Sự xuất hiện của các lớp token trên Bitcoin

Tổng quan về mô hình “Client-Side Validation”, token RGB & Taro

Diamond Hands

09/02/2023

BitcoinVN

Bản dịch Tiếng Việt: 08/2023 - BitcoinVN News

Trình bày bởi	**Diamond Hands** Bitcoin Công nghệ Nhà cung cấp & Cộng đồng Lightning số 1 Nhật Bản Diamond Hands Các dịch vụ • Nghiên cứu & Tư vấn • Xử lý thanh toán Lightning • Hệ thống tích hợp • LSP, hoạt động của node định tuyến • Giáo dục cộng đồng
Các tác giả	Kishin Kato | CEO của Trustless Services K.K. Koji Higashi | Đồng sáng lập Diamond Hands & Trưởng phòng Phát triển Kinh doanh Yuya Ogawa | Đồng sáng lập Diamond Hands & Giám đốc Công nghệ

Diamond Hands

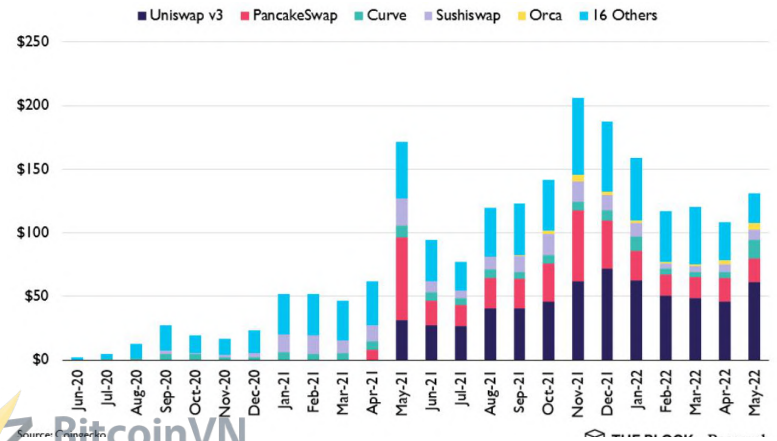
Hiện nay các token theo mô hình “Đồng thuận Toàn cầu” đang được sử dụng như thế nào?

Việc phát hành và sử dụng token đang tăng lên. Và hầu hết đều phát hành trên chuỗi hợp đồng thông minh như Ethereum

Diamond Hands

Thị trường lưu thông & Giao dịch token trên chuỗi đang phát triển

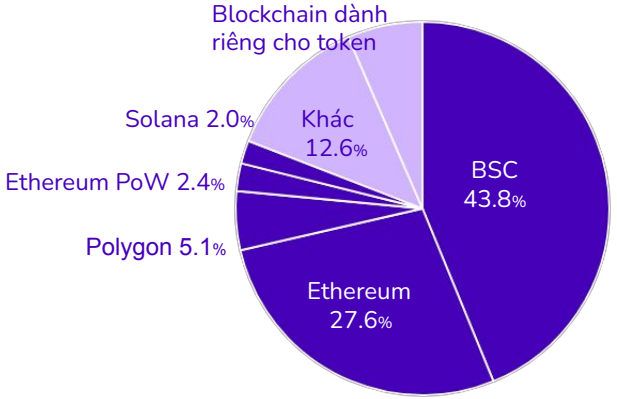
- Khối lượng giao dịch trên sàn giao dịch phi tập trung (DEX) theo thời gian ($bn)



Nguồn: "Cung cấp thanh khoản tổng hợp trong DeFi", tháng 6 năm 2022, The Block Crypto, Inc.

Hầu hết việc phát hành token đang diễn ra trên chuỗi hợp đồng thông minh

- Tổng hợp các nền tảng lưu thông token trong 2 tháng qua (số liệu tổng do các sàn giao dịch cung cấp)



Nguồn: CoinGecko https://www.coingecko.com/ja/new-cryptocurrencies

Chuỗi hợp đồng thông minh mô hình “Đồng thuận Toàn cầu”. Đây là một cách tiếp cận đơn giản nhưng không hiệu quả

Diamond Hands

Mô hình Đồng thuận Toàn cầu:

- Tất cả các node xác nhận tất cả giao dịch
- Dễ dàng chia sẻ trạng thái giao dịch trên toàn cầu
- Ai cũng có thể truy cập nhờ tính minh bạch

Nhược điểm

Giới hạn khả năng mở rộng

Các node phải xác thực tất cả các tương tác hợp đồng khiến phí giao dịch cao, gây tốn kém

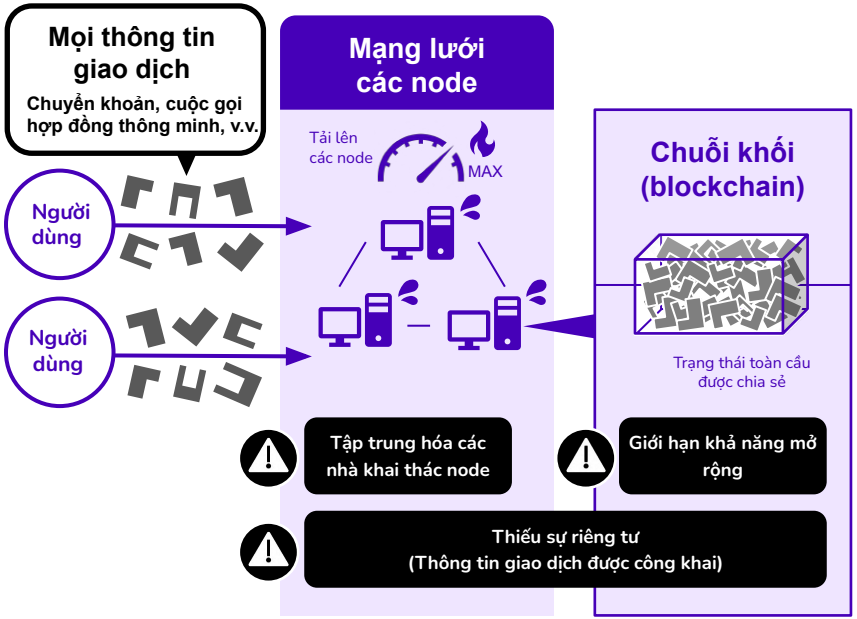
Tập trung hóa các nhà khai thác node

Chi phí cao không khuyến khích người dùng chạy node

Thiếu sự riêng tư

Giao dịch được công khai và bên thứ ba có thể xem thông tin giao dịch bất cứ khi nào

Cách hoạt động của mô hình Đồng thuận Toàn cầu



Diamond Hands

Mô hình Xác thực phía Máy khách (Client-Side Validation - CSV) cho các Token

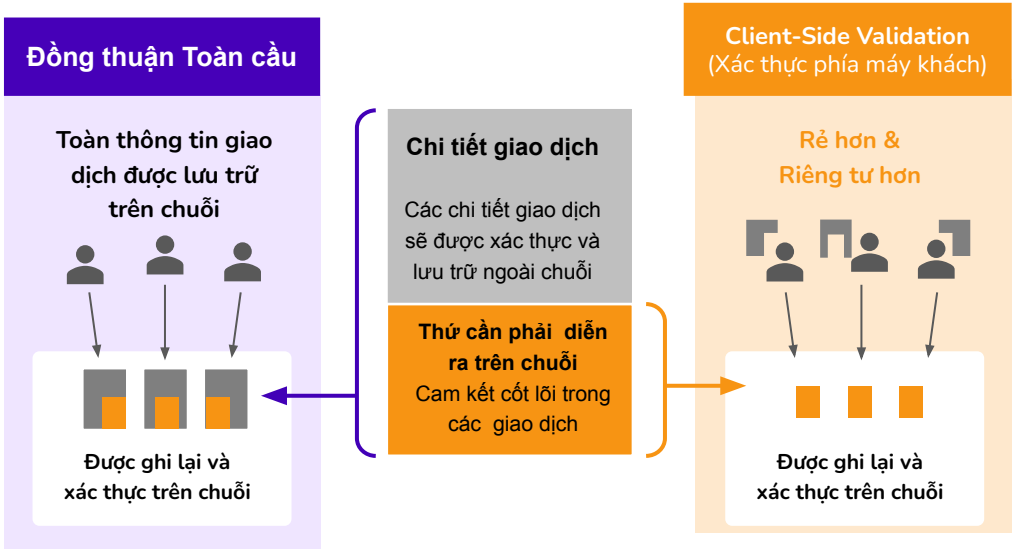
Chi tiết giao dịch có thể được chuyển ra khỏi chuỗi mà không ảnh hưởng đến tính bất biến

1. Mục đích cơ bản của blockchain là trở thành **một cuốn sổ cái bất biến ghi lại các giao dịch** (thông tin giao dịch trên blockchain không thể sửa đổi)

2. **Chi tiết giao dịch được xác thực riêng tư và lưu trữ ngoài chuỗi**.

3. **Người dùng lưu trữ các dữ liệu & kết quả một cách riêng tư,** cam kết sử dụng dữ liệu này trong các giao dịch trực tuyến mà không cần mô tả trên chuỗi.

Chỉ lưu trữ các cam kết cốt lõi trên chuỗi. Chi tiết các giao dịch được xác thực và lưu trữ riêng tư ngoài chuỗi



Mô hình "Xác thực Phía Máy khách" cải thiện khả năng mở rộng và quyền riêng tư bằng cách chuyển xác thực giao dịch ra khỏi chuỗi

Diamond Hands

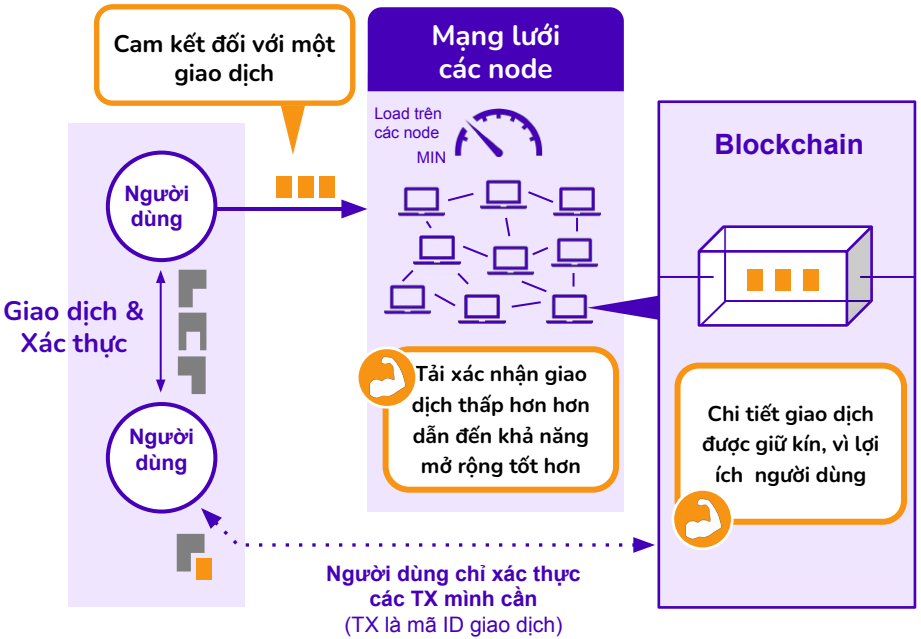
Mô hình Xác thực Phía Máy khách

- Chỉ lưu trữ các cam kết giao dịch trên chuỗi
- Thông tin chi tiết giao dịch nằm ngoài chuỗi và chỉ được xác thực ở phía máy khách
- Chỉ xác thực các giao dịch cốt lõi

Ưu điểm

- **Khả năng mở rộng**
  - Chi phí thấp hơn và ít tính toán hơn
- **Quyền riêng tư**
  - Giao dịch "đánh đố" bên thứ ba
- **Tính khả dụng trên Bitcoin**
  - Không cần các giao dịch phức tạp trên chuỗi; có thể sử dụng ngay trên Bitcoin

Mô hình "Xác thực phía Máy khách" hoạt động như thế nào?



So sánh mô hình Xác thực Phía Máy khách & Đồng thuận Toàn cầu trong việc phát hành token

Diamond Hands

	Xác thực Phía Máy khách (CSV) (ví dụ token. RGB, Taro)	Đồng thuận Toàn cầu (Ví dụ: token ERC20)
Phí giao dịch token trên chuỗi	Thực hiện hợp đồng và chuyển token gốc có cùng mức phí không đổi	Chuyển token đắt hơn chuyển token gốc. Chi phí của các cuộc gọi phụ thuộc vào quy mô hợp đồng và độ phức tạp khi thực hiện hợp đồng.
Bảo mật	Các bên thứ ba không thể theo dõi việc phân phối, số dư hoặc chuyển token	Các bên thứ ba có thể dễ dàng quan sát hoạt động của chủ sở hữu token; không có sự riêng tư
Hợp tác với bên thứ ba	Không sử dụng trạng thái công khai toàn cầu mà đòi hỏi sự hợp tác từ những người nắm giữ token/tài sản riêng lẻ… Vì vậy, tạo snapshots (ảnh chụp nhanh để lưu lại bản sao quyền sở hữu token tại thời điểm chụp) là điều không thể	Mọi giao dịch được công khai toàn cầu nên cho phép mọi người dễ dàng tạo snapshots & xác thực quyền sở hữu token tại một thời điểm nhất định mà không cần sự tương tác của bên thứ ba
Hệ sinh thái nhà phát triển	Hệ sinh thái nhà phát triển vẫn còn sơ khai	Qua nhiều năm ứng dụng, mô hình Đồng thuận Toàn cầu xây dựng được hệ sinh thái nhà phát triển tương đối lớn với nhiều công cụ tốt
Vấn đề về tính khả dụng của dữ liệu	Cần lưu trữ dữ liệu ngoài chuỗi để sử dụng token trong tương lai	Khóa riêng tư đủ để lưu trữ các token
Yêu cầu online	Người dùng phải online khi nhận thanh toán hoặc sử dụng dịch vụ ủy quyền để nhận, xác thực và lưu trữ dữ liệu ngoài chuỗi.	Người dùng có thể nhận thanh toán ngoại tuyến bằng cách cung cấp địa chỉ ví của mình

Diamond Hands

Lợi ích của các token sử dụng mô hình CSV trên Bitcoin

BitcoinVN News

Các token trên Bitcoin sử dụng CSV có lợi thế về tính ổn định và khả năng mở rộng

Lợi ích của việc phát hành các token trên Bitcoin:

1 Cơ sở hạ tầng chuỗi khối ổn định nhất

Bitcoin là blockchain phi tập trung nhất và an toàn nhất hiện nay.

Blockchain Bitcoin giảm tối đa sự phụ thuộc vào bên thứ ba nên ít gặp phải thất bại đột ngột nhất.

2 Khả năng tương tác với Bitcoin

Các token đã phát hành trên blockchain Bitcoin sẽ có khả năng tương tác cao với BTC - loại tiền điện tử phổ biến và được sở hữu nhiều nhất trên thế giới.

Thuận tiện cho việc giao dịch với các hợp đồng tài chính đáng tin cậy được xây dựng trên Bitcoin.

3 Kết nối với Lightning Network

Các token phát hành trên Bitcoin hoàn toàn có thể tận dụng các lợi ích của Lightning, giúp giao dịch nhanh - rẻ và ổn định hơn.

Cơ sở hạ tầng Lightning Network có thể được áp dụng để giao dịch các token trên blockchain Bitcoin

Việc kết nối các "kênh thanh toán Lightning Network dành riêng cho token" có thể mang lại lợi ích cho toàn bộ hệ sinh thái của người dùng, nhà phát triển và nhà điều hành node Lightning

Người dùng

Thực hiện **thanh toán & hoán đổi nhanh chóng với chi phí cực rẻ** qua Lightning.

Các nhà phát triển

Sử dụng cơ sở hạ tầng hiện có như triển khai node và các ví Lightning

Nhà vận hành node Lightning

Giao dịch token và hoán đổi mang lại nhiều **mô hình kinh doanh mới và thu nhiều phí định tuyến hơn**

Về Lightning Network | Đọc báo cáo "Hiểu về Lightning" tại đây: https://news.bitcoinvn.io/wp-content/uploads/2023/02/Lightning_Network_Report_VI_2022.pdf

Sự phát triển của các token CSV sẽ mở rộng khả năng của Bitcoin và góp phần phát triển hệ sinh thái của nó

Diamond Hands

Ảnh hưởng của các token đối với Bitcoin

1 Bitcoin giống như cửa hàng 1 điểm đến (one-stop shop)

Khi Bitcoin sử dụng CSV sẽ mở ra nhiều tính năng mới, giúp các nhà phát triển dễ dàng xây dựng vô số giải pháp cho token ngay tại blockchain Bitcoin

2 Hỗ trợ việc chấp nhận Bitcoin

Trong quá trình áp dụng đại trà, stablecoin trên Bitcoin sẽ tạo điều kiện thuận lợi cho các giao dịch bằng fiat. Đổi lại, các token trên Bitcoin sẽ thúc đẩy việc hoán đổi token sang BTC.

3 Sự tham gia của nhiều nhà phát triển & công ty hơn

Khi việc phát hành token và các hợp đồng tài chính phức tạp dần tích hợp sẵn trên blockchain Bitcoin, hi vọng sẽ có nhiều nhà phát triển tham gia xây dựng & phát triển Bitcoin nhiều hơn nữa. Đồng thời, sẽ có nhiều tập đoàn bắt đầu sử dụng tài sản và mạng lưới Bitcoin trong các sản phẩm và dịch vụ của mình.

*Việc phát hành token trên Bitcoin không được chấp nhận được coi là một tín hiệu tích cực; một số phản đối khái niệm này với những lo ngại và phản biện rất thuyết phục. Xem phụ lục để biết các phương pháp thay thế.

Diamond Hands

Tương lai & Thách thức của các token trên Bitcoin

BitcoinVN News

Việc thực hiện các xác thực phức tạp ngoài chuỗi cho phép phát triển một lớp tài chính có thể mở rộng trên Bitcoin

Diamond Hands

Trái ngược với mô hình "Đồng thuận Toàn cầu" trong các chuỗi khối hợp đồng thông minh, chúng tôi hy vọng "Hợp đồng Phía Máy khách" (Client-Side Contracts) và các giao thức ngoài chuỗi khác sẽ trở thành thành nền tảng để xây dựng các chức năng tài chính phức tạp và tinh vi trên Bitcoin.

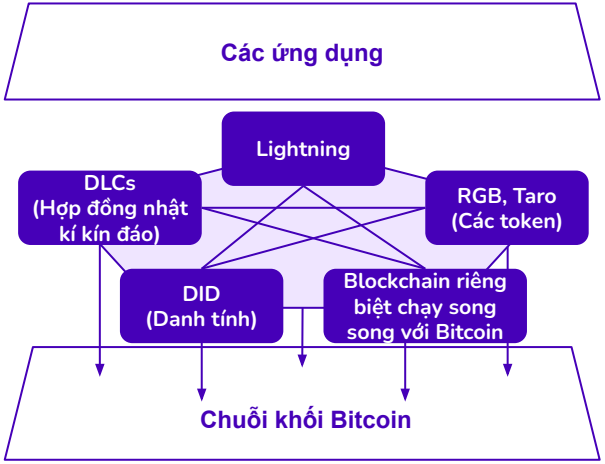
Client-Side Contracts là gì?

a. Hợp đồng chỉ được chia sẻ bởi các bên liên quan

b. Bạn toàn quyền kiểm soát khóa cá nhân

c. Có khả năng mở rộng hơn so với hợp đồng thông minh bằng cách sử dụng mô hình Đồng thuận Toàn cầu

d. Chống kiểm duyệt cực cao



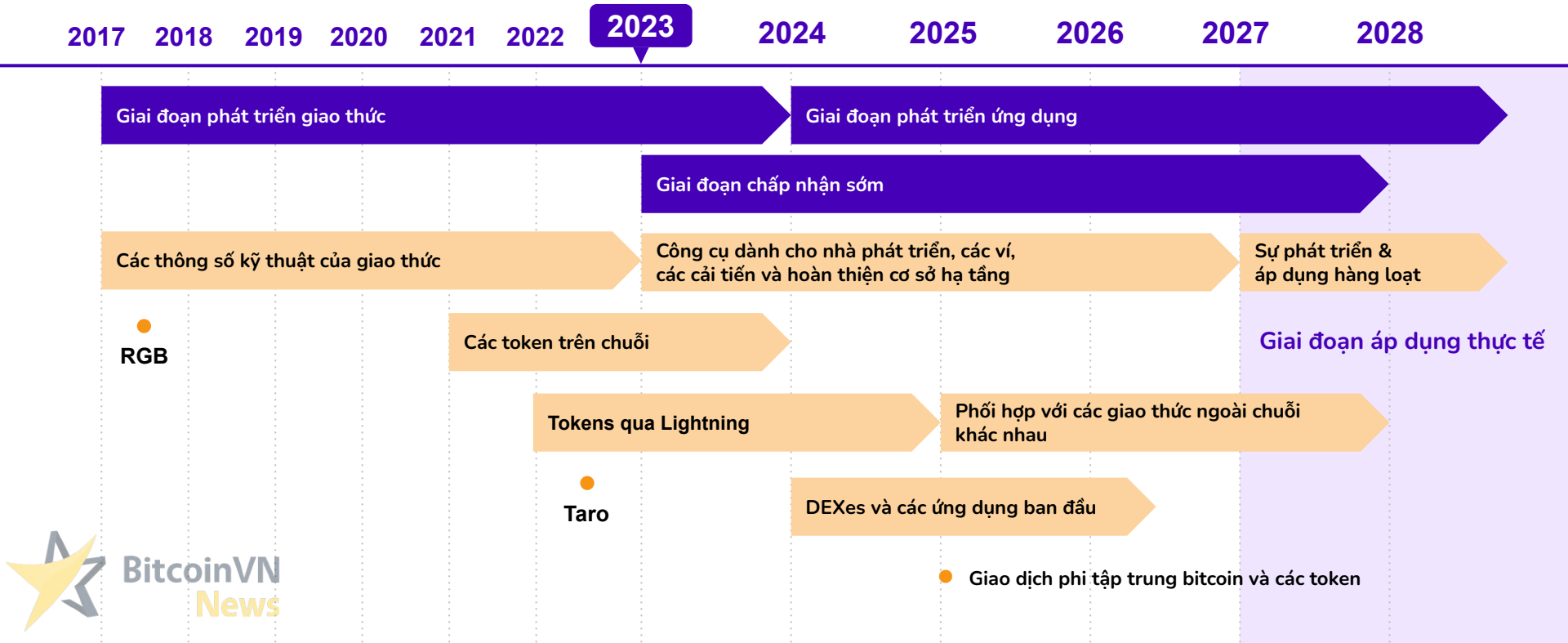
- Các ứng dụng riêng tư, bạn tự giữ khóa
- Có thể mở rộng ứng dụng tài chính

- Hợp đồng P2P ngoài chuỗi
- Khả năng tương tích với dữ liệu ngoài chuỗi
- Giảm thiểu việc sử dụng trên chuỗi

- Neo dữ liệu ngoài chuỗi
- Bảo mật và bất biến từ PoW (bằng chứng công việc)

Các token CSV đang được xây dựng trên Bitcoin; Vài năm nữa mới có thể áp dụng đại trà

Diamond Hands



Mô hình CSV không lỗi thời trong tất cả các trường hợp đang sử dụng cho mô hình Đồng thuận Toàn cầu

Diamond Hands

Ưu điểm của Xác thực Phía Máy khách (CSV)

Khả năng mở rộng, Quyền riêng tư, Chống kiểm duyệt

Ví dụ 1 : Các stablecoin

Ngoài các lợi ích về quyền riêng tư, CSV còn có, khả năng tương thích với Lightning, **cho phép thanh toán nhanh, rẻ.**

Ví dụ 2: Trao đổi các Token ngang hàng

CSV cho phép người dùng giao dịch token và bitcoin theo cách riêng tư, tự chủ và có thể mở rộng.

Ví dụ 3: Tài chính dựa trên Bitcoin

Xây dựng dựa trên Bitcoin cho phép hội nhập tài chính mà không cần các sản phẩm tập trung và rủi ro như Wrapped BTC.

Lợi thế của mô hình Đồng thuận Toàn cầu

Tính minh bạch, Nhóm Thanh khoản, Tương tác giữa Hợp đồng với Hợp đồng

Ví dụ 1: Các NFT

Vì trạng thái toàn cầu là công khai nên các bên thứ ba có thể dễ dàng xác định thông tin quyền sở hữu và giao dịch.

Ví dụ 2: AMM (Công cụ đem lại tính thanh khoản tự động)

Nhiều người dùng có thể chỉ cần gửi thanh khoản của họ vào trạng thái chia sẻ khi giao dịch diễn ra, chẳng hạn như với Uniswap.

Ví dụ 3: Sản phẩm Composable Financial, Aggregators

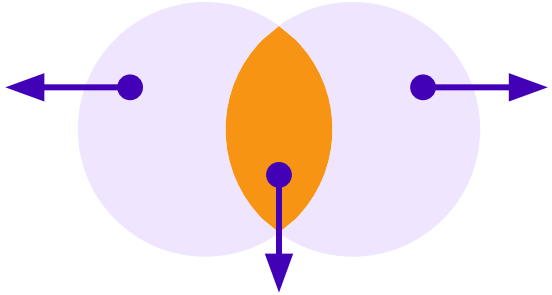
Trạng thái hợp đồng công khai cho phép mức độ liên kết cao, trong đó các hợp đồng có thể gọi cho các hợp đồng khác.

Sự chậm trễ khi xây dựng hệ sinh thái token trên Bitcoin và những thách thức cụ thể

Diamond Hands

Những thách thức của mô hình Xác thực Phía Máy khách

- **Giới hạn xác thực ngoài chuỗi**
  Khi lượng người dùng tăng lên đáng kể sẽ làm tăng chi phí xác thực cho các token CSV phổ biến.
- **Phải lưu trữ nhiều khóa hơn**
  Nếu các dữ liệu ngoài chuỗi dùng để xác thực giao dịch bị mất thì người dùng không thể chi tiêu token. Chính điều này buộc chúng ta phải lưu trữ nhiều khóa hơn.



Hệ sinh thái vẫn còn sơ khai

Hệ sinh thái mới bắt đầu xây dựng. Công cụ dành cho nhà phát triển và quá trình tích hợp của người dùng có thể mất vài năm.

Những thách thức của việc phát hành token trên Bitcoin

- **Thông lượng trên chuỗi bị hạn chế**
  Thông lượng giao dịch của Bitcoin hạn chế hơn rất nhiều so với các chuỗi khối khác.
- **Ưu đãi có thể gây ra các sai lệch**
  Các token trên Bitcoin với nhiều chính sách kích cầu có thể thu hút một lượng người dùng lớn chú ý vào Bitcoin. Điều này có thể ảnh hưởng vào các động lực khiến Bitcoin hoạt động sai lệch (ví dụ: trong các cuộc chia tách gây tranh cãi).

Diamond Hands

Tổng quan về các giao thức CSV

- RGB
- TARO

BitcoinVN News

RGB

1. RGB là một nền tảng hợp đồng thông minh trên Bitcoin
2. Một phiên bản MVP đã được phát hành vào năm 2019
3. Hiệp hội LNP/BP phi lợi nhuận dẫn đầu trong việc phát triển giao thức
4. Các hợp đồng đầu tiên có sẵn là các hợp đồng token

Mục tiêu của RGB là tăng khả năng mở rộng và giúp "Hợp đồng Thông minh" bảo mật hơn trên Bitcoin

RGB là hợp đồng thông minh được xây dựng theo mô hình Xác thực Phía Máy khách

Con dấu sử dụng một lần được dùng để liên kết trạng thái hợp đồng ngoài chuỗi với UTXO Bitcoin. Dấu đóng 1 lần là "tấm vé thông hành" xác thực rằng: giao dịch RGB ngoài chuỗi sẽ được tiếp tục thực hiện ở bước tiếp theo.

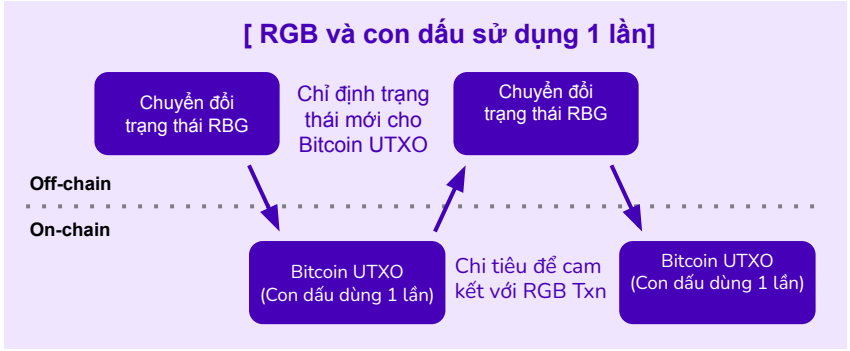
Các ưu điểm của RGB:

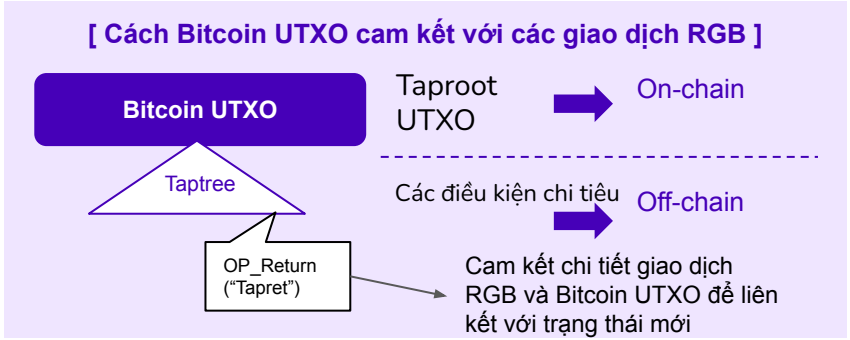
1. Bảo mật

Các bên thứ ba không nhìn thấy các giao dịch RGB cũng như Con dấu sử dụng một lần trong các bước giao dịch.

2. Khả năng thực hiện hợp đồng thông minh

Các hợp đồng thông minh được thực thi ở phía máy của khách hàng. Nhờ đó, chúng đảm bảo sự riêng tư hơn và linh hoạt hơn so với các hợp đồng Bitcoin Script được thực hiện trên chuỗi.





Quá trình chuyển đổi trạng thái RGB được xác thực ngoài chuỗi bởi UTXO được chi tiêu trên blockchain

Alice phát hành một tài sản RGB mới cho chính mình bằng cách chỉ định trạng thái cho UTXO Bitcoin mà cô ấy sở hữu.

Alice sử dụng UTXO của mình để gửi tiền cho Bob và chính mình, mỗi người chọn một UTXO khác.

Alice không biết UTXO Bob đã chọn vì nó được bảo mật.

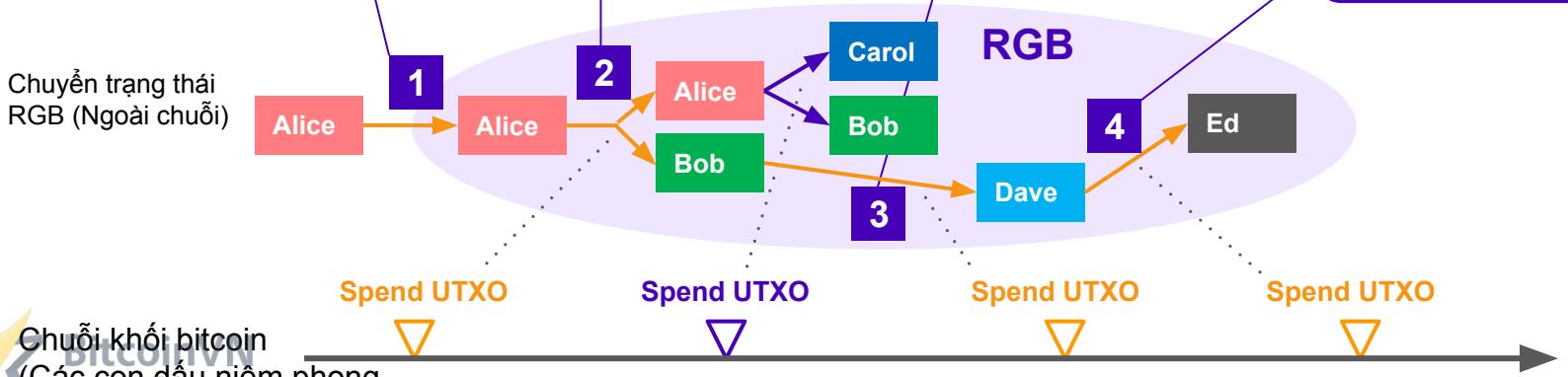
Bob sử dụng UTXO của mình để gửi cho Dave.

Cả Alice và Carol đều không biết về quá trình chuyển đổi này vì họ không biết UTXO mà Bob đã sử dụng.

Dave cũng dùng UTXO của mình để gửi mọi thứ cho Ed.

Ed xác thực các chuyển đổi 1~4, sử dụng dữ liệu từ Dave để đảm bảo nguồn gốc của các token của anh ấy.

Bulletproofs bảo vệ quyền riêng tư của Alice và Bob trong quá trình này.

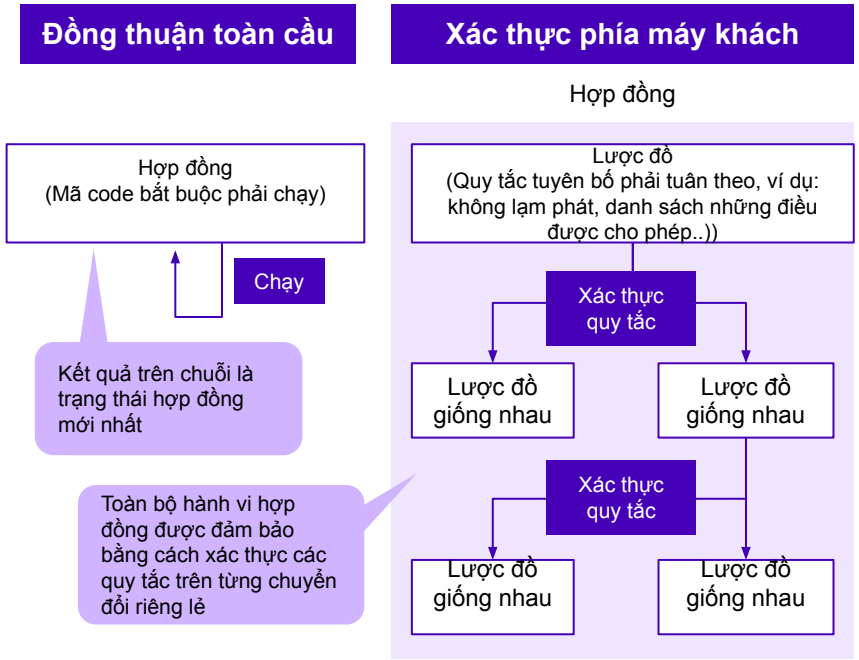


Hợp đồng RGB giới hạn các chuyển đổi trạng thái riêng lẻ để đảm bảo một thuộc tính toàn cầu được bảo mật

Hợp đồng RGB là tập hợp các "quy tắc cục bộ"

Cũng như giao dịch token, trạng thái hợp đồng RGB được phân phối giữa nhiều người dùng. Hợp đồng thông minh trên RGB mô tả các quy tắc dưới dạng **Lược đồ**. Mỗi quá trình chuyển đổi trạng thái phải tuân theo bộ quy tắc trong Lược đồ này để đảm bảo mục tiêu cuối cùng là toàn bộ hợp đồng tuân thủ đúng Lược đồ.

Các trạng thái của người dùng có thể được xử lý trên chuỗi bằng quyền sở hữu UTXO. Trong khi đó, cách các trạng thái ấy được thực hiện như thế nào sẽ được viết dưới dạng hợp đồng RGB. Trong tương lai, máy ảo AluVM sẽ được sử dụng để xác thực các lược đồ. Tuy nhiên, các lược đồ phổ biến sẽ được cài đặt sẵn và không cần xác thực (ví dụ: RGB20).



RGB dù đầy tiềm năng nhưng sự phức tạp và quy mô của nó đặt ra một thách thức

Những thách thức mà RGB phải đối mặt:

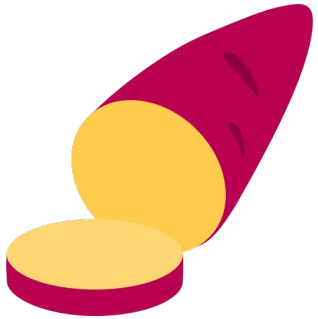
1. Bước khởi đầu gian nan

Ngoài các giao dịch Bitcoin dùng **con dấu sử dụng một lần**, các nhà phát triển phải học cách xử lý các khái niệm mới như **chuyển đổi trạng thái RGB và hợp đồng**. Thêm vào đó, việc có đường cong tiếp cận khá dốc (dù bỏ ra nhiều nỗ lực học tập nhưng trình độ không tăng lên bao nhiêu) có thể sẽ làm chậm quá trình áp dụng RGB rộng rãi.

2. Mục tiêu quá rộng

Để đạt được mục tiêu đầy tham vọng là kích hoạt các hợp đồng thông minh khác nhau ngoài chuỗi, RGB phải đối mặt với một khối lượng công việc khá lớn đếu muốn xây dựng hệ sinh thái các nhà phát triển của mình. Giao diện người dùng mới lạ cũng sẽ cần nhiều thời gian để thị trường chấp nhận.

TARO



1. Taro là một giao thức token áp dụng Taproot trên Bitcoin
2. Lightning Labs là đơn vị dẫn đầu cho sự phát triển Taro
3. Được công bố tại hội nghị Bitcoin tháng 4/2022
4. Taro là viết tắt của “Taproot Asset Representation Overlay" - "Lớp phủ đại diện cho tài sản Taproot"

Taro là một giao thức token áp dụng Taproot, tập trung vào khả năng tương thích với Lightning

Diamond Hands

Taro là một giao thức token CSV

Các UTXO Bitcoin Taproot ủy thác **Cây tài sản chứa số Taro được dùng trong các giao dịch Bitcoin** để tạo các **UTXO Taproot mới** chứa số Taro vừa thu được. *(Xem thêm ở sơ đồ bên phải để hiểu rõ quá trình tạo ra Taro mới)*

Thế mạnh của TARO:

1. Khả năng tương thích với Lightning

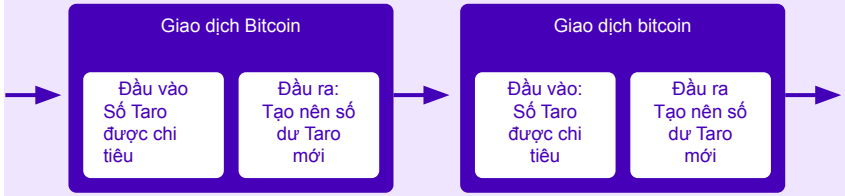
Thiết kế của Taro tương thích tốt với Lightning. Và khái niệm về mô hình chuyển đổi trạng thái sử dụng giao dịch Bitcoin rất dễ hiểu đối với các nhà phát triển.

2. Sự hậu thuẫn của Lightning Labs

Với sự hỗ trợ của Lightning Labs, Taro có khả năng sẽ sớm triển khai node Lightning (LND). Qua đó, Taro có thể nhanh chóng thu hút lượng người dùng đáng kể.

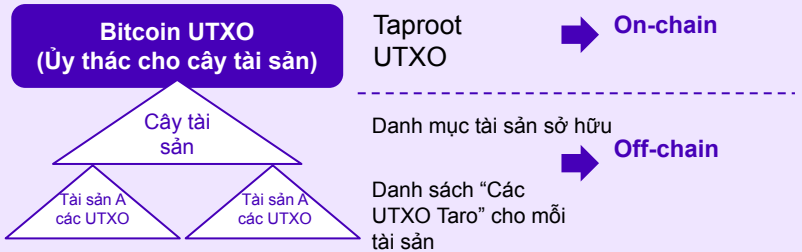
※Taproot đã giới thiệu khả năng cho nhiều tập lệnh mở khóa UTXO được lưu trữ trong cấu trúc dữ liệu dạng cây. Người dùng có thể chi tiêu UTXO bằng khóa tương ứng (chi tiêu khóa) hoặc hoàn thành một trong các tập lệnh này (chi tiêu tập lệnh); tập lệnh không bao giờ được tiết lộ ngoại trừ tập lệnh duy nhất được sử dụng trong chi tiêu tập lệnh.

[Các giao dịch bitcoin được dùng để chuyển đổi trạng thái]



Các Bitcoin TX tiêu thụ và tạo UTXO mới chứa tài sản Taro

[Bitcoin UTXO ủy thác tài sản Taro như thế nào?]

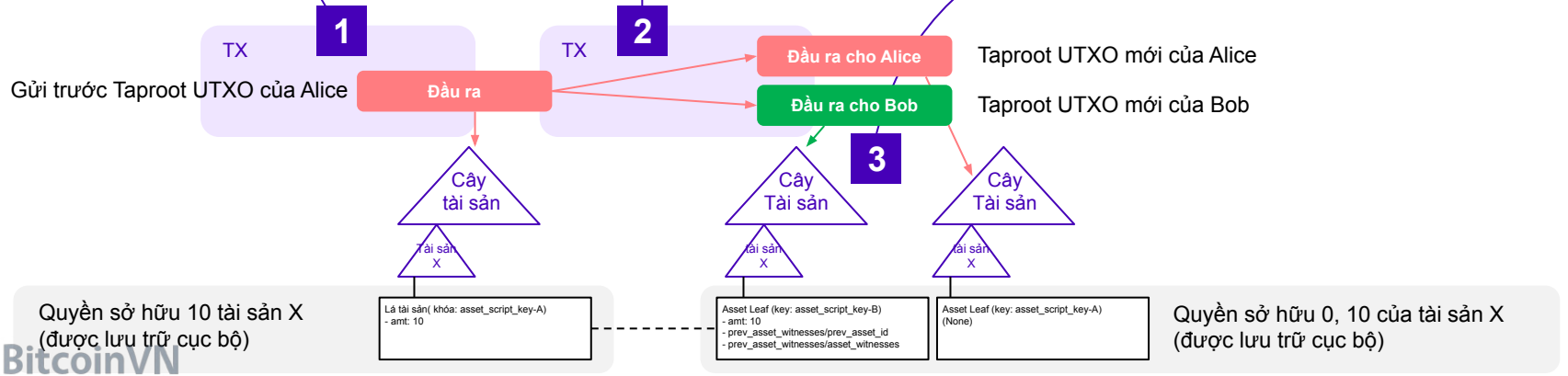


Giao dịch Taro sử dụng giao dịch Bitcoin để dùng số dư cũ - tạo số dư mới

Alice phát hành một tài sản Taro mới cho chính mình bằng cách tạo một Taproot UTXO mới cam kết với tài sản Taro.

Alice gửi tất cả 10 tài sản của mình cho Bob bằng cách gửi UTXO trước đó của cô ấy tới các UTXO mới của Bob và của chính mình, mỗi UTXO của cô ấy cam kết với số dư mới là 0 và 10.

Cũng như RGB, Bob xác thực các giao dịch 1～2 để đảm bảo nguồn gốc của các tài sản này. Alice phải cung cấp dữ liệu này.



Taro ít tập trung vào giao dịch trên chuỗi nên người dùng buộc phải sử dụng các công cụ tổng hợp giao dịch khác

Những thách thức mà Taro phải đối mặt:

Thông số kỹ thuật trên chuỗi chưa hoàn chỉnh và sức hấp dẫn của các dịch vụ được cấp phép

Sự phát triển của Taro dường như tập trung vào các giao dịch ngoài chuỗi hơn là gửi trên chuỗi. Chẳng hạn, giao thức trên chuỗi chưa hoàn thiện và có thể sẽ yêu cầu nhiều sự phối hợp khác phức tạp. Taro cũng không mang lại lợi ích về khả năng mở rộng trên chuỗi. Vì vậy, người dùng buộc phải hướng tới Lightning và các công cụ tổng hợp giao dịch khác.

Trong Taro, bất kỳ ai cũng có thể vận hành Pocket Universe (trình kiểm tra giao dịch giúp bạn tránh lừa đảo tiền điện tử). Trong đó 1 Bitcoin UTXO cam kết với nhiều tài sản Taro của người dùng, cho phép tổng hợp nhiều lần chuyển Taro. Mặc dù rẻ và thuận tiện, nhưng những người điều hành Pocket Universe có thể đóng băng các tài sản này, ngăn không cho chúng bị chuyển hoặc rút.

	🔑Người dùng sở hữu chìa khóa để mở **Bitcoin UTXO**	🚫Người khác sở hữu chìa khóa **Bitcoin UTXO**
🔑Người dùng sở hữu khóa để mở **Taro UTXO**	Người dùng đang tự quản lý tài sản Taro	Người dùng có thể bị đóng băng tài sản của họ, nhưng tài sản ấy không bị đánh cắp **(Sử dụng một Pocket Universe)**
🚫Người khác sở hữu chìa khóa **Taro UTXO**	Người dùng đang vận hành một **Pocket Universe**	Người dùng đang trong mối quan hệ giám hộ truyền thống

RGB và Taro khác nhau về đặc điểm, thuộc tính và chúng sẽ được sử dụng trong các trường hợp khác nhau

	RGB	Taro
Bảo mật	■ Các bên thứ ba không thể phát hiện các giao dịch và thậm chí cả người gửi và người nhận đều được bảo vệ ■ Không thể truy xuất nguồn gốc trên chuỗi	■ Trong một số trường hợp, các bên thứ ba có thể phát hiện các khoản thanh toán Taro nhưng thông tin chi tiết chỉ thuộc về người gửi, người nhận và những người nhận trong tương lai. ■ Việc chuyển tiền có thể để lại dấu vết trên chuỗi.
Khả năng tương thích với Lightning	■ Chuyển đổi trạng thái RGB có các khái niệm trừu tượng và khó hiểu hơn rất nhiều so với các giao dịch Bitcoin. Điều này đặt ra thách thức cho các nhà phát triển Lightning.	■ Các khái niệm bổ sung khá dễ hiểu và thân thuộc với các nhà phát triển Lightning. ■ Có sự hỗ trợ của Lightning Labs nên thúc đẩy Taro phát triển nhanh
Hợp đồng thông minh	■ Có các kế hoạch trong tương lai để hỗ trợ các ứng dụng tài chính phức tạp thông qua việc xây dựng các hợp đồng thông minh hoàn chỉnh.	■ Hiện tại, Taro đang tập trung vào các token thay vì các hợp đồng thông minh
Hiện trạng của dự án	■ Có sẵn Ví GUI hỗ trợ token ■ Các tính năng hỗ trợ Lightning và các lược đồ non-token vẫn chưa xuất hiện.	■ Có sẵn Ví CLI nhưng chưa xác định các thông số kỹ thuật chính ■ Chưa hỗ trợ Lightning
Phí trên chuỗi	■ Phí rẻ hơn so với giao dịch bitcoin tiêu chuẩn.	■ Phí tương tự như giao dịch bitcoin; nhiều người nhận dẫn đến phí cao hơn.
Những trường hợp sử dụng lý tưởng	■ Sử dụng cho các stablecoin và IOU, Bitcoin Finance	■ Stablecoin, điểm thưởng, các IOU

Kết luận

Có thể thấy rõ những lợi ích của token CSV trên Bitcoin

Khi so sánh với hiện trạng của token theo mô hình Đồng thuận Toàn cầu, có thể thấy rõ Mô hình Xác thực phía Máy khách (CSV) mang lại lợi thế to lớn về khả năng mở rộng và quyền riêng tư.

Các ứng dụng tài chính của CSV có tiềm năng to lớn

Các giao thức ngoài chuỗi, bao gồm cả những giao thức sử dụng mô hình CSV sẽ phối hợp với nhau để tạo ra một lớp tài chính phức tạp trên blockchain Bitcoin. Sự phát triển này sẽ đẩy nhanh việc chấp nhận bitcoin thông qua tiện ích gia tăng.

Công nghệ còn non trẻ và con đường phát triển vẫn còn dài

Token CSV là một khái niệm mới, đòi hỏi phải xây dựng giao diện người dùng và công cụ mới. Quá trình xây dựng này cần có thời gian. Ngoài ra, phải tìm thấy các trường hợp sử dụng CSV cụ thể và có khả năng tạo sự liên kết với người dùng để thuyết phục họ sử dụng.

RGB và Taro có nhiều điểm khác biệt

RGB và Taro có thể cạnh tranh, nhưng mỗi giao thức lại khác nhau về mức độ ưu tiên và sự đánh đổi của chúng. Điều này dẫn đến các trường hợp sử dụng khác nhau. Hợp đồng thông minh ngoài chuỗi mới lạ của RGB và token định hướng Lightning của Taro có thể tồn tại cùng lúc.

Diamond Hands

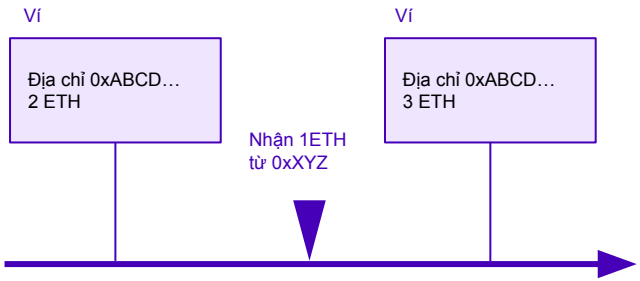
Phụ lục

BitcoinVN News

Mô hình Tài khoản so với Mô hình UTXO

Các tài khoản:

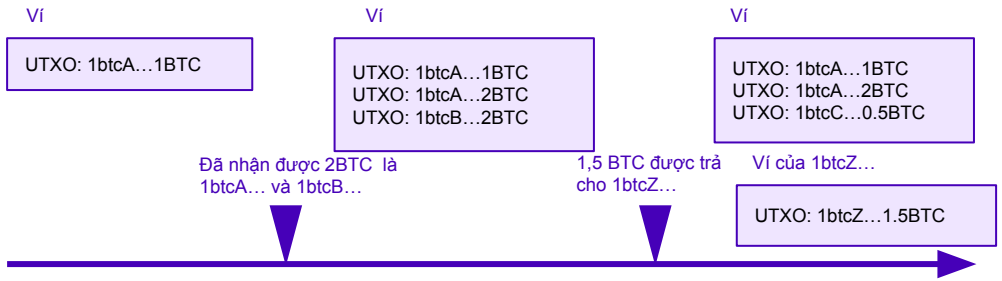
Mỗi tài khoản có một số dư. Số dư này được cập nhật theo kết quả của các giao dịch.
Người dùng thường sử dụng lại một địa chỉ duy nhất.
Nói cách khác, địa chỉ == tài khoản.



Ví dụ. Ethereum

Các UTXO:

Các giao dịch tạo đầu ra cho các địa chỉ, đảm bảo tổng (đầu ra) không vượt quá tổng (đầu vào). Đầu vào được chọn từ các đầu ra chưa sử dụng trước đó.
Tiền được quản lý dưới dạng đầu ra, ngay cả khi chúng được gửi đến cùng một địa chỉ.
Người dùng thường có nhiều địa chỉ.



Ví dụ. Bitcoin

Nhiều công nghệ tài chính trên Bitcoin không yêu cầu sử dụng các token

Một số nghiên cứu đã chỉ ra rằng: các token có ảnh hưởng tiêu cực có thể xuất hiện trên Bitcoin. Vì vậy, các nhà phát triển đã nghiên cứu các giải pháp và kỹ thuật tài chính **chỉ sử dụng bitcoin** để thay thế.

Công nghệ tài chính trên Bitcoin không yêu cầu token

Các hợp đồng nhật ký kín đáo - DLCs

Giao thức hợp đồng cho phép người dùng giao dịch một cách đáng tin cậy dựa trên kết quả được báo cáo bởi một nhà tiên tri thuộc bên thứ ba. Giao dịch qua DLCs là giao dịch tài chính P2P, riêng tư, không giam giữ.

【Các sản phẩm sử dụng DLC】

Atomic Finance, DLC.link

Stablesats

Đây là bảo hiểm rủi ro tự động cho bitcoin trên sàn giao dịch phái sinh nhằm đảm bảo ổn định giá trị đồng USD của kênh Lightning. Stablesats cho phép người dùng thay thế rủi ro tín dụng của stablecoin bằng rủi ro đối tác trao đổi tương lai.

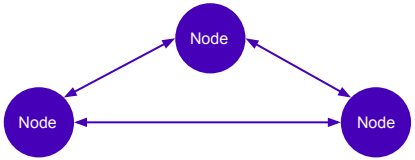
【Các sản phẩm Stablesats】

Ví Bitcoin Beach, Kollider

Các token có thể tương tác với Lightning như thế nào?

Diamond Hands

Ngang hàng



◎ Quyền riêng tư tối đa

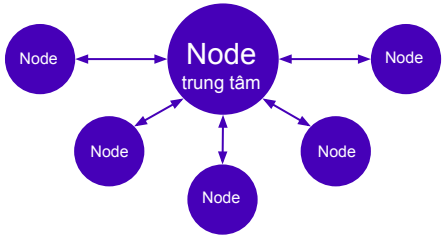
◎ Thanh toán ngang hàng miễn phí

× Vốn kém hiệu quả - hiệu suất sử dụng thấp

× Các node không lợi nhuận có thể không đáng tin cậy

→Tốt cho các tài sản coi trọng quyền riêng tư hoặc phù hợp cho các giao dịch thường xuyên với một đối tác nhất định

Hub-and-Spoke



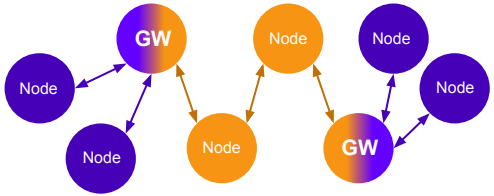
◎ Hiệu quả về vốn - token được giữ tại 1 kênh duy nhất

× Dựa vào dịch vụ trung tâm

× Quyền riêng tư có thể rất thấp

→Tốt cho các tài sản dựa vào các nhà khai thác tập trung hoặc khi bạn muốn tiết kiệm chi phí. Nhưng quyền riêng tư thì không được đảm bảo.

Các cổng Gateway (GW)



◎ Kết nối với thanh khoản Bitcoin LN

◎ Có thể được sử dụng để giao dịch tài sản, BTC

× Độ phức tạp cao, không đáng tin cậy

× Trao đổi tài sản khá tốn kém

× Gateways chỉ dành cho token có khối lượng cao

→Tốt để sử dụng cho DEX

Taro và RGB đều có thể được sử dụng theo bất kỳ cách nào ở trên. Đa phần người dùng thích kết nối với một trung tâm hơn. Và một số node trung tâm cung cấp dịch vụ dưới dạng Gateways, cho phép người dùng gửi hoặc trao đổi token, thậm chí trên các giao thức token khác nhau.

Liquid Network có các hợp đồng thông minh giúp mở rộng khả năng viết script của Bitcoin

The Liquid Network

Liquid Network là sản phẩm của tập đoàn sidechain được điều hành bởi Liquid Federation & Blockstream. Mặc dù được xây dựng trên Bitcoin nhưng các tính năng bổ sung của Liquid Network cải thiện quyền riêng tư và hợp đồng thông minh. Đồng thời, chúng cho phép phát hành các tài sản kỹ thuật số, ví dụ như stablecoin, token và các công cụ tài chính khác.

Các ứng dụng

- Liquid Network cho phép các ứng dụng tài chính vượt xa những gì mà chúng có thể xây dựng trên Bitcoin. Ví dụ: phát hành, giao dịch và giải quyết các token, hợp đồng tùy chọn có thể chuyển nhượng trên chuỗi…
- Một số người dùng Bitcoin cũng sử dụng Liquid L-BTC để cân bằng lại các kênh Lightning của họ bằng cách tận dụng khả năng tương thích cao và chi phí xác thực tương đối thấp của Liquid L-BTC.

Client-Side Validation tương tự như Rollup trên Ethereum

Rollup là gì?

Là một giải pháp mở rộng quy mô của Ethereum, Rollup cho phép người dùng gửi token trong một hợp đồng thông minh. Sau các token này có thể được chuyển giữa những người dùng ngoài chuỗi Rollup. Theo định kỳ, các giao dịch này sẽ được tổng hợp và xác thực trên chuỗi để kiểm chứng.

Xác thực Phía Máy khách	Optimistic Rollup	Zero-Knowledge Rollup
Điểm tương đồng	• Các note Ethereum không tự xác thực các cam kết tổng hợp mà người dùng phải làm điều đó (nếu họ quan tâm)	• Người dùng có thể xác thực các chuyển đổi trạng thái và số dư từ dữ liệu giao dịch và bằng chứng hợp lệ
Sự khác biệt	• Thiếu sự riêng tư • Hợp đồng thông minh trên chuỗi được sử dụng để ngăn chặn quyền thoát và chứng minh gian lận • Các node phải lưu trữ một lượng lớn dữ liệu giao dịch	• Chuyển đổi và xác thực trạng thái được thực hiện bởi tất cả các node Ethereum thông qua hợp đồng trực tuyến; đây không phải là Xác thực Phía Máy khách • Bằng chứng hợp lệ phải được gửi đến chuỗi khối • Khả năng chống kiểm duyệt bị bào mòn nếu dữ liệu giao dịch không được lưu trữ trên chuỗi

Tài liệu tham khảo①

Client-Side Validation)

- https://scalingbitcoin.org/transcript/milan2016/client-side-validation
- https://github.com/LNP-BP/presentations/blob/master/Presentation%20slides/PRISM%20-%20RGB%20computing%20model.pdf

Single-Use Seals

- https://petertodd.org/2016/commitments-and-single-use-seals

Lightning Network

- https://lightning.network
- https://docsend.com/view/e67t2yst5yvjjt76

RGB

- https://rgb.info
- https://github.com/LNP-BP/LNPBPs
- https://github.com/RGB-WG
- https://medium.com/@FedericoTenga/understanding-rgb-protocol-7dc7819d3059
- https://bitcoinmagazine.com/technical/rgb-magic-client-contracts-on-bitcoin
- https://www.rgbfaq.com/

Taro

- https://github.com/lightninglabs/taro
- https://docs.lightning.engineering/the-lightning-network/taro
- https://medