sử dụng các ví như Yoroi, Daedalus, hoặc Nami để nhận airdrop; Ví cần hỗ trợ token gốc và khả năng tương tác với mạng Cardano.

+ Snapshot và staking:

Một số dự án yêu cầu người dùng staking ADA (đặt cược vào pool) để đủ điều kiện nhận airdrop; Snapshot sẽ được thực hiện vào một thời điểm nhất định để xác định số dư hoặc hoạt động của ví.

+ Phí giao dịch thấp:

Nhờ cơ chế đồng thuận Proof-of-Stake (PoS) và khả năng tối ưu hóa chi phí, việc airdrop trên Cardano thường rẻ hơn so với Ethereum.

*) Foundation reserve (dự trữ của quỹ nền tảng):

Đây là phần tài sản hoặc token được dành riêng bởi các dự án blockchain để hỗ trợ các hoạt động dài hạn của tổ chức hoặc nền tảng đứng sau dự án. Đây là một chiến lược quan trọng nhằm đảm bảo sự bền vững và phát triển lâu dài của dự án, đặc biệt trong giai đoạn mở rộng hoặc đối mặt với các thách thức tài chính.

Ví dụ về Foundation Reserve trong các dự án nổi bật

- Cardano (ADA):

Cardano Foundation quản lý một phần lớn quỹ dự trữ để tài trợ cho nghiên cứu, phát triển hệ sinh thái, và mở rộng cộng đồng.

Quỹ này cũng được sử dụng để thúc đẩy các mối quan hệ hợp tác chiến lược.

- Ethereum (ETH):

Ethereum Foundation giữ một quỹ dự trữ để tài trợ cho các hoạt động nghiên cứu, phát triển mạng lưới, và cải tiến giao thức.

- Binance Smart Chain (BNB):

Binance Foundation sử dụng quỹ dự trữ để thúc đẩy sự phát triển của hệ sinh thái Binance, tài trợ các dự án DeFi, GameFi, và NFT.

- Polkadot (DOT):

Web3 Foundation quản lý quỹ dự trữ của Polkadot để hỗ trợ các dự án parachain, cộng đồng phát triển, và nghiên cứu dài hạn.

*) Token release (phát hành):

Đây là quá trình giải phóng token từ nguồn cung đã được phân bổ trước đó để đưa vào lưu thông trên thị trường hoặc đến tay người sở hữu. Đây là một bước quan trọng trong các dự án blockchain, giúp quản lý nguồn cung token một cách hợp lý, duy trì giá trị và đảm bảo tính minh bạch trong hoạt động của dự án.

Ví dụ về Token Release của các dự án nổi bật:

- Ethereum (ETH):

Ban đầu, Ethereum phát hành token ETH cho các nhà đầu tư tham gia ICO (Initial Coin Offering), với nguồn cung ban đầu là 72 triệu ETH. Phần còn lại được khai thác dần qua cơ chế PoW và sau này là PoS.

- Cardano (ADA):

Cardano sử dụng mô hình vesting cho đội ngũ sáng lập và quỹ phát triển, với phần lớn token được phân phối cho cộng đồng thông qua staking rewards.

- Polkadot (DOT):

DOT token được phát hành dần dần để hỗ trợ các parachain, khuyến khích staking và tài trợ các dự án phát triển trên nền tảng.

- Uniswap (UNI):

UNI token được phát hành theo lộ trình rõ ràng: 60% dành cho cộng đồng và được phân phối dần trong vòng 4 năm.

2.5. NFT

2.5.1. Khái niệm

NFT (Non-Fungible Token) là một loại tài sản kỹ thuật số được xây dựng trên công nghệ blockchain, đại diện cho quyền sở hữu hoặc quyền truy cập duy nhất vào một sản phẩm hoặc dịch vụ số cụ thể. Điểm đặc trưng của NFT là tính không thể thay thế (non-fungible), nghĩa là mỗi NFT là duy nhất và không thể thay thế bằng một NFT khác có giá trị tương đương, khác với các tài sản "có thể thay thế" như tiền điện tử (ví dụ: 1 Bitcoin có giá trị ngang bằng với 1 Bitcoin khác).

NFT (Non-Fungible Token) là một loại tài sản kỹ thuật số độc nhất, được sử dụng để tạo và xác thực quyền sở hữu đối với các tài sản số như hình ảnh, âm nhạc, video clip và bất động sản ảo. Mỗi NFT được đánh dấu bằng một mã nhận dạng duy nhất và được lưu trữ trên blockchain, đảm bảo tính xác thực và quyền sở hữu của tài sản.

Khác với các tài sản truyền thống như cổ phiếu hoặc tiền tệ, NFT không thể thay thế hoặc trao đổi ngang giá với một vật phẩm tương tự khác, do tính chất độc nhất của chúng. Điều này làm cho NFT tương tự như các vật phẩm sưu tầm quý hiếm trong thế giới thực. Sự quan tâm đến NFT đã tăng mạnh trong những năm gần đây, đặc biệt là vào năm 2021, khi giá trị của các tác phẩm nghệ thuật số và các tài sản số khác tăng cao.

Công nghệ blockchain đóng vai trò quan trọng trong việc xác lập quyền sở hữu của NFT. Blockchain hoạt động như một sổ cái phi tập trung, cho phép công khai xác thực các NFT. Công nghệ này sử dụng chữ ký số để chứng minh quyền sở hữu và tính nguyên bản của tác phẩm. Người mua NFT không sở hữu một tác phẩm vật lý để treo trên tường, mà thay vào đó là một hình ảnh số của tác phẩm đó cùng với chứng chỉ xác thực số.

Những đặc tính độc đáo của NFT khiến chúng không thể thay thế. Điều này trái ngược với các tài sản có thể thay thế, chẳng hạn như Bitcoin và các loại tiền điện tử khác, tờ đô la, thỏi vàng và cổ phiếu, có giá trị một số tiền cụ thể và có thể hoán đổi cho nhau. Mặc dù một tờ đô la có thể được đổi lấy một tờ đô la khác hoặc một bitcoin có thể dễ dàng được hoán đổi cho một tờ khác, nhưng điều đó không đúng với NFT.

NFT thường không thể chia nhỏ. Đơn vị cơ bản của NFT là token, thường không thể chia thành các mệnh giá nhỏ hơn, vì một đô la có thể được chia thành 10 xu. Tuy nhiên, quyền sở hữu một phần của NFT đã được một số nền tảng giới thiệu gần đây, chẳng hạn như Fractional. Quyền sở hữu một phần cho phép NFT được chia thành các NFT nhỏ hơn, có thể bán cho nhiều người mua.

Ngoài ra, NFT không thể thay đổi. Chúng không thể bị thay đổi sau khi được mã hóa bằng công nghệ blockchain . Tính nguyên bản và tính hợp pháp của mặt hàng được xác thực thông qua blockchain nơi nó được lưu trữ.

Tại sao NFT lại quan trọng?

Justin Herzig, đồng sáng lập của Own the Moment NFT , một công ty cung cấp nội dung, công cụ và phân tích về NFT, giải thích rằng sự gia tăng mức độ phổ biến của NFT là kết quả của "tính dễ sử dụng, bản chất đầu cơ như một vật phẩm sưu tầm và đầu tư, cùng cộng đồng cơ sở phát triển xung quanh các sản phẩm".

NFT cho phép cá nhân mua và bán tài sản kỹ thuật số theo những cách mới. Chúng giúp các nghệ sĩ và những người sáng tạo nội dung khác thể hiện kỹ năng của họ dưới dạng kỹ thuật số và cung cấp khả năng định giá, mua và trao đổi nghệ thuật kỹ thuật số một cách an toàn bằng sổ cái kỹ thuật số. Sử dụng NFT, những tác nhân mới và trước đây phi tập trung có thể phát triển các trao đổi giá trị sáng tạo để xây dựng các cấu trúc thị trường mới.

Herzig cho biết NFT là một hình thức đầu tư thay thế quan trọng, hấp dẫn sở thích và đam mê cá nhân của người mua. Với NFT, các nhà đầu tư bán lẻ sẽ có thể đầu tư vào những thứ mà họ có mối liên hệ cá nhân, cũng như những thứ mang lại giá trị tài chính và tiện ích.

Người mua NFT hy vọng giá trị của token sẽ tăng theo thời gian, tương tự như mọi khoản đầu tư khác. Giống như những người anh em họ có thể thay thế của chúng, NFT phụ thuộc vào sự thay đổi về cung và cầu. Theo Grand View Research , thị trường NFT được định giá 20,44 tỷ đô la vào năm 2022 và dự kiến sẽ tăng lên 211,72 tỷ đô la vào năm 2030.

NFT trên nền tảng cardano?

NFT đầu tiên trên nền tảng Cardano được ra mắt vào tháng 3 năm 2021 với dự án SpaceBudz. Đây là bộ sưu tập gồm 10.000 hình ảnh động vật phi hành gia độc đáo, mỗi hình ảnh được mã hóa dưới dạng NFT trên blockchain Cardano. SpaceBudz đã tiên phong trong việc áp dụng tiêu chuẩn siêu dữ liệu NFT và triển khai thị trường dựa trên hợp đồng thông minh đầu tiên trên Cardano.

Sự ra mắt của SpaceBudz đánh dấu bước ngoặt quan trọng trong việc phát triển hệ sinh thái NFT trên Cardano, mở đường cho nhiều dự án NFT khác trên nền tảng này.

Để tham gia vào thị trường NFT trên Cardano, người dùng cần có ví tiền điện tử tương thích với Cardano, như Nami hoặc Daedalus, và kết nối với các sàn giao dịch NFT như CNFT.io hoặc jpg.store.

2.5.2. Đặc điểm

a) Tính độc nhất (Uniqueness)

Mỗi NFT là duy nhất và không thể sao chép. Thông tin metadata của NFT được lưu trữ trên blockchain, đảm bảo rằng mỗi token có các đặc điểm riêng biệt.

b) Không thể thay thế (Non-fungibility)

Không giống như các tài sản có thể thay thế (như Bitcoin hoặc tiền mặt), NFT không thể trao đổi ngang giá. Mỗi NFT có giá trị riêng dựa trên độ hiếm, tính độc đáo, hoặc giá trị thị trường.

c) Quyền sở hữu rõ ràng (Ownership)

NFT ghi lại quyền sở hữu trong blockchain. Người sở hữu có thể chứng minh quyền sở hữu của mình và chuyển nhượng token nếu muốn.

d) Tính bền vững và minh bạch (Immutability & Transparency)

Thông tin và lịch sử giao dịch của NFT được lưu trữ công khai trên blockchain, không thể bị thay đổi hoặc xóa bỏ.

e) Khả năng chia nhỏ hạn chế (Indivisibility)

Hầu hết NFT không thể chia nhỏ như tiền điện tử. Bạn chỉ có thể sở hữu toàn bộ NFT, không phải một phần của nó (trừ một số trường hợp đặc biệt).

f) Khả năng tương tác (Interoperability)

NFT có thể được sử dụng trên nhiều nền tảng và ứng dụng khác nhau, miễn là chúng tương thích với cùng một blockchain hoặc tiêu chuẩn.

Ví dụ:

- NFT trên Ethereum tuân theo tiêu chuẩn ERC-721 hoặc ERC-1155.

- NFT trên blockchain Cardano được gọi là CNFTs (Cardano Non-Fungible Tokens). Cardano sử dụng tiêu chuẩn CIP-721, tương tự ERC-721 trên Ethereum, để định nghĩa và quản lý NFT. Tiêu chuẩn này đảm bảo tính nhất quán và khả năng tương thích cho các dự án NFT trên mạng lưới.

g) Ứng dụng đa dạng

NFT không chỉ giới hạn trong nghệ thuật số mà còn áp dụng cho:

- Gaming (vật phẩm, nhân vật, tài sản trong game).
- Bất động sản ảo.
- Vé sự kiện hoặc tài sản trí tuệ.
- Sưu tập kỹ thuật số (thẻ bài, tác phẩm nghệ thuật).

h) Khả năng kiếm thu nhập thụ động

Một số NFT cho phép người sở hữu nhận hoa hồng hoặc thu nhập từ việc sử dụng tác phẩm, ví dụ khi tác phẩm được bán lại.

Ví dụ: Trung tuần tháng 3 năm 2022, rapper Binz (Việt nam) kết hợp cùng Công ty blockchain Tuniver ra mắt bộ sưu tập NFT cho ca khúc mới 'Don't Break My Heart'. Bản quyền bài hát này được anh phân chia thành các NFT với 4 hạng khác nhau, tương ứng với 4 mức tỷ lệ chia sẻ bản quyền doanh thu.

2.5.3. Ứng dụng

NFT (Non-Fungible Token) có rất nhiều ứng dụng thực tế trong các lĩnh vực khác nhau, từ nghệ thuật, giải trí đến giáo dục và tài chính. Dưới đây là các ứng dụng phổ biến của NFT:

1. Nghệ thuật số (Digital Art)

Sưu tầm và bán tác phẩm nghệ thuật số. Nghệ sĩ có thể bán tác phẩm của họ trực tiếp cho người mua dưới dạng NFT mà không cần thông qua trung gian. Ví dụ: Beeple đã bán tác phẩm "Everydays: The First 5000 Days" với giá 69,3 triệu USD.

Xác thực và bảo vệ bản quyền. NFT ghi lại nguồn gốc và quyền sở hữu của tác phẩm, giúp ngăn chặn sao chép hoặc giả mạo.

2. Gaming (Trò chơi)

Sở hữu vật phẩm trong game:

Người chơi có thể mua, bán hoặc trao đổi tài sản trong game (vũ khí, nhân vật, trang phục) dưới dạng NFT. Ví dụ: Axie Infinity cho phép người chơi sở hữu và giao dịch các sinh vật kỹ thuật số trong game.

Play-to-Earn:

Các trò chơi NFT thưởng cho người chơi bằng tiền điện tử, biến việc chơi game thành một nguồn thu nhập.

3. Metaverse và bất động sản ảo

Mua bán đất ảo: Người dùng có thể sở hữu và phát triển đất ảo trong các nền tảng metaverse. Ví dụ: Decentraland, The Sandbox, và Pavia (trên Cardano).

Tài sản kỹ thuật số trong metaverse: NFT được sử dụng để giao dịch các tài sản trong thế giới ảo, như nhà cửa, đồ nội thất, và vật phẩm trang trí.

4. Âm nhạc và giải trí

Bản quyền âm nhạc: Nghệ sĩ có thể phát hành các bài hát hoặc album dưới dạng NFT, cho phép người hâm mộ mua và sở hữu một phần doanh thu bản quyền. Ví dụ: Kings of Leon phát hành album dưới dạng NFT.

Vé sự kiện: NFT có thể được sử dụng như vé điện tử, chống gian lận và tạo trải nghiệm độc quyền cho người tham dự.

5. Sưu tập kỹ thuật số (Digital Collectibles)

Thẻ bài và đồ sưu tập: Các thẻ bài kỹ thuật số, hình ảnh hoặc video nổi bật được phát hành dưới dạng NFT.

Ví dụ: NBA Top Shot cung cấp các khoảnh khắc nổi bật của các trận đấu bóng rổ dưới dạng NFT.

6. Giáo dục và tài liệu số

Bằng cấp và chứng chỉ: NFT có thể dùng để lưu trữ và xác thực bằng cấp, chứng chỉ, đảm bảo không thể làm giả.

Tài liệu học tập: Sách giáo khoa, bài giảng có thể được phát hành dưới dạng NFT, cho phép theo dõi và quản lý bản quyền.

7. Tài chính (DeFi)

Tài sản thế chấp: NFT có thể được sử dụng làm tài sản thế chấp trong các giao dịch tài chính, vay mượn trên nền tảng blockchain.

Quản lý tài sản: NFT đại diện cho quyền sở hữu đối với tài sản trong thế giới thực như bất động sản hoặc cổ phiếu.

8. Thời trang và thương mại điện tử

Quần áo kỹ thuật số: Các thương hiệu thời trang lớn phát hành sản phẩm kỹ thuật số dưới dạng NFT để sử dụng trong metaverse. Ví dụ: Gucci và Nike đã bắt đầu thử nghiệm bán NFT thời trang.

Theo dõi và xác thực: NFT có thể được sử dụng để chứng minh tính xác thực và nguồn gốc của sản phẩm trong chuỗi cung ứng.

9. Từ thiện và gây quỹ cộng đồng

Gây quỹ thông qua NFT: NFT được bán để gây quỹ cho các tổ chức từ thiện hoặc các dự án cộng đồng.

Ví dụ: WWF phát hành NFT về các loài động vật đang bị đe dọa để kêu gọi bảo vệ môi trường.

10. Bản quyền và sở hữu trí tuệ

Bảo vệ bản quyền: Các tác phẩm sáng tạo như video, bài viết, hoặc hình ảnh có thể được lưu trữ dưới dạng NFT để theo dõi và quản lý bản quyền.

Phân phối lợi nhuận: Người sáng tạo có thể kiếm được tiền bản quyền mỗi khi NFT của họ được giao dịch trên thị trường.

