Ethereum Network

ONE LOVE. ONE FUTURE.

Introduce to Ethereum Network

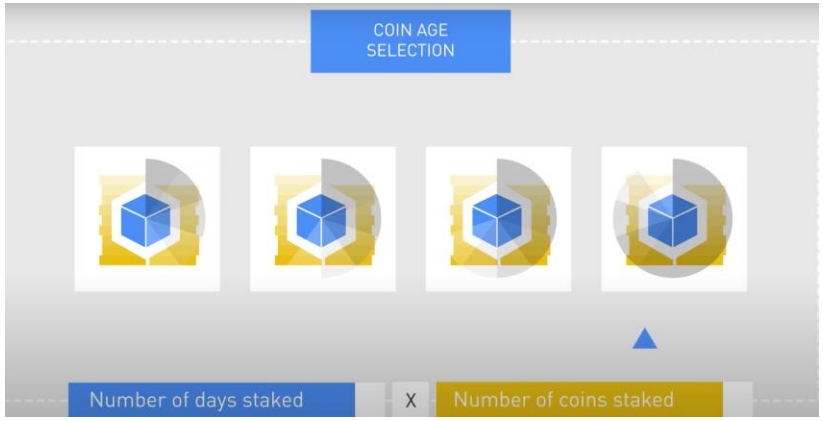
- Ethereum là một nền tảng blockchain phi tập trung, cho phép xây dựng các ứng dụng và tổ chức mà không cần cấp phép và chống kiểm duyệt.
- Nền tảng này nhúng một Máy ảo Ethereum (EVM) mà tất cả các nút trên mạng đều đồng ý về trạng thái của nó.
- Mỗi nút giữ bản sao của EVM và có thể phát yêu cầu tính toán, được gọi là giao dịch, để thay đổi trạng thái của EVM.
- Các giao dịch sau khi được xác minh sẽ được lưu trữ vĩnh viễn trên blockchain, đảm bảo tính toàn vẹn và an toàn nhờ cơ chế mã hóa.
- Turing – Complete: cho phép xây dựng dapp
- Đơn vị tiền tệ: ETHER, wei, gwei

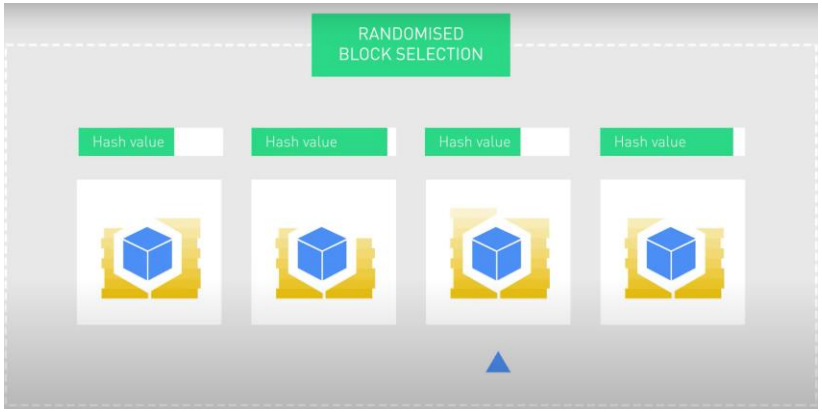
Cơ chế đồng thuận

- **Cơ chế đồng thuận**: Đây là một tập hợp các giao thức, động cơ, và ý tưởng giúp các nút trong mạng blockchain đồng ý về trạng thái của sổ cái.
- Proof – of – Work
- Proof – of – Stake

How does it work?

- "Block" một lượng tiền nhất định (32 ETH) vào mạng lưới dưới dạng cổ phần
- Để không ưu tiên các node "giàu" => Hai phương pháp phổ biến nhất:
- 1. Lựa chọn Khối Ngẫu nhiên (Randomized Block Selection)
- 2. Lựa chọn Tuổi Tiền (Coin Age Selection).





Xác thực

- Khi một nút được chọn để validate khối tiếp theo, nó sẽ kiểm tra xem các giao dịch trong khối có hợp lệ hay không.
- Sau đó, nó sẽ ký khối và thêm nó vào blockchain. Nút này nhận được phí giao dịch từ khối và, trong một số blockchain, phần thưởng bằng coin.
- Nếu một nút muốn ngừng forged, cổ phần và phần thưởng kiếm được của nó sẽ được giải phóng sau một thời gian nhất định, cho phép mạng lưới xác minh rằng không có khối gian lận nào được thêm vào blockchain bởi nút đó.

Một số Blockchain sử dụng PoS

1. BNB Chain
2. BNB Smart Chain
3. Solana
4. Avalanche
5. Polkadot

Ưu điểm PoS

Proof of Stake (PoS) có nhiều ưu điểm so với Proof of Work (PoW), khiến các blockchain mới thường sử dụng PoS:

1. **Khả năng thích ứng:** PoS linh hoạt, dễ dàng điều chỉnh theo nhu cầu của blockchain và người dùng.
2. **Phi tập trung:** Nhiều người dùng có thể chạy nút với chi phí thấp hơn, làm mạng lưới phi tập trung hơn.
3. **Hiệu quả năng lượng:** PoS tiêu tốn ít năng lượng hơn, dựa trên staking thay vì giải bài toán phức tạp.
4. **Khả năng mở rộng:** Không cần máy móc vật lý lớn, dễ thêm trình xác thực và mở rộng mạng lưới.
5. **Bảo mật:** Trình xác thực mất cổ phần nếu gian lận, và việc chiếm 51% mạng lưới là gần như không thể.

Nhược điểm PoS

1.Forking:

Trong PoS, không có động lực ngăn chặn việc "rèn" cả hai phía của một fork, vì chi phí thấp hơn nhiều so với PoW. Điều này có thể khuyến khích người dùng "đặt cược" vào cả hai phía của fork. => Slashing, Finality

2. Khả năng tiếp cận:

Để bắt đầu staking, bạn cần mua token của blockchain, có thể đòi hỏi một khoản đầu tư lớn. Trong khi đó, PoW cho phép mua hoặc thuê thiết bị rẻ hơn và tham gia khai thác nhanh chóng.

2. Tấn công 51%:

PoS có thể bị tấn công 51% hơn nếu giá token giảm mạnh hoặc blockchain có vốn hóa thị trường thấp, khiến việc mua hơn 50% số token để kiểm soát mạng trở nên khả thi.

Proof of Work vs. Proof of Stake

When we compare the two consensus mechanisms, there are a few core differences.

	Proof of Work (PoW)	Proof of Stake (PoS)
Equipment required	Mining equipment	Minimal amount or none
Energy consumption	High	Low
Tendency towards	Centralization	Decentralization
Validation method	Computational proof	Staking of coins

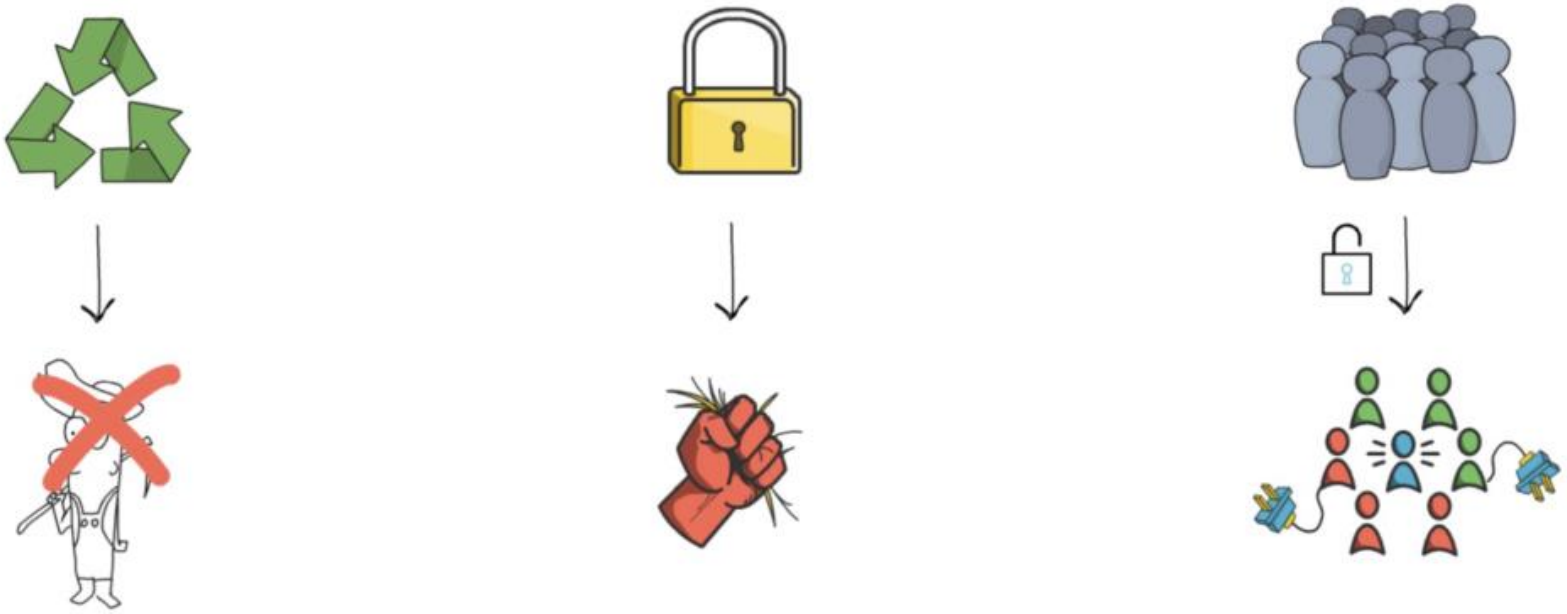
SOICT

Các cơ chế đồng thuận xây dựng trên PoS

1. **Delegated Proof of Stake (DPoS):**
2. **Nominated Proof of Stake (NPoS):**
3. **Proof of Staked Authority (PoSA):**

