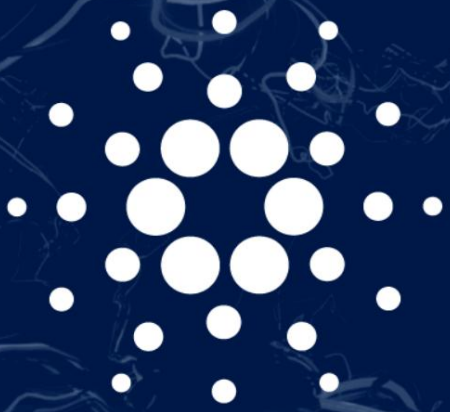


CARDANO

EUTXO Handbook

Giới thiệu

Mạng lưới chuỗi khối là cấu trúc dữ liệu phức tạp. Các giao dịch liên tục đan xen trong chuỗi, tạo ra dấu chân kỹ thuật số yêu cầu theo dõi và quản lý cẩn thận để duy trì tính toàn vẹn và độ tin cậy của sổ cái cơ bản.

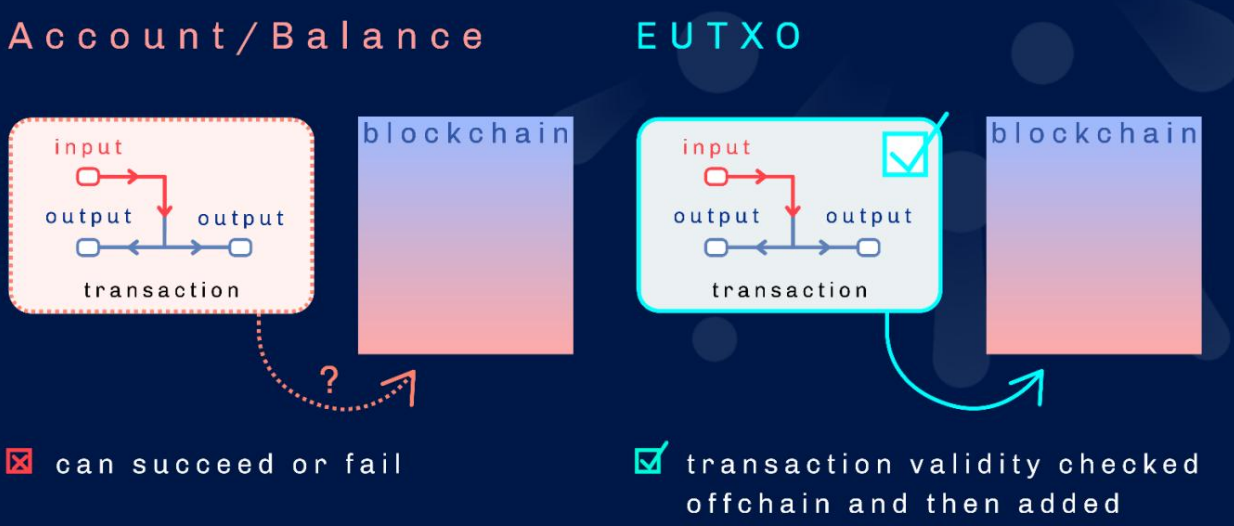
Hai sổ cái kế toán chính tồn tại trong không gian blockchain: chuỗi khối dựa trên UTXO (ví dụ: Bitcoin) và chuỗi Tài khoản / Số dư (Ethereum và các chuỗi khác).

Cardano kết hợp mô hình UTXO của Bitcoin với khả năng xử lý các hợp đồng thông minh thành một mô hình kế toán Đầu ra giao dịch chưa được trả trước mở rộng (EUTXO). Việc áp dụng EUTXO tạo điều kiện thuận lợi cho việc triển khai hợp đồng vào chuỗi Cardano.

The EUTXO model offers unique advantages over other accounting models.

Mô hình EUTXO cung cấp những ưu điểm độc đáo so với các mô hình kế toán khác. Ví dụ: sự thành công hay thất bại của việc xác thực giao dịch chỉ phụ thuộc vào bản thân giao dịch và các đầu vào của nó, chứ không phụ thuộc vào bất kỳ thứ gì khác trên blockchain. Do đó, tính hợp lệ của một giao dịch có thể được kiểm tra ngoài chuỗi, trước khi giao dịch được gửi đến chuỗi khối. Một giao dịch vẫn có thể thất bại nếu một số giao dịch đồng thời sử dụng một đầu vào mà giao dịch đang mong đợi, nhưng nếu tất cả các đầu vào vẫn còn,

giao dịch được đảm bảo thành công. Điều này hoàn toàn trái ngược với Ethereum, nơi mà các giao dịch có thể không thực hiện được giữa chừng.



Hiểu được EUTXO đòi hỏi bạn phải hiểu mô hình kế toán blockchain là gì, tại sao nó cần, chức năng và đặc điểm của nó.

Mô hình kế toán blockchain là gì?

Mọi công ty, doanh nghiệp hoặc tổ chức thương mại đều yêu cầu một bảng cân đối kế toán để ghi chép chính xác về lãi, lỗ, dòng tiền và các thông số khác. Bằng cách duy trì kế toán cẩn thận tất cả dữ liệu này, các công ty có thể, trong nháy mắt, hình dung tình trạng tài chính của họ tại bất kỳ thời điểm nào. Sổ cái kế toán của một công ty cung cấp một lợi thế khác: Khả năng theo dõi nguồn gốc và quyền sở hữu của các quỹ.

Mạng lưới chuỗi khối cũng yêu cầu một mô hình kế toán để xác định ai sở hữu những đồng tiền nào (và bao nhiêu đồng tiền trong số chúng), theo dõi những đồng tiền đó đi đâu, những đồng nào đã được sử dụng hết và những đồng nào còn khả dụng để chi tiêu.

Mô hình UTXO so với mô hình Tài khoản / Số dư: một tổng quan ngắn gọn

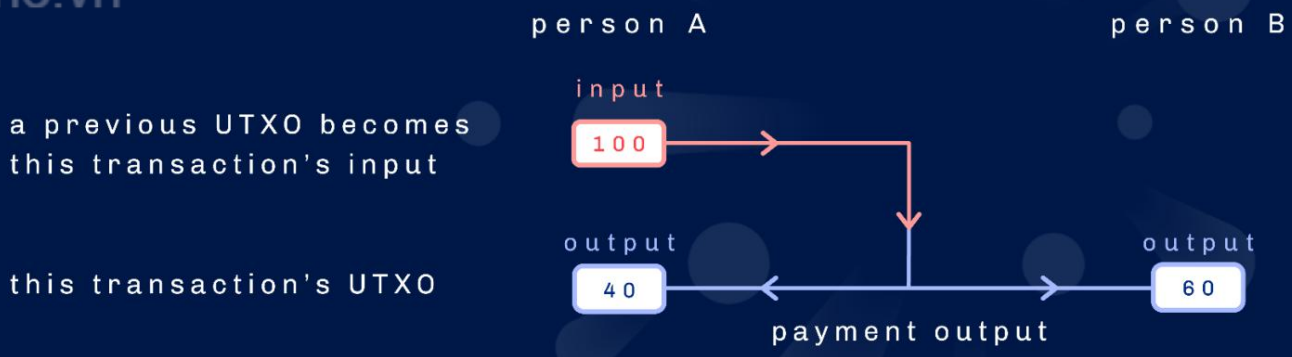
Nhiều thập kỷ trước, kế toán sử dụng sổ cái với các bút toán viết tay để ghi chép về chuyển động của các quỹ. Ngày nay, các công ty sử dụng phiên bản điện tử của cùng một thứ. Các blockchain sử dụng các giao dịch như các bản ghi (giống như các mục nhập trên sổ cái) để theo dõi nguồn gốc và quyền sở hữu. Các giao dịch này chứa rất nhiều thông tin (tiền đến từ đâu, chúng đi đâu và bất kỳ thay đổi nào còn sót lại từ các giao dịch này).

Dưới đây là tổng quan ngắn gọn về các mô hình UTXO và Tài khoản / Số dư:

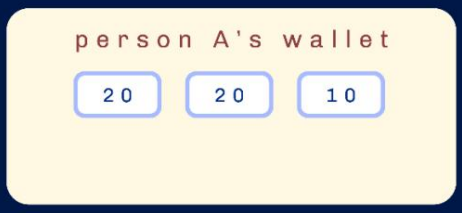
UTXO

Trong mô hình UTXO, chuyển động của nội dung được ghi lại trong dạng của một đồ thị xoay chiều có hướng trong đó các nút là các giao dịch và các cạnh là các đầu ra giao dịch, trong đó mỗi giao dịch bổ sung tiêu tốn một số UTXO và thêm những cái mới. Ví của người dùng theo dõi danh sách các kết quả đầu ra chưa sử dụng được liên kết với tất cả các địa chỉ do người dùng sở hữu và tính toán số dư của người dùng.

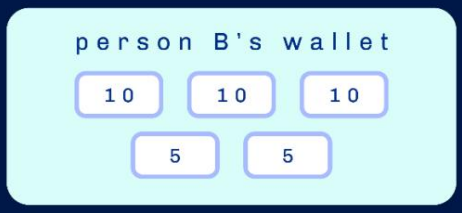
...each additional transaction consumes some of the UTXOs and adds new ones.



UTXO, theo nhiều cách, tương tự như tiền mặt. Một phép tương tự tốt là thế này: hãy tưởng tượng bạn có 50 đô la trong ví của mình. Số tiền này có thể được tạo thành từ một số kết hợp: hai tờ 20 đô la và một tờ 10 đô la, bốn tờ 10 đô la và hai tờ 5 đô la, và nhiều loại khác. Nhưng bất kể hoán vị, số tiền ($ 50) vẫn bằng nhau. UTXO hoạt động theo cách tương tự. Bất kỳ số dư nào bạn có trong ví blockchain của mình (ví dụ: 150 đồng tiền) có thể được tạo thành từ nhiều kết hợp UTXO khác nhau, dựa trên các giao dịch trước đó, nhưng số dư vẫn giữ nguyên. Nói cách khác, số dư được giữ trong một địa chỉ ví nhất định là tổng của tất cả các UTXO chưa sử dụng từ các giao dịch trước đó.