2.5.4. Thách thức và cơ hội

2.5.4.1. Thách thức của NFT

Mặc dù NFT đã mang lại nhiều cơ hội sáng tạo và kinh tế, chúng cũng đối mặt với nhiều thách thức đáng chú ý. Dưới đây là các vấn đề chính mà NFT đang phải giải quyết:

a) Tính bất ổn của thị trường

- Biến động giá: Giá trị của NFT thường không ổn định, dễ tăng hoặc giảm mạnh trong thời gian ngắn. Điều này làm cho NFT trở thành một khoản đầu tư rủi ro.

- Thiếu tiêu chuẩn định giá: Việc đánh giá giá trị của một NFT phụ thuộc nhiều vào cảm nhận và thị hiếu của người mua, dẫn đến tình trạng đầu cơ.

- Ví dụ:

+) Beeple’s NFT - “Everydays: The First 5000 Days”:

Sự kiện: Tác phẩm này được bán với giá kỷ lục 69,3 triệu USD tại Christie's vào tháng 3/2021, gây chấn động thị trường NFT.

Tính bất ổn: Sau cơn sốt, hàng loạt NFT khác cũng ra đời nhưng không thể đạt được mức giá tương tự. Thị trường trở nên bão hòa và giảm nhiệt nhanh chóng.

+) Axie Infinity (AXS):

Sự kiện: Trò chơi Axie Infinity từng rất phổ biến trong năm 2021 với mô hình "play-to-earn". Người chơi mua NFT để tham gia và kiếm tiền từ game.

Tính bất ổn: Khi số lượng người chơi giảm, giá trị của token AXS và các Axie NFT giảm hơn 90%, khiến nhiều nhà đầu tư rơi vào tình trạng thua lỗ nặng nề.

+) Ethereum Gas Fee

Sự kiện: Trong thời gian cao điểm của thị trường NFT, phí giao dịch trên Ethereum tăng cao, có lúc lên đến hàng trăm USD cho một giao dịch đơn lẻ.

Tính bất ổn: Chi phí giao dịch đắt đỏ đã khiến người dùng rời xa các nền tảng NFT dựa trên Ethereum, dẫn đến sự giảm sút đáng kể về khối lượng giao dịch.

b) Vấn đề bản quyền và quyền sở hữu

- Tranh chấp bản quyền: Một số NFT bị tạo ra từ tác phẩm của người khác mà không có sự cho phép, gây tranh cãi về quyền sở hữu trí tuệ.

Ví dụ: Hermès vs. Mason Rothschild: Hermès kiện nhà sáng tạo Mason Rothschild vì bộ sưu tập NFT "MetaBirkins" sử dụng hình ảnh của túi xách Birkin mà không được phép. Hermès thắng kiện vào năm 2023, khẳng định quyền sở hữu thương hiệu.

- Tách biệt giữa quyền sở hữu NFT và nội dung: Khi mua một NFT, người mua sở hữu token kỹ thuật số liên kết với một nội dung (tác phẩm nghệ thuật, âm nhạc, video, v.v.), nhưng không đồng nghĩa với việc sở hữu bản quyền của tác phẩm đó. Người mua thường hiểu lầm rằng họ có quyền sao chép, phân phối hoặc chỉnh sửa tác phẩm, trong khi các quyền này vẫn thuộc về người sáng tạo gốc, trừ khi có thỏa thuận khác.

Ví dụ: Bored Ape Yacht Club (BAYC): Chủ sở hữu NFT trong bộ sưu tập này được quyền thương mại hóa hình ảnh của các "Bored Ape" họ sở hữu. Tuy nhiên, điều này là ngoại lệ nhờ điều khoản rõ ràng do nhà sáng tạo đưa ra, không phải quy tắc chung của NFT.

c) Chi phí giao dịch cao

Chi phí giao dịch trong thị trường NFT thường rất cao, đặc biệt trên các nền tảng hoạt động dựa trên blockchain như Ethereum. Đây là một thách thức lớn đối với người dùng và nhà phát triển, gây ra rào cản trong việc mở rộng quy mô thị trường và khuyến khích sự tham gia của người dùng mới.

Ví dụ:

- OpenSea và phí gas cao trên Ethereum:

Trong thời kỳ bùng nổ NFT vào năm 2021, phí gas trên Ethereum từng đạt mức 200–300 USD chỉ để thực hiện một giao dịch đơn giản như mua hoặc bán NFT.

Người dùng nhỏ lẻ bị loại khỏi thị trường do không thể chi trả khoản phí cao này. Chẳng hạn, nếu một NFT có giá 50 USD nhưng phí giao dịch lên đến 200 USD, người mua sẽ khó chấp nhận.

- Mint NFT tốn kém:

Để mint một NFT trên Ethereum, người sáng tạo thường phải trả từ 50–200 USD phí gas, tùy thuộc vào mức độ tắc nghẽn mạng.

Một nghệ sĩ độc lập muốn mint 10 NFT sẽ phải trả 500–2.000 USD phí gas, khiến họ do dự trong việc tham gia thị trường.

d) Lo ngại về môi trường

Tiêu thụ năng lượng lớn: Công nghệ blockchain, đặc biệt là các mạng lưới dựa trên cơ chế Proof of Work (PoW), tiêu thụ một lượng lớn năng lượng, góp phần vào biến đổi khí hậu.

Áp lực chuyển đổi: Các mạng lưới đang phải tìm cách chuyển sang cơ chế thân thiện hơn như Proof of Stake (PoS), nhưng quá trình này không dễ dàng.

Ví dụ:

- Beeple và "Everydays: The First 5000 Days":

Tác phẩm của Beeple được bán với giá kỷ lục 69,3 triệu USD trên Ethereum vào năm 2021;

Tác động môi trường: Các giao dịch đấu giá và chuyển quyền sở hữu tiêu thụ lượng lớn năng lượng, với tổng khí thải carbon tương đương hàng nghìn tấn CO_2.

- Bộ sưu tập NFT "Space Cat":

NFT "Space Cat" (hình ảnh một con mèo du hành vũ trụ) được mint và phát hành trên Ethereum. Việc tạo ra và giao dịch Space Cat tiêu thụ **hơn 200 kWh**, tương đương với lượng điện năng tiêu thụ của một gia đình châu Âu trong một tháng.

e) Gian lận và lừa đảo

NFT giả: Một số người tạo NFT từ nội dung không thuộc sở hữu của họ hoặc sao chép NFT của người khác để lừa đảo người mua.

Sàn giao dịch không đáng tin cậy: Một số nền tảng giao dịch thiếu sự minh bạch, dễ bị tấn công hoặc sập đổ, gây thiệt hại cho người dùng.

Ví dụ:

- Frosties NFT (2022): Một trong những vụ rug pull lớn nhất trong năm 2022, nhóm sáng lập Frosties NFT đã lừa đảo người dùng hơn 1,3 triệu USD trước khi xóa bỏ các tài khoản mạng xã hội và ngừng giao tiếp.

- OpenSea và NFT giả mạo (2022): Một trong những sự cố lớn là các nghệ sĩ phát hiện ra rằng tác phẩm của họ đã bị sao chép và bán lại như NFT trên OpenSea mà không có sự cho phép. OpenSea đã phải xử lý hàng nghìn NFT giả mạo, khiến người mua gặp rủi ro lớn.

- Giả mạo MetaMask và OpenSea (2021): Trong một loạt các vụ lừa đảo, hacker gửi email giả mạo OpenSea và MetaMask, yêu cầu người dùng xác minh tài khoản hoặc cung cấp thông tin cá nhân. Sau khi người dùng làm theo, hacker lấy được khóa riêng và chiếm đoạt NFT từ ví của họ.

- The Evolved Apes (2021): Một dự án NFT tên là Evolved Apes đã thu hút hàng triệu USD từ các nhà đầu tư, nhưng nhóm phát triển đột ngột biến mất và không có gì thực sự được phát triển. Người dùng không thể tiếp tục giao dịch NFT và dự án đã chết ngay sau khi thu tiền.

f) Thiếu tính tiện dụng

Độ phức tạp kỹ thuật: Việc tạo, giao dịch hoặc lưu trữ NFT yêu cầu người dùng hiểu biết về công nghệ blockchain, ví tiền điện tử, và các quy trình liên quan.

Hạn chế về trải nghiệm người dùng: Giao diện của các nền tảng NFT hiện tại còn khó sử dụng đối với người mới.

Ví dụ:

- Khó khăn trong việc sử dụng MetaMask và ví tiền mã hóa khác

Một người mới tham gia vào thị trường NFT có thể gặp khó khăn trong việc thiết lập ví MetaMask, kết nối ví với các nền tảng như OpenSea, và thực hiện giao dịch. Quá trình này có thể mất thời gian và dễ gây nhầm lẫn nếu người dùng không có kinh nghiệm.

Người dùng có thể bỏ lỡ cơ hội đầu tư hoặc thậm chí mất tài sản do không thể thực hiện giao dịch chính xác.

- Quá trình mint NFT tốn thời gian và phức tạp

Một nghệ sĩ muốn mint một NFT nhưng gặp khó khăn trong việc tạo và cấu hình hợp đồng thông minh, lựa chọn nền tảng, và thanh toán phí gas. Điều này có thể làm họ cảm thấy bối rối và dễ từ bỏ.

Người sáng tạo không thể phát triển dự án của mình, dẫn đến sự thiếu tham gia của các nghệ sĩ độc lập vào thị trường NFT.

- Phí gas cao gây khó chịu cho người dùng

Một nhà đầu tư muốn mua một NFT có giá 100 USD nhưng phải trả thêm 80 USD phí gas để hoàn tất giao dịch trên Ethereum. Điều này làm giảm tính tiện dụng và có thể khiến người dùng không hài lòng với chi phí giao dịch.

Nhà đầu tư có thể quyết định không mua hoặc bỏ lỡ các cơ hội tiềm năng vì phí giao dịch quá cao.

g) Quy định pháp lý chưa rõ ràng

Thiếu khung pháp lý: Nhiều quốc gia chưa có luật rõ ràng về NFT, dẫn đến rủi ro pháp lý cho cả người mua và người bán.

Quản lý thuế: Các quy định về thuế đối với giao dịch NFT chưa được thống nhất, gây khó khăn trong việc tuân thủ pháp luật.

Ví dụ:

- Vấn đề bản quyền của NFT trên OpenSea:

Trên nền tảng OpenSea, một nghệ sĩ phát hiện ra rằng tác phẩm của mình đã bị sao chép và bán lại dưới dạng NFT mà không có sự cho phép. Tuy nhiên, khi họ cố gắng khiếu nại, họ gặp khó khăn vì không có quy định pháp lý rõ ràng về quyền sở hữu tác phẩm nghệ thuật trong thế giới NFT.

Người sáng tạo không thể bảo vệ quyền lợi của mình do thiếu cơ chế pháp lý và nền tảng cũng không thể đảm bảo bảo vệ quyền sở hữu trí tuệ một cách hiệu quả.

- Vấn đề bảo vệ người tiêu dùng trong vụ scam NFT:

Một nhóm người lừa đảo đã tạo ra một dự án NFT "Bored Ape" giả mạo và lừa đảo người mua số tiền lớn. Sau khi bị phát hiện, người mua không thể yêu cầu bồi thường hay bảo vệ vì không có quy định pháp lý nào điều chỉnh hành vi lừa đảo trong thị trường NFT.

Người tiêu dùng không được bảo vệ và không thể khôi phục tài sản đã mất, dẫn đến việc mất lòng tin vào thị trường NFT.

h) Khả năng tồn tại dài hạn

Giá trị lâu dài: Nhiều người lo ngại rằng sự quan tâm đến NFT chỉ là một trào lưu tạm thời và giá trị của chúng có thể giảm mạnh trong tương lai.

Sự phụ thuộc vào nền tảng: Nếu nền tảng lưu trữ nội dung NFT ngừng hoạt động, nội dung liên kết với NFT có thể bị mất.

Ví dụ:

- NFT trong ngành game:

NFT đã được ứng dụng trong ngành công nghiệp game, đặc biệt trong các trò chơi điện tử cho phép người chơi sở hữu, trao đổi và bán các vật phẩm trong trò chơi dưới dạng NFT. Ví dụ, trò chơi Axie Infinity đã thu hút hàng triệu người chơi và sử dụng NFT để đại diện cho các sinh vật trong trò chơi.

NFT trong ngành game có thể tồn tại lâu dài nếu các trò chơi duy trì sự hấp dẫn và cộng đồng người chơi, đồng thời đảm bảo giá trị thực tế của các vật phẩm NFT.

- NFT trong ngành nghệ thuật số:

NFT đã mang lại cơ hội cho các nghệ sĩ bán tác phẩm nghệ thuật của mình dưới dạng tài sản kỹ thuật số. Ví dụ, các nghệ sĩ như Beeple đã bán tác phẩm nghệ thuật kỹ thuật số dưới dạng NFT với giá hàng triệu đô la, và điều này cho thấy một phần của NFT có thể tồn tại lâu dài nếu thị trường nghệ thuật kỹ thuật số tiếp tục phát triển.

Nếu NFT tiếp tục tạo ra giá trị thực tế cho các nghệ sĩ và người mua, thị trường NFT trong ngành nghệ thuật số có thể duy trì và phát triển trong dài hạn.

2.5.4.1. Cơ hội của NFT

NFT (Token không thể thay thế) không chỉ là một phần của thị trường đầu tư tài sản số mà còn mở ra nhiều cơ hội mới trong các lĩnh vực nghệ thuật, giải trí, bất động sản, game và nhiều ngành công nghiệp khác. Dưới đây là một số cơ hội tiềm năng của NFT trong tương lai.

a) NFT trong ngành nghệ thuật và sáng tạo

NFT tạo ra một cơ hội lớn cho các nghệ sĩ và nhà sáng tạo nội dung khi cho phép họ bán và phân phối tác phẩm nghệ thuật dưới dạng tài sản số. Điều này giúp nghệ sĩ tiếp cận một thị trường toàn cầu và nhận được sự công nhận xứng đáng.

- Cơ hội:

+) Nghệ sĩ có thể bảo vệ bản quyền và nhận doanh thu từ việc bán tác phẩm nghệ thuật mà không bị can thiệp.

+) NFT cho phép phân phối và chứng minh quyền sở hữu đối với tác phẩm nghệ thuật số.

+) Các nghệ sĩ không còn phụ thuộc vào các nhà đấu giá hay các công ty lớn để bán tác phẩm của mình.

- Ví dụ

Beeple: Một nghệ sĩ kỹ thuật số nổi tiếng đã bán tác phẩm "Everydays: The First 5000 Days" dưới dạng NFT với giá 69 triệu USD vào năm 2021. Điều này đã mở ra một cơ hội lớn cho các nghệ sĩ số khác để tiếp cận thị trường và kiếm tiền từ các tác phẩm của mình mà không cần qua các trung gian.

b) NFT trong ngành game

NFT có thể thay đổi hoàn toàn cách thức trao đổi tài sản trong các trò chơi điện tử. Người chơi có thể sở hữu và giao dịch các vật phẩm trong game dưới dạng NFT, mang lại cho họ quyền kiểm soát và sở hữu tài sản số lâu dài.

- Cơ hội:

+) Người chơi có thể sở hữu, mua bán và trao đổi vật phẩm trong game như vũ khí, nhân vật, trang phục hoặc đất đai dưới dạng NFT.

+) NFT có thể làm cho các trò chơi có giá trị hơn khi cho phép người chơi sở hữu các vật phẩm có thể giao dịch với người khác.

- Ví dụ:

Axie Infinity: Đây là một trò chơi blockchain cho phép người chơi nuôi, huấn luyện và chiến đấu với các sinh vật gọi là Axies. Các Axies được đại diện dưới dạng NFT, và người chơi có thể mua bán chúng trên thị trường. Trò chơi này đã thu hút hàng triệu người tham gia và trở thành một ví dụ điển hình về NFT trong game.

c) NFT trong bất động sản

NFT có thể được áp dụng trong ngành bất động sản để đại diện cho quyền sở hữu tài sản vật lý, giúp đơn giản hóa các giao dịch và giảm thiểu thủ tục hành chính phức tạp.

- Cơ hội:

+) Bất động sản có thể được token hóa và đại diện dưới dạng NFT, giúp việc chuyển nhượng quyền sở hữu và giao dịch tài sản trở nên nhanh chóng và minh bạch.

+) NFT có thể giúp giảm thiểu các vấn đề về pháp lý và giấy tờ, đồng thời tạo điều kiện cho những người đầu tư nhỏ lẻ tham gia vào thị trường bất động sản.

- Ví dụ:

RealT: Đây là một nền tảng cho phép các nhà đầu tư mua cổ phần bất động sản thông qua các NFT. Người sở hữu NFT có thể nhận phần lợi nhuận từ bất động sản mà họ đầu tư vào. Nền tảng này đang thử nghiệm với việc token hóa bất động sản và đã thu hút sự quan tâm từ các nhà đầu tư.

d) NFT trong âm nhạc và giải trí

NFT đang mở ra cơ hội mới cho các nghệ sĩ âm nhạc và nhà sản xuất nội dung để bán sản phẩm của họ trực tiếp cho người hâm mộ mà không cần thông qua các trung gian như các công ty thu âm hoặc nền tảng trực tuyến.

e) NFT trong bất động sản

NFT có thể được áp dụng trong ngành bất động sản để đại diện cho quyền sở hữu tài sản vật lý, giúp đơn giản hóa các giao dịch và giảm thiểu thủ tục hành chính phức tạp.

- Cơ hội:

+) Nghệ sĩ có thể phát hành album, bài hát, video âm nhạc và thậm chí là vé concert dưới dạng NFT, giúp họ giữ lại phần lớn doanh thu và xây dựng một cộng đồng fan trung thành.

+) NFT có thể tạo ra các cơ hội độc quyền cho người hâm mộ, chẳng hạn như quyền truy cập sớm vào các sự kiện hoặc các bản thu âm đặc biệt.

- Ví dụ:

Kings of Leon: Ban nhạc này đã phát hành album "When You See Yourself" dưới dạng NFT, cung cấp quyền truy cập đặc biệt cho người mua, bao gồm những nội dung độc quyền và vé tham dự các buổi hòa nhạc.

f) NFT trong ngành thể thao

NFT có thể được sử dụng để tạo ra các thẻ giao dịch thể thao kỹ thuật số, các bộ sưu tập hoặc các vật phẩm lưu niệm độc đáo liên quan đến các vận động viên và sự kiện thể thao.

- Cơ hội:

+) Người hâm mộ có thể mua và sở hữu các thẻ cầu thủ hoặc các khoảnh khắc nổi bật trong các trận đấu thể thao dưới dạng NFT.

+) Các đội thể thao và vận động viên có thể tạo ra các nguồn thu mới từ việc bán các NFT đặc biệt như thẻ cầu thủ hoặc video khoảnh khắc đáng nhớ.

- Ví dụ:

NBA Top Shot: Đây là một nền tảng cho phép người hâm mộ NBA mua, bán và trao đổi các khoảnh khắc đặc biệt từ các trận đấu của NBA dưới dạng NFT. Các video khoảnh khắc như các cú dunk nổi bật hay các pha bóng quyết định có thể được sở hữu như một tài sản kỹ thuật số duy nhất.

g) NFT trong việc xác thực danh tính và chứng nhận

NFT có thể giúp xác thực danh tính hoặc chứng nhận các thành tích, chứng chỉ trong nhiều lĩnh vực như giáo dục, công nghệ hoặc y tế, giúp việc xác nhận các thông tin trở nên nhanh chóng và bảo mật hơn.

- Cơ hội:

+) NFT có thể được sử dụng để tạo ra các chứng chỉ học vấn, giải thưởng, hoặc các danh hiệu được lưu trữ an toàn và không thể làm giả.

+) Những tổ chức, trường học, công ty có thể sử dụng NFT để cấp phát chứng chỉ hoặc danh hiệu, giúp việc xác thực trở nên dễ dàng và minh bạch.

- Ví dụ:

Coursera và các nền tảng giáo dục khác: Một số nền tảng giáo dục trực tuyến đang thử nghiệm với việc phát hành chứng chỉ khóa học dưới dạng NFT, giúp học viên có thể chứng minh thành tích học tập mà không lo bị làm giả.

g) NFT trong việc xác thực danh tính và chứng nhận

NFT có thể giúp bảo vệ quyền sở hữu trí tuệ của các tác phẩm sáng tạo, đặc biệt trong các lĩnh vực như nghệ thuật, âm nhạc, và viết lách, khi tác phẩm được bảo vệ và chứng minh bằng blockchain.

- Cơ hội:

+) NFT có thể là công cụ mạnh mẽ để bảo vệ bản quyền và quyền sở hữu của người sáng tạo, giúp họ nhận được phần lợi nhuận công bằng khi tác phẩm được sử dụng.

+) NFT có thể tạo ra một cách thức minh bạch để theo dõi và phân phối lợi nhuận từ việc sử dụng tác phẩm.

- Ví dụ:

Async Art: Nền tảng này cho phép các nghệ sĩ tạo ra các tác phẩm nghệ thuật động (dynamic art) dưới dạng NFT. Những tác phẩm này có thể thay đổi theo thời

gian, và mỗi tác phẩm NFT đều có thể theo dõi được việc sở hữu và giao dịch trên blockchain, giúp bảo vệ quyền lợi của nghệ sĩ.

Tóm lại:

NFT mở ra nhiều cơ hội tiềm năng trong các ngành nghệ thuật, giải trí, game, bất động sản và nhiều lĩnh vực khác. Bằng cách cung cấp các giải pháp sáng tạo, NFT có thể giúp các nghệ sĩ, nhà sáng tạo, vận động viên, và người tiêu dùng xây dựng các giá trị mới và cải thiện các mô hình kinh doanh truyền thống. Khi công nghệ blockchain phát triển và các quy định pháp lý rõ ràng hơn, thị trường NFT có thể tiếp tục mở rộng và mang lại nhiều cơ hội hơn nữa.

2.6. VÍ VÀ ĐỊA CHỈ

Ví và địa chỉ là hai khái niệm quan trọng trong thế giới blockchain và tài sản kỹ thuật số, bao gồm cả tiền mã hóa (cryptocurrency) và NFT. Các ví và địa chỉ đóng vai trò quan trọng trong việc quản lý tài sản kỹ thuật số, giao dịch và bảo mật thông tin.

2.6.1 Ví (wallet)

2.6.1.1 Khái niệm

Ví trong ngữ cảnh của tài sản kỹ thuật số là một phần mềm, thiết bị hoặc dịch vụ giúp người dùng lưu trữ, gửi và nhận tài sản số, bao gồm tiền mã hóa (cryptocurrency) và NFT. Ví không phải là nơi lưu trữ tài sản thực sự, mà là công cụ để quản lý và truy cập vào tài sản đó thông qua các khóa riêng (private key) và khóa công khai (public key).

Ví có thể được sử dụng cho nhiều mục đích khác nhau, từ việc giao dịch tiền mã hóa cho đến việc quản lý các tài sản kỹ thuật số khác, như các bộ sưu tập NFT hoặc chứng chỉ số.

Với tiền mã hóa , không có loại tiền tệ hữu hình, không có tiền giấy để đặt trong ví hoặc túi xách vật lý. Tiền mã hóa tồn tại trên blockchain và không có biểu hiện vật lý nào mà người dùng chạm vào. Nhưng vẫn cần có cá nhân và tổ chức hiểu được quyền sở hữu tài sản tiền mã hóa và có thể biết được số tiền được nắm giữ, giống như tài khoản ngân hàng cung cấp số dư ngân hàng.

Ví tiền mã hóa cung cấp cho người dùng cách xác thực số dư tài khoản để cung cấp khả năng hiển thị số tiền mã hóa mà người dùng sở hữu. Ví tiền mã hóa cho phép người dùng gửi và nhận các giao dịch tiền mã hóa, một cách tiếp cận tương tự về khái niệm là cách một tài khoản ngân hàng truyền thống cho phép người dùng thực hiện giao dịch. Đối với nhiều người dùng, ví tiền mã hóa là cơ chế chính để quản lý số dư tiền mã hóa.

Tại sao ví tiền mã hóa lại quan trọng?

Giống như bất kỳ loại tiền tệ nào, tiền mã hóa có thể được tích lũy và sử dụng cho nhiều mục đích và giao dịch khác nhau. Ví tiền mã hóa đóng vai trò nền tảng

trong việc cho phép tài sản tiền mã hóa và tiền mã hóa có chức năng hữu ích cho cá nhân và tổ chức, giống như tài khoản ngân hàng là nền tảng cho tiền pháp định.

Ví tiền mã hóa là cần thiết cho một số mục đích quan trọng giúp tận dụng tiện ích thực tế của tiền mã hóa, bao gồm:

- *Quản lý tiền mã hóa:* Ví tiền điện tử cung cấp cho người dùng khả năng theo dõi số dư tài sản tiền mã hóa.

- *Giao dịch:* Gửi và nhận thanh toán bằng tiền điện tử là một tính năng quan trọng của ví tiền mã hóa.

- *Kết nối với các ứng dụng phi tập trung (dApp)*: Cần có ví tiền mã hóa để kết nối và tương tác với các dApp Web 3.0 .

- *Nhận dạng tên người dùng:* Tất cả tiền mã hóa đều được lưu trữ trên blockchain. Ví tiền mã hóa cho phép giao dịch bằng tên người dùng có thể được liên kết với địa chỉ khóa công khai trên blockchain.

- *Quản lý khóa*: Về mặt chức năng, tiền mã hóa tồn tại trên blockchain dưới dạng địa chỉ khóa công khai. Ví tiền mã hóa giúp người dùng quản lý khóa mã hóa riêng được sử dụng để truy cập vào một địa chỉ nhất định và cho phép giao dịch.

2.6.1.2 Phân loại ví

Ví (wallet) trong thế giới tài sản kỹ thuật số có thể được phân loại theo các tiêu chí khác nhau, chủ yếu là dựa trên cách thức lưu trữ, mức độ bảo mật và khả năng sử dụng. Dưới đây là phân loại ví và các loại ví phổ biến hiện nay:

1. Ví Phần Mềm (Software Wallet)

Ví phần mềm là loại ví phổ biến, được cài đặt trên máy tính, điện thoại hoặc thiết bị di động. Ví này cung cấp cho người dùng khả năng truy cập vào tài sản kỹ thuật số và dễ dàng giao dịch. Ví phần mềm có thể kết nối với internet để thực hiện các giao dịch.

Các loại ví phần mềm:

a) Ví di động (Mobile Wallet): Cài đặt trên điện thoại di động, giúp người dùng có thể thực hiện giao dịch mọi lúc, mọi nơi. Đây là lựa chọn phổ biến cho người dùng tiền mã hóa khi di chuyển.

Ví phổ biến:

- Trust Wallet: Một ví di động phổ biến hỗ trợ nhiều loại tiền mã hóa và NFT.

- MetaMask: Một ví di động và trình duyệt dành cho Ethereum và các token ERC-20.

- Yoroi Wallet: Yoroi Wallet là một ví phần mềm nhẹ dành cho Cardano, được phát triển bởi Emurgo (một tổ chức con của Cardano). Yoroi hỗ trợ người dùng quản lý ADA và các tài sản Cardano khác. Đây là một ví thân thiện với người dùng và dễ dàng truy cập qua trình duyệt web hoặc ứng dụng di động.

b) Ví Desktop (Desktop Wallet): Cài đặt trên máy tính để bàn hoặc laptop. Ví desktop thường an toàn hơn ví trực tuyến nhưng có thể dễ bị mất nếu máy tính bị hỏng hoặc bị tấn công.

Ví phổ biến:

- Exodus: Một ví phần mềm với giao diện dễ sử dụng và hỗ trợ nhiều loại tiền mã hóa.

- Electrum: Một ví Bitcoin nhẹ, cho phép người dùng kiểm soát giao dịch tốt hơn.

- Yoroi Wallet

2. Ví Cứng (Hardware Wallet)

Ví cứng là thiết bị vật lý được thiết kế để lưu trữ tiền mã hóa và NFT ngoại tuyến, giúp bảo vệ tài sản khỏi các mối đe dọa trực tuyến như phần mềm độc hại hoặc hack. Ví cứng được coi là lựa chọn bảo mật nhất vì nó không kết nối trực tiếp với internet khi lưu trữ khóa riêng.

Các loại ví cứng:

a) Ví Ledger:

Là một trong những ví cứng phổ biến nhất, hỗ trợ nhiều loại tiền mã hóa và cung cấp bảo mật cao với khóa riêng được lưu trữ trong thiết bị.

Ví phổ biến:

- Ledger Nano S: Thiết bị ví cứng nhỏ gọn, giá phải chăng, thích hợp cho người mới bắt đầu.

- Ledger Nano X: Phiên bản nâng cấp của Nano S với tính năng kết nối Bluetooth và dung lượng lưu trữ cao hơn.

b) Ví Trezor:

Một ví cứng khác với bảo mật cao, hỗ trợ nhiều đồng tiền và token khác nhau.

Ví phổ biến:

- Trezor One: Một ví cứng cơ bản, dễ sử dụng và tương thích với nhiều nền tảng.

- Trezor Model T: Phiên bản cao cấp với màn hình cảm ứng và khả năng hỗ trợ nhiều loại tiền mã hóa.

3. Ví Trực Tuyến (Web Wallet)

Ví trực tuyến (hoặc ví web) là ví được lưu trữ trên các nền tảng trực tuyến, cho phép người dùng truy cập và quản lý tài sản kỹ thuật số thông qua trình duyệt web. Ví trực tuyến có thể dễ dàng sử dụng nhưng bảo mật thấp hơn vì các khóa riêng có thể bị lộ nếu nền tảng bị hack.

Các loại ví trực tuyến:

a) Ví Blockchain: Một ví trực tuyến đơn giản cho phép người dùng lưu trữ và giao dịch tiền mã hóa như Bitcoin và Ethereum.

Ví phổ biến:

Blockchain Wallet: Ví dễ sử dụng với giao diện thân thiện và khả năng lưu trữ Bitcoin, Ethereum.

b) Ví Coinbase: Là ví trực tuyến và cũng là một nền tảng trao đổi tiền mã hóa, cho phép người dùng dễ dàng giao dịch và lưu trữ các loại tiền mã hóa.

Ví phổ biến:

Coinbase Wallet: Ví di động và ví web giúp người dùng lưu trữ tài sản và tương tác với các ứng dụng phi tập trung (dApp).

c) Daedalus Wallet: Daedalus là ví chính thức của Cardano, được phát triển bởi IOHK (Input Output Hong Kong), công ty đứng sau Cardano. Đây là một ví đầy đủ tính năng, chạy trên desktop và cung cấp cho người dùng khả năng lưu trữ toàn bộ blockchain Cardano, giúp đồng bộ hóa và xác nhận giao dịch trực tiếp từ mạng Cardano.

Các tính năng chính của Daedalus:

+) Ví đầy đủ: Daedalus là một ví đầy đủ (full-node wallet), nghĩa là nó tải toàn bộ blockchain Cardano về máy tính của người dùng để đảm bảo tính toàn vẹn và bảo mật.

+) Bảo mật cao: Hỗ trợ tính năng bảo mật mạnh mẽ với khóa riêng và mã PIN.

+) Hỗ trợ nhiều ví: Cho phép người dùng tạo và quản lý nhiều ví cùng lúc trong một ứng dụng.

+) Hỗ trợ Staking: Người dùng có thể stake ADA ngay trong ví Daedalus để kiếm phần thưởng từ Cardano.

+) Tương thích với ví cứng: Có thể tích hợp với ví cứng như Ledger hoặc Trezor.

Các nền tảng hỗ trợ: Máy tính để bàn (Windows, macOS, Linux

d) Adalite Wallet: Adalite là một ví Cardano web nhẹ, dễ sử dụng và không yêu cầu tải toàn bộ blockchain. Nó cho phép người dùng tương tác với mạng Cardano, gửi và nhận ADA, cũng như tham gia vào các hoạt động staking mà không cần phải cài đặt phần mềm nặng.

Các tính năng chính của Adalite:

+) Ví web nhẹ: Không cần tải toàn bộ blockchain, giúp người dùng tiết kiệm dung lượng và thời gian đồng bộ.

+) Tương thích với Ledger: Có thể kết nối với ví cứng Ledger để tăng cường bảo mật.

+) Hỗ trợ staking: Người dùng có thể stake ADA và kiếm phần thưởng trong ví.

+) Bảo mật tốt: Mặc dù là ví web, nhưng Adalite hỗ trợ bảo mật mạnh mẽ với khóa riêng được mã hóa.

Các nền tảng hỗ trợ: Trình duyệt web (Chrome, Firefox, Safari)

4. Ví Giấy (Paper Wallet)

Ví giấy là một phương pháp lưu trữ khóa riêng và khóa công khai dưới dạng bản in vật lý. Ví này giúp lưu trữ tài sản ngoài mạng internet, nhưng người dùng phải rất cẩn thận khi lưu trữ vì dễ bị mất hoặc hư hỏng.

Ví giấy Bitcoin (Bitcoin Paper Wallet): Đây là ví giấy đơn giản được tạo ra bằng cách in khóa công khai và khóa riêng của Bitcoin. Các dịch vụ như *bitaddress.org* giúp người dùng tạo ví giấy miễn phí.

Ví phổ biến:

Bitaddress.org: Dịch vụ tạo ví giấy Bitcoin miễn phí, giúp người dùng tạo ví an toàn và bảo mật.

5. Ví Thẻ (Card Wallet)

Ví thẻ là loại ví mới và tương đối ít phổ biến, giúp người dùng lưu trữ tiền mã hóa và NFT trong một thẻ vật lý tương tự như thẻ ngân hàng. Đây là một phương pháp lưu trữ tiện lợi, an toàn và dễ dàng mang theo.

Ví thẻ:

Ví thẻ Trezor: Một loại ví cứng tích hợp dưới dạng thẻ, cho phép người dùng lưu trữ tiền mã hóa trên một thẻ vật lý.

Ví phổ biến:

Trezor Model T (thẻ): Cung cấp bảo mật cao cho tiền mã hóa và có màn hình cảm ứng để dễ dàng kiểm tra giao dịch.

2.6.1.3 Nguyên lý hoạt động

Ví (wallet) trong thế giới blockchain và tài sản kỹ thuật số hoạt động dựa trên các nguyên lý bảo mật mạnh mẽ và cấu trúc của mạng blockchain. Dưới đây là cách thức hoạt động cơ bản của một ví kỹ thuật số:

1. Khóa Công Khai và Khóa Riêng

Ví kỹ thuật số chủ yếu dựa trên hai thành phần quan trọng: khóa công khai (public key) và khóa riêng (private key). Chúng tạo ra một cặp khóa cho mỗi ví.

Khóa công khai (Public Key): Đây là địa chỉ ví mà người khác có thể gửi tiền hoặc tài sản kỹ thuật số (như tiền mã hóa hoặc NFT). Khóa công khai là công khai và có thể chia sẻ với bất kỳ ai.

Khóa riêng (Private Key): Đây là khóa bí mật, chỉ người sở hữu ví mới biết được. Khóa riêng dùng để xác thực giao dịch và chứng minh quyền sở hữu tài sản. Nếu mất khóa riêng, người dùng sẽ mất quyền truy cập vào tài sản của mình.

2. Quản lý Tài Sản (Chữ Ký Số)

Khi một người dùng muốn thực hiện một giao dịch (ví dụ: gửi ADA hoặc NFT cho người khác), họ sẽ phải sử dụng khóa riêng của mình để ký giao dịch đó. Việc ký giao dịch bằng khóa riêng giúp đảm bảo rằng chỉ người sở hữu ví mới có thể thực hiện các giao dịch liên quan đến tài sản của mình. Đây là quá trình xác thực quyền sở hữu tài sản.

Quy trình giao dịch:

Tạo giao dịch: Người dùng tạo giao dịch bằng cách nhập địa chỉ ví người nhận và số lượng tài sản muốn chuyển.

Chữ ký số: Giao dịch được ký bằng khóa riêng của người gửi, giúp chứng minh rằng họ có quyền chuyển giao tài sản.

Xác nhận giao dịch: Giao dịch sau đó được phát lên mạng blockchain để được xác nhận bởi các nút (nodes) trong mạng (ví dụ, qua cơ chế Proof of Work hoặc Proof of Stake).

Giao dịch sẽ chỉ được chấp nhận khi ký số của người gửi hợp lệ và phù hợp với khóa riêng của họ.

3. Lưu trữ và Quản lý Khóa Riêng

Khóa riêng không được lưu trữ trong ví dưới dạng thông tin dễ nhìn thấy. Thay vào đó, nó được bảo mật trong ví và có thể được mã hóa, giúp bảo vệ người dùng khỏi các mối đe dọa từ bên ngoài.

Ví phần mềm: Thông tin khóa riêng được lưu trữ cục bộ trên máy tính hoặc điện thoại của người dùng. Ví phần mềm sử dụng các biện pháp bảo mật, như mã hóa, để bảo vệ khóa riêng khỏi bị truy cập trái phép.

Ví cứng: Ví cứng lưu trữ khóa riêng trong một thiết bị ngoại vi không kết nối với internet. Điều này giúp bảo vệ tài sản khỏi các mối đe dọa từ phần mềm độc hại hoặc hack.

4. Quản lý Tài Sản (Blockchain và Giao Dịch)

Khi giao dịch được thực hiện, ví sẽ không thực sự chuyển tài sản (ví dụ: ADA hoặc NFT) giữa các ví, mà nó sẽ thay đổi trạng thái của tài sản trên blockchain. Blockchain là sổ cái phân tán ghi lại mọi giao dịch, giúp duy trì tính minh bạch và không thể thay đổi.

Tài sản không thực sự tồn tại trong ví: Thay vào đó, ví chỉ lưu trữ thông tin về quyền sở hữu tài sản, được xác nhận thông qua các giao dịch trên blockchain.

Địa chỉ ví: Địa chỉ ví là nơi tài sản "sống", và ví chỉ giúp người dùng truy cập vào các tài sản này bằng cách ký các giao dịch và quản lý quyền sở hữu.

5. Xác Thực và Bảo Mật

Các ví sử dụng nhiều biện pháp bảo mật để bảo vệ tài sản kỹ thuật số của người dùng:

Mã hóa: Khóa riêng của người dùng được mã hóa và chỉ có người sở hữu ví mới có thể giải mã để sử dụng.

Xác thực hai yếu tố (2FA): Một số ví hỗ trợ 2FA để tăng cường bảo mật, yêu cầu người dùng cung cấp thông tin xác thực thứ hai ngoài mật khẩu.

Phục hồi ví: Một số ví cung cấp phím phục hồi (recovery phrase) hoặc từ khóa dự phòng, giúp người dùng khôi phục ví nếu bị mất hoặc hư hỏng thiết bị.

6. Giao Dịch và Tương Tác với DApps

Ví không chỉ dùng để lưu trữ tiền mã hóa mà còn hỗ trợ người dùng tương tác với các ứng dụng phi tập trung (DApps) trên blockchain.

Ví như một cổng kết nối: Ví là cổng kết nối giữa người dùng và các ứng dụng phi tập trung trên mạng blockchain. Người dùng có thể sử dụng ví để thực hiện các giao dịch, tham gia staking, giao dịch NFT, hoặc tương tác với các smart contract.

Các DApp hỗ trợ ví: Ví như MetaMask (trên Ethereum) hoặc Yoroi (trên Cardano) cho phép người dùng tương tác trực tiếp với DApps mà không cần phải rời khỏi ứng dụng ví.

Tóm lại ví hoạt động theo nguyên lý:

1. Cặp khóa công khai và khóa riêng giúp người dùng quản lý quyền truy cập và bảo mật tài sản.

2. Chữ ký số đảm bảo giao dịch chỉ có thể thực hiện bởi chủ sở hữu khóa riêng.

3. Ví phần mềm và ví cứng bảo mật khóa riêng và lưu trữ tài sản trong mạng blockchain.

4. Tài sản kỹ thuật số không thực sự lưu trữ trong ví mà được ghi lại trong blockchain.

5. Biện pháp bảo mật như mã hóa, xác thực hai yếu tố và từ khóa phục hồi giúp bảo vệ tài sản của người dùng.

6. Ví còn giúp người dùng tương tác với các DApp và tham gia vào các hoạt động staking, giao dịch, hoặc quản lý NFT trên blockchain.

Nguyên lý hoạt động của ví đảm bảo tính an toàn và bảo mật cho người dùng khi họ thực hiện giao dịch hoặc quản lý tài sản kỹ thuật số.

2.6.1.4 Vấn đề bảo mật và rủi ro

Khi sử dụng ví kỹ thuật số để lưu trữ và giao dịch tài sản trên các blockchain như Bitcoin, Ethereum, Cardano, hay bất kỳ nền tảng nào, người dùng cần phải cẩn thận với các mối nguy cơ bảo mật. Mặc dù ví mang lại nhiều tiện ích, nhưng chúng

cũng tiềm ẩn các rủi ro có thể dẫn đến mất mát tài sản hoặc dữ liệu cá nhân. Dưới đây là một số vấn đề bảo mật và các rủi ro phổ biến mà người dùng ví cần lưu ý:

1. Mất hoặc Lộ Khóa Riêng (Private Key)

Rủi ro:

Mất khóa riêng: Nếu người dùng mất khóa riêng của mình, họ sẽ không thể truy cập vào tài sản kỹ thuật số của mình. Điều này rất nghiêm trọng vì blockchain là hệ thống phân tán và không thể khôi phục giao dịch hoặc tài sản một khi khóa riêng đã bị mất.

Lộ khóa riêng: Nếu khóa riêng bị lộ (do người dùng chia sẻ sai, bị hack, hoặc lưu trữ không an toàn), kẻ xấu có thể chiếm đoạt tài sản của người dùng.

Ví dụ:

Ví phần mềm bị hack: Một số ví phần mềm như Exodus hoặc Electrum đã bị các nhóm hacker tấn công, và nếu người dùng không bảo vệ khóa riêng của mình bằng mã hóa hoặc các phương pháp bảo mật khác, họ có thể mất tài sản. Một ví dụ đáng chú ý là vụ hack MyEtherWallet vào năm 2018, nơi các hacker đã tấn công DNS và lừa người dùng cung cấp khóa riêng.

2. Mất Ví hoặc Hư Hỏng Thiết Bị

Rủi ro:

Mất ví cứng: Nếu người dùng mất ví cứng (như Ledger hoặc Trezor) và không sao lưu đủ thông tin (như từ khóa phục hồi), họ sẽ không thể phục hồi tài sản.

Hư hỏng thiết bị: Ví cứng hoặc ví phần mềm có thể hỏng hoặc bị mất nếu không sao lưu dữ liệu ví một cách an toàn.

Ví dụ:

Mất ví cứng Trezor: Một người dùng có thể vô tình làm rơi hoặc mất ví Trezor của mình. Nếu không sao lưu cụm từ khôi phục, họ sẽ không thể khôi phục quyền truy cập vào tài sản của mình.

Hư hỏng ví phần mềm: Ví như Exodus có thể gặp sự cố nếu máy tính hoặc điện thoại của người dùng bị hỏng và không có bản sao lưu khóa riêng hoặc từ khóa phục hồi.

3. Tấn Công Phishing và Lừa Đảo

Rủi ro:

Tấn công Phishing: Đây là một kỹ thuật lừa đảo nơi hacker giả mạo các trang web hoặc email từ các ví nổi tiếng như MetaMask, Trust Wallet, hoặc Coinbase Wallet để lấy cắp khóa riêng hoặc thông tin cá nhân.

Lừa đảo qua liên kết giả mạo: Người dùng có thể bị lừa nhấp vào các liên kết giả mạo trong email hoặc tin nhắn và nhập thông tin vào các trang web không chính thức.

Ví dụ:

MetaMask Phishing: Một số người dùng MetaMask đã bị lừa khi nhấp vào các liên kết phishing và nhập mật khẩu hoặc khóa riêng vào các trang web giả mạo, dẫn đến mất hết tài sản.

Lừa đảo qua email giả mạo Coinbase: Có các cuộc tấn công phishing, nơi hacker giả mạo email từ Coinbase và yêu cầu người dùng cung cấp thông tin đăng nhập ví hoặc mã xác thực 2FA.

4. Tấn Công Mạng và Malware (Phần Mềm Độc Hại)

Rủi ro:

Phần mềm độc hại: Máy tính hoặc điện thoại của người dùng có thể bị nhiễm phần mềm độc hại (malware) để theo dõi hoạt động ví, đánh cắp thông tin khóa riêng, và thực hiện các giao dịch mà người dùng không hề hay biết.

Tấn công từ xa: Nếu ví được lưu trữ trên máy tính hoặc điện thoại có phần mềm độc hại, hacker có thể xâm nhập và rút tiền mà không cần sự đồng ý của người dùng.

Ví dụ:

Malware trên máy tính: Một người dùng đã tải xuống một phần mềm miễn phí, nhưng phần mềm này thực chất là malware đã theo dõi các hoạt động của ví Bitcoin và rút tiền từ ví mà không có sự đồng ý của chủ sở hữu.

Tấn công man-in-the-middle (MITM): Khi người dùng thực hiện giao dịch qua một mạng không an toàn, như Wi-Fi công cộng, hacker có thể nghe lén và can thiệp vào giao dịch của người dùng.

5. Các Lỗ Hổng Bảo Mật trong Ví

Rủi ro:

Lỗ hổng phần mềm: Ví phần mềm có thể gặp phải các lỗ hổng bảo mật trong mã nguồn, giúp hacker có thể khai thác và chiếm đoạt tài sản của người dùng.

Lỗ hổng trong giao thức: Các giao thức blockchain hoặc ví có thể có lỗi lập trình hoặc thiếu sót, dẫn đến việc tài sản bị rút ra mà không có sự đồng ý của người dùng.

Ví dụ:

Lỗi bảo mật trong ví Ethereum: Trước đây, một số ví Ethereum đã gặp phải các lỗi bảo mật trong hợp đồng thông minh (smart contracts), khiến người dùng có thể bị mất tiền trong các giao dịch hoặc khi tham gia staking.

6. Nguy Cơ Từ Mạng Xã Hội và Quảng Cáo Giả Mạo

Rủi ro:

Quảng cáo giả mạo: Một số quảng cáo trên mạng xã hội hoặc các trang web không chính thống có thể dụ dỗ người dùng tải xuống ví hoặc ứng dụng giả mạo.

Lừa đảo đầu tư (Ponzi scheme): Các mánh lừa đảo liên quan đến việc đầu tư vào các tài sản kỹ thuật số hoặc NFT với lời hứa lợi nhuận cao, chỉ để người dùng mất tiền.

Ví dụ:

Ví giả mạo trên Twitter: Có những tài khoản giả mạo ví nổi tiếng như MetaMask hoặc Trust Wallet trên Twitter hoặc Telegram, quảng cáo các chương trình khuyến mãi hoặc giảm giá, và khi người dùng tải về, họ cài đặt ứng dụng giả mạo để lấy cắp tài sản.

7. Quyền Sở Hữu và Tranh Chấp Pháp Lý

Rủi ro:

Tranh chấp pháp lý: Trong trường hợp pháp luật không rõ ràng về quyền sở hữu tài sản kỹ thuật số, người dùng có thể gặp khó khăn trong việc bảo vệ tài sản của mình nếu có tranh chấp với đối tác hoặc chính quyền.

Mất tài sản vì pháp lý không rõ ràng: Nếu có vấn đề pháp lý như bị hack hoặc bị chiếm đoạt tài sản, người dùng không thể khôi phục tài sản từ cơ quan chính phủ hoặc hệ thống pháp lý.

Ví dụ:

Tranh chấp pháp lý về NFT: Có thể xảy ra tranh chấp về quyền sở hữu hoặc bản quyền đối với NFT, đặc biệt khi NFT đó đuaợc bán lại hoặc trao đổi mà không có sự chấp thuận của người sáng tạo.

2.6.1.5 Các ứng dụng

Ví kỹ thuật số không chỉ đơn thuần là công cụ lưu trữ tài sản kỹ thuật số mà còn đóng vai trò quan trọng trong nhiều ứng dụng khác nhau trong thế giới blockchain và tài sản mã hóa.

Các ứng dụng thông dụng của ví:

1. Lưu trữ và quản lý tài sản kỹ thuật số (Bitcoin, Ethereum, ADA, NFT).
2. Giao dịch và thanh toán tiền mã hóa.
3. Tham gia DApp (DeFi, trò chơi blockchain, NFT).
4. Staking tài sản để nhận phần thưởng.
5. Quản lý NFT (Non-Fungible Tokens).
6. Giao dịch ngoài hệ sinh thái blockchain.
7. Lưu trữ token bảo mật và chứng nhận quyền sở hữu tài sản.
8. Xác thực danh tính (KYC).

Ví kỹ thuật số là một công cụ mạnh mẽ không chỉ để lưu trữ và giao dịch tiền mã hóa, mà còn hỗ trợ người dùng tham gia vào các ứng dụng phi tập trung, staking, quản lý NFT, và nhiều dịch vụ tài chính khác.

2.6.2. Địa chỉ

Trong hệ sinh thái blockchain, địa chỉ (address) là một chuỗi các ký tự hoặc mã nhận dạng duy nhất dùng để xác định vị trí nơi người dùng có thể nhận hoặc gửi tài sản kỹ thuật số, như tiền mã hóa, token, hoặc NFT. Địa chỉ này thường liên quan trực tiếp đến các ví kỹ thuật số và là một phần quan trọng trong các giao dịch blockchain. Trong hệ sinh thái blockchain, địa chỉ (address) là một chuỗi các ký tự hoặc mã nhận dạng duy nhất dùng để xác định vị trí nơi người dùng có thể nhận hoặc gửi tài sản kỹ thuật số, như tiền mã hóa, token, hoặc NFT. Địa chỉ này thường liên quan trực tiếp đến các ví kỹ thuật số và là một phần quan trọng trong các giao dịch blockchain.

2.6.2.1. Khái niệm

Địa chỉ blockchain có thể được coi như một "số tài khoản" trong ngân hàng hoặc "số điện thoại" dùng để nhận tiền hoặc tài sản. Tuy nhiên, thay vì sử dụng tên hoặc số tài khoản, blockchain sử dụng các chuỗi ký tự số và chữ để làm địa chỉ.

Một địa chỉ thường được tạo ra thông qua các hàm băm (hashing) từ khóa công khai (public key) và các thuật toán mã hóa mạnh mẽ để đảm bảo tính bảo mật và bảo vệ quyền sở hữu tài sản.

Ví dụ:

Bitcoin Address (BTC): Địa chỉ Bitcoin thường bắt đầu bằng ký tự "1" hoặc "3", ví dụ: 1A1Z6MEAnqvhwxc9u3Uuu62W8AQu2D9UuC.

Ethereum Address (ETH): Địa chỉ Ethereum bắt đầu bằng "0x", ví dụ: 0x740ECBbCe82c3F000E01a0038e281f3097d403C5.

Cardano (ADA): Địa chỉ Cardano có thể bắt đầu bằng "addr1" và được mã hóa theo một cấu trúc khác so với Bitcoin và Ethereum. ví dụ:
addr1q9knwn2jptp5eqlk5jlg8ldqu8pndw4fkp9dyxj69f9pdhpyh98ak8wjl5qlfuwqkcl96f40h5r

2.6.2.2. Phân loại

Địa chỉ blockchain có thể được phân loại theo từng loại blockchain và cách mà địa chỉ được sử dụng trong mỗi hệ thống. Các loại địa chỉ phổ biến bao gồm:

a) Địa Chỉ Bitcoin (BTC)

Khái niệm: Địa chỉ Bitcoin dùng để nhận và gửi Bitcoin trong mạng lưới Bitcoin.

Đặc điểm: Địa chỉ Bitcoin có thể bắt đầu bằng ký tự "1", "3" hoặc "bc1".

Ví dụ: *1A1Z6MEAnqvhwxc9u3Uuu62W8AQu2D9UuC*

Ví: Các địa chỉ "P2PKH" (Pay-to-PubKey-Hash) bắt đầu bằng "1", "P2SH" (Pay-to-Script-Hash) bắt đầu bằng "3", và địa chỉ SegWit bắt đầu bằng "bc1".

b) Địa Chỉ Ethereum (ETH)

Khái niệm: Địa chỉ Ethereum là một chuỗi 40 ký tự (không tính tiền tố "0x") được sử dụng để nhận và gửi Ethereum và các token ERC-20.

Đặc điểm: Địa chỉ Ethereum bắt đầu bằng "0x".

Ví dụ: *0x740ECBbCe82c3F000E01a0038e281f3097d403C5*

c) Địa Chỉ Cardano (ADA)

Khái niệm: Địa chỉ Cardano là một chuỗi ký tự được tạo ra từ các quy tắc đặc biệt của blockchain Cardano.

Đặc điểm: Địa chỉ Cardano có thể bắt đầu bằng "addr1" và được mã hóa theo một cấu trúc khác so với Bitcoin và Ethereum.

Ví dụ:
addr1q9knwn2jptp5eqlk5jlg8ldqu8pndw4fkp9dyxj69f9pdhpyh98ak8wjl5qlfuwqkcl96f40h5r

d) Địa Chỉ Binance Smart Chain (BSC)

Khái niệm: Địa chỉ BSC là địa chỉ dùng để nhận và gửi tài sản trên mạng Binance Smart Chain.

Đặc điểm: Địa chỉ BSC tương tự như địa chỉ Ethereum, bắt đầu bằng "0x".

Ví dụ: *0x6f99fcd64af42c4e2c7289cab0f039080d997f21*

e) Địa Chỉ Solana (SOL)

Khái niệm: Địa chỉ Solana là một chuỗi ký tự dài được sử dụng trong hệ sinh thái Solana.

Đặc điểm: Địa chỉ Solana dài khoảng 32 ký tự và không có tiền tố đặc biệt.

Ví dụ: *6rKWh6j8jfTpzcsYXsdvxdTt2EZSY61qbb9XfX5g97DE*

2.6.2.3. Nguyên lý hoạt động

Địa chỉ blockchain hoạt động chủ yếu dựa trên nguyên lý liên kết giữa khóa công khai (public key) và khóa riêng tư (private key). Quy trình này giúp xác thực và bảo vệ giao dịch:

1. Tạo Địa Chỉ

Bước 1: Tạo khóa công khai (public key): Quá trình tạo địa chỉ bắt đầu từ việc tạo khóa công khai thông qua các thuật toán như Elliptic Curve Cryptography (ECC) (trong Bitcoin, Ethereum, v.v.).

Bước 2: Băm và mã hóa: Để tạo địa chỉ, khóa công khai được băm lại bằng các hàm băm như SHA-256 và RIPEMD-160, sau đó mã hóa thành địa chỉ.

Bước 3: Kết quả, địa chỉ sẽ là một chuỗi ký tự đại diện cho một địa chỉ duy nhất trong mạng blockchain, có thể gửi và nhận tài sản.

2. Giao Dịch với Địa Chỉ

Khi bạn muốn gửi tiền hoặc tài sản đến một địa chỉ blockchain, bạn sử dụng khóa riêng để ký xác thực giao dịch.

Giao dịch này được truyền tải qua mạng lưới và được xác nhận bởi các node (nút) trên blockchain.

Khi giao dịch hoàn tất, tài sản sẽ chuyển từ ví của bạn sang địa chỉ đích. Quá trình này được ghi lại trên sổ cái công khai của blockchain.

3. Bảo Mật và Xác Thực

Khóa riêng (private key): Chỉ người sở hữu khóa riêng mới có thể ký và phê duyệt giao dịch từ địa chỉ của mình. Việc bảo mật khóa riêng cực kỳ quan trọng, nếu mất khóa riêng, bạn sẽ mất quyền truy cập vào tài sản trong ví.

Khóa công khai (public key): Đây là thông tin công khai và được sử dụng để tạo địa chỉ nhận tiền từ các giao dịch khác. Khóa công khai không thể dùng để ký giao dịch, mà chỉ để nhận tài sản.

2.6.2.4. Vấn đề bảo mật và các rủi ro

Địa chỉ trên blockchain đóng vai trò quan trọng trong việc nhận và gửi tài sản kỹ thuật số. Tuy nhiên, như với bất kỳ công nghệ nào, vấn đề bảo mật và các rủi ro liên quan đến địa chỉ trên blockchain là rất lớn và có thể gây thiệt hại nghiêm trọng nếu không được quản lý đúng cách. Dưới đây là các vấn đề bảo mật và các rủi ro chính của địa chỉ trên blockchain.

1. Mất Khóa Riêng (Private Key)

Rủi ro:

Khóa riêng là yếu tố bảo mật quan trọng nhất để quản lý tài sản trong ví blockchain. Nếu bạn mất khóa riêng của mình, bạn sẽ không thể truy cập vào tài sản của mình. Điều này có thể xảy ra khi:

Mất hoặc quên khóa riêng.

Khóa riêng bị xóa mà không sao lưu.

Khóa riêng bị đánh cắp do vi phạm bảo mật hoặc hành vi lừa đảo.

Ví dụ:

Một người dùng Bitcoin mất khóa riêng của mình và không có bản sao lưu, dẫn đến việc mất toàn bộ số Bitcoin trong ví mà không thể khôi phục lại.

Giải pháp:

Sao lưu khóa riêng ở nhiều nơi an toàn, chẳng hạn như giấy, phần mềm bảo mật hoặc thiết bị phần cứng.

Sử dụng các ví phần cứng (hardware wallet) để lưu trữ khóa riêng một cách an toàn.

2. Tấn Công Lừa Đảo (Phishing)

Rủi ro:

Phishing là phương thức mà kẻ lừa đảo giả mạo các trang web hoặc dịch vụ ví, yêu cầu người dùng nhập khóa riêng hoặc thông tin nhạy cảm của họ.

Kẻ tấn công có thể giả mạo địa chỉ ví của người dùng và thay đổi địa chỉ ví nhận trong một giao dịch, khiến tài sản bị gửi vào ví của kẻ lừa đảo.

Ví dụ:

Một người dùng nhận được email giả mạo từ một sàn giao dịch, yêu cầu cập nhật thông tin tài khoản và nhập khóa riêng của mình. Sau khi làm theo hướng dẫn, tài sản của người dùng bị chuyển vào ví của kẻ lừa đảo.

Giải pháp:

Luôn kiểm tra URL và các liên kết trước khi nhập thông tin vào các trang web hoặc dịch vụ ví.

Kích hoạt xác thực hai yếu tố (2FA) để bảo vệ tài khoản ví.

3. Tấn Công 51% (51% Attack)

Rủi ro:

Một tấn công 51% có thể xảy ra nếu kẻ tấn công kiểm soát hơn 50% sức mạnh tính toán của mạng blockchain. Điều này có thể dẫn đến khả năng thay đổi lịch sử giao dịch, thao túng giao dịch hoặc gây ra các vấn đề bảo mật nghiêm trọng khác.

Nếu có một số địa chỉ ví bị tấn công hoặc bị kiểm soát bởi một nhóm tấn công, có thể dẫn đến việc lừa đảo hoặc chi tiêu gấp đôi (double-spending).

Ví dụ:

Mạng Bitcoin Cash từng phải đối mặt với cuộc tấn công 51% vào năm 2018, dẫn đến việc một số giao dịch bị đảo ngược và tiền bị chi tiêu gấp đôi.

Giải pháp:

Sử dụng các blockchain có sức mạnh tính toán phân tán cao hoặc chuyển sang proof-of-stake (PoS) thay vì proof-of-work (PoW) để giảm thiểu nguy cơ này.

4. Lỗi Phát Sinh trong Quá Trình Tạo Địa Chỉ (Address Generation Flaws)

Rủi ro:

Các lỗi trong quá trình tạo địa chỉ có thể xảy ra khi phần mềm tạo địa chỉ không đúng cách hoặc sử dụng thuật toán không bảo mật. Điều này có thể dẫn đến việc tạo ra các địa chỉ ví có thể bị dễ dàng dự đoán hoặc thậm chí bị tấn công.

Ví dụ:

Một số ví lỗi có thể tạo ra địa chỉ dễ dàng đoán được, làm tăng khả năng tấn công từ kẻ xấu.

Giải pháp:

Sử dụng các công cụ và phần mềm ví có chứng nhận bảo mật cao, luôn cập nhật các bản vá bảo mật mới nhất.

5. Giao Dịch Sai Địa Chỉ (Wrong Address Transactions)

Rủi ro:

Việc gửi tài sản đến địa chỉ sai có thể xảy ra nếu người dùng sao chép và dán sai địa chỉ ví, hoặc khi có sự nhầm lẫn giữa các địa chỉ ví (ví dụ: địa chỉ Bitcoin và Ethereum có cấu trúc tương tự).

Các giao dịch trên blockchain là không thể hoàn tác (irreversible), vì vậy nếu tài sản được gửi nhầm, người dùng sẽ không thể lấy lại.

Ví dụ:

Người dùng gửi Bitcoin đến một địa chỉ Ethereum, và do sự khác biệt giữa các blockchain, giao dịch không thể thực hiện được, gây mất mát tài sản.

Giải pháp:

Kiểm tra kỹ địa chỉ ví trước khi gửi giao dịch.

Sử dụng mã QR hoặc các công cụ hỗ trợ để tránh lỗi nhập sai địa chỉ.

6. Rủi Ro từ Các Ví Trung Gian (Hot Wallets)

Rủi ro:

Ví nóng (Hot Wallets) là các ví được kết nối trực tiếp với internet và dễ bị tấn công từ các mối đe dọa bên ngoài như virus, phần mềm độc hại hoặc hacker.

Các ví trung gian trên các sàn giao dịch cũng có thể là mục tiêu tấn công.

Ví dụ:

Vào năm 2014, sàn giao dịch Mt. Gox bị hack và mất 850.000 Bitcoin, phần lớn tài sản này là của người dùng đang lưu trữ trong ví nóng của sàn.

Giải pháp:

Lưu trữ tài sản trên ví lạnh (cold wallet), đặc biệt là các tài sản lớn, và chỉ sử dụng ví nóng cho giao dịch ngắn hạn hoặc thử nghiệm.

Kích hoạt xác thực hai yếu tố (2FA) và bảo vệ tài khoản ví với các phương thức bảo mật khác.

7. Các Vấn Đề Liên Quan đến Quyền Riêng Tư

Rủi ro:

Blockchain là sổ cái công khai (public ledger), có nghĩa là tất cả các giao dịch có thể được xem xét trên toàn cầu. Điều này có thể dẫn đến lộ thông tin cá nhân nếu địa chỉ ví của bạn được liên kết với một danh tính thực.

Mặc dù các giao dịch trên blockchain là pseudonymous (ẩn danh), việc có thể truy vết địa chỉ ví đến một cá nhân cụ thể vẫn có thể xảy ra nếu thông tin cá nhân bị tiết lộ.

Ví dụ:

Người dùng không nhận ra rằng địa chỉ ví của mình có thể được theo dõi qua các công cụ phân tích blockchain, dẫn đến nguy cơ lộ thông tin tài chính và danh tính cá nhân.

Giải pháp:

Sử dụng địa chỉ mới cho mỗi giao dịch để tăng cường sự bảo mật và ẩn danh.

Xem xét sử dụng các giải pháp layer 2 như CoinJoin để làm cho các giao dịch trở nên khó theo dõi hơn.

Tóm lại

Bảo mật địa chỉ trên blockchain là vấn đề quan trọng đối với người dùng và các tổ chức sử dụng công nghệ này. Việc hiểu rõ các rủi ro và cách thức bảo vệ tài sản là rất cần thiết để tránh mất mát tài sản và các cuộc tấn công có thể xảy ra.

2.6.2.5. Ứng dụng

Địa chỉ trên blockchain không chỉ là nơi lưu trữ tài sản, mà còn đóng vai trò quan trọng trong nhiều ứng dụng và dịch vụ khác nhau.

1. Giao Dịch Tiền Mã Hóa (Cryptocurrency Transactions)

Ứng dụng: Địa chỉ trên blockchain chủ yếu được sử dụng để gửi và nhận tiền mã hóa (cryptocurrency). Mỗi địa chỉ ví trên blockchain là một điểm nhận tài sản, cho phép các giao dịch tiền mã hóa diễn ra giữa các người dùng.

Ví dụ:

Một người dùng Bitcoin có thể gửi BTC từ địa chỉ 1A1Z6MEAnqvhwxc9u3Uuu62W8AQu2D9UuC tới địa chỉ của người nhận.

Tương tự, người dùng Ethereum gửi ETH từ địa chỉ 0x740ECBbCe82c3F000E01a0038e281f3097d403C5 tới một địa chỉ Ethereum khác.

Mục đích: Thực hiện các giao dịch thanh toán trực tuyến. Chuyển tiền xuyên biên giới mà không cần sự tham gia của các tổ chức tài chính trung gian.

2. Sử Dụng Trong Hợp Đồng Thông Minh (Smart Contracts)

Ứng dụng: Các hợp đồng thông minh (smart contracts) trên blockchain sử dụng địa chỉ ví để thực hiện các giao dịch tự động khi điều kiện nhất định được đáp ứng. Địa chỉ trong trường hợp này có thể là địa chỉ của hợp đồng thông minh hoặc địa chỉ của người tham gia hợp đồng.

Ví dụ: Một hợp đồng thông minh trên Ethereum có thể nhận các khoản thanh toán từ người dùng và sau đó tự động thực hiện một hành động (ví dụ: giao hàng hoặc cấp phép) khi thanh toán hoàn tất.

Mục đích: Tự động hóa các thỏa thuận mà không cần bên trung gian. Đảm bảo tính minh bạch và đáng tin cậy trong các giao dịch phức tạp.

3. Địa Chỉ Liên Kết Với NFT (Non-Fungible Tokens)

Ứng dụng: Trong hệ sinh thái NFT, địa chỉ ví được sử dụng để mua, bán và lưu trữ các NFT. Mỗi NFT có thể được chuyển từ địa chỉ này sang địa chỉ khác khi giao dịch được thực hiện. Người dùng sở hữu các NFT sẽ giữ chúng trong ví của mình dưới các địa chỉ ví riêng biệt.

Ví dụ: Một nghệ sĩ có thể tạo ra và bán NFT trên các nền tảng như OpenSea, nơi địa chỉ ví của người mua và người bán đóng vai trò quyết định trong việc chuyển nhượng quyền sở hữu NFT.

Mục đích: Chuyển nhượng tài sản số độc nhất (NFT). Xác nhận quyền sở hữu và tính xác thực của các vật phẩm kỹ thuật số.

4. Quản Lý và Lưu Trữ Tài Sản Kỹ Thuật Số (Digital Asset Management)

Ứng dụng: Địa chỉ blockchain cũng được sử dụng trong việc quản lý các tài sản kỹ thuật số ngoài tiền mã hóa, như token hóa tài sản (real estate, cổ phiếu, hoặc vật phẩm số). Các tài sản này có thể được chuyển nhượng hoặc bán lại dưới dạng các token, và việc quản lý những token này được thực hiện qua địa chỉ ví blockchain.

Ví dụ: Các tổ chức tài chính có thể phát hành Security Tokens để đại diện cho các cổ phiếu hoặc tài sản. Các nhà đầu tư sẽ sở hữu các token này thông qua địa chỉ ví của mình.

Mục đích: Đảm bảo quyền sở hữu và tính hợp pháp của các tài sản kỹ thuật số. Tạo điều kiện thuận lợi cho việc giao dịch các tài sản trong môi trường blockchain.

5. Giao Dịch và Quản Lý Token Trong Các DApp (Decentralized Applications)

Ứng dụng: Các ứng dụng phi tập trung (DApp) sử dụng địa chỉ ví để thực hiện giao dịch token, tham gia vào các trò chơi blockchain, staking, hay voting. Người dùng tương tác với các DApp thông qua địa chỉ ví của mình, qua đó thực hiện các hành động như đặt cược token, tham gia quản trị, hoặc kiếm phần thưởng.

Ví dụ: Trong trò chơi blockchain như Axie Infinity, người chơi có thể sở hữu các token trong ví và sử dụng chúng để mua các vật phẩm hoặc tham gia chiến đấu. Trong các dự án DeFi (tài chính phi tập trung), người dùng có thể sử dụng ví của mình để staking hoặc cho vay token.

Mục đích:Tạo ra các dịch vụ tài chính phi tập trung (DeFi) mà không cần sự tham gia của ngân hàng hoặc tổ chức tài chính trung gian. Đảm bảo quyền kiểm soát hoàn toàn tài sản và thông tin cá nhân cho người dùng.

6. Quyền Sở Hữu và Quản Lý Danh Tính (Identity Management)

Ứng dụng: Blockchain cung cấp một cách thức để người dùng có thể quản lý danh tính của mình một cách an toàn thông qua địa chỉ ví. Các địa chỉ này có thể được sử dụng để xác minh danh tính, lưu trữ và bảo vệ thông tin cá nhân trên các nền tảng blockchain mà không cần phải dựa vào các tổ chức trung gian.

Ví dụ: Self-sovereign identity (SSO) cho phép người dùng kiểm soát thông tin cá nhân của mình và chia sẻ chúng khi cần thiết mà không cần phải thông qua cơ quan chứng nhận tập trung.

Mục đích: Cung cấp một phương thức bảo mật cho việc xác minh danh tính trực tuyến. Giảm thiểu các vấn đề về lừa đảo và bảo vệ quyền riêng tư của người dùng.

7. Thanh Toán và Microtransactions

Ứng dụng: Địa chỉ ví trên blockchain cũng được sử dụng để thực hiện thanh toán và microtransactions. Các dịch vụ thanh toán như Lightning Network (Bitcoin) hoặc các giao thức thanh toán trên các nền tảng blockchain khác cho phép thanh toán nhanh chóng và chi phí thấp, giúp người dùng giao dịch một cách tiện lợi và dễ dàng.

Ví dụ: Sử dụng Bitcoin Lightning Network để thực hiện các giao dịch nhỏ với chi phí thấp, ví dụ: trả tiền cho nội dung số, sử dụng dịch vụ trực tuyến, hoặc gửi tiền nhỏ cho bạn bè.

Mục đích: Tăng cường khả năng thanh toán trực tuyến với các khoản tiền nhỏ mà không gặp phải phí giao dịch cao. Đẩy mạnh ứng dụng blockchain trong các dịch vụ thanh toán truyền thống.

8. Tạo và Quản Lý Mã Thẻ Quà Tặng (Gift Cards)

Ứng dụng: Một số nền tảng sử dụng blockchain để phát hành và quản lý thẻ quà tặng (gift cards). Địa chỉ ví blockchain có thể được sử dụng để nhận và thanh toán bằng các thẻ quà tặng này.

Ví dụ: Một dịch vụ thẻ quà tặng có thể phát hành mã thẻ dưới dạng token trên blockchain, và người nhận có thể sử dụng ví blockchain để thanh toán các sản phẩm và dịch vụ.

Mục đích: Giảm thiểu rủi ro gian lận và nâng cao tính bảo mật trong việc trao đổi thẻ quà tặng. Sử dụng blockchain để minh bạch hóa và bảo mật quá trình phát hành và sử dụng thẻ.

Tóm lại: Địa chỉ trên blockchain không chỉ đóng vai trò như một công cụ để lưu trữ và chuyển nhượng tài sản mà còn hỗ trợ rất nhiều ứng dụng khác nhau từ tài chính phi tập trung (DeFi), trò chơi blockchain, cho đến các nền tảng quản lý danh tính và thẻ quà tặng. Việc sử dụng địa chỉ ví blockchain mở ra rất nhiều cơ hội cho việc phát triển và ứng dụng công nghệ blockchain trong đời sống thực tế, đồng thời giúp tạo ra các giao dịch an toàn, minh bạch và hiệu quả.

2.7. SỔ CÁI (LEDGE)

2.7.1. Khái niệm

Trong blockchain, **sổ cái (ledger)** là một cơ sở dữ liệu phân tán, liên tục được cập nhật và lưu trữ tất cả các giao dịch đã được xác thực trên mạng lưới blockchain. Khác với sổ cái truyền thống, sổ cái trong blockchain không được kiểm soát bởi một tổ chức trung gian, mà thay vào đó được duy trì và xác nhận bởi tất cả các nút (nodes) tham gia trong mạng lưới. Mỗi giao dịch trên blockchain sẽ được ghi nhận trong các khối (blocks) và liên kết với nhau thành một chuỗi (chain), tạo thành một

"sổ cái" công khai, không thể thay đổi, giúp đảm bảo tính toàn vẹn và bảo mật của các giao dịch.

2.7.2. Đặc điểm của Sổ Cái trong Blockchain?

1. Phân tán và không có trung gian:

Blockchain là một hệ thống phân tán, nghĩa là không có một cơ quan hoặc tổ chức trung gian nào kiểm soát sổ cái. Mỗi nút trong mạng đều có một bản sao của sổ cái, giúp tăng cường tính minh bạch và an toàn.

2. Không thể thay đổi (immutability):

Một khi giao dịch đã được ghi nhận và xác thực trong blockchain, nó không thể bị thay đổi hoặc xóa bỏ. Điều này đảm bảo tính toàn vẹn của dữ liệu và ngăn chặn các hành vi gian lận.

3. Công khai và minh bạch:

Sổ cái blockchain là công khai, có thể truy cập và kiểm tra bởi bất kỳ ai. Tuy nhiên, các thông tin nhạy cảm như danh tính của người tham gia giao dịch thường được bảo vệ thông qua các mã hóa và địa chỉ ví.

4. Bảo mật:

Sổ cái blockchain sử dụng các phương pháp mã hóa mạnh mẽ để bảo vệ dữ liệu khỏi bị thay đổi hoặc truy cập trái phép. Các giao dịch được xác nhận bởi các nút mạng thông qua các cơ chế đồng thuận như Proof of Work (PoW) hoặc Proof of Stake (PoS).

5. Tự động hóa và không cần sự tin cậy vào bên thứ ba:

Các giao dịch trên blockchain được xác thực và ghi nhận tự động mà không cần phải có sự tham gia của bên thứ ba trung gian, giúp giảm thiểu chi phí và rủi ro liên quan đến các bên trung gian.

2.7.3. Nguyên lý hoạt động của Sổ Cái trong Blockchain?

1. Giao dịch và khối:

Mỗi giao dịch trên blockchain được ghi nhận và xác nhận bởi các nút trong mạng lưới. Sau khi giao dịch được xác nhận, chúng sẽ được gom lại thành một "khối" (block) và được thêm vào sổ cái.

2. Cơ chế đồng thuận (Consensus Mechanism):

Các nút trong mạng lưới phải đạt được sự đồng thuận để chấp nhận một khối giao dịch mới. Các cơ chế đồng thuận phổ biến như Proof of Work (PoW), Proof of Stake (PoS) giúp đảm bảo rằng các giao dịch là hợp lệ và không có sự gian lận.

3. Xác thực và ghi nhận:

Sau khi đạt được đồng thuận, giao dịch trong khối sẽ được ghi nhận vào blockchain. Mỗi khối đều chứa một mã băm (hash) của khối trước đó, tạo ra một chuỗi liên kết chặt chẽ giữa các khối, giúp bảo vệ sự toàn vẹn của dữ liệu.

4. Chống gian lận và bảo mật:

Các giao dịch trong blockchain sử dụng mã hóa bất đối xứng để bảo vệ danh tính và các thông tin quan trọng. Một khi thông tin đã được ghi vào blockchain, nó không thể bị thay đổi mà không làm thay đổi tất cả các khối phía sau, điều này giúp bảo vệ khỏi các hành vi gian lận.

Tóm lại:Sổ cái trong blockchain là một hệ thống phân tán, bảo mật, và không thể thay đổi, giúp ghi nhận và lưu trữ tất cả các giao dịch trong mạng lưới. Với các đặc điểm như tính minh bạch, bảo mật, và không cần sự tin cậy vào bên trung gian, blockchain đã mang lại những lợi ích đáng kể trong nhiều lĩnh vực và mở ra các cơ hội mới cho các ứng dụng tài chính và phi tài chính.

2.8. CÁC LĨNH VỰC ỨNG DỤNG

Blockchain có nhiều lĩnh vực ứng dụng thực tiễn, bao gồm cả các ngành công nghiệp truyền thống lẫn các lĩnh vực công nghệ mới. Dưới đây là một số lĩnh vực cụ thể:

2.8.1. Tài chính và ngân hàng

Blockchain đã mang đến nhiều đột phá trong lĩnh vực tài chính và ngân hàng, giúp tối ưu hóa các quy trình, giảm chi phí và tăng tính minh bạch. Các lĩnh vực cụ thể như: thanh toán quốc tế, hợp đồng thông minh, quản lý tài sản, quản lý dữ liệu khách hàng, tự động hóa các quy trình bồi thường thông qua hợp đồng thông minh, …

Ví dụ: Bitcoin, Ethereum và các loại tiền điện tử khác sử dụng blockchain để cung cấp một phương thức thanh toán an toàn, nhanh chóng và không phụ thuộc vào ngân hàng trung gian. Ethereum**:** Cho phép xây dựng các hợp đồng thông minh để tự động xử lý khoản vay, bảo hiểm, hoặc phân bổ cổ tức.

2.8.2. Quản lý chuỗi cung ứng (Supply Chain Management)

Quản lý chuỗi cung ứng (Supply Chain Management - SCM) là một trong những lĩnh vực quan trọng và đang được cải thiện mạnh mẽ nhờ sự ứng dụng của công nghệ blockchain. Blockchain giúp cải thiện các vấn đề về minh bạch, bảo mật, hiệu quả và khả năng truy xuất trong quản lý chuỗi cung ứng. Dưới đây là một số ứng dụng của blockchain trong SC:

1. Tăng Cường Minh Bạch và Truy Xuất Nguồn Gốc

Blockchain giúp các doanh nghiệp theo dõi toàn bộ quá trình sản xuất và vận chuyển của sản phẩm từ nhà cung cấp đến người tiêu dùng cuối cùng. Với tính chất không thể thay đổi và minh bạch của blockchain, mọi giao dịch sẽ được ghi lại trên một cuốn sổ điện tử công khai và có thể kiểm tra được.

Ví dụ: *IBM Food Trust* là một nền tảng blockchain được sử dụng để theo dõi các sản phẩm thực phẩm từ trang trại đến bàn ăn của người tiêu dùng. Điều này giúp đảm bảo chất lượng sản phẩm, kiểm soát an toàn thực phẩm và hạn chế gian lận.

2. Giảm Chi Phí và Thời Gian Giao Dịch

Blockchain giúp giảm chi phí và thời gian giao dịch bằng cách loại bỏ các trung gian (ví dụ: ngân hàng, nhà cung cấp dịch vụ chứng thực) trong quá trình thanh toán và vận chuyển.

Ví dụ: *VeChain* là một công ty sử dụng blockchain để theo dõi và quản lý chuỗi cung ứng, đặc biệt trong các ngành công nghiệp như ô tô và thời trang. Blockchain giúp giảm chi phí hành chính và giảm thiểu sai sót.

3. Bảo Mật và Giảm Thiểu Gian Lận

Các giao dịch trong chuỗi cung ứng có thể bị gian lận hoặc giả mạo, nhưng với blockchain, mỗi giao dịch được xác nhận và lưu trữ một cách an toàn, không thể thay đổi. Điều này giúp ngăn chặn gian lận và đảm bảo tính trung thực của dữ liệu.

Ví dụ: *Everledger* là một công ty sử dụng blockchain để theo dõi và xác thực nguồn gốc của kim cương. Mỗi viên kim cương có một hồ sơ trên blockchain, giúp ngăn chặn việc trao đổi kim cương giả và xác nhận nguồn gốc hợp pháp.

4. Cải Thiện Quản Lý Hợp Đồng và Thanh Toán

Thông qua việc sử dụng hợp đồng thông minh (smart contracts), blockchain có thể tự động hóa quá trình thực hiện hợp đồng và thanh toán mà không cần sự can thiệp của bên thứ ba. Các hợp đồng này có thể tự động thực thi khi các điều kiện đã được đáp ứng.

Ví dụ: Một nhà sản xuất có thể thiết lập hợp đồng thông minh với các nhà cung cấp vật liệu, yêu cầu thanh toán khi hàng hóa được giao đủ số lượng và chất lượng. Blockchain sẽ ghi lại tất cả các bước và điều kiện, giúp tự động thực hiện các giao dịch mà không cần người kiểm soát trung gian.

5. Quản Lý Tồn Kho

Blockchain có thể giúp các doanh nghiệp dễ dàng theo dõi tình trạng tồn kho và điều phối nguồn lực, giúp giảm thiểu tình trạng thiếu hàng hoặc thừa hàng trong chuỗi cung ứng.

Ví dụ: Walmart sử dụng blockchain để theo dõi tình trạng tồn kho và lưu trữ dữ liệu về các sản phẩm trong kho. Việc này không chỉ giúp cải thiện quản lý tồn kho mà còn đảm bảo rằng mọi sản phẩm đều có thể được truy xuất nguồn gốc một cách dễ dàng và nhanh chóng.

6. Xác Minh Sản Phẩm và Chứng Nhận

Blockchain có thể hỗ trợ chứng nhận chất lượng sản phẩm, từ đó nâng cao niềm tin của người tiêu dùng. Các thông tin như tiêu chuẩn chất lượng, quy trình sản xuất, và thành phần sản phẩm sẽ được ghi lại trên blockchain.

Ví dụ: Các sản phẩm như cà phê, hạt cacao, hoặc sản phẩm hữu cơ có thể được xác minh nguồn gốc thông qua blockchain, giúp người tiêu dùng yên tâm rằng họ đang mua các sản phẩm đáp ứng tiêu chuẩn đạo đức và môi trường.

7. Hợp Tác Giữa Các Bên Liên Quan

Blockchain thúc đẩy sự hợp tác giữa các bên trong chuỗi cung ứng, tạo ra một hệ thống đồng thuận nơi mọi thông tin được chia sẻ một cách an toàn và minh bạch. Điều này giúp giảm rủi ro và tăng cường hiệu quả trong hoạt động của chuỗi cung ứng.

Ví dụ: *TradeLens*, một nền tảng blockchain do Maersk và IBM phát triển, giúp các công ty vận chuyển và cảng biển chia sẻ thông tin về các chuyến hàng một cách nhanh chóng và minh bạch, giảm thiểu thời gian chờ đợi và giảm chi phí.

Tóm lại: Blockchain giúp tối ưu hóa rất nhiều khía cạnh trong quản lý chuỗi cung ứng từ việc tăng cường minh bạch, bảo mật, giảm chi phí, đến việc tự động hóa và quản lý hợp đồng. Các công ty hiện nay đang ngày càng nhận thức rõ hơn về tiềm năng của công nghệ này trong việc tối ưu hóa các quy trình chuỗi cung ứng, tạo ra môi trường giao dịch an toàn và minh bạch hơn.

2.8.3. Quản trị và hợp đồng thông minh

Quản trị và hợp đồng thông minh (Smart Contracts) là một trong những ứng dụng nổi bật và quan trọng của blockchain, giúp tự động hóa các quy trình quản trị và thực thi hợp đồng mà không cần sự can thiệp của bên thứ ba. Dưới đây là một cái nhìn chi tiết về cách blockchain hỗ trợ quản trị và hợp đồng thông minh:

1. Quản Trị với Blockchain

Quản trị trong bối cảnh blockchain không chỉ đề cập đến việc quản lý các giao dịch mà còn là sự quản lý quy trình và quyết định trong các hệ thống phân tán. Các tổ chức và dự án có thể sử dụng blockchain để đảm bảo rằng các quyết định được đưa ra một cách minh bạch, công bằng và không bị can thiệp bởi bất kỳ ai.

Ví dụ: DAO (Decentralized Autonomous Organization): Là một tổ chức tự trị phi tập trung, nơi các quyết định quan trọng được thực hiện qua các cuộc bỏ phiếu do các thành viên tổ chức quyết định. Các quyết định này thường được thực hiện tự động thông qua hợp đồng thông minh.

2. Hợp Đồng Thông Minh (Smart Contracts)

Hợp đồng thông minh là các hợp đồng tự động thực thi khi các điều kiện đã được xác nhận. Thay vì phải thông qua các bên trung gian như luật sư hay ngân hàng để thực thi một hợp đồng, blockchain giúp tự động hóa mọi quy trình và giao dịch mà không cần sự can thiệp của con người.

Ví dụ ứng dụng hợp đồng thông minh:

Sử dụng trong tài chính (DeFi - Tài chính phi tập trung): Các hợp đồng thông minh trong lĩnh vực tài chính giúp thực hiện các giao dịch tự động như cho vay, vay, và giao dịch chứng khoán mà không cần sự tham gia của ngân hàng hay các tổ chức

tài chính truyền thống. Ví dụ như **Compound**, nơi người dùng có thể cho vay và vay tiền điện tử mà không cần thông qua một tổ chức tài chính trung gian.

Hợp đồng lao động và thanh toán: Các hợp đồng thông minh có thể tự động thanh toán cho nhân viên khi công việc đã hoàn thành hoặc khi các điều kiện hợp đồng được thực thi. Ví dụ, nếu một freelancer hoàn thành một nhiệm vụ, hợp đồng thông minh có thể tự động thanh toán cho họ ngay lập tức.

2.8.4. Sở hữu và sưu tầm tài sản Kỹ thuật số (NFT)

Sở hữu và sưu tầm tài sản kỹ thuật số (NFTs - Non-Fungible Tokens) là một trong những ứng dụng nổi bật của công nghệ blockchain, đặc biệt trong lĩnh vực nghệ thuật, giải trí, và các ngành công nghiệp sáng tạo. NFTs đã tạo ra một xu hướng mới trong việc mua, bán và sưu tầm tài sản kỹ thuật số với tính chất duy nhất và không thể thay thế.

Các ứng dụng của NFT trong sở hữu và sưu tầm tài sản kỹ thuật số:

1. Nghệ thuật số (Digital Art)

NFTs đã tạo ra một cuộc cách mạng trong lĩnh vực nghệ thuật, giúp các nghệ sĩ bán tác phẩm của mình dưới dạng kỹ thuật số và nhận được thanh toán trực tiếp mà không cần qua các nhà đấu giá hoặc các bên trung gian.

Ví dụ: Một trong những nghệ sĩ nổi tiếng nhất trong thế giới NFT là Beeple, người đã bán một tác phẩm nghệ thuật kỹ thuật số của mình, "Everydays: The First 5000 Days", với giá gần 70 triệu USD tại một buổi đấu giá của Christie's.

Ứng dụng: Mỗi tác phẩm nghệ thuật kỹ thuật số được mã hóa thành một NFT duy nhất, giúp người mua xác nhận quyền sở hữu và đảm bảo tính độc đáo của tác phẩm.

2. Sưu tầm và Vật phẩm Hiếm

NFTs cũng được sử dụng để sưu tầm các vật phẩm kỹ thuật số hiếm, chẳng hạn như thẻ giao dịch thể thao, vật phẩm trong game, hay thậm chí các video, âm nhạc, và các tác phẩm sáng tạo khác.

Ví dụ: CryptoKitties là một trong những trò chơi sưu tầm NFT nổi tiếng, nơi người chơi có thể mua, bán và lai tạo những con mèo kỹ thuật số độc đáo. Mỗi con mèo là một NFT duy nhất.

Ứng dụng: Các vật phẩm trong trò chơi như skin, nhân vật, hay vũ khí cũng có thể được mã hóa thành NFT, giúp người chơi sở hữu và giao dịch chúng.

3. Sự kiện và Vé Sự Kiện

NFT có thể được sử dụng để tạo ra vé sự kiện kỹ thuật số, chẳng hạn như vé hòa nhạc, các sự kiện thể thao, hoặc các buổi hòa nhạc trực tuyến.

Ví dụ: Nifty Gateway là một nền tảng cho phép bán vé NFT cho các sự kiện nghệ thuật trực tuyến và các buổi hòa nhạc ảo.

Ứng dụng: Mỗi vé NFT có thể chứa thông tin về sự kiện, bao gồm ngày, giờ, địa điểm, và thậm chí quyền lợi đặc biệt, và không thể bị làm giả.

4. Thế giới ảo và Metaverse

NFTs đóng một vai trò quan trọng trong các thế giới ảo và Metaverse, nơi người dùng có thể sở hữu đất đai, vật phẩm, hoặc các tài sản kỹ thuật số khác trong một không gian ảo.

Ví dụ: Trong các thế giới như Decentraland hoặc Sandbox, người dùng có thể mua và sở hữu đất ảo dưới dạng NFT, xây dựng các dự án và giao dịch chúng.

Ứng dụng: NFTs cung cấp chứng nhận quyền sở hữu tài sản ảo trong các môi trường 3D, giúp người dùng tạo dựng tài sản và giá trị trong Metaverse.

2.8.5. Ứng dụng trong Y tế

Blockchain ứng dụng trong y tế là một lĩnh vực đang ngày càng nhận được sự quan tâm và phát triển, nhờ vào khả năng bảo mật, minh bạch và khả năng xử lý dữ liệu hiệu quả của công nghệ này. Blockchain có thể giúp cải thiện nhiều khía cạnh trong ngành y tế, từ việc quản lý dữ liệu bệnh nhân đến cải thiện quy trình thanh toán và bảo hiểm.

1. Quản lý và chia sẻ dữ liệu bệnh nhân

Blockchain có thể giúp cải thiện việc quản lý và chia sẻ dữ liệu bệnh nhân, đảm bảo rằng thông tin bệnh nhân được bảo vệ, minh bạch và dễ dàng truy cập khi cần thiết. Các dữ liệu như hồ sơ y tế, kết quả xét nghiệm, và thông tin điều trị có thể được lưu trữ một cách an toàn trên blockchain.

Minh bạch và bảo mật: Dữ liệu được lưu trữ trên blockchain không thể thay đổi hoặc xóa bỏ, giúp bảo vệ sự toàn vẹn của thông tin bệnh nhân. Chỉ những người có quyền truy cập mới có thể xem hoặc thay đổi dữ liệu.

Chia sẻ thông tin nhanh chóng và dễ dàng: Các bệnh viện, phòng khám và bác sĩ có thể chia sẻ thông tin với nhau một cách nhanh chóng và bảo mật mà không cần qua các hệ thống trung gian phức tạp.

Ví dụ: Dự án MedRec là một nền tảng dựa trên blockchain cho phép bệnh nhân kiểm soát hồ sơ y tế của mình, đồng thời cho phép bác sĩ và các cơ sở y tế khác dễ dàng truy cập thông tin khi cần thiết, giúp giảm thiểu sai sót và cải thiện chăm sóc sức khỏe.

2. An toàn và bảo mật thông tin y tế

Thông tin y tế là một trong những loại dữ liệu nhạy cảm nhất và thường xuyên là mục tiêu của các cuộc tấn công mạng. Blockchain có thể cung cấp một giải pháp bảo mật mạnh mẽ, đảm bảo rằng dữ liệu bệnh nhân được lưu trữ an toàn và chỉ có những người được phép mới có quyền truy cập.

Chống gian lận và truy xuất nguồn gốc: Blockchain có khả năng ghi lại tất cả các giao dịch và thay đổi, giúp dễ dàng theo dõi và xác minh các thay đổi đối với hồ sơ y tế, ngăn chặn gian lận và đảm bảo tính chính xác của dữ liệu.

Ví dụ: Các nền tảng như Healthereum sử dụng blockchain để bảo mật thông tin bệnh nhân và theo dõi việc tham gia vào các chương trình y tế, giúp đảm bảo rằng tất cả các hành động đều minh bạch và không thể thay đổi.

3. Quản lý dược phẩm và chuỗi cung ứng thuốc

Blockchain có thể giúp theo dõi và quản lý chuỗi cung ứng thuốc, từ khi sản xuất đến khi đến tay người tiêu dùng. Việc theo dõi này có thể giúp ngăn chặn thuốc giả, đảm bảo chất lượng và tính hợp pháp của thuốc.

Ngăn chặn thuốc giả: Các thông tin về nguồn gốc của thuốc và quá trình vận chuyển có thể được ghi lại trên blockchain, giúp đảm bảo rằng thuốc không bị giả mạo hoặc bị can thiệp trong quá trình vận chuyển.

Theo dõi thuốc và thiết bị y tế: Blockchain giúp theo dõi tình trạng thuốc và thiết bị y tế từ khi sản xuất đến khi sử dụng, đảm bảo rằng các sản phẩm luôn ở trong tình trạng tốt nhất.

Ví dụ: Modum sử dụng blockchain để theo dõi các sản phẩm dược phẩm và đảm bảo rằng các điều kiện lưu trữ được đáp ứng trong suốt quá trình vận chuyển.

4. Thanh toán và bảo hiểm y tế

Blockchain có thể cải thiện quy trình thanh toán và xử lý bảo hiểm y tế, giúp giảm chi phí, thời gian xử lý và tăng cường sự minh bạch trong các giao dịch này. Blockchain có thể hỗ trợ các hợp đồng thông minh (smart contracts) để tự động hóa các quy trình này.

Tự động hóa thanh toán: Các hợp đồng thông minh có thể tự động xử lý các khoản thanh toán giữa bệnh nhân, nhà cung cấp dịch vụ y tế và công ty bảo hiểm, giúp giảm thiểu sai sót và gian lận.

Quy trình bảo hiểm nhanh chóng và chính xác: Các công ty bảo hiểm có thể sử dụng blockchain để lưu trữ và truy xuất thông tin bệnh nhân, giúp quá trình thanh toán yêu cầu bảo hiểm trở nên nhanh chóng và chính xác hơn.

Ví dụ: Solve.Care là một nền tảng sử dụng blockchain để quản lý các dịch vụ chăm sóc sức khỏe và bảo hiểm y tế, giúp tự động hóa quá trình thanh toán và giảm thiểu chi phí hành chính.

5. Quản lý quyền sở hữu và chia sẻ thông tin gen di truyền

Với sự phát triển của y học chính xác, việc chia sẻ và quản lý thông tin gen di truyền trở nên rất quan trọng. Blockchain có thể giúp bảo vệ thông tin này và đảm bảo quyền sở hữu và quyền riêng tư cho các cá nhân.

Bảo vệ quyền riêng tư: Blockchain có thể giúp bệnh nhân kiểm soát quyền truy cập vào thông tin gen của họ và quyết định ai có thể xem hoặc sử dụng dữ liệu gen này cho mục đích nghiên cứu hoặc điều trị.

Ví dụ: Nebula Genomics sử dụng blockchain để bảo mật dữ liệu gen của người dùng và cung cấp cho họ quyền kiểm soát dữ liệu của mình.

2.8.6. Bầu cử và Quản lý chính phủ

Ứng dụng blockchain trong bầu cử và quản lý chính phủ đang trở thành một chủ đề được quan tâm mạnh mẽ, nhờ vào khả năng cải thiện tính minh bạch, bảo mật, và hiệu quả của các quy trình chính trị và hành chính. Blockchain có thể giúp các quốc gia và chính phủ thực hiện các cuộc bầu cử công bằng, bảo mật và minh bạch hơn, đồng thời quản lý các hệ thống công cộng hiệu quả hơn.

1. Bầu cử và bỏ phiếu điện tử (e-Voting)

Blockchain có thể giúp cải thiện quy trình bầu cử và bỏ phiếu điện tử bằng cách cung cấp một hệ thống an toàn và minh bạch cho việc ghi nhận và xác minh phiếu bầu.

Bảo mật và chống gian lận: Mỗi lá phiếu có thể được mã hóa thành một transaction (giao dịch) và lưu trữ trên blockchain, giúp bảo vệ dữ liệu khỏi bị thay đổi hoặc xóa bỏ. Điều này ngăn ngừa các hành vi gian lận như việc thay đổi phiếu bầu hoặc giả mạo kết quả bầu cử.

Minh bạch và công khai: Mọi thông tin về phiếu bầu và kết quả sẽ được ghi lại trên blockchain, giúp mọi người có thể kiểm tra và xác minh kết quả mà không cần phụ thuộc vào một bên thứ ba. Blockchain đảm bảo tính minh bạch và chính xác trong toàn bộ quá trình.

Bỏ phiếu từ xa: Blockchain có thể giúp triển khai hệ thống bỏ phiếu từ xa, cho phép cử tri bỏ phiếu từ bất kỳ đâu mà không phải đến các điểm bỏ phiếu truyền thống. Điều này đặc biệt hữu ích trong các cuộc bầu cử toàn cầu, nơi cử tri có thể bỏ phiếu từ nước ngoài.

Ví dụ: Dự án Voatz là một nền tảng bỏ phiếu điện tử dựa trên blockchain đã được thử nghiệm trong một số cuộc bầu cử ở Mỹ, cho phép người dân bỏ phiếu qua ứng dụng di động với mức độ bảo mật cao.

2. Quản lý hồ sơ công dân và giấy tờ điện tử

Blockchain có thể được sử dụng để quản lý hồ sơ công dân, giấy tờ điện tử và các thông tin quan trọng khác mà chính phủ lưu trữ. Điều này giúp cải thiện tính minh bạch, bảo mật và giảm thiểu sự giả mạo dữ liệu.

Hồ sơ công dân an toàn: Các hồ sơ công dân như giấy khai sinh, chứng minh nhân dân, hộ khẩu, hay thông tin thuế có thể được lưu trữ trên blockchain, giúp bảo vệ thông tin cá nhân khỏi bị làm giả hoặc mất mát.

Giảm thiểu thủ tục hành chính: Chính phủ có thể giảm thiểu các thủ tục hành chính phức tạp và tiết kiệm thời gian cho người dân bằng cách sử dụng blockchain để tự động hóa các quy trình liên quan đến việc cấp phát các giấy tờ hoặc chứng nhận.

Ví dụ: **Estonia** là quốc gia tiên phong trong việc sử dụng blockchain cho các dịch vụ công cộng, bao gồm việc cấp thẻ căn cước điện tử, quản lý hồ sơ công dân và các dịch vụ y tế.

3. Quản lý ngân sách và tài chính công

Blockchain có thể giúp cải thiện quy trình quản lý ngân sách và tài chính công của chính phủ, từ việc theo dõi thu chi đến việc phân phối ngân sách.

Minh bạch trong chi tiêu công: Blockchain giúp theo dõi mọi khoản chi tiêu của chính phủ, giúp người dân và các tổ chức giám sát việc sử dụng ngân sách công một cách minh bạch và chính xác.

Giảm thiểu tham nhũng: Blockchain đảm bảo rằng mọi giao dịch tài chính công đều được ghi lại một cách rõ ràng và không thể thay đổi, từ đó giảm thiểu khả năng tham nhũng và lạm dụng quyền lực trong việc phân phối ngân sách.

Ví dụ: Các quốc gia như Georgia đã sử dụng blockchain trong việc quản lý đất đai và tài chính công để tăng cường tính minh bạch và giảm thiểu tham nhũng.

4. Hợp đồng thông minh (Smart Contracts) trong quản lý chính phủ

Hợp đồng thông minh có thể được sử dụng trong các quy trình hành chính và pháp lý của chính phủ, giúp tự động hóa việc thực thi các hợp đồng mà không cần đến sự can thiệp của bên thứ ba.

Tự động hóa quy trình pháp lý: Các hợp đồng thông minh có thể tự động thực thi các điều khoản trong hợp đồng mà không cần sự can thiệp của luật sư hay tổ chức trung gian. Điều này giúp tiết kiệm chi phí và thời gian cho các quy trình pháp lý.

Chuyển nhượng tài sản công: Blockchain và hợp đồng thông minh có thể hỗ trợ việc chuyển nhượng tài sản công một cách nhanh chóng và hiệu quả. Ví dụ, khi một công dân mua tài sản công hoặc tham gia các chương trình nhà ở xã hội, hợp đồng thông minh có thể tự động xử lý các điều khoản hợp đồng mà không cần phải qua các thủ tục phức tạp.

Ví dụ: Ukraine đã thử nghiệm sử dụng hợp đồng thông minh để tự động hóa quy trình cấp giấy chứng nhận quyền sở hữu đất đai.

5. Quản lý quyền sở hữu và phân phối tài sản công

Blockchain có thể giúp quản lý quyền sở hữu các tài sản công, chẳng hạn như đất đai, tài nguyên thiên nhiên và các tài sản quốc gia khác. Nó giúp xác định rõ quyền sở hữu, tránh tranh chấp và cung cấp một hệ thống phân phối tài sản công minh bạch.

Quản lý tài nguyên thiên nhiên: Blockchain có thể giúp chính phủ theo dõi việc khai thác tài nguyên thiên nhiên và đảm bảo rằng việc phân phối tài nguyên này là hợp pháp và công bằng.

Quản lý đất đai: Các hồ sơ đất đai có thể được lưu trữ trên blockchain, giúp giảm thiểu tình trạng tranh chấp quyền sở hữu đất và đảm bảo tính minh bạch trong việc giao dịch đất đai.

Ví dụ: Ghana và Rwanda là hai quốc gia đã bắt đầu triển khai blockchain trong việc quản lý quyền sở hữu đất đai, giúp giảm thiểu tranh chấp và tăng cường tính minh bạch trong giao dịch đất đai.

6. Chống tham nhũng và tăng cường tính minh bạch

Blockchain có thể giúp tăng cường tính minh bạch trong hoạt động của chính phủ và giảm thiểu tham nhũng.

Giám sát tài chính: Các khoản chi tiêu công có thể được theo dõi trực tiếp trên blockchain, giúp người dân và các tổ chức giám sát chính phủ trong việc sử dụng ngân sách.

Giám sát các quyết định chính trị: Các quyết định của các quan chức chính phủ có thể được ghi lại trên blockchain, đảm bảo rằng các quyết định được đưa ra là công khai và minh bạch.

Ví dụ: Sierra Leone đã thử nghiệm sử dụng blockchain để theo dõi và giám sát các cuộc bầu cử của họ, giúp đảm bảo tính minh bạch và công bằng.

Tóm lại, *Ứng dụng blockchain trong bầu cử và quản lý chính phủ có thể giúp cải thiện tính minh bạch, bảo mật và hiệu quả của các quy trình chính trị và hành chính. Mặc dù blockchain mang lại nhiều lợi ích đáng kể, nhưng việc triển khai công nghệ này vẫn gặp phải một số thách thức, bao gồm sự thay đổi trong cơ cấu tổ chức, vấn đề về pháp lý và bảo mật, và việc đảm bảo sự chấp nhận của người dân. Tuy nhiên, với những lợi ích mà blockchain mang lại, các quốc gia có thể tận dụng công nghệ này để xây dựng một hệ thống chính phủ minh bạch và công bằng hơn.*

2.8.7. Bảo mật và quyền sở hữu dữ liệu

Ứng dụng blockchain trong bảo mật và quyền sở hữu dữ liệu là một trong những lĩnh vực quan trọng, khi công nghệ blockchain có thể giải quyết các vấn đề về bảo mật, quyền riêng tư và kiểm soát dữ liệu trong một thế giới ngày càng số hóa. Blockchain giúp người dùng kiểm soát dữ liệu cá nhân của mình, đảm bảo rằng thông tin không bị thay đổi, sao chép hay truy cập trái phép.

1. Bảo mật dữ liệu cá nhân và quyền riêng tư

Blockchain giúp bảo vệ dữ liệu cá nhân của người dùng bằng cách lưu trữ thông tin trong một mạng lưới phân tán, nơi không có một cơ sở dữ liệu trung tâm duy nhất, điều này giúp giảm thiểu rủi ro bị tấn công hoặc xâm phạm.

Mã hóa dữ liệu: Blockchain sử dụng các phương pháp mã hóa mạnh mẽ để đảm bảo rằng dữ liệu chỉ có thể được truy cập bởi người có quyền. Khi thông tin được lưu trữ trên blockchain, nó được phân mảnh và mã hóa, khiến cho việc truy cập trái phép trở nên rất khó khăn.

Kiểm soát quyền truy cập: Người dùng có thể tự quyết định ai có quyền truy cập vào dữ liệu của mình thông qua việc sử dụng khóa riêng và công nghệ mã hóa. Điều này giúp họ giữ quyền kiểm soát và bảo vệ dữ liệu cá nhân khỏi sự xâm phạm của các bên thứ ba.

Ví dụ: **SelfKey** là một nền tảng cho phép người dùng kiểm soát quyền sở hữu và truy cập thông tin cá nhân của mình. Thông qua blockchain, người dùng có thể chia sẻ hoặc giữ lại dữ liệu của mình mà không cần dựa vào các tổ chức trung gian.

2. Quản lý quyền sở hữu tài sản dữ liệu

Blockchain có thể cung cấp một cách thức để chứng nhận quyền sở hữu đối với tài sản số, bao gồm dữ liệu, tệp tin, hình ảnh, video, và các tài nguyên kỹ thuật số khác. Thông qua blockchain, người dùng có thể xác minh quyền sở hữu và bảo vệ tài sản số của mình.

Chứng nhận quyền sở hữu dữ liệu: Blockchain giúp ghi lại quyền sở hữu tài sản số bằng cách mã hóa tài sản dưới dạng token và lưu trữ nó trên một blockchain. Mỗi tài sản sẽ có một mã nhận dạng duy nhất và không thể thay đổi, giúp xác định ai là chủ sở hữu của tài sản.

Quản lý bản quyền và quyền sử dụng: Blockchain có thể giúp các tổ chức và cá nhân quản lý quyền bản quyền của các tài sản kỹ thuật số. Hợp đồng thông minh (smart contracts) có thể tự động xác nhận và thực thi các thỏa thuận về quyền sử dụng, phân phối và trả phí cho việc sử dụng tài sản.

Ví dụ: Filecoin là một dự án sử dụng blockchain để tạo ra một nền tảng lưu trữ phi tập trung, nơi người dùng có thể lưu trữ và truy cập dữ liệu trong khi duy trì quyền sở hữu và bảo mật thông tin.

3. Quản lý quyền sở hữu trong các ngành công nghiệp sáng tạo

Blockchain có thể giúp bảo vệ quyền sở hữu trí tuệ trong các ngành công nghiệp sáng tạo như âm nhạc, nghệ thuật số, phim ảnh, và văn học. Thông qua blockchain, các nghệ sĩ và tác giả có thể chứng nhận quyền sở hữu và kiểm soát việc sử dụng tác phẩm của họ.

Chứng nhận quyền sở hữu tác phẩm: Các tác phẩm nghệ thuật số, âm nhạc, video và các sản phẩm sáng tạo khác có thể được mã hóa thành các token NFT (Non-Fungible Token) trên blockchain, giúp xác minh quyền sở hữu và giúp các nghệ sĩ nhận được lợi nhuận từ việc bán và chuyển nhượng tác phẩm.

Quản lý bản quyền: Các hợp đồng thông minh có thể tự động thực thi các điều khoản bản quyền, giúp các nghệ sĩ và tác giả quản lý và bảo vệ quyền lợi của mình.

Ví dụ: Audius là một nền tảng âm nhạc phi tập trung, nơi các nghệ sĩ có thể đăng tải và quản lý nhạc của mình, bảo vệ quyền sở hữu và nhận thù lao trực tiếp từ người nghe.

Tóm lại, Ứng dụng blockchain trong bảo mật và quyền sở hữu dữ liệu mở ra một tương lai sáng lạn cho việc quản lý và bảo vệ dữ liệu trong nhiều lĩnh vực khác nhau, từ y tế, tài chính, đến ngành công nghiệp sáng tạo. Blockchain không chỉ giúp bảo mật và bảo vệ quyền riêng tư mà còn giúp người dùng duy trì quyền kiểm soát đối với dữ liệu của chính mình. Với những lợi ích này, blockchain đang dần trở thành công cụ quan trọng trong việc giải quyết các vấn đề về bảo mật và quyền sở hữu dữ liệu trong kỷ nguyên số.

CÂU HỎI VÀ BÀI TẬP

1. Blockchain là gì? Hãy giải thích ngắn gọn khái niệm này.
2. Nêu các đặc điểm quan trọng của blockchain và giải thích tại sao tính bất biến là yếu tố quan trọng nhất.
3. Thuật toán đồng thuận là gì? So sánh PoW và PoS.
4. Hợp đồng thông minh là gì? Cho một ví dụ về ứng dụng của nó.
5. Mô tả cách các khối (blocks) liên kết với nhau trong blockchain.
6. Ai là người đã phát triển giao thức Paxos, đặt nền móng cho các cơ chế đồng thuận trong mạng máy tính?
   a. Satoshi Nakamoto
   b. Leslie Lamport
   c. Stuart Haber
   d. David Chaum
7. Năm nào bài báo "Bitcoin: A Peer-to-Peer Electronic Cash System" được xuất bản?
   a. 1991
   b. 2008
   c. 2009
   d. 2016
8. Đặc điểm nào dưới đây không thuộc tính chất của công nghệ blockchain?
   a. Sổ cái chỉ cho phép ghi thêm (Ledger)
   b. Bảo mật bằng mật mã (Secure)
   c. Tập trung hóa quản lý
   d. Phân tán và chia sẻ thông tin
9. Ứng dụng blockchain đầu tiên là gì?
   a. Ethereum
   b. Bitcoin
   c. NFT
   d. Hashcash
10. Blockchain chính thức được giới thiệu với công chúng vào năm nào?
    a. 1989
    b. 1991
    c. 2009
    d. 2016
11. So sánh sự khác biệt cơ bản giữa blockchain công khai và blockchain riêng tư.
12. Blockchain lai có thể được ứng dụng vào lĩnh vực bất động sản như thế nào? Đưa ra một ví dụ minh họa.

13. Vì sao blockchain liên minh được xem là một giải pháp kết hợp giữa blockchain công khai và riêng tư?

14. Hãy giải thích tại sao việc một tổ chức khởi tạo blockchain công khai ngừng hoạt động không làm ảnh hưởng đến sự vận hành của mạng.

15. Theo bạn, nhược điểm "kém minh bạch" của blockchain liên minh có ảnh hưởng như thế nào đến các ứng dụng trong thực tế?

16. Tiền mã hóa là gì?

17. Tiền mã hóa hoạt động như thế nào?

18. Kể tên một số loại tiền mã hóa phổ biến.

19. Phân biệt tiền mã hóa và tiền fiat.
    Hãy trình bày sự khác biệt giữa tiền mã hóa và tiền fiat, đặc biệt là trong các yếu tố như cơ chế phát hành, kiểm soát và tính thanh khoản.

20. Phân tích cách mà công nghệ blockchain đảm bảo tính bảo mật cho giao dịch tiền mã hóa.
    Hãy giải thích các cơ chế bảo mật mà blockchain sử dụng để bảo vệ các giao dịch tiền mã hóa, bao gồm vai trò của mật mã học, cơ chế đồng thuận, và cấu trúc phân tán.

21. Nghiên cứu các ứng dụng của tiền mã hóa trong các ngành khác nhau.
    Chọn một ứng dụng cụ thể của tiền mã hóa (ví dụ: tài chính phi tập trung - DeFi) và nghiên cứu cách nó ảnh hưởng đến ngành đó. Trình bày một ví dụ thực tế về việc sử dụng tiền mã hóa trong ứng dụng này.

22. Tokenomics là gì?
Giải thích một cách đơn giản về tokenomics và tầm quan trọng của nó trong hệ sinh thái blockchain.

23. So sánh sự khác biệt giữa kinh tế token (tokenomics) và kinh tế truyền thống?
Hãy giải thích những điểm khác biệt chính giữa việc sử dụng tiền tệ trong nền kinh tế truyền thống và sử dụng token trong blockchain.

24. Bitcoin có một số đặc điểm quan trọng trong tokenomics. Bạn có thể liệt kê và giải thích các đặc điểm này không?
Đưa ra các yếu tố chính trong tokenomics của Bitcoin và cách chúng ảnh hưởng đến giá trị của Bitcoin.

25. Lý do tại sao việc dự đoán số lượng token đang lưu hành là quan trọng trong các dự án blockchain?
Phân tích tầm quan trọng của việc kiểm soát số lượng token và kế hoạch phân phối token trong các dự án tiền mã hóa.

26. NFT là gì?

Giải thích khái niệm NFT và sự khác biệt giữa NFT và các tài sản có thể thay thế như tiền điện tử.

27. Tại sao NFT lại quan trọng đối với nghệ sĩ và người sáng tạo nội dung?
Hãy giải thích tầm quan trọng của NFT đối với nghệ sĩ và người sáng tạo nội dung trong việc xác thực quyền sở hữu và tạo ra giá trị cho các tác phẩm kỹ thuật số.

28. NFT không thể chia nhỏ, tại sao lại có một số nền tảng giới thiệu quyền sở hữu một phần?
Phân tích lý do tại sao việc chia nhỏ NFT thành các phần nhỏ hơn lại trở thành xu hướng mới, và nền tảng Fractional đã giúp gì cho thị trường NFT.

29. Hãy nêu ví dụ về một dự án NFT trên nền tảng Cardano và cách nó đã phát triển hệ sinh thái NFT trên Cardano.
Giới thiệu về dự án NFT đầu tiên trên nền tảng Cardano và những tác động của nó đối với sự phát triển của hệ sinh thái NFT trên Cardano.

30. NFT phụ thuộc vào yếu tố nào để giá trị của chúng tăng theo thời gian?
Phân tích yếu tố cung và cầu ảnh hưởng như thế nào đến giá trị của NFT trong thị trường đầu tư.

31. NFT là gì?
Giải thích khái niệm NFT và sự khác biệt giữa NFT và các tài sản có thể thay thế như tiền điện tử.

32. Tại sao NFT lại quan trọng đối với nghệ sĩ và người sáng tạo nội dung?
Hãy giải thích tầm quan trọng của NFT đối với nghệ sĩ và người sáng tạo nội dung trong việc xác thực quyền sở hữu và tạo ra giá trị cho các tác phẩm kỹ thuật số.

33. NFT không thể chia nhỏ, tại sao lại có một số nền tảng giới thiệu quyền sở hữu một phần?
Phân tích lý do tại sao việc chia nhỏ NFT thành các phần nhỏ hơn lại trở thành xu hướng mới, và nền tảng Fractional đã giúp gì cho thị trường NFT.

34. Hãy nêu ví dụ về một dự án NFT trên nền tảng Cardano và cách nó đã phát triển hệ sinh thái NFT trên Cardano.
Giới thiệu về dự án NFT đầu tiên trên nền tảng Cardano và những tác động của nó đối với sự phát triển của hệ sinh thái NFT trên Cardano.

35. NFT phụ thuộc vào yếu tố nào để giá trị của chúng tăng theo thời gian?
Phân tích yếu tố cung và cầu ảnh hưởng như thế nào đến giá trị của NFT trong thị trường đầu tư.

36. Thách thức lớn nhất của NFT trong thị trường hiện tại là gì? a) Tính bất ổn của thị trường
b) Tính bảo mật của blockchain
c) Giá trị nghệ thuật của NFT
d) Khả năng xác thực danh tính

37. Tại sao phí giao dịch cao lại là một thách thức lớn đối với người dùng NFT?
a) Phí giao dịch cao chỉ ảnh hưởng đến người bán
b) Phí giao dịch làm giảm lợi nhuận từ việc đầu tư vào NFT

c) Phí giao dịch làm giảm sự tham gia của người tiêu dùng và tạo ra rào cản đầu vào
d) Phí giao dịch không ảnh hưởng đến sự phát triển của NFT

38. NFT có thể giúp nghệ sĩ trong việc bảo vệ bản quyền của tác phẩm như thế nào? a) Bằng cách cho phép nghệ sĩ sao chép tác phẩm của mình dưới dạng NFT
b) Bằng cách giúp nghệ sĩ nhận doanh thu trực tiếp từ việc bán NFT
c) Bằng cách cho phép nghệ sĩ bán tác phẩm qua các công ty lớn
d) Bằng cách giảm giá trị tác phẩm nghệ thuật gốc

39. Ví trong blockchain là gì? Giải thích tầm quan trọng của ví đối với người dùng tiền mã hóa.

40. Phân biệt các loại ví phần mềm, ví cứng, ví trực tuyến và ví giấy. Nêu ưu nhược điểm của từng loại ví.

41. Khóa công khai và khóa riêng trong ví có vai trò như thế nào trong việc bảo mật tài sản kỹ thuật số?

42. Ví tiền mã hóa có ảnh hưởng gì đến việc giao dịch và quản lý tài sản số như tiền mã hóa hoặc NFT?

43. Hãy giải thích nguyên lý hoạt động của ví trong thế giới blockchain, đặc biệt trong việc ký giao dịch và bảo mật tài sản.

44. Liệt kê các biện pháp bảo mật mà ví sử dụng để bảo vệ tài sản của người dùng.

45. Những vấn đề bảo mật và rủi ro phổ biến mà người dùng ví cần lưu ý khi sử dụng ví kỹ thuật số?

46. Tại sao địa chỉ trên blockchain lại quan trọng đối với giao dịch tiền mã hóa?

47. Hợp đồng thông minh có thể sử dụng địa chỉ ví blockchain như thế nào để tự động thực hiện các hành động?

48. Trong hệ sinh thái NFT, địa chỉ ví có vai trò gì trong việc chuyển nhượng tài sản?

49. Làm thế nào blockchain có thể giúp quản lý và lưu trữ các tài sản kỹ thuật số ngoài tiền mã hóa?

50. Ứng dụng của địa chỉ trên blockchain trong các DApp là gì và nó mang lại lợi ích gì cho người dùng?

51. Những ứng dụng nào có thể sử dụng blockchain để quản lý danh tính cá nhân và bảo vệ quyền riêng tư?

52. Microtransactions trên blockchain được thực hiện như thế nào và tại sao chúng lại có chi phí thấp?

53. Chức năng của địa chỉ ví blockchain trong việc tạo và quản lý thẻ quà tặng là gì?

54. Sổ cái trong blockchain khác với sổ cái truyền thống như thế nào?

55. Tại sao blockchain không cần một tổ chức trung gian để duy trì sổ cái?

56. Giải thích khái niệm "immutability" trong blockchain và tại sao nó quan trọng đối với tính bảo mật của giao dịch?

57. Những đặc điểm nào của sổ cái blockchain giúp tăng cường tính minh bạch và bảo mật?

58. Cơ chế đồng thuận như Proof of Work (PoW) hoặc Proof of Stake (PoS) hoạt động như thế nào trong việc xác nhận các giao dịch trên blockchain?

59. Mô tả quy trình ghi nhận và xác thực giao dịch trong blockchain.

60. Blockchain sử dụng mã hóa bất đối xứng để bảo vệ giao dịch như thế nào?

61. Tại sao việc không thể thay đổi dữ liệu trong blockchain lại giúp bảo vệ khỏi gian lận?

62. Giải thích các lợi ích mà sổ cái blockchain mang lại cho các ứng dụng tài chính và phi tài chính.

TÀI LIỆU THAM KHẢO

1. https://www.pcmag.com - *By Rob Marvin*
2. https://www.techtarget.com - by *Ron Karjian and Robert Sheldon*
3. https://www.kaspersky.com -
4. https://www.coinbase.com -
5. https://www.businessinsider.com -
6. https://www.techtarget.com -
7. https://academy.binance.com -
8. https://www.researchgate.net
9. https://cointelegraph.com - by Guneet kaur
10. https://coin68.com - by Phong – Update 04/2023
11. https://www.gao.gov/assets/gao-19-704sp.pdf - GAO-19-704SP Blockchain & Distributed Ledger Technologies