Kết luận

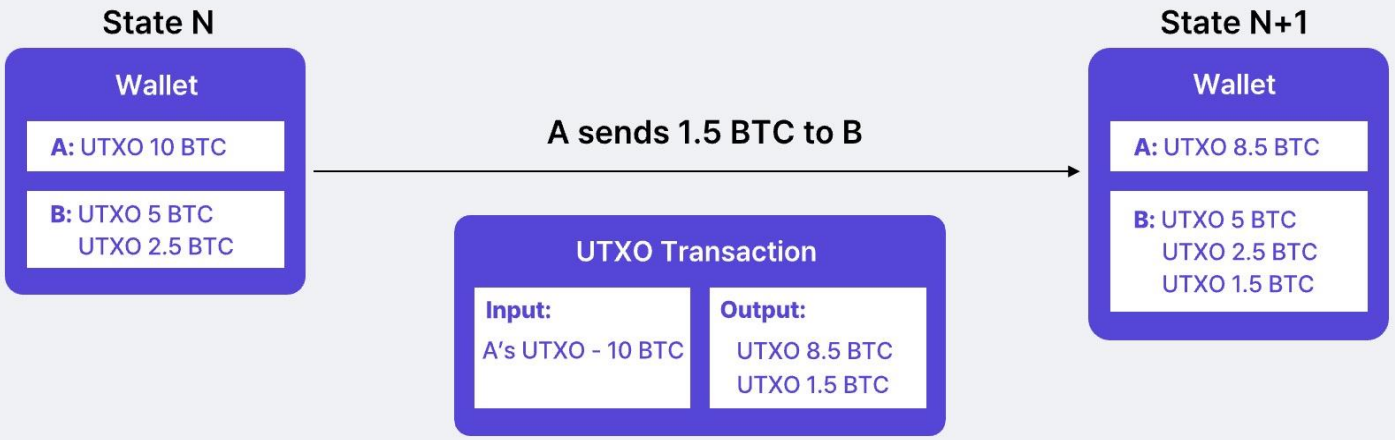
Proof-of-Stake



UTXO Bitcoin

Bitcoin's UTXO Model

The UTXO model is similar to a cash payment in which you rely on your counterparty to return the change.



Date: Apr 8, 2022

Source: Xangle, Horizon Academy

Xangle

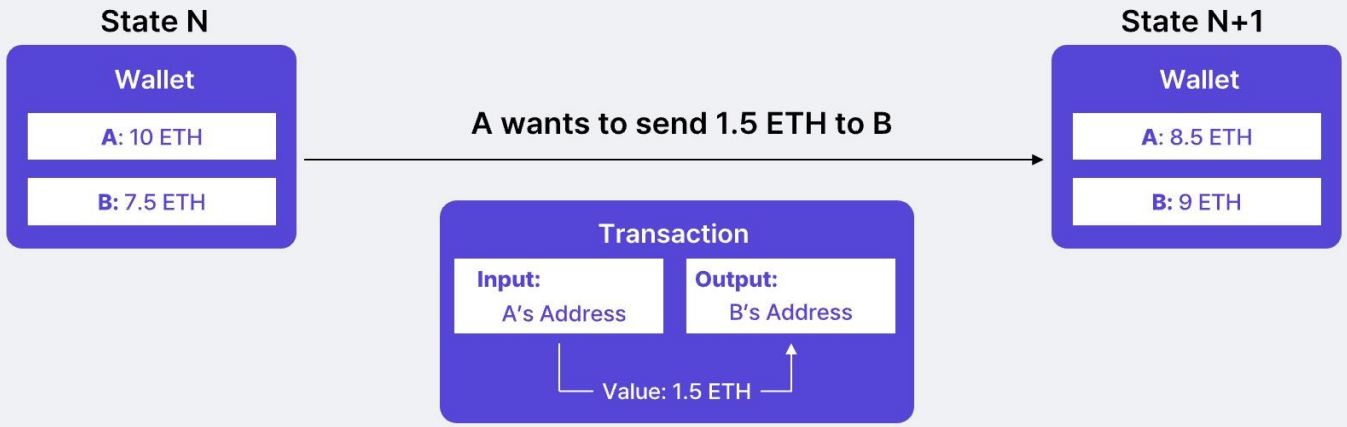
Continued...

- **Hiệu quả xác thực:** Các node trong mạng có thể dễ dàng xác minh tính hợp lệ của một giao dịch bằng cách kiểm tra xem các UTXO được sử dụng trong giao dịch đó có tồn tại và chưa được chi tiêu trước đó hay không.
- **Phù hợp với các giao dịch đơn giản:** Mô hình UTXO rất phù hợp cho các loại tiền điện tử như Bitcoin, nơi mà các giao dịch chủ yếu là chuyển tiền đơn thuần.
- **Nhược điểm:**
- **Khó khăn trong việc triển khai hợp đồng thông minh:** Mô hình UTXO không linh hoạt bằng mô hình Account/Balance, do đó khó khăn hơn trong việc triển khai các hợp đồng thông minh phức tạp.

Ethereum Account/Balance

Ethereum's Account/Balance Model

The Account/Balance model represents assets as balances within accounts, similar to bank accounts.



Date: Apr 8, 2022

Source: Xangle, Horizon Academy

Xangle

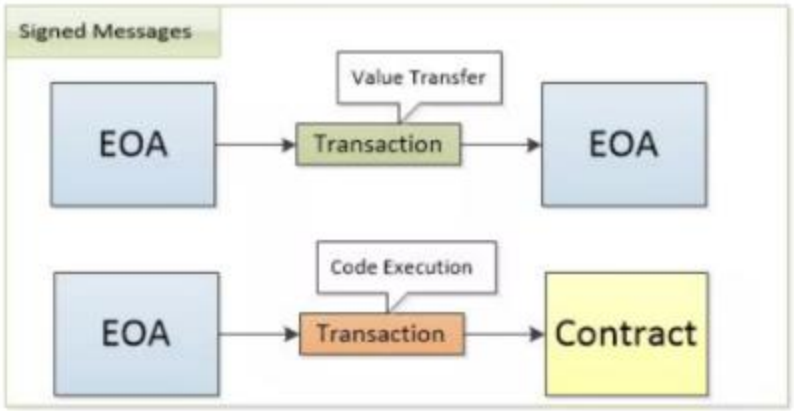
Ethereum Account/Balance

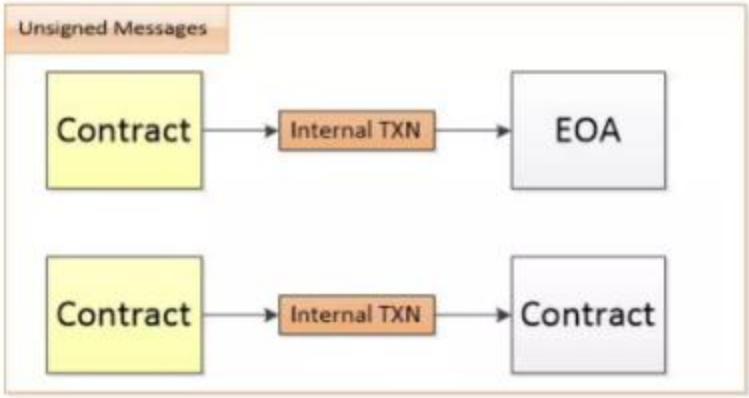
- **Ưu điểm:**
- **Linh hoạt:** Mô hình Account/Balance rất linh hoạt, cho phép triển khai các hợp đồng thông minh phức tạp và các ứng dụng phi tập trung khác.
- **Dễ hiểu:** Mô hình này dễ hiểu hơn so với mô hình UTXO, vì nó gần gũi với cách chúng ta quản lý tiền trong cuộc sống hàng ngày.
- **Nhược điểm:**
- **Yêu cầu tính toán phức tạp:** Các giao dịch trong mô hình Account/Balance thường yêu cầu nhiều tính toán hơn so với mô hình UTXO, do đó có thể làm giảm hiệu suất của mạng.
- **Rủi ro bảo mật:** Các hợp đồng thông minh có thể chứa các lỗ hổng bảo mật, dẫn đến việc mất tài sản của người dùng.

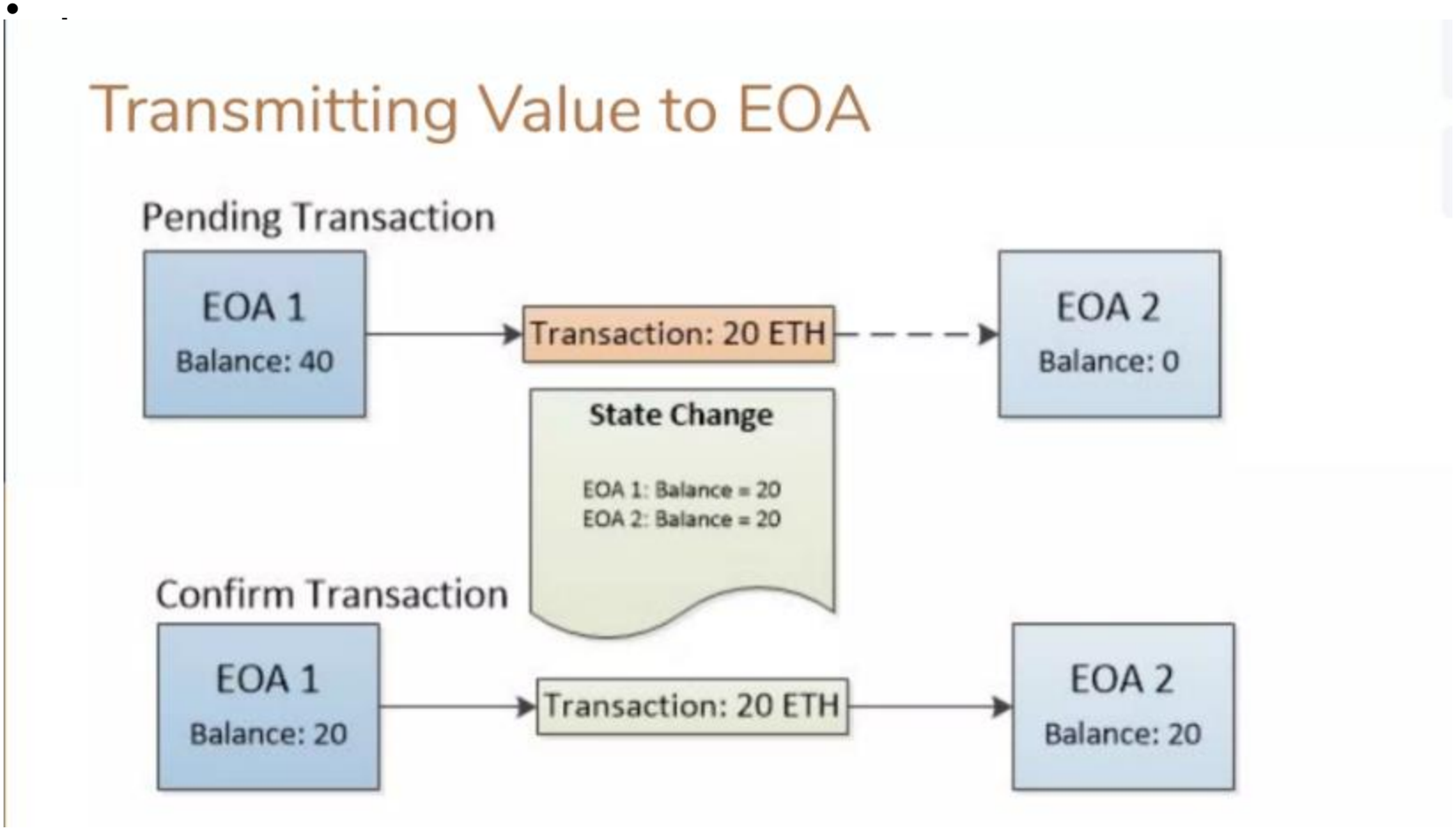
Ethereum Transactions

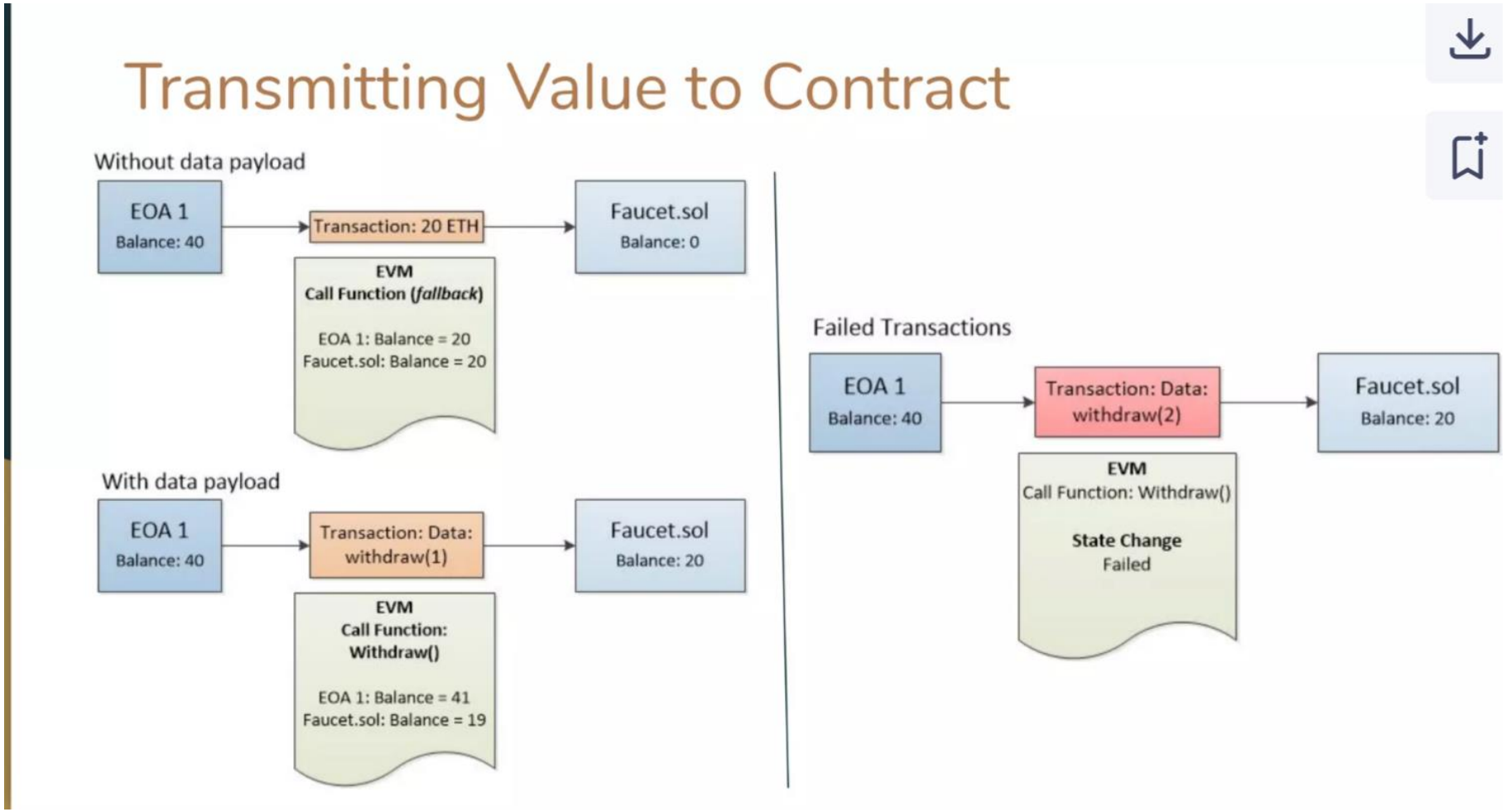
- **Giao dịch là các thông điệp được ký:** Mỗi giao dịch trên Ethereum thực chất là một thông điệp được mã hóa bằng chữ ký số. Chữ ký này chứng minh rằng người gửi thực sự sở hữu tiền điện tử mà họ đang chuyển đi.
- **Xuất phát từ một tài khoản do người dùng sở hữu (EOA):** Mọi giao dịch đều bắt nguồn từ một ví Ethereum mà người dùng trực tiếp kiểm soát.
- **Được truyền qua mạng lưới Ethereum:** Sau khi được tạo ra, giao dịch sẽ được gửi đi trên mạng lưới Ethereum.
- **Và được ghi lại trên blockchain:** Cuối cùng, giao dịch sẽ được thêm vào một khối (block) và trở thành một phần vĩnh viễn của blockchain Ethereum.
- **Giao dịch là yếu tố duy nhất có thể kích hoạt thay đổi trạng thái:** Chỉ có giao dịch mới có thể làm thay đổi trạng thái của Ethereum, ví dụ như chuyển tiền, thực thi hợp đồng thông minh, v.v.
- **Ethereum là một máy trạng thái toàn cầu:** Có thể hiểu Ethereum như một chiếc máy tính khổng lồ, liên tục cập nhật trạng thái của nó dựa trên các giao dịch.
- **Giao dịch là yếu tố khởi động:** Không có giao dịch nào, Ethereum sẽ không hoạt động. Mọi thứ trên Ethereum đều bắt đầu từ một giao dịch.
- **Hợp đồng thông minh không tự chạy:** Hợp đồng thông minh chỉ được thực thi khi có một giao dịch gọi đến nó.

Type of Transactions






Transmitting Value to EOA
Pending Transaction
EOA 1
Balance: 40
Transaction: 20 ETH
EOA 2
Balance: 0
State Change
EOA 1: Balance = 20
EOA 2: Balance = 20
Confirm Transaction
EOA 1
Balance: 20
Transaction: 20 ETH
EOA 2
Balance: 20


Transmitting Value to Contract
Without data payload
EOA 1
Balance: 40
Transaction: 20 ETH
Faucet.sol
Balance: 0
EVM
Call Function (fallback)
EOA 1: Balance = 20
Faucet.sol: Balance = 20
With data payload
EOA 1
Balance: 40
Transaction: Data: withdraw(1)
Faucet.sol
Balance: 20
EVM
Call Function: Withdraw()
EOA 1: Balance = 41
Faucet.sol: Balance = 19
Failed Transactions
EOA 1
Balance: 40
Transaction: Data: withdraw(2)
Faucet.sol
Balance: 20
EVM
Call Function: Withdraw()
State Change
Failed

Transaction Structure

Nonce	A sequence number, issued by the originating EOA, used to prevent message replay. This number represents the number of transactions sent from the account's address
Gas Price	The price of gas (in wei) the originator is willing to pay
Gas Limit	The maximum amount of gas the originator is willing to buy for this transaction
Recipient	The destination Ethereum address
Value	The amount of ether to send to the destination
Data	The variable-length binary data payload
v,r,s	The three components of an ECDSA digital signature of the originating EOA

Nonce

- **Đối với tài khoản do người dùng sở hữu (EOA):** Nonce biểu thị số lượng giao dịch đã được xác nhận (confirmed) từ địa chỉ đó. Mỗi khi gửi một giao dịch mới, bạn cần tăng giá trị nonce lên 1 đơn vị so với giao dịch trước đó.

- **Đối với hợp đồng:** Nonce biểu thị số lượng hợp đồng đã được tạo ra từ địa chỉ đó. Mỗi khi triển khai một hợp đồng mới, giá trị nonce sẽ tăng lên.

- **Đảm bảo tính duy nhất của giao dịch**

- **Quản lý thứ tự các giao dịch**

- **Ngăn chặn các cuộc tấn công**

- **Không thể bỏ qua giao dịch**

Gas

- **Ethereum sử dụng gas để kiểm soát việc sử dụng tài nguyên của giao dịch**:

Mô hình tính toán mở (Turing-complete) yêu cầu một hình thức đo lường để tránh các cuộc tấn công từ chối dịch vụ hoặc các giao dịch tiêu tốn quá nhiều tài nguyên

- **Gas Price and Gas Limit**

- **Base Fee and Tips**

•Jordan has to pay Taylor 1 ETH. An ETH transfer requires 21,000 units of gas, and the base fee is 10 gwei. Jordan includes a tip of 2 gwei.

•The total fee would now be equal to:

•`units of gas used * (base fee + priority fee)`

•where the `base fee` is a value set by the protocol and the `priority fee` is a value set by the user as a tip to the validator.

•i.e. `21,000 * (10 + 2) = 252,000 gwei` (0.000252 ETH).

•When Jordan sends the money, 1.000252 ETH will be deducted from Jordan's account. Taylor will be credited 1.0000 ETH. The validator receives the tip of 0.000042 ETH. The `base fee` of 0.00021 ETH is burned.

So sánh với Bitcoin

Thành Phần	Bitcoin	Ethereum
Mục Đích	Tiền tệ kỹ thuật số	Nền tảng cho hợp đồng thông minh và dApps
Địa Chỉ	Địa chỉ Bitcoin (Bằng chuỗi ký tự)	Địa chỉ Ethereum (Bằng chuỗi ký tự, bắt đầu bằng "0x")
Inputs	Tham chiếu đến các giao dịch trước đó (txid)	Không có thành phần input giống như Bitcoin; thay vào đó có `nonce` để xác định thứ tự giao dịch
Outputs	Địa chỉ người nhận và số lượng Bitcoin	Địa chỉ người nhận Ether, số lượng Ether và có thể có dữ liệu (data) cho hợp đồng thông minh
Nonce	Không có	Số lượng giao dịch đã gửi từ địa chỉ đó, đảm bảo tính duy nhất của mỗi giao dịch
Gas Limit	Không có	Giới hạn về số lượng gas mà người gửi sẵn sàng tiêu cho giao dịch
Gas Price	Không có	Giá cho mỗi đơn vị gas, phụ thuộc vào cung cầu trong mạng lưới
Phí Giao Dịch	Phí dựa trên kích thước giao dịch (bytes) và điều kiện mạng	Phí dựa trên `gas limit` và `gas price`, tính toán theo độ phức tạp của giao dịch
Thời Gian Xử Lý	Trung bình 10 phút	Trung bình 15 giây
Dữ Liệu	Không có	Có thể có dữ liệu bổ sung cho hợp đồng thông minh, cho phép gửi mã thực thi
Chữ Ký	Chữ ký số xác nhận quyền sở hữu và tính hợp lệ của giao dịch	Chữ ký số xác nhận quyền sở hữu và tính hợp lệ của giao dịch, nhưng có thêm mã thực thi cho hợp đồng thông minh
Khả Năng Mở Rộng	Giới hạn bởi kích thước khối (1MB) và thời gian tạo khối	Đang trong quá trình cải thiện khả năng mở rộng với Ethereum 2.0, chuyển sang Proof of Stake

Khía Cạnh	Bitcoin	Ethereum
Mục Đích	Tiền tệ kỹ thuật số	Nền tảng cho hợp đồng thông minh và ứng dụng phi tập trung
Tạo Giao Dịch	Người dùng chỉ định: - Địa chỉ nhận (public key) - Số lượng Bitcoin muốn gửi - Chọn các đầu vào (inputs) từ các giao dịch trước đó	Người dùng chỉ định: - Địa chỉ nhận (public key) - Số lượng Ether muốn gửi - Dữ liệu (nếu có) cho hợp đồng thông minh
Chữ Ký Giao Dịch	Sử dụng khóa riêng (private key) để ký giao dịch - Đảm bảo rằng chỉ người sở hữu Bitcoin mới có quyền gửi nó	Sử dụng khóa riêng (private key) để ký giao dịch - Tương tự như Bitcoin
Kiểm Tra Tính Hợp Lệ	- Kiểm tra tính hợp lệ của các đầu vào (inputs): - Địa chỉ người nhận hợp lệ - Số lượng Bitcoin không vượt quá số dư của người gửi - Giao dịch không phải là một giao dịch "đã tiêu" (double spend)	- Kiểm tra tính hợp lệ của giao dịch: - Địa chỉ người nhận hợp lệ - Số dư của người gửi đủ để thực hiện giao dịch - Giá trị `nonce` là chính xác (không được gửi lại giao dịch)

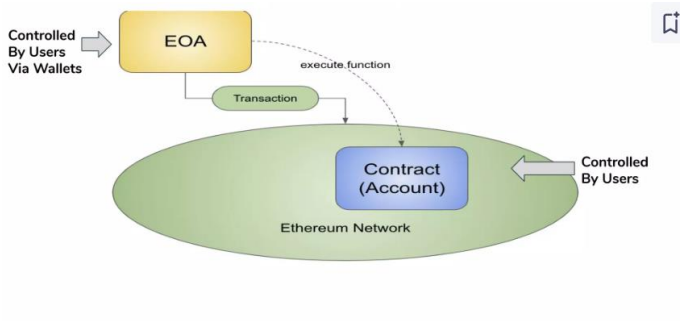
	mempool	
Khai Thác/Giao Dịch	- Các thợ mỏ chọn giao dịch từ mempool - Bao gồm giao dịch vào khối đang khai thác - Thợ mỏ tìm kiếm hash hợp lệ cho khối	- Các thợ mỏ hoặc validator chọn giao dịch từ mempool - Thực thi hợp đồng thông minh nếu có - Xác nhận giao dịch và cập nhật trạng thái mạng
Thời Gian Tạo Khối	Khoảng 10 phút cho mỗi khối	Khoảng 15 giây cho mỗi khối
Xác Nhận Giao Dịch	Giao dịch được xác nhận khi khối chứa giao dịch được thêm vào blockchain	Giao dịch được xác nhận khi khối chứa giao dịch được thêm vào blockchain
Số Lần Xác Nhận	Được xem là an toàn sau 6 xác nhận (khoảng 1 giờ)	An toàn hơn sau 12-30 xác nhận, tùy thuộc vào độ phức tạp
Phí Giao Dịch	Phí giao dịch dựa trên kích thước của giao dịch (số byte) - Người dùng có thể điều chỉnh phí để ưu tiên xử lý nhanh hơn	Phí giao dịch (gas fee) dựa trên `gas limit` và `gas price` - Phí có thể thay đổi nhanh chóng trong thời điểm cao điểm
Khả Năng Mở Rộng	Bị hạn chế bởi kích thước khối (1MB) và thời gian tạo khối	Đang chuyển đổi từ Proof of Work sang Proof of Stake để cải thiện khả năng mở rộng

So Sánh Phần Thưởng:

Tiêu chí	Bitcoin (Proof of Work)	Ethereum (Proof of Stake)
Phần thưởng khối	6.25 BTC (năm 2024, giảm sau halving)	Phần thưởng ETH (tùy thuộc vào số lượng ETH đã stake)
Phí giao dịch	Người đào nhận toàn bộ phí giao dịch	Validator nhận **priority fee**, còn **base fee** bị đốt
Halving	Mỗi 210.000 khối (~4 năm, phần thưởng giảm một nửa)	Không có cơ chế halving, phần thưởng thay đổi dựa trên số lượng ETH được stake
Cơ chế phạt	Không có cơ chế phạt riêng cho người đào	Validator có thể bị phạt slashing nếu gian lận
MEV	Không áp dụng	Validator có thể kiếm thêm từ MEV

Smart Contracts

•**Hợp đồng thông minh** là một chương trình máy tính được triển khai trực tiếp lên blockchain, tự động thực thi các điều khoản của một hợp đồng khi các điều kiện nhất định được đáp ứng. Nó giống như một hợp đồng pháp lý, nhưng được mã hóa và thực thi tự động trên một mạng lưới phân tán.
•Các đặc tính chính của hợp đồng thông minh:
•**Chương trình máy tính:** Hợp đồng thông minh được viết bằng một ngôn ngữ lập trình đặc biệt (ví dụ như Solidity cho Ethereum) và được triển khai lên blockchain.
•**Bất biến (Immutable):** Một khi hợp đồng được triển khai, mã nguồn của nó không thể thay đổi. Điều này đảm bảo tính minh bạch và tin cậy của hợp đồng.
•**Xác định (Deterministic):** Cho cùng một đầu vào, hợp đồng luôn cho ra cùng một kết quả. Điều này giúp đảm bảo tính nhất quán và tránh các hành vi gian lận.
•**Môi trường thực thi Ethereum Virtual Machine (EVM):** Hợp đồng thông minh được thực thi trong một môi trường ảo gọi là EVM. EVM cung cấp một nền tảng an toàn và cách ly để thực thi các hợp đồng.
•**Máy tính thế giới phi tập trung:** Hợp đồng thông minh đóng góp vào việc xây dựng một máy tính thế giới phi tập trung, nơi bất kỳ ai cũng có thể truy cập và tương tác với các ứng dụng.



Smart Contracts

- **Được viết bằng ngôn ngữ cấp cao:** Hợp đồng thông minh ban đầu được viết bằng một ngôn ngữ lập trình dễ hiểu hơn cho con người, ví dụ như Solidity.
- **Được biên dịch thành bytecode:** Mã nguồn viết bằng ngôn ngữ cấp cao sẽ được biên dịch thành bytecode - một dạng mã máy mà máy tính có thể trực tiếp thực thi. Bytecode này sẽ được đưa vào Ethereum Virtual Machine (EVM) để chạy.
- **Được triển khai bằng một giao dịch đặc biệt:** Để đưa hợp đồng lên blockchain, người ta sẽ thực hiện một giao dịch đặc biệt. Giao dịch này sẽ gửi bytecode của hợp đồng lên mạng lưới.
- **Có một địa chỉ duy nhất:** Sau khi được triển khai, hợp đồng sẽ có một địa chỉ duy nhất trên blockchain. Địa chỉ này giống như một căn nhà có địa chỉ riêng, giúp người khác có thể tìm thấy và tương tác với hợp đồng đó.
- **Chỉ hoạt động khi được gọi:** Hợp đồng thông minh không tự động chạy. Nó chỉ thực hiện các chức năng khi có một giao dịch gửi đến địa chỉ của nó.
- **Không chạy ngầm:** Hợp đồng thông minh không thể tự chạy nền hoặc thực hiện các tác vụ trong nền.
- **Không chạy song song:** Các hợp đồng thông minh không thể thực hiện nhiều tác vụ cùng một lúc. Mỗi giao dịch sẽ được xử lý tuần tự.

Cách thức hoạt động

- Hợp đồng này có thể gọi một hợp đồng khác, và hợp đồng đó lại có thể gọi một hợp đồng khác nữa, cứ như vậy.
- Hợp đồng đầu tiên trong một chuỗi thực thi luôn được gọi bởi một giao dịch từ một tài khoản do người dùng sở hữu (EOA).
- Chỉ được ghi nhận nếu tất cả các quá trình thực thi hoàn thành thành công, nếu không sẽ quay trở lại trạng thái ban đầu (Roll Back).
- Giao dịch thất bại vẫn được ghi nhận là đã được thực hiện.
- Số Ether tiêu tốn cho phí gas để thực thi giao dịch sẽ được trừ vào tài khoản khởi tạo giao dịch.
- Nếu không, sẽ không có ảnh hưởng nào khác đến trạng thái của hợp đồng hoặc tài khoản.

Xóa contract

1. Mã nguồn của hợp đồng không thể thay đổi.
2. Bằng cách xóa mã nguồn và trạng thái nội bộ (lưu trữ) của nó khỏi địa chỉ.
3. Để lại một tài khoản trống.
4. Thực thi một opcode của EVM gọi là SELFDESTRUCT.
5. Tốn "gas âm", tức là hoàn lại gas (khuyến khích giải phóng tài nguyên mạng).
6. **IMMUTABILITY:** Không xóa lịch sử giao dịch (quá khứ) của hợp đồng. - Tính bất biến.
7. **SELFDESTRUCT :** Khả năng tự hủy chỉ có sẵn nếu hợp đồng được thiết kế để có chức năng đó.

PHẦN 2: COIN, TOKENS

2.1 Các khái niệm cơ bản

2.1.1 Coin và Token

Coin

- Định nghĩa: Tiền điện tử có blockchain riêng.
- Mục đích: Thanh toán, giao dịch, hoặc làm phương tiện trao đổi giá trị.
  Ví dụ: Bitcoin (BTC), Ethereum (ETH), Binance Coin (BNB).

Token

- Định nghĩa: Tài sản kỹ thuật số được xây dựng trên blockchain của nền tảng khác (thường là Ethereum).
- Mục đích: Đại diện cho tài sản, quyền sở hữu, hoặc phục vụ trong các dApps (ứng dụng phi tập trung).
- Ví dụ: Uniswap (UNI), Chainlink (LINK), NFT (CryptoPunks),

=>**Coin**: Blockchain riêng, ví dụ BTC, ETH.
Token: Xây dựng trên blockchain khác.

2.1.2 Fungible token và Non-Fungible token

Fungible Tokens

- Định nghĩa**: Fungible tokens** là các tài sản có thể chia nhỏ và có giá trị tương đương nhau.
- Đặc điểm:

- Có thể thay thế lẫn nhau (ví dụ: 1 BTC ở New York luôn có giá trị bằng 1 BTC ở London).
- Có thể chia nhỏ thành các đơn vị nhỏ hơn (ví dụ: Bitcoin có thể chia thành Satoshi).

Ví dụ:

Bitcoin (BTC): Dùng để thanh toán và lưu trữ giá trị như tiền tệ.

Ether (ETH): Dùng để trả phí giao dịch trên Ethereum.

Stablecoins (USDT, USDC): Gắn với giá trị của đồng đô la Mỹ, dùng để giao dịch trong các nền tảng tiền điện tử.

2.1.2 Fungible token và Non-Fungible token

Non-Fungible Tokens (NFTs)

- **Định nghĩa**: NFTs là các tài sản độc nhất và không thể thay thế lẫn nhau.
- **Đặc điểm**:
  - Không chia nhỏ, đại diện cho quyền sở hữu của một tài sản duy nhất (ví dụ: hình ảnh, âm nhạc, tác phẩm nghệ thuật).
  - Mỗi NFT có thông tin riêng biệt và duy nhất.

Ví dụ:

CryptoKitties (phát triển bởi hệ sinh thái Eth): Mỗi "mèo kỹ thuật số" là duy nhất và người chơi có thể mua, bán hoặc nhân giống chúng.

Tác phẩm nghệ thuật số: Beeple bán tác phẩm “Everydays: The First 5000 Days” dưới dạng NFT với giá 69.3 triệu đô la.

Tài sản kỹ thuật số khác: Vé sự kiện, nhạc phẩm, video game item (nhân vật, vật phẩm trong game).

2.1.3 Stable coin

Định nghĩa: Stable coin là tiền điện tử có giá trị ổn định, được gắn với tài sản tham chiếu như tiền pháp định, hàng hóa, hoặc các thuật toán.

Chức năng chính:

- Ổn định giá trị trong giao dịch
- Giảm biến động so với các loại tiền điện tử khác
- Cầu nối giữa thế giới tiền điện tử và tiền pháp định

2.1.3 Stable coin

Các loại Stable coin:

- **Fiat-Collateralized** (Thế chấp bằng tiền pháp định): Được hỗ trợ bởi tiền pháp định như USD, EUR. Ví dụ: USDT, USDC được các sàn giao dịch như Binance,.. cho phép bán để lấy USD
- **Crypto-Collateralized** (Thế chấp bằng tiền điện tử): Thế chấp bằng các loại tiền điện tử khác. Ví dụ: DAI (thế chấp bởi ETH)
- **Algorithmic Stablecoin** (Thuật toán): Duy trì giá trị bằng cách điều chỉnh cung cầu tự động, rủi ro cao hơn. Ví dụ: UST của Terra (đã sụp đổ do sự phụ thuộc vào mô hình cung – cầu của thị trường)

2.1.2 Stable coin

Ứng dụng trong thực tế:

- Giao dịch: Tránh biến động giá
- DeFi (Decentralized Finance): Cho vay, thế chấp, farming
- Chuyển tiền: Chi phí thấp, nhanh chóng

Rủi ro:

- Thiếu minh bạch về dự trữ tài sản
- Quy định pháp lý chưa hoàn chỉnh
- Rủi ro hệ thống khi giá trị tiền thế chấp giảm mạnh

2.2 CÁC CHUẨN TOKENS

2.2.1 ERC-20 tokens

1. Khái niệm

ERC-20:

- **ERC-20** là một chuẩn token khác trên nền tảng Ethereum
- Được sử dụng chủ yếu cho các Fungible Tokens. Điều này có nghĩa là mỗi token **ERC-20** có giá trị và loại hình giống hệt nhau, tương tự như **ETH**.
- Đây là chuẩn token được sử dụng rộng rãi trong các dự án DeFi, thanh toán và quản trị trên blockchain Ethereum, giúp các token có thể tương tác và trao đổi một cách linh hoạt giữa các ứng dụng và dịch vụ khác nhau.

ERC-20

infina

2.2.1 ERC-20 token

2. Kĩ thuật

a. Smart Contract:

ERC-20 token được triển khai thông qua **smart contract**, có các hàm chuẩn để kiểm soát việc tạo, phân phối và quản lý token.

b. Các tính năng chính:

- *TotalSupply*: hiển thị thông tin về tổng nguồn cung, tổng số token có thể được tạo ra trong hệ thống.
- *BalanceOf*: cung cấp thông tin về số dư token của một địa chỉ Ethereum cụ thể. Nó giống như việc xem ai đó có bao nhiêu tiền trong ví của họ.
- *Transfer*: đây là tính năng thú vị nhất, cho phép bạn chuyển giao một lượng token xác định từ ví của bạn sang ví của người khác một cách nhanh chóng và tiện lợi.
- *TransferFrom*: tưởng tượng bạn cần chuyển một số token từ một người bạn sang người khác, nhưng người bạn đó cần phải cho phép điều này trước. Nó giống như một loại "xác nhận" trước khi chuyển token.
- *Approve*: cho phép người dùng cấp quyền cho địa chỉ khác để rút một số lượng token cụ thể từ ví của họ.
- *Allowance*: Cho phép kiểm tra số dư của người dùng đồng thời xác định một số token có sẵn để rút từ ví của họ.

2.2.1 ERC-20 token

```
contract ERC20Interface {
    ftrace | funcSig
    function totalSupply() public view returns (uint);

    // Lấy số dư của chủ sở hữu token
    ftrace | funcSig
    function balanceOf(address tokenOwner) public view returns (uint balance);

    // Kiểm tra số lượng token mà spender được phép tiêu từ tokenOwner
    ftrace | funcSig
    function allowance(address tokenOwner, address spender) public view returns (uint remaining);

    // Chuyển tokens tới địa chỉ '_to' trả về giao dịch succes hoặc không '
    ftrace | funcSig
    function transfer(address to, uint tokens) public returns (bool success);

    // Cho phép 'spender' tiêu số lượng token
    ftrace | funcSig
    function approve(address spender, uint tokens) public returns (bool success);

    // Chuyển token từ 'from' tới 'to' thông qua cơ chế allowance
    ftrace | funcSig
    function transferFrom(address from, address to, uint tokens) public returns (bool success);

    // Sự kiện khi có chuyển token
    event Transfer(address indexed from, address indexed to, uint tokens);

    // Sự kiện khi một tài khoản cấp quyền cho tài khoản khác
    event Approval(address indexed tokenOwner, address indexed spender, uint tokens);
}
```

2.2.1 ERC-20 token

ERC-20 còn có các sự kiện (cách để Contract thông báo rằng một điều gì đó đã xảy ra trên blockchain) trong Smart Contract như sau:

```
// Sự kiện khi có chuyển token
event Transfer(address indexed from, address indexed to, uint tokens);

// Sự kiện khi một tài khoản cấp quyền cho tài khoản khác
event Approval(address indexed tokenOwner, address indexed spender, uint tokens);
```

Ngoài ra, **ERC-20** còn có các tính năng tùy chọn khác như name, symbol và decimal (xác định đơn vị nhỏ nhất có thể giao dịch được).

```
contract CongDat is ERC20Interface {
    // Các thông tin cơ bản của token
    string public name;     // Tên của token
    string public symbol;   // Ký hiệu của token
    uint8 public decimals;  // Số thập phân (đề xuất là 18)

    uint256 public _totalSupply;  // Tổng nguồn cung
```

2.2.1 ERC-20 token

3. Ứng dụng

- **Thanh toán và giao dịch:**

- **ERC-20** chủ yếu được sử dụng làm phương tiện thanh toán trong các giao dịch và các nền tảng DeFi. (trong đó có token hóa tài sản thực,...)
- Các dự án sử dụng ERC-20 để huy động vốn thông qua các đợt **ICO (Initial Coin Offering)**, là cách mà họ bán token lần đầu để kêu gọi đầu tư từ cộng đồng.
- Stable coin.

- **Quản trị phi tập trung:**

Token **ERC-20** có thể được sử dụng trong các hệ thống quản trị phi tập trung, nơi người sở hữu token có quyền bỏ phiếu về các quyết định quan trọng của dự án.

2.2.1 ERC-20 token

4. Ưu và nhược điểm của ERC-20

Ưu điểm của ERC20 Token

- **Khả năng thay thế lẫn nhau**: Các token ERC20 có giá trị và chức năng đồng nhất, thuận tiện cho giao dịch và trao đổi.
- **Linh hoạt**: Có thể điều chỉnh để phù hợp với nhiều ứng dụng như AMM, lending.
- **Phổ biến**: Được hỗ trợ rộng rãi bởi các sàn giao dịch, ví và hợp đồng thông minh, dễ dàng tích hợp vào hệ sinh thái blockchain.

Nhược điểm của ERC20 Token

- **Khả năng mở rộng**: Mạng Ethereum gặp khó khăn trong việc mở rộng, gây ra phí gas cao và chậm trễ giao dịch.
- **Nguy cơ lừa đảo**: Việc tạo token dễ dàng có thể dẫn đến các dự án lừa đảo, yêu cầu người dùng phải cẩn trọng khi đầu tư.

2.2.1 ERC20 token

5. Ví dụ thực tế

Tether (USDT) : Stablecoin chạy trên ERC-20, giúp giao dịch nhanh chóng trên Ethereum.

Uniswap (UNI): Token quản trị của Uniswap, cho phép bỏ phiếu và quản lý trên nền tảng.

Chainlink (LINK): Token ERC-20 dùng cho dịch vụ oracle, kết nối dữ liệu thực tế với blockchain.

Thorn (THORN): Token DeFi cung cấp nền tảng giao dịch tài sản kỹ thuật số phi tập trung.

2.2.2 ERC-721 token

1. Khái niệm

- **ERC-721** là một chuẩn token trên nền tảng Ethereum, được sử dụng để tạo ra các **Non-Fungible Tokens (NFTs).**
- Đây là loại token đặc biệt, mỗi token là duy nhất và không thể thay thế trực tiếp với nhau.
- Giá trị của mỗi token có thể khác nhau tùy thuộc vào các yếu tố như độ hiếm, tuổi đời, hoặc đặc điểm hình ảnh.
- **ERC-721** được áp dụng rộng rãi trong các lĩnh vực như vật phẩm sưu tầm, vé tham dự sự kiện, hoặc các sản phẩm có tính độc đáo.

2.2.2 ERC-721 token

2. Kĩ thuật

a. Smart Contract:

ERC-721 sử dụng smart contract để tạo và quản lý các NFT, với các hàm chuẩn xác nhận tính độc đáo của từng token.

b. Các tính năng chính:

balanceOf: Trả về số lượng NFT của chủ sở hữu.

ownerOf: Trả về chủ sở hữu của một NFT.

safeTransferFrom: Chuyển NFT an toàn với có hoặc không có có dữ liệu tùy chỉnh.

transferFrom: Chuyển NFT mà không kiểm tra an toàn.

approve: Phê duyệt quyền chuyển NFT cho địa chỉ khác.

setApprovalForAll: Phê duyệt/quản lý tất cả NFT của chủ sở hữu.

getApproved: Trả về địa chỉ được phê duyệt cho một NFT.

isApprovedForAll: Kiểm tra quyền quản lý NFT của operator(người này có quyền thực hiện các hành động trên tất cả NFT của chủ sở hữu)

2.2.2 ERC-721 token

```
contract ERC721 { //Contract này định nghĩa chuẩn Tokens Non-fungible coin (NFT): ERC721.
    // Các hàm cơ bản của chuẩn ERC721
    // ---------------------------------------------------------------------
    ftrace | funcSig
    function balanceOf(address _owner) external view returns (uint256);
    // trả về số lượng NFT mà '_owner' sở hữu
    ftrace | funcSig
    function ownerOf(uint256 _tokenId) external view returns (address);
    //  trả về địa chỉ của chủ sở hữu token với ID cụ thể ('_tokenId)
    ftrace | funcSig
    function safeTransferFrom(address _from, address _to, uint256 _tokenId, bytes data) external payable;
    //  chuyển token từ địa chỉ '_from' sang địa chỉ '_to', kèm theo tham số data để gửi thêm dữ liệu khi chuyển.
    ftrace | funcSig
    function safeTransferFrom(address _from, address _to, uint256 _tokenId) external payable;
    //  chuyển token từ địa chỉ '_from' sang địa chỉ '_to', nhưng không có tham số data.
    ftrace | funcSig
    function transferFrom(address _from, address _to, uint256 _tokenId) external payable;
    // àm chuyển token từ địa chỉ '_from' sang địa chỉ '_to' (là phương thức thông thường, có thể không an toàn)
    ftrace | funcSig
    function approve(address _approved, uint256 _tokenId) external payable;
    // phê duyệt địa chỉ _approved để chứng minh quyền sở hữu với một số lượng tôken cụ thể.
    ftrace | funcSig
    function setApprovalForAll(address _operator, bool _approved) external;
     // phê duyệt hoặc hủy quyền cho `_operator` để quản lý tất cả các token của chủ sở hữu.

    ftrace | funcSig
    function getApproved(uint256 _tokenId) external view returns (address);
    // trả về địa chỉ được phê duyệt sử dụng token với ID cụ thể (`_tokenId`).
    ftrace | funcSig
    function isApprovedForAll(address _owner, address _operator) external view returns (bool);
    // kiểm tra xem `_operator` có được phê duyệt để quản lý tất cả các token của `_owner` hay không.

//-------------------------------------------------------------
    event Transfer(address indexed _from, address indexed _to, uint256 indexed _tokenId);
    event Approval(address indexed _owner, address indexed _approved, uint256 indexed _tokenId);
    event ApprovalForAll(address indexed _owner, address indexed _operator, bool _approved);

}
```

2.2.2 ERC-721 token

ERC-721 gồm các sự kiện phát sinh giao dịch, sự kiện một tài khoản cấp phép cho tài khoản khác, sự kiện phê duyệt quyền tất cả NFT của chủ sở hữu,

```
//------------------------------------------------------------
    event Transfer(address indexed _from, address indexed _to, uint256 indexed _tokenId);
    event Approval(address indexed _owner, address indexed _approved, uint256 indexed _tokenId);
    event ApprovalForAll(address indexed _owner, address indexed _operator, bool _approved);
```

Ngoài ra, **ERC-721** còn có thêm các tùy chọn khác như name, metadata (siêu dữ liệu)

```
contract MyNFT is ERC721, Ownable{
    // Các thuộc tính cơ bản của NFT
    struct NFT {
        string name;      // Tên của NFT
        string metadata;  // URL chứa metadata (siêu dữ liệu) mô tả NFT
    }
```

2.2.2 ERC-721 token

3. Ứng dụng

- Sưu tầm và quyền sở hữu:

ERC-721 cho phép tạo các tài sản số độc nhất, dùng trong các bộ sưu tập nghệ thuật, trò chơi blockchain và các sản phẩm giải trí.

Tính duy nhất của token giúp chứng minh quyền sở hữu tài sản một cách rõ ràng và minh bạch.

- Định giá và giao dịch:

Các NFT có thể được định giá và giao dịch tự do trên các nền tảng như OpenSea, Rarible, và các nền tảng NFT khác.

2.2 ERC-721 tokens

4. Ưu và nhược điểm

- **Ưu điểm:**

- Độc nhất: Mỗi token là duy nhất và không thể thay thế, phù hợp cho các tài sản như nghệ thuật số, vé sự kiện, bất động sản, v.v.

- Quyền sở hữu rõ ràng: Dễ dàng xác định quyền sở hữu tài sản số qua blockchain.

- Khả năng tương tác: Hỗ trợ các ứng dụng phi tập trung (dApps) khác nhau và có thể chuyển nhượng qua nhiều nền tảng.

- **Nhược điểm:**

- Chi phí giao dịch cao: Tạo và chuyển ERC-721 thường tốn nhiều gas hơn ERC-20 do tính phức tạp.

- Tính thanh khoản thấp: Khó mua bán hơn so với token có thể thay thế vì không có giá trị chuẩn.

- Yêu cầu bảo mật cao: Phải bảo vệ kỹ lưỡng để tránh mất tài sản số độc nhất.

2.2 ERC-721 tokens

5. Ví dụ thực tế

- **CryptoPunks:** Bộ sưu tập NFT đầu tiên trên Ethereum, gồm 10,000 nhân vật 8-bit độc nhất. Mỗi NFT đều có giá trị riêng biệt.
- **Bored Ape Yacht Club (BAYC):** Cộng đồng NFT với các avatar độc nhất, người sở hữu có quyền tham gia các sự kiện VIP và lợi ích đặc biệt.
- **Decentraland**: NFT đất đai ảo trong thế giới Metaverse, cho phép người dùng sở hữu và xây dựng trên mảnh đất của mình.
- **CryptoKitties**: Trò chơi sưu tầm NFT, mỗi con mèo là một NFT độc đáo với các đặc điểm riêng biệt, cho phép giao dịch và lai giống.

2.3 ERC20 tokens và ERC721 tokens

Tiêu chí	ERC-20	ERC-721
Tính hoán đổi	Có thể hoán đổi	Không thể hoán đổi
Danh tính token	Không có sự khác biệt rõ ràng giữa các token	Mỗi token có danh tính riêng, dễ phân biệt
Sưu tầm token	Không thể sưu tầm	Có thể sưu tầm như tiền pháp định
Biến động giá trị	Giá trị của token ERC-20 không thay đổi	Giá trị ERC-721 thay đổi theo độ hiếm và độc đáo
Mức độ chấp nhận	Được chấp nhận rộng rãi	Hạn chế hơn trong việc chấp nhận
Thay thế	Dễ thay thế	Không có khả năng thay thế
Khả năng chia nhỏ	Có thể chia thành các phần nhỏ	Token ERC-721 không thể chia nhỏ
Chức năng sở hữu	Không có chức năng sở hữu đặc biệt	ERC-721 có thể cho phép các chức năng sở hữu đặc biệt

2.3 ERC-1155

1. Khái niệm

ERC-1155 là chuẩn token đa năng (multi token standard) trên Ethereum, hỗ trợ cả token fungible (có thể thay thế) và non-fungible (không thể thay thế). Đây là một cải tiến của **ERC-721**, cho phép quản lý nhiều loại token trong một hợp đồng duy nhất.

2.3 ERC-1155

2. Kỹ thuật của ERC-1155

a. Smart Contract:

ERC-1155 cung cấp một smart contract đa năng có thể tạo và quản lý nhiều loại token khác nhau trong cùng một hợp đồng.

b. Các hàm chuẩn:

balanceOf(address, id): Kiểm tra số lượng token của một ví theo loại token ID.

safeTransferFrom(from, to, id, amount, data): Chuyển token từ một ví này sang ví khác.

mint(id, amount): Tạo thêm token mới cho một ID nhất định.

c. Batch Operations:

- **Batch Transfers:**

Chuyển nhiều token cùng lúc: Cho phép chuyển nhiều NFT và FT trong một giao dịch duy nhất.

- Lợi ích:

Tiết kiệm phí gas: Giảm thiểu chi phí giao dịch trên blockchain.

Tăng hiệu quả: Giảm thời gian và số lượng giao dịch khi quản lý nhiều tài sản.

- **Batch Balance:**

Kiểm tra số dư nhiều token: Cho phép kiểm tra số dư của nhiều token (FT & NFT) cho nhiều địa chỉ cùng lúc.

- Lợi ích:

Giảm số lần gọi hàm: Tối ưu hóa bằng cách kiểm tra nhiều số dư token trong một lần gọi.

Tăng tốc độ xử lý: Thích hợp cho các hệ thống quản lý tài sản lớn hoặc game blockchain với nhiều loại vật phẩm.

2.3 ERC-1155

Batch Approval:
Cấp quyền cho nhiều token: Cấp phép cho một địa chỉ (operator) quản lý nhiều loại token (FT & NFT) cùng một lúc mà không cần cấp quyền từng token riêng lẻ.
Lợi ích:
Dễ dàng quản lý: Không cần phải thiết lập quyền riêng biệt cho mỗi loại token.
Tối ưu hóa giao dịch: Tiết kiệm thời gian và phí gas khi cấp quyền cho nhiều loại token hoặc cho nhiều operator trong một lần gọi hàm.

3. Ứng dụng của ERC-1155

- Tối ưu hóa giao dịch:

ERC-1155 cho phép quản lý nhiều token trong cùng một giao dịch, tiết kiệm chi phí gas khi thực hiện giao dịch nhiều token.

- Được sử dụng trong trò chơi và nền tảng NFT:

ERC-1155 hỗ trợ việc phát hành các vật phẩm game, NFT hoặc thẻ bài trong các trò chơi blockchain.

2.3 ERC-1155

4. Ưu và nhược điểm của ERC-1155

- **Ưu điểm:**

Linh hoạt: Hỗ trợ cả NFT (token không thể thay thế) và FT (token có thể thay thế) trong cùng một hợp đồng thông minh.
Tối ưu chi phí: Giảm phí gas khi thực hiện nhiều giao dịch cùng một lúc nhờ tính năng batch transfers (chuyển nhiều token trong một giao dịch).
Hiệu quả: Giảm số lượng hợp đồng thông minh cần triển khai cho mỗi loại tài sản, giúp tiết kiệm không gian lưu trữ và tối ưu hóa hiệu suất.
Tương tác: Dễ dàng giao tiếp giữa các hợp đồng thông minh khác nhau và tăng cường tính tương tác trong các dự án blockchain.

- **Nhược điểm:**

Phức tạp: Do tính đa năng, cấu trúc của ERC-1155 phức tạp hơn so với ERC-721 và ERC-20, đòi hỏi người phát triển phải hiểu rõ hơn về cách triển khai.
Chưa phổ biến: So với ERC-20 và ERC-721, ERC-1155 vẫn chưa được sử dụng rộng rãi, dẫn đến hệ sinh thái hỗ trợ (ví, sàn giao dịch) chưa phát triển mạnh mẽ.

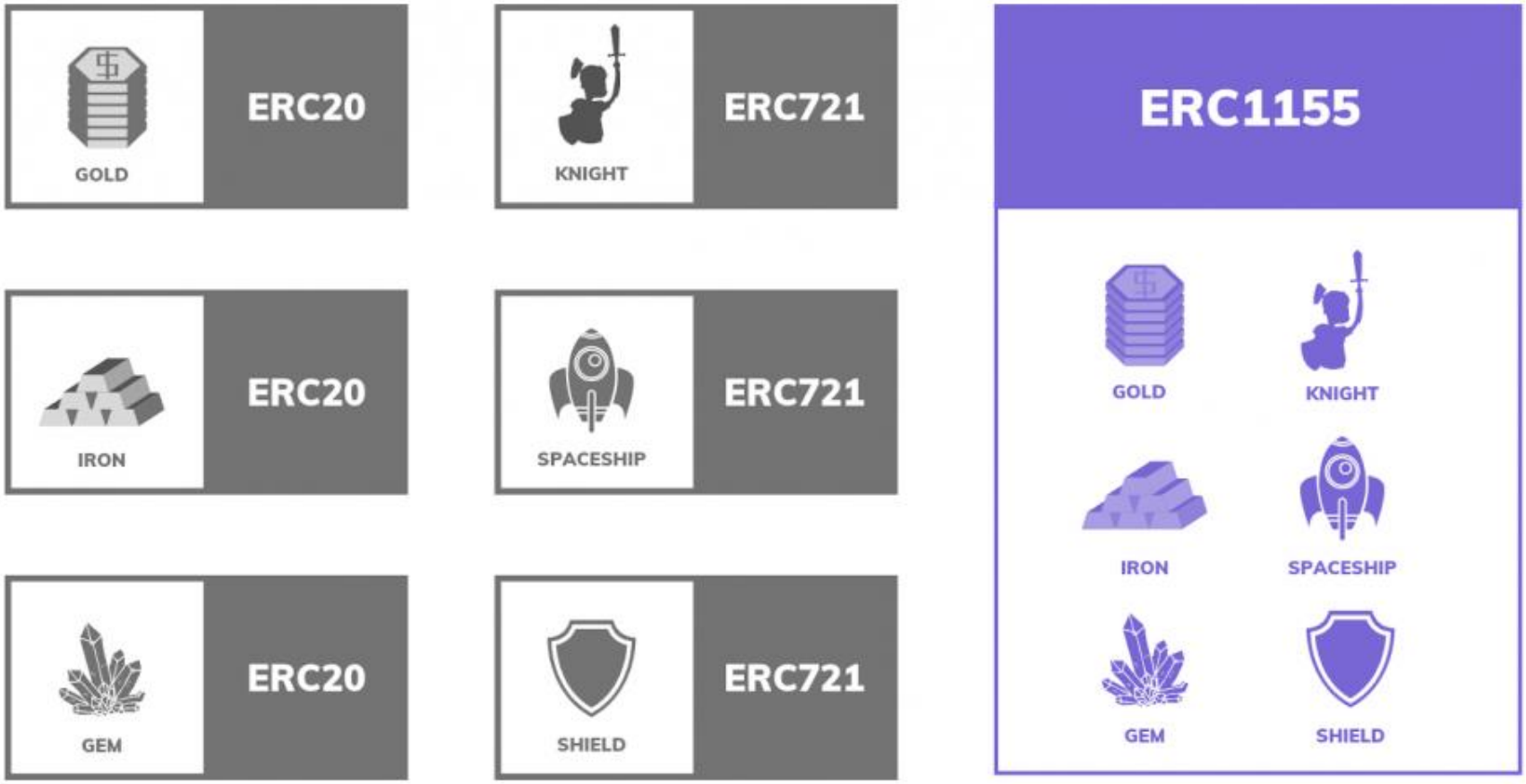
2.3 ERC-1155

4. Ví dụ thực tế của ERC-1155

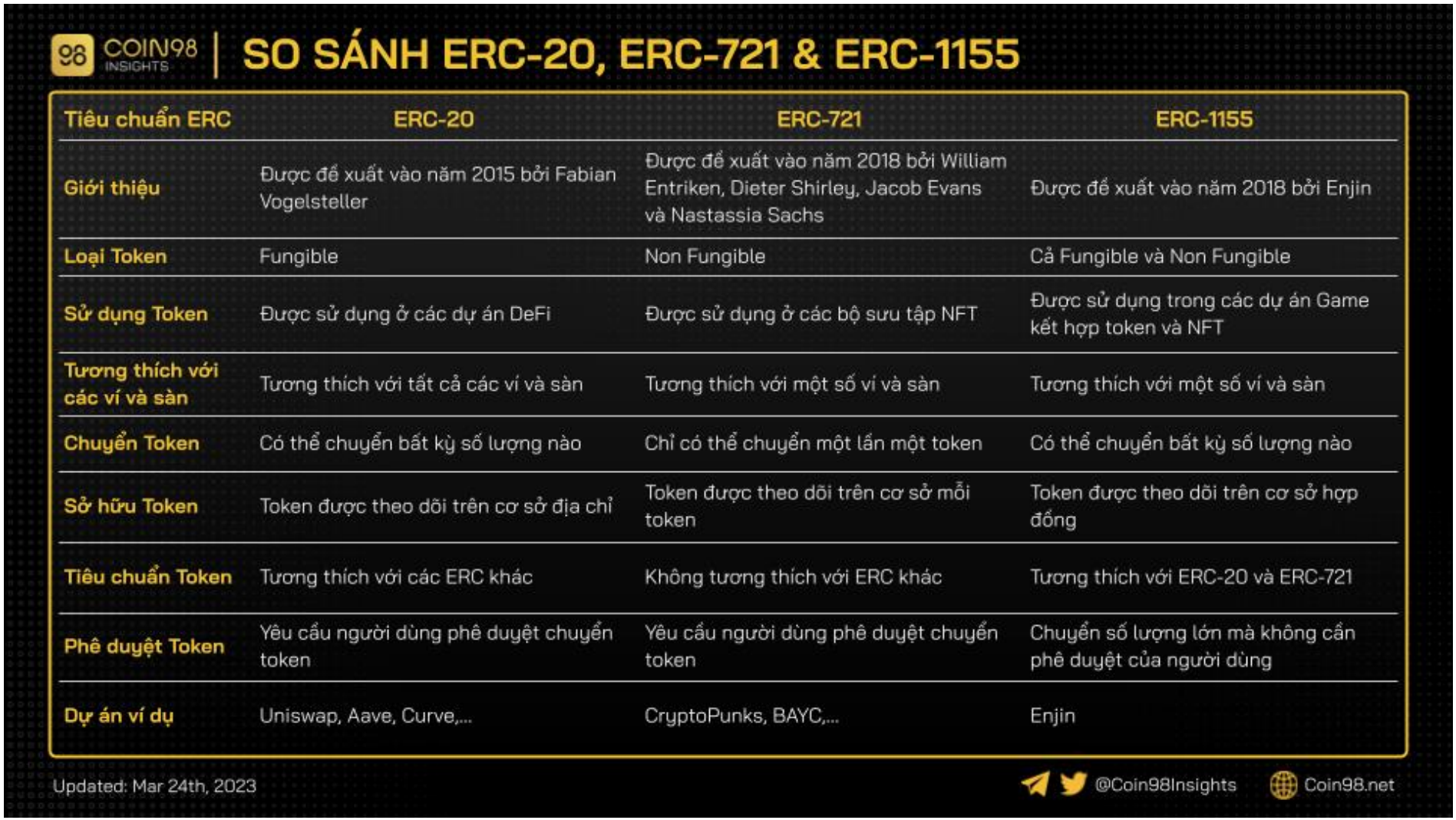
Gods Unchained: Trò chơi blockchain sử dụng ERC-1155 để phát hành các thẻ bài NFT.

Enjin Coin (ENJ): Token hỗ trợ nền tảng cho các trò chơi sử dụng NFT.

2.4 Tổng kết


GOLD
ERC20
KNIGHT
ERC721
IRON
ERC20
SPACESHIP
ERC721
GEM
ERC20
SHIELD
ERC721
ERC1155
GOLD
KNIGHT
IRON
SPACESHIP
GEM
SHIELD

2.4 Tổng kết



Tiêu chuẩn ERC	ERC-20	ERC-721	ERC-1155
Giới thiệu	Được đề xuất vào năm 2015 bởi Fabian Vogelsteller	Được đề xuất vào năm 2018 bởi William Entriken, Dieter Shirley, Jacob Evans và Nastassia Sachs	Được đề xuất vào năm 2018 bởi Enjin
Loại Token	Fungible	Non Fungible	Cả Fungible và Non Fungible
Sử dụng Token	Được sử dụng ở các dự án DeFi	Được sử dụng ở các bộ sưu tập NFT	Được sử dụng trong các dự án Game kết hợp token và NFT
Tương thích với các ví và sàn	Tương thích với tất cả các ví và sàn	Tương thích với một số ví và sàn	Tương thích với một số ví và sàn
Chuyển Token	Có thể chuyển bất kỳ số lượng nào	Chỉ có thể chuyển một lần một token	Có thể chuyển bất kỳ số lượng nào
Sở hữu Token	Token được theo dõi trên cơ sở địa chỉ	Token được theo dõi trên cơ sở mỗi token	Token được theo dõi trên cơ sở hợp đồng
Tiêu chuẩn Token	Tương thích với các ERC khác	Không tương thích với ERC khác	Tương thích với ERC-20 và ERC-721
Phê duyệt Token	Yêu cầu người dùng phê duyệt chuyển token	Yêu cầu người dùng phê duyệt chuyển token	Chuyển số lượng lớn mà không cần phê duyệt của người dùng
Dự án ví dụ	Uniswap, Aave, Curve,...	CryptoPunks, BAYC,...	Enjin

2.4 Tổng kết

Mỗi chuẩn token có mục đích và ứng dụng khác nhau trong hệ sinh thái blockchain.
ERC-20: Dành cho thanh toán và giao dịch token (DeFi).
ERC-721: Tạo ra các **NFT** độc nhất.
ERC-1155: Hỗ trợ cả **NFT** và **token** thông thường trong cùng một hệ thống.

The End

ONE LOVE. ONE FUTURE.