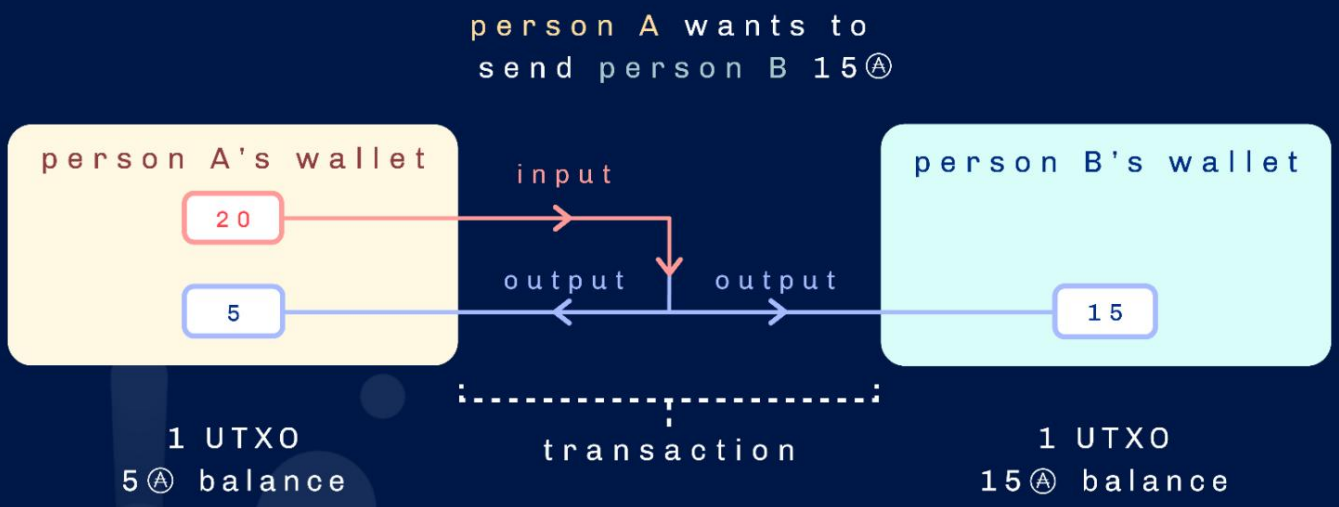
3 UTXOs
50Ⓐ balance



5 UTXOs
40Ⓐ balance

Khái niệm 'thay đổi' trong các mô hình UTXO

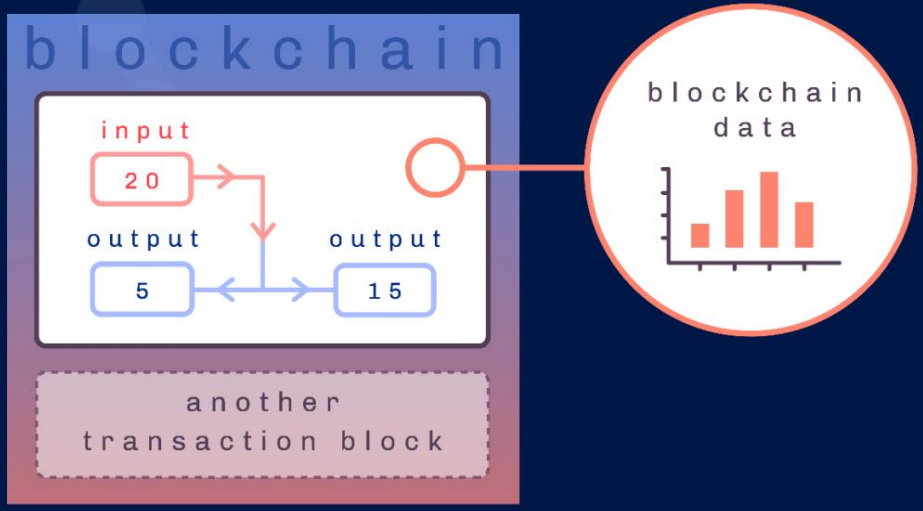
Giống như giao dịch tiền mặt trong bất kỳ cửa hàng nào, UTXO giới thiệu 'tiền lẻ'. Ví dụ, khi bạn lấy ra một tờ 50 đô la từ ví của mình, bạn không thể xé tờ tiền đó thành nhiều phần nhỏ hơn để thanh toán cho một thứ có giá 15 đô la chẳng hạn. Bạn phải giao toàn bộ hóa đơn 50 đô la và nhận tiền lẻ từ nhân viên thu ngân. UTXO hoạt động theo cách tương tự. Bạn không thể 'tách' UTXO thành các bit nhỏ hơn. UTXO được sử dụng toàn bộ và thay đổi được trả lại cho địa chỉ ví của bạn dưới dạng UTXO nhỏ hơn.



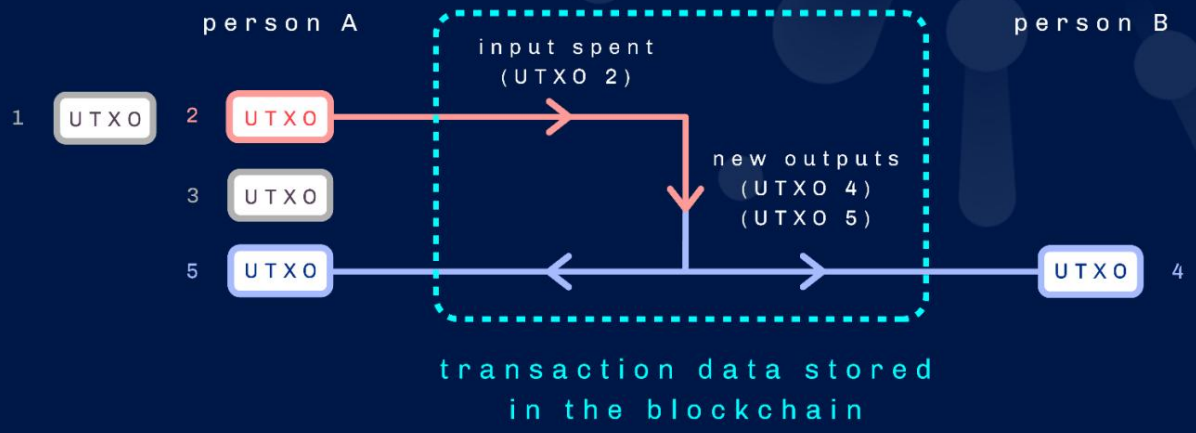
UTXOs are used whole, and change is given back to your wallet's address in the form of a smaller UTXO.

Ưu điểm của mô hình UTXO

Bằng cách kiểm tra và theo dõi kích thước, độ tuổi và số lượng UTXO được chuyển đi xung quanh, người ta có thể trích xuất các số liệu chính xác về việc sử dụng blockchain và hoạt động tài chính của chuỗi.



Các mô hình UTXO cung cấp các lợi thế khác. Ví dụ: khả năng mở rộng tốt hơn nhờ song song hợp đồng thông minh và quyền riêng tư. Ngoài ra, logic giao dịch được đơn giản hóa, vì mỗi UTXO chỉ có thể được sử dụng một lần và toàn bộ, điều này làm cho việc xác minh giao dịch đơn giản hơn nhiều.



Để tổng hợp UTXO:

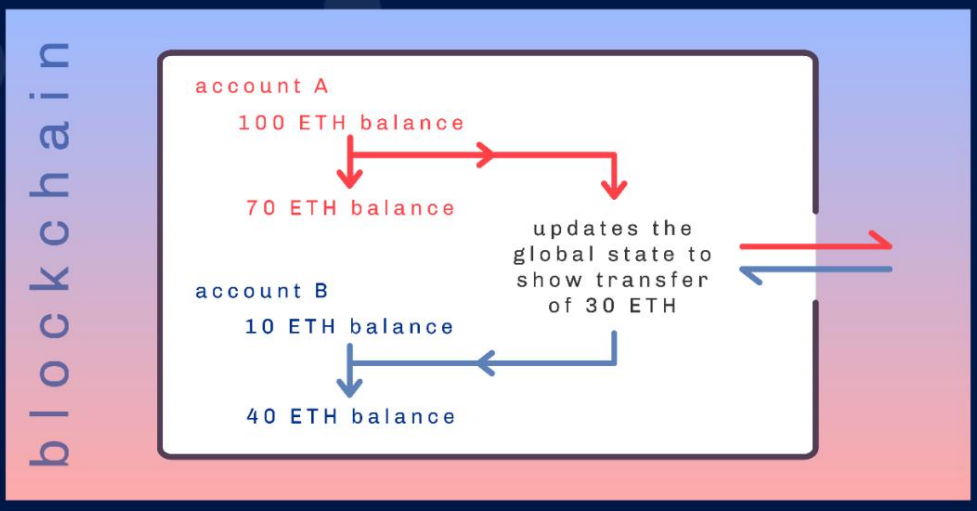
- UTXO là đầu ra của giao dịch trước đó, có thể được chi tiêu trong Tương lai
- Chuỗi UTXO không có tài khoản. Thay vào đó, tiền xu được lưu trữ dưới dạng danh sách các UTXO, và các giao dịch được tạo ra bằng cách sử dụng các UTXO hiện có và tạo ra các UTXO mới ở vị trí của chúng
- Số dư là tổng số UTXO được kiểm soát bởi một địa chỉ nhất định
- UTXO giống tiền mặt ở chỗ chúng sử dụng 'tiền lẻ' và không thể phân chia (UTXO được sử dụng toàn bộ)

Mô hình Tài khoản / Số dư

Như tên đã chỉ ra, các mô hình blockchain triển khai mô hình kế toán Tài khoản / Số dư sử dụng tài khoản (có thể được kiểm soát bằng khóa cá nhân hoặc hợp đồng thông minh) để giữ số dư tiền xu. Trong mô hình này, tài sản được biểu thị dưới dạng số dư trong tài khoản của người dùng và số dư được lưu trữ dưới dạng trạng thái toàn cầu của tài khoản, được giữ bởi mỗi nút và được cập nhật với mọi giao dịch.

Theo nhiều khía cạnh, chuỗi Tài khoản / Số dư (chẳng hạn như Ethereum) hoạt động theo cách tương tự như ngân hàng truyền thống các tài khoản. Số dư của ví tăng lên khi tiền xu ký gửi và giảm khi tiền xu được chuyển đi nơi khác. Sự khác biệt quan trọng ở đây là, không giống như UTXO, bạn có thể sử dụng một phần số dư của mình. Vì vậy, ví dụ: nếu bạn có 100 ETH trong tài khoản của mình, bạn có thể gửi một phần trong số đó (giả sử, 30 ETH) cho người khác. Số dư kết quả sẽ còn lại 70 ETH trong tài khoản của bạn và địa chỉ nơi bạn gửi tiền đến sẽ tăng thêm 30 ETH. Khái niệm thay đổi không áp dụng trong các mô hình kế toán Tài khoản / Số dư vì nó làm trong những cái UTXO.

Account/Balance chains operate in a similar fashion to traditional bank accounts.



Để tổng hợp mô hình Tài khoản / Số dư:

- Mô hình kế toán này giống với cách hoạt động của một ngân hàng
- Người dùng có tài khoản giữ số dư tiền xu của họ
- Có thể chi tiêu một phần số dư
- Không áp dụng khái niệm thay đổi.

Mô hình EUTXO

Để hiểu về EUTXO, điều quan trọng là phải hiểu cách thức hoạt động của các giao dịch trong Cardano. Đặc biệt là vai trò của đầu ra và đầu vào của giao dịch.

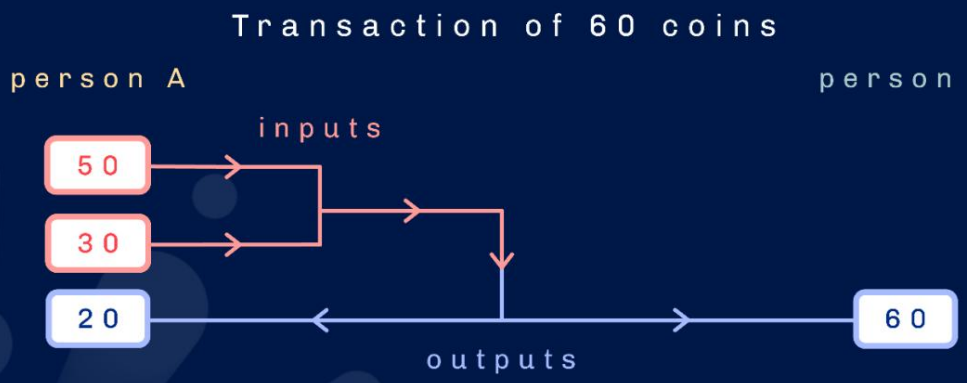
Chúng ta cần nói về các giao dịch: Đầu ra và Đầu vào

Think of a transaction as the action that unlocks previous outputs, and creates new ones.

Kỳ hạn giao dịch thường gợi lên tiếng vang về tài chính. Mặc dù ý nghĩa như vậy sẽ áp dụng cho Bitcoin (vì chuỗi khối Bitcoin được sử dụng để chuyển tiền giữa các đồng nghiệp), nhiều blockchain khác (bao gồm cả Cardano) linh hoạt hơn nhiều. Trong những trường hợp này, thuật ngữ 'giao dịch' có nhiều sắc thái hơn. Người ta có thể coi các giao dịch là sự chuyển giao giá trị.

Trong môi trường blockchain, mỗi giao dịch có thể có một hoặc nhiều đầu vào và một hoặc nhiều

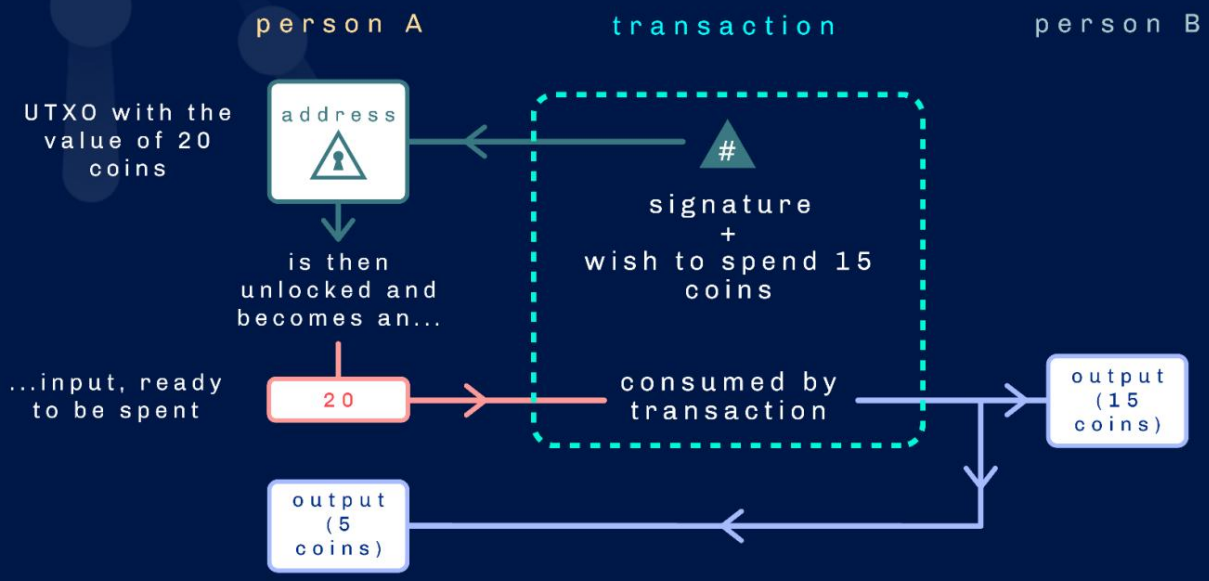
kết quả đầu ra. Các khái niệm về Đầu vào và Đầu ra phải được hiểu, nếu người ta muốn hiểu cách một giao dịch hoạt động và nó liên quan như thế nào đến UTXO. Nói một cách trừu tượng, hãy nghĩ về một giao dịch là hành động mở khóa các đầu ra trước đó và tạo những cái mới.



Sản lượng giao dịch

Đầu ra giao dịch bao gồm một địa chỉ (mà bạn có thể coi là một khóa) và một giá trị. Để phù hợp với sự tương tự này, chữ ký thuộc địa chỉ là chìa khóa để mở khóa đầu ra. Sau khi mở khóa, một đầu ra có thể được sử dụng làm đầu vào.

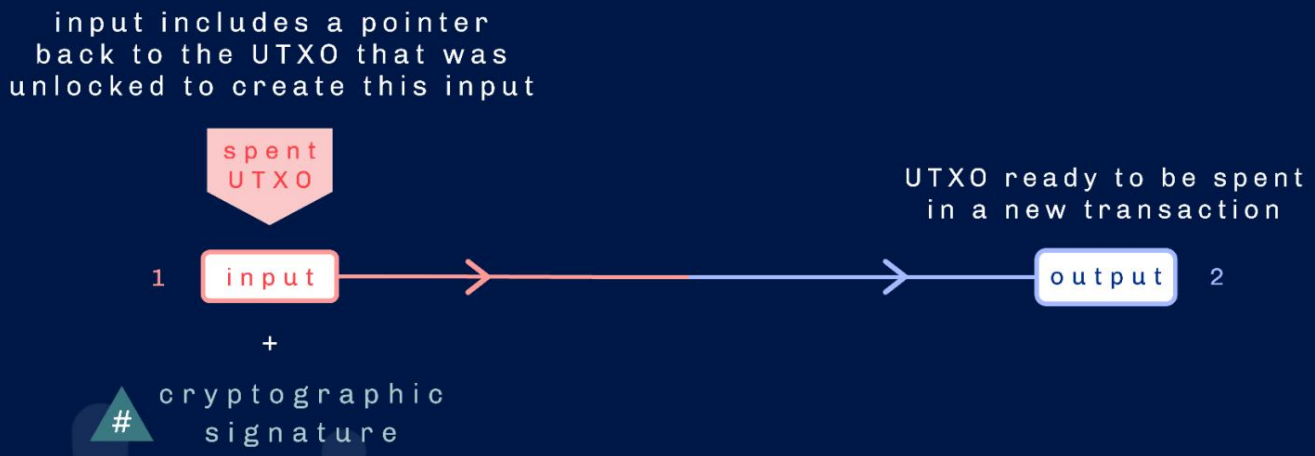
Các giao dịch mới chi tiêu kết quả đầu ra của các giao dịch trước đó và tạo ra kết quả đầu ra mới có thể được sử dụng bởi các giao dịch trong tương lai. Mỗi UTXO chỉ có thể được sử dụng một lần và toàn bộ. Mỗi đầu ra có thể được chi tiêu bởi chính xác một đầu vào và chỉ một đầu vào.



Đầu vào giao dịch

Đầu vào giao dịch là đầu ra của giao dịch trước đó. Đầu vào giao dịch bao gồm một con trỏ và một chữ ký mật mã đóng vai trò là chìa khóa mở khóa.
Con trỏ tham chiếu trở lại đầu ra giao dịch trước đó và khóa sẽ mở đầu ra này. Khi một đầu ra được mở khóa bởi một đầu vào, blockchain sẽ đánh dấu đầu ra đã mở khóa là "đã chi tiêu". Các đầu ra mới được tạo ra bởi một giao dịch nhất định sau đó có thể được trỏ đến bởi các đầu vào mới và do đó, chuỗi tiếp tục. Các đầu ra mới này (chưa được mở khóa, tức là đã sử dụng) là UTXO. Kết quả đầu ra chưa được chi tiêu chỉ đơn giản là kết quả đầu ra chưa được chi tiêu.

Transaction inputs include a pointer and a cryptographic signature that acts as the unlocking key.



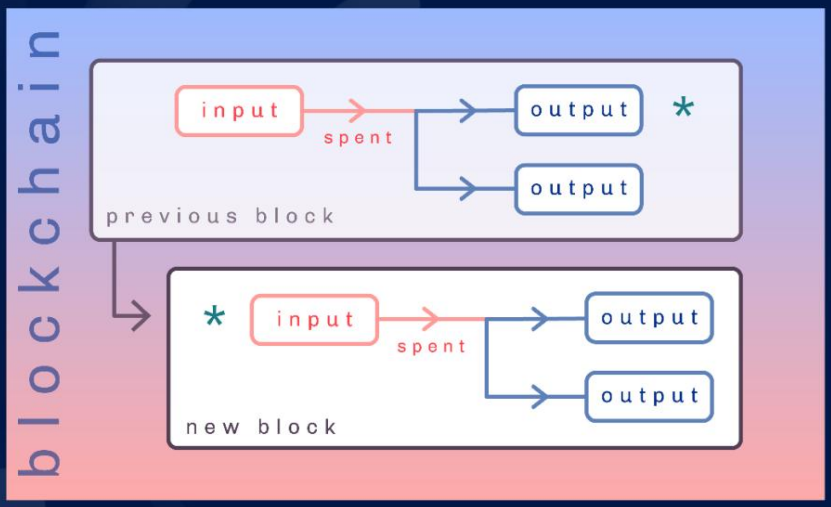
Tóm lại, UTXO hoạt động như thế nào

Trong mô hình kế toán UTXO, các giao dịch sử dụng các kết quả đầu ra chưa sử dụng từ các giao dịch trước đó và tạo ra các kết quả đầu ra mới có thể được sử dụng làm đầu vào cho giao dịch trong tương lai.

Every blockchain node maintains a record of the subset of all UTXOs at all times.

Ví của người dùng quản lý các UTXO này và bắt đầu các giao dịch liên quan đến các UTXO do người dùng sở hữu. Mỗi nút blockchain duy trì một bản ghi của tập hợp con của tất cả các UTXO tại mọi thời điểm. Đây được gọi là Bộ UTXO. Về mặt kỹ thuật, đây là chainstate, được lưu trữ trong thư mục dữ liệu của mọi nút.

Khi một khối mới được thêm vào chuỗi, chuỗi sẽ được cập nhật tương ứng. Khối mới này chứa danh sách các giao dịch mới nhất (tất nhiên bao gồm cả bản ghi của các UTXO đã sử dụng và các giao dịch mới được tạo kể từ khi hội thảo được cập nhật lần cuối). Mỗi nút duy trì một bản sao chính xác của chainstate.



* UTXO is unlocked and becomes new input

EUTXO là một cơ chế giao dịch kết hợp:

- Hợp đồng thông minh: các UTXO khóa kín này, ada, nội dung gốc và NFT.
- Người quản lý: dữ liệu do người dùng cung cấp được cung cấp để mở khóa tài sản bị khóa và chi tiêu họ.
- Datum: dữ liệu như điểm cao, thông tin người dùng hoặc thông tin khác có liên quan đến ứng dụng của bạn

- Bối cảnh: thông tin như siêu dữ liệu về giao dịch đang được xác thực.

EUTXO components

Contract

Smart contracts are programmes stored on the blockchain that run when preexisting conditions are met. They can be thought of as locks that hold UTXOs, ada on the Cardano blockchain

Redeemer

The data passed from the user to the smart contract. In a simple UTXO a redeemer could be a signature which provides proof of ownership of the UTXO and access to the contents

Datum

A piece of information that can be associated with a UTXO. It is used to carry script state information such as its owner or the timing details (which define when the UTXO can be spent)

Context

The context is essentially a summary of the pending transaction and includes information about witnesses, certificates as well as how value is flowing as it allows access to transactions inputs and outputs

EUTXO: lý do đằng sau sự lựa chọn của Cardano

Mô hình kế toán UTXO 'vani' của Bitcoin sẽ không phù hợp với Cardano, vì Cardano được thiết kế để làm nhiều việc hơn là xử lý các khoản thanh toán. Đặc biệt, nhu cầu về khả năng diễn đạt lập trình nhiều hơn cho chức năng hợp đồng thông minh đã yêu cầu một giải pháp mới ('Mở rộng').

Mô hình UTXO 'cơ bản' có hạn chế về khả năng lập trình.
Mô hình kế toán Tài khoản / Số dư của Ethereum đã giải quyết vấn đề cụ thể này bằng việc phát triển sổ cái Tài khoản / Số dư và các tài khoản hợp đồng liên quan. Nhưng khi làm như vậy, ngữ nghĩa của mã hợp đồng trở nên phức tạp hơn nhiều, điều này có tác dụng không mong muốn là buộc các tác giả hợp đồng phải nắm bắt đầy đủ các sắc thái của ngữ nghĩa để tránh việc giới thiệu có khả năng rất tốn kém
lỗ hổng trong mã.

Giải pháp UTXO 'mở rộng' sẽ yêu cầu hai phần chức năng bổ sung mà mô hình UTXO hiện tại không thể cung cấp:

1 - Để có thể duy trì trạng thái hợp đồng

2 - Để có thể thực thi rằng cùng một mã hợp đồng là được sử dụng dọc theo toàn bộ chuỗi giao dịch. Đây được gọi là tính liên tục.

A powerful feature of the EUTXO model is that the fees required for a valid transaction can be predicted precisely prior to posting it.

Một tính năng mạnh mẽ của mô hình EUTXO là các khoản phí cần thiết cho một giao dịch hợp lệ có thể được dự đoán chính xác trước khi đăng nó. Đây là một tính năng độc đáo không có trong các mô hình Tài khoản / Số dư.

Plutus Core

Việc triển khai EUTXO bao gồm hai yếu tố chính giúp phân biệt nó với mô hình Tài khoản / Số dư: tập lệnh và dữ liệu. Tập lệnh yêu cầu một ngôn ngữ kịch bản xác định, được chỉ định rõ ràng và điều quan trọng là phải xác định loại dữ liệu

được gắn vào kết quả đầu ra và được sử dụng như bộ định nghĩa lại. Dữ liệu của Redeemer là một kiểu dữ liệu đơn giản (đại số) có thể dễ dàng xác định trong Haskell.

Plutus Core, ngôn ngữ kịch bản của Cardano, cung cấp hai yếu tố này. Nó là một ngôn ngữ đơn giản và có chức năng tương tự như Haskell. Thật vậy, một tập hợp con lớn của Haskell có thể được sử dụng để viết các tập lệnh Plutus Core. Các nhà phát triển không viết bất kỳ mã Plutus Core nào. Một trình cắm thêm trình biên dịch Haskell tạo ra tất cả các tập lệnh Plutus Core.

The implementation of EUTXO includes two key elements that differentiates it from an Account/Balance model: script and data.

Các nút thực thi các tập lệnh này trong quá trình xác thực giao dịch 'trực tiếp' trên chuỗi. Các tập lệnh có thể khóa các UTXO dưới dạng các tập lệnh trình xác thực hoặc dưới dạng các chính sách đúc tiền, kiểm soát việc in và ghi mã thông báo gốc.

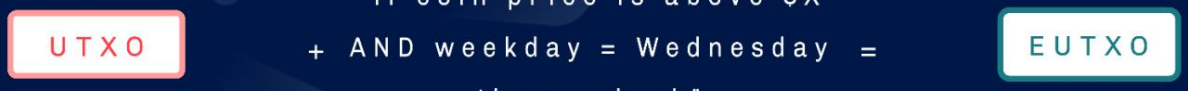
Các thư viện Haskell thích hợp đơn giản hóa việc viết logic xác thực như vậy bằng cách cung cấp các kiểu dữ liệu cốt lõi để kiểm tra các giao dịch trong quá trình xác thực và bằng cách cung cấp nhiều chức năng trợ giúp và trừu tượng cấp cao hơn. Điều này cho phép các tác giả hợp đồng tập trung vào logic nghiệp vụ và không phải lo lắng về quá nhiều chi tiết cấp thấp.

Làm thế nào để mô hình EUTXO mở rộng UTXO?

EUTXO mở rộng mô hình UTXO 'cơ bản' theo hai hướng:

1. Nó khái quát khái niệm 'địa chỉ' bằng cách sử dụng phép tương tự khóa và chìa khóa.

   Thay vì giới hạn khóa đối với khóa công khai và khóa đối với chữ ký, địa chỉ trong mô hình EUTXO có thể chứa logic tùy ý dưới dạng tập lệnh. Ví dụ: khi một nút xác thực một giao dịch, nút
   xác định xem giao dịch có được phép sử dụng một số
   đầu ra như một đầu vào. Giao dịch sẽ tra cứu tập lệnh được cung cấp bởi địa chỉ của đầu ra và sẽ thực thi tập lệnh nếu giao dịch có thể sử dụng đầu ra làm đầu vào.



2. Sự khác biệt thứ hai giữa UTXO và EUTXO là đầu ra có thể mang (hầu như) dữ liệu tùy ý ngoài một địa chỉ và giá trị. Điều này làm cho các tập lệnh trở nên mạnh mẽ hơn nhiều bằng cách cho phép chúng mang trạng thái.

Ở đây, chúng tôi trình bày điều gì làm cho EUTXO trở nên độc đáo và tại sao mô hình kế toán này lại vượt trội hơn so với UTXO 'vani'.

Các tính năng của EUTXO	Tại sao nó quan trọng
Mỗi UTXO có một địa chỉ, một giá trị và một số liệu, là một phần dữ liệu theo hợp đồng cụ thể. Datum còn được gọi là đối tượng datum. Dữ liệu được chuyển vào như một đối số bổ sung trong quá trình xác thực.	Nó cho phép một hợp đồng mang một số trạng thái (datum) mà không cần thay đổi mã của nó.
Trình xác thực nhận được ngữ cảnh, đó là thông tin về giao dịch đang được xác thực. Thông tin này được chuyển vào như một đối số bổ sung của loại Ngữ cảnh.	Thông tin được cung cấp trong ngữ cảnh cho phép trình xác thực để thực thi nhiều điều kiện tốt hơn có thể với mô hình UTXO 'trần'. Đặc biệt, nó có thể kiểm tra đầu ra của giao dịch hiện tại, điều này rất cần thiết để đảm bảo tính liên tục của hợp đồng.
EUTXO cung cấp một mức độ truy cập nhất định vào thời gian bằng cách thêm khoảng thời gian hiệu lực vào các giao dịch. Đây là khoảng thời gian của bọ ve (được định nghĩa là	Khoảng thời gian này cho phép bất kỳ tập lệnh nào đang chạy trong quá trình xác thực để giả định rằng đánh dấu hiện tại nằm trong khoảng thời gian đó, nhưng tập lệnh không

một đơn vị tiến trình tăng đơn điệu trong hệ thống sổ cái. Điều này thường tương ứng với số khối hoặc chiều cao khối) mà trong đó một giao dịch có thể xử lý.	không biết giá trị chính xác của đánh dấu hiện tại.

Tại sao EUTXO lại vượt trội hơn UTXO?

- Khả năng phân quyền và bảo mật của Cardano được cải thiện hơn so với Bitcoin. Cardano cũng cung cấp các tính năng hợp đồng thông minh vượt trội so với chuỗi Tài khoản / Số dư. • Hỗ trợ đa tài sản và hợp đồng thông minh. • Tính linh hoạt, bảo mật, ổn định và khả năng mở rộng cao hơn. • Nhiều giao dịch đồng thời hơn trên hệ thống bằng chứng cổ phần chỉ thu hút một phần nhỏ năng lượng được yêu cầu bởi chuỗi khối bằng chứng công việc.

- IOG đã hợp tác với bảy blockchain dựa trên UTXO khác thuộc Liên minh UTXO để thúc đẩy ranh giới của sự đổi mới và khả năng tương tác, đồng thời cải thiện nó hơn nữa.

EUTXO làm bàn đạp để mở rộng quy mô Cardano vào năm 2022

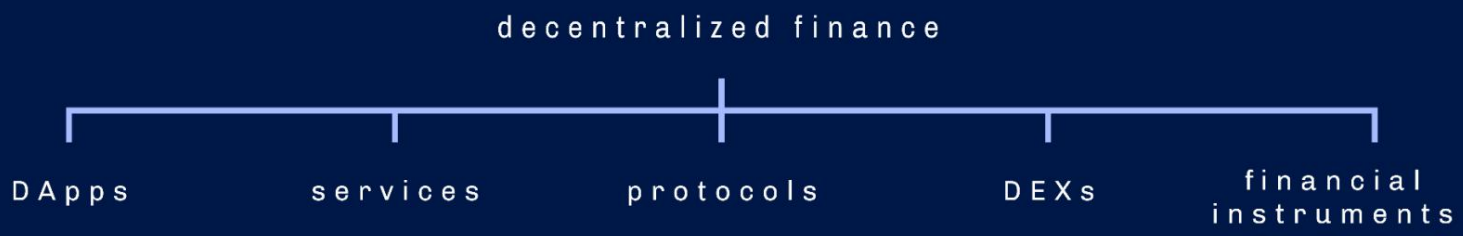
Mặc dù nó đưa ra một mô hình và cách suy nghĩ mới, nhưng EUTXO cung cấp cho các nhà phát triển hợp đồng thông minh một nền tảng khá mạnh mẽ và linh hoạt để xây dựng và triển khai các ứng dụng của họ.

Năm nay, Input Output Global Inc. đang tận dụng sức mạnh của EUTXO để tối ưu hóa các hợp đồng thông minh được xây dựng trên Cardano theo ba cách:

- Đầu vào tham chiếu (CIP-0031) - Tập lệnh Plutus có thể kiểm tra giao dịch đầu vào mà không cần phải chi tiêu chúng. Điều này có nghĩa là không cần thiết phải tạo UTXO chỉ để kiểm tra thông tin do đầu vào nắm giữ
- Plutus Datums (CIP-0032) - Datums có thể được gắn trực tiếp vào đầu ra thay vì băm dữ liệu. Điều này đơn giản hóa cách dữ liệu được sử dụng, vì người dùng có thể thấy dữ liệu thực tế hơn là phải cung cấp dữ liệu khớp với hàm băm đã cho
- Chia sẻ tập lệnh (CIP-0033) - Có thể liên kết các tham chiếu tập lệnh Plutus với kết quả đầu ra của giao dịch, nghĩa là chúng có thể được ghi lại trên chuỗi để sử dụng lại sau này. Sẽ không cần thiết phải cung cấp một bản sao của tập lệnh với mỗi giao dịch, giảm đáng kể sự cọ xát cho các nhà phát triển. Việc sử dụng lại các tập lệnh trong nhiều giao dịch làm giảm đáng kể kích thước giao dịch, cải thiện thông lượng và giảm chi phí thực thi tập lệnh.

Mọi điều bạn luôn muốn biết về sự mất mát vô thường và đã ngại hỏi

Tài chính phi tập trung (DeFi) là một thuật ngữ bao hàm đề cập đến các ứng dụng phi tập trung (DApps), dịch vụ, giao thức và công cụ tài chính được xây dựng trên blockchain. Đây là một phân khúc ngành tương đối mới được kích hoạt bởi công nghệ sổ cái phi tập trung, có nghĩa là không có cơ quan quyền lực duy nhất có quyền kiểm soát tập trung đối với hệ thống. Và bất cứ ai quen thuộc với môi trường DeFi có lẽ đều biết về sự mất mát vô thường. Đó là một khái niệm đơn giản với một cái tên gây hiểu lầm.



Cardano là một blockchain thế hệ thứ ba có các tính năng mở rộng của vũ trụ DeFi , trong số nhiều DApp khác, các sàn giao dịch phi tập trung (DEX). Đây là các giao thức trao đổi tiền điện tử cho phép các đồng nghiệp giao dịch tiền điện tử với nhau. DEX sử dụng hai kiến trúc thiết kế chính: nhà tạo lập thị trường tự động (AMM) và sổ đặt hàng. Việc triển khai AMM tương đối đơn giản và thiết kế này đã trở thành sự lựa chọn trên thực tế cho các chuỗi Tài khoản / Số dư, bao gồm cả Ethereum. Tuy nhiên, thiết kế này có một số khiếm khuyết cố hữu. Ví dụ, khuynh hướng của họ là gánh chịu sự mất mát vô thường.

Decentralized exchanges (DEXs) are crypto exchange protocols that enable peers to trade cryptocurrencies with each other.

Cardano sử dụng mô hình kế toán EUTXO để theo dõi sự di chuyển của tài sản trong toàn bộ chuỗi. EUTXO là xác định, cung cấp khả năng dự đoán tốt hơn về mất mát vô thường.

Những khái niệm dường như không liên quan này kết hợp thành một tác động qua lại rất thú vị trên blockchain. Bài viết này xem xét các thiết kế của DEX và giải thích tại sao EUTXO cung cấp khả năng dự đoán về tổn thất vô thường tốt hơn so với kế toán Tài khoản / Số dư các mô hình.

Tổn thất vĩnh viễn: định nghĩa

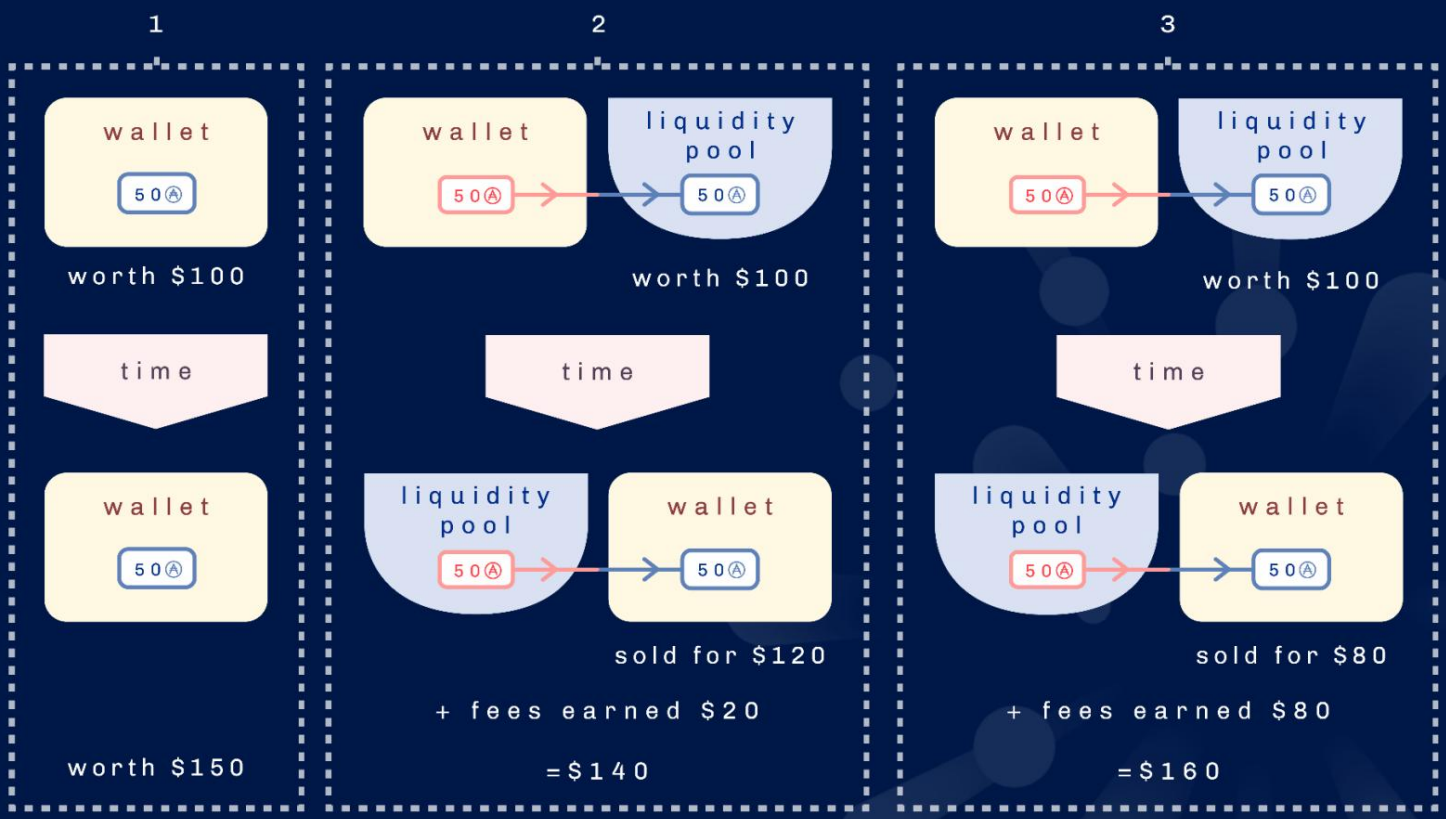
Khi tổng giá trị của tài sản được cung cấp dưới dạng tính thanh khoản thấp hơn giá trị mà lẽ ra bạn đã tích lũy được nếu bạn chỉ cần nắm giữ chúng.

Đây là định nghĩa đơn giản nhất về tổn thất vô thường, một khái niệm gây sợ hãi cho các nhà cung cấp thanh khoản.

Tổn thất vĩnh viễn xảy ra khi giá của tài sản được gửi vào quỹ thanh khoản thay đổi (lên hoặc xuống) so với thời điểm chúng được ký gửi. Nói cách khác, giá trị tài sản của bạn khi bạn rút ra khác với khi bạn gửi chúng vào nhóm thanh khoản.

Tên gọi vô thường hơi gây hiểu nhầm, vì việc giảm giá mã thông báo có thể chỉ là tạm thời và giá có thể tăng trở lại sau thị trường hoặc điều kiện giao dịch, v.v. Trong trường hợp này, tổn thất sẽ là tạm thời (tức là vô thường), vì giá sửa chữa trở lên. Thay đổi chỉ trở thành vĩnh viễn nếu giá đô la của mã thông báo khi rút thấp hơn so với khi mã thông báo được gửi.

Người ta có thể tranh luận rằng tổn thất vô thường là rủi ro mà các nhà cung cấp thanh khoản phải trả để đổi lấy phí kiếm được bằng cách giao dịch các cặp tiền điện tử trên các nhóm thanh khoản. Nếu khoản lỗ lớn hơn số phí kiếm được, nhà cung cấp thanh khoản sẽ nhận ra khoản lỗ, điều này có thể đã không xảy ra nếu thay vào đó, họ nắm giữ các mã thông báo của mình. Điều thú vị cần lưu ý là một người có thể không thực sự mất tiền, nhưng lợi nhuận của một người có thể ít hơn nếu một người chỉ nắm giữ các mã thông báo.



AMM so với đặt hàng

Hiểu được tổn thất vô thường đòi hỏi phải có hiểu biết cơ bản về cách hoạt động của DEX. Hiện tại, các DEX sử dụng hai mô hình thiết kế: AMM và sổ đặt hàng. Mỗi thứ đi kèm với một loạt các ưu điểm và nhược điểm khi nói đến sự mất mát vô thường, được khám phá dưới đây.

AMM

Chế độ DEX của Nhà tạo lập thị trường tự động (AMM) cho phép giao dịch tự động các cặp tiền điện tử bằng cách sử dụng hợp đồng thông minh. Các cặp này thường (nhưng không phải luôn luôn) là một mã thông báo dựa trên Ethereum và một đồng ổn định.

AMM dựa vào nhóm thanh khoản, đây là cơ chế tạo điều kiện cho người dùng gộp tài sản của họ vào các hợp đồng thông minh. Nhóm càng có nhiều tính thanh khoản, thì việc giao dịch trên DEX mà nhóm liên kết với nó càng trở nên dễ dàng hơn, đồng thời các nhà cung cấp thanh khoản thu được phí và phần thưởng càng cao. Nhóm thanh khoản tổng hợp thanh khoản được cung cấp bởi các nhà đầu tư vào cả hai bên của cặp giao dịch. Nhóm sử dụng một thuật toán xem xét tính thanh khoản hiện tại để tính toán giá thị trường của cặp tiền tại thời điểm đó. Nói một cách khác, thuật toán xem xét tính khả dụng của một tài sản cụ thể trong nhóm để xác định giá của nó.

AMMs rely on liquidity pools, which are mechanisms that facilitate users to pool their assets into smart contracts.

Các AMM hầu như dựa hoàn toàn vào các nhà cung cấp thanh khoản để cung cấp thanh khoản nhằm mở rộng quy mô của nhóm và đảm bảo tài sản được giao dịch ở mức giá hợp lý. Đặc điểm thiết kế này hiệu quả có nghĩa là các nhà cung cấp thanh khoản là các nhà tạo lập thị trường.

Tất nhiên, các nhà cung cấp thanh khoản cần có động cơ để đầu tư. Điều này xảy ra dưới hình thức canh tác lợi nhuận, về cơ bản là phần thưởng mã thông báo kiếm được thông qua việc cho vay hoặc đặt cọc kỹ thuật số tài sản.

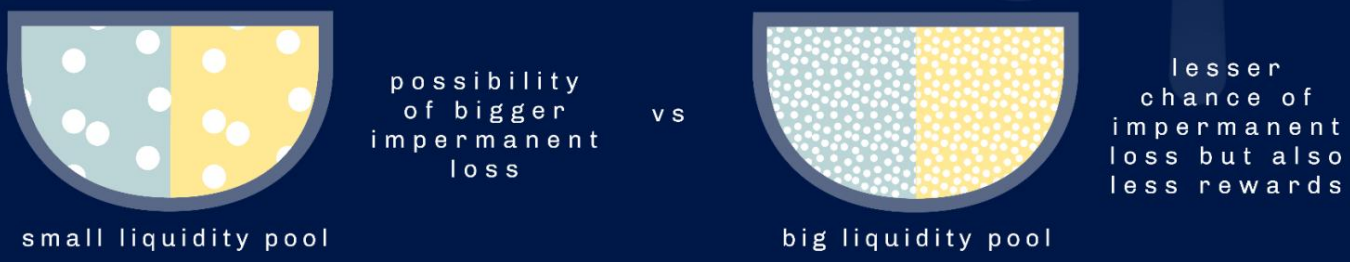
Cơ chế đằng sau việc thiết kế sổ đặt hàng đã tồn tại trong lĩnh vực kinh tế trong một thời gian dài. Đó là một mô hình rất đơn giản. Sổ lệnh chỉ đơn giản là liệt kê tất cả các lệnh mua / bán (hỏi / đặt giá, trong ngữ cảnh này), vì vậy khi các nhà giao dịch đặt lệnh, sổ lệnh sẽ sắp xếp chúng theo giá của tài sản. Nếu có cung và cầu, tài sản có thể được giao dịch.

UTXO-based ledgers, like Cardano, are far more suitable for order book architecture.

Sổ cái dựa trên UTXO, như Cardano, phù hợp hơn nhiều với kiến trúc sổ đặt hàng, vì thiết kế này, cùng với các tính năng EUTXO của Cardano, giảm thiểu tác động của mất mát vô thường.

Khả năng dự đoán (không) của mất mát vô thường

Các nhà cung cấp thanh khoản cung cấp tính thanh khoản cho các nhóm để thu lợi nhuận tài chính. Nhưng điều này mang lại rủi ro. Số lượng mã thông báo trong nhóm và số lượng nhà cung cấp thanh khoản đóng góp vào nó là các yếu tố chính về khả năng xảy ra tổn thất vô thường và việc xem xét như vậy là quan trọng đối với các nhà cung cấp thanh khoản tiềm năng. Tổn thất thường xuyên dẫn đến các hồ bơi cạn kiệt và các nhà cung cấp thanh khoản phải tìm kiếm nơi khác.



Đây là điều tối kỵ về sự mất mát vô thường: rất khó đoán liệu nó có xảy ra hay không, và ở mức độ nào.

Tổn thất vĩnh viễn trong chuỗi dựa trên UTXO so với Tài khoản / Số dư

Giới thiệu nhanh:

- Chuỗi dựa trên UTXO: không có tài khoản nào giữ số dư. Thay vì, ví của người dùng theo dõi danh sách các kết quả đầu ra chưa sử dụng được liên kết với tất cả các địa chỉ do người dùng sở hữu và tính toán số dư của người dùng. UTXO, theo nhiều cách, tương tự như giao dịch tiền mặt. Mô hình EUTXO của Cardano thêm một dữ liệu, là dữ liệu theo hợp đồng cụ thể. Điều này rất quan trọng vì nó mang lại cho Cardano khả năng hỗ trợ đa tài sản và hợp đồng thông minh.

- Mô hình Tài khoản / Số dư - Mô hình kế toán này sử dụng một tài khoản (mà có thể được kiểm soát bằng khóa riêng hoặc hợp đồng thông minh) để giữ số dư tiền xu. Trong mô hình này, tài sản được biểu thị dưới dạng số dư trong tài khoản của người dùng và số dư được lưu trữ dưới dạng trạng thái toàn cầu của tài khoản. Trạng thái được giữ bởi mỗi nút và được cập nhật với mọi giao dịch.

Có một số khác biệt cơ bản giữa hai mô hình này, nhưng khi nói đến AMM và mất mát vô thường, có một điểm khác biệt chính. Các AMM hoạt động trên chuỗi Tài khoản / Số dư (như Ethereum) có xu hướng sử dụng công thức định giá Constant Formula Market Maker (CFMM), đây là một trong những thuật toán được sử dụng phổ biến hơn cho AMM. Công thức này chứa đựng sự kém hiệu quả vốn có. Ví dụ: Tổng giá trị đã khóa (TVL) - được xác định là tổng của tất cả các tài sản tiền điện tử đặt cọc kiếm được phần thưởng, tiền lãi, v.v. - được phân bổ trên toàn bộ phạm vi giá, điều này ngụ ý rằng giá của một tài sản có khả năng bằng nhau là 1 đô la hoặc $ 10.000.

While CFMM is a popular choice for AMMs, these inefficiencies might result in the dilution of revenues for liquidity providers.

Theo giả định này, giá CFMM là không thực tế và có xu hướng không phản ánh các điều kiện thị trường thực tế. Ngoài ra, các giao dịch với khối lượng mã thông báo thấp có xu hướng dẫn đến trượt giá cao (chênh lệch giữa giá dự kiến của một đơn đặt hàng và giá khi lệnh thực sự được thực hiện.) Mặc dù CFMM là một lựa chọn phổ biến cho AMM, nhưng sự thiếu hiệu quả này có thể dẫn đến việc pha loãng doanh thu cho các nhà cung cấp thanh khoản. Quan trọng hơn, tính thanh khoản này có thể chịu tổn thất vô thường.

EUTXO và đặt hàng cuốn sách thiết kế DEX như một bức tường thành chống lại sự mất mát vô thường

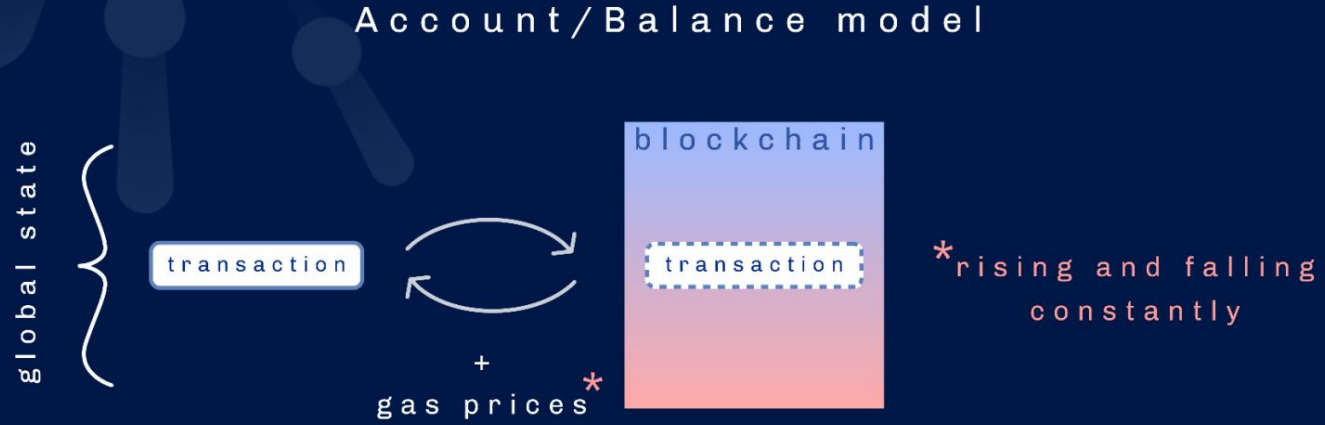
Các lợi thế vốn có của kiến trúc EUTXO về tính bảo mật, tính xác định, tính song song và khả năng mở rộng mang lại một môi trường lý tưởng cho các DEX sử dụng thiết kế sổ đặt hàng, vì nó thể hiện khả năng phục hồi mạnh mẽ hơn đối với tổn thất vô thường. Một ưu điểm chính của thiết kế này là tính thanh khoản tập trung (thanh khoản được phân bổ trong phạm vi giá tùy chỉnh.) Tính năng này tối đa hóa hiệu quả của tính thanh khoản và giảm thiểu tổn thất vô thường.

Tại sao trạng thái toàn cầu không phải là vấn đề trong chuỗi dựa trên EUTXO

Không giống như các blockchain Tài khoản / Số dư trong đó mọi kết quả giao dịch đơn lẻ đều thay đổi trạng thái toàn cầu, trong các blockchain dựa trên UTXO, tính hợp lệ của một giao dịch được đánh giá ở cấp độ giao dịch và số dư là tổng các UTXO còn lại.
Nói cách khác, ở trạng thái địa phương.

A transaction's gas fees might spike significantly in the interval between the transaction being submitted and validated.

Điều này ngay lập tức đặt ra vấn đề cho chuỗi Tài khoản / Số dư. Vô số các hợp đồng thông minh và các tác nhân khác liên tục tương tác và ảnh hưởng đến trạng thái toàn cầu, có nghĩa là tài sản và tài nguyên bị tiêu thụ, đồng thời giá khí đốt lên xuống liên tục. Một tác dụng phụ của điều này là phí giao dịch có thể (và do) dao động. Về mặt hiệu quả, điều này có nghĩa là phí gas của giao dịch có thể tăng đáng kể trong khoảng thời gian giữa giao dịch được gửi và xác thực. Do đó, một giao dịch như vậy có thể không được chuỗi chấp nhận, nhưng dù sao thì phí gas vẫn được tính, có khả năng dẫn đến thiệt hại tài chính cho người sử dụng. Đây là một trong những lỗi thiết kế chính của chuỗi Ethereum.



Không thể xảy ra lãng phí phí trong mô hình EUTXO của Cardano, vì các giao dịch được xử lý và xác thực ở trạng thái địa phương. Điều này đạt được bằng cách thêm một dữ liệu (dữ liệu bổ sung) vào giao dịch. Dữ liệu chứa thông tin theo hợp đồng cụ thể, được chuyển tới logic xác thực của giao dịch, do đó duy trì ngữ cảnh xác định của EUTXO. Điều này có nghĩa là phí giao dịch được biết trước và sẽ không thay đổi. Một tác dụng phụ đáng hoan nghênh của

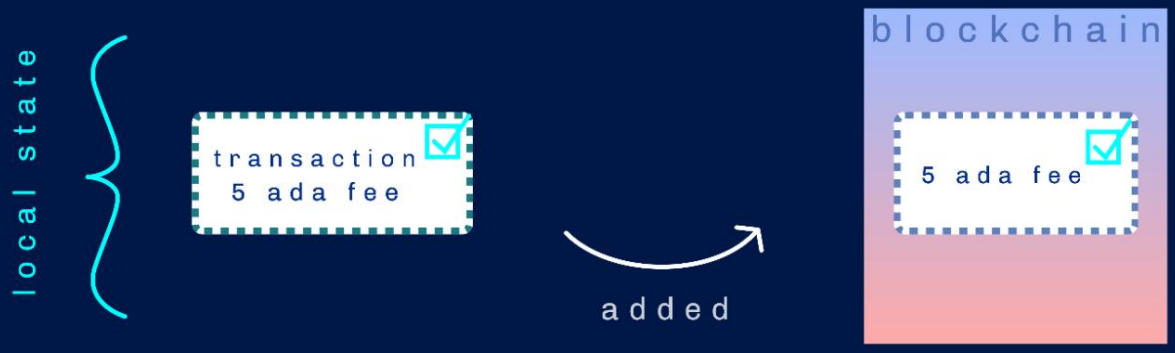
EUTXO và thuyết xác định là các giao dịch không thể

sắp xếp lại bởi các tác nhân xấu, rủi ro khác

của mô hình Tài khoản / Số dư.

Fee wastage cannot occur in Cardano's EUTXO model, since transactions are processed and validated at the local state.

EUTXO model



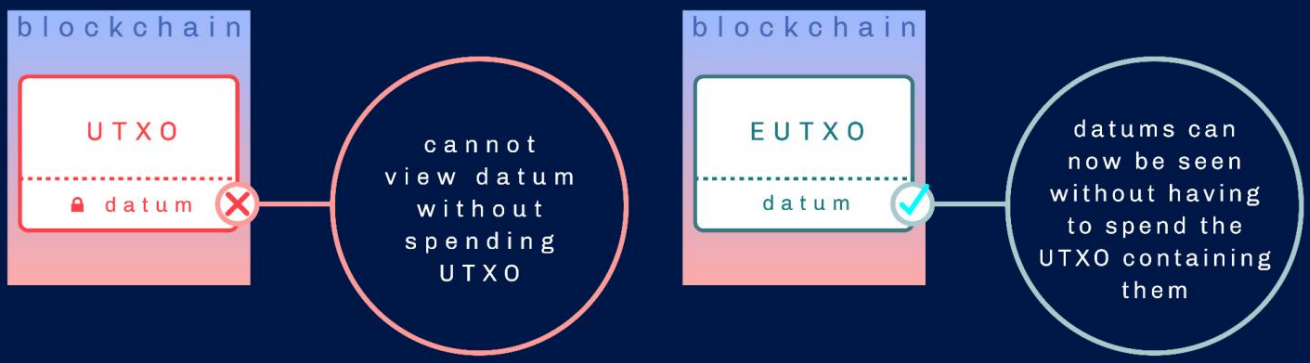
Bản chất cục bộ của xác thực giao dịch cung cấp một lợi thế đáng kể khác: mức độ song song cao. Một nút có thể xác thực các giao dịch song song, miễn là các giao dịch đó không cố gắng sử dụng cùng một đầu vào. Điều này không thể được thực hiện trong chuỗi Tài khoản / Số dư, vì các giao dịch phải được xử lý tuần tự theo thiết kế.

Cải tiến hơn nữa

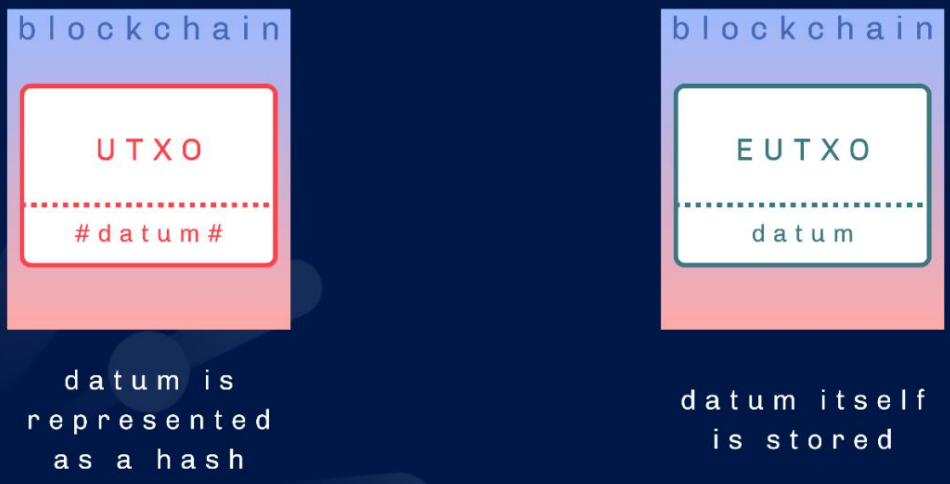
Nền tảng Plutus cung cấp ngôn ngữ hợp đồng thông minh bản địa cho Cardano chuỗi khối.

Các Đề xuất Cải tiến Cardano (CIP) sắp tới cho Plutus bao gồm:

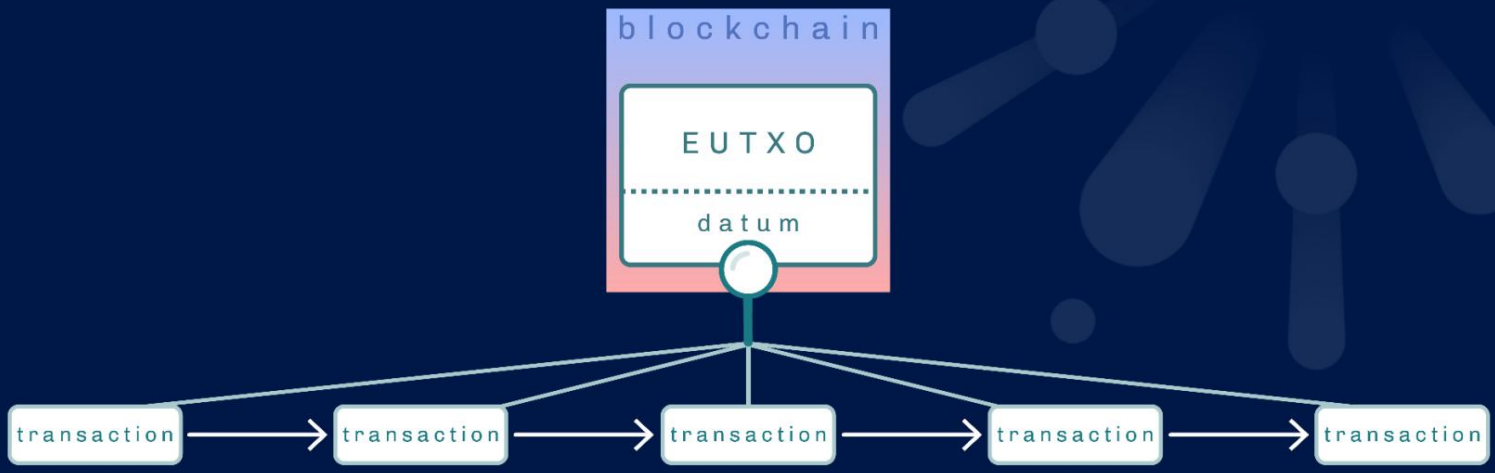
- CIP-31: Đầu vào tham chiếu



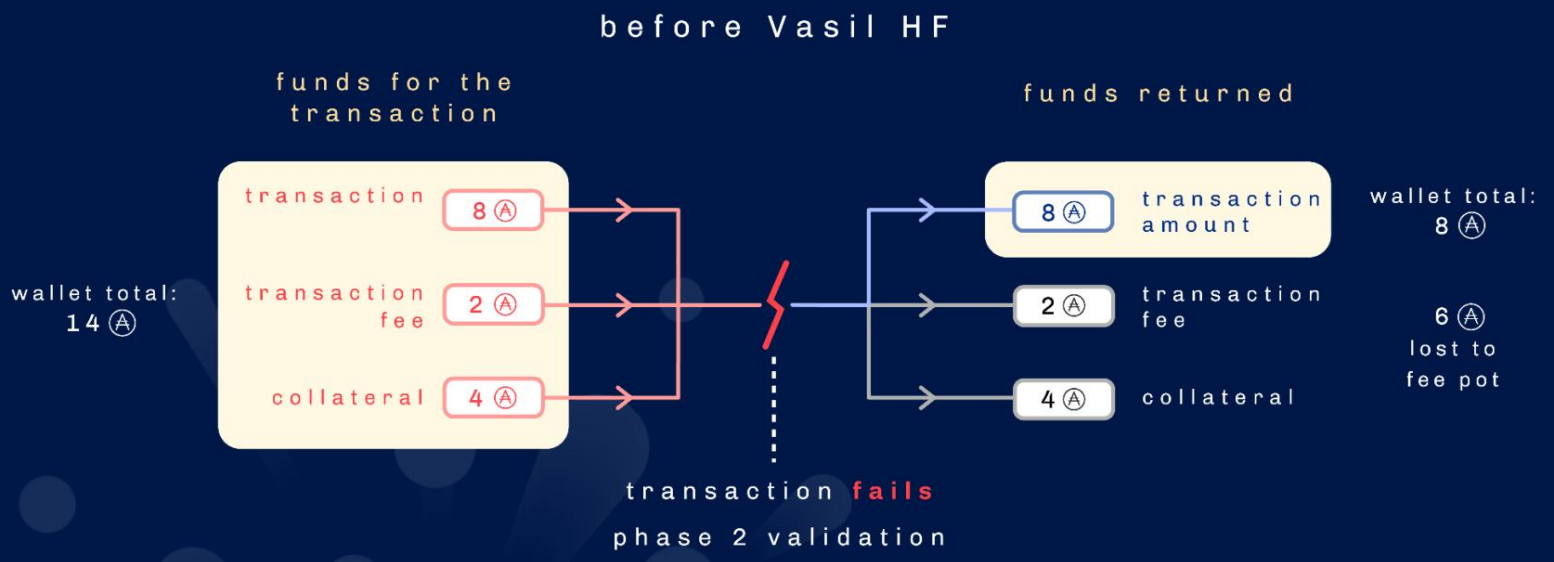
- CIP-32: Dữ liệu nội tuyến

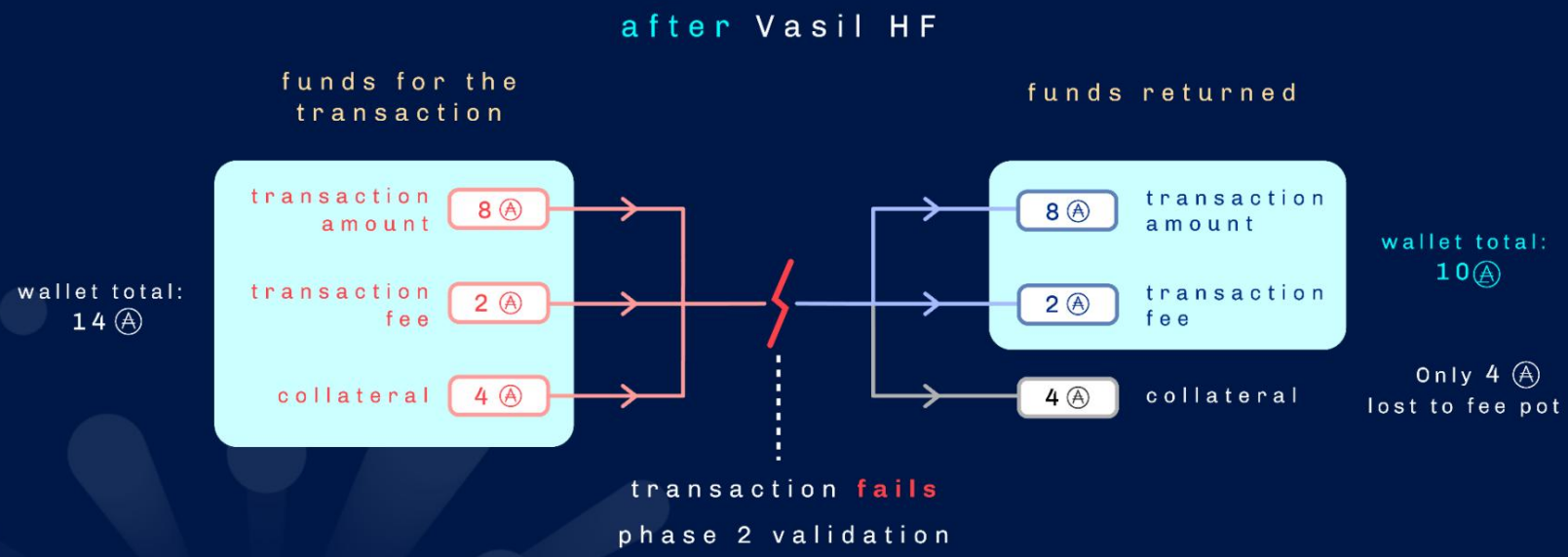


- CIP-33: Tập lệnh tham chiếu



- CIP-40: Đầu ra tài sản thế chấp





Kết luận: điều gì tạo nên mô hình EUTXO sáng tạo và phù hợp?

Mô hình sổ cái của Cardano mở rộng mô hình UTXO để hỗ trợ nhiều tài sản và hợp đồng thông minh mà không ảnh hưởng đến các lợi thế cốt lõi của mô hình UTXO. Nghiên cứu sáng tạo của chúng tôi cung cấp chức năng vượt xa những gì được hỗ trợ trong bất kỳ sổ cái UTXO nào khác, biến Cardano trở thành đối thủ cạnh tranh duy nhất trong không gian blockchain thế hệ tiếp theo.

đọc thêm

Tìm hiểu thêm về mô hình EUTXO của Cardano với các nguồn sau:

~~Báo cáo chính thức của EUTXO~~

Mô hình kế toán UTXO mở rộng của Cardano - được xây dựng để hỗ trợ nhiều tài sản và hợp đồng thông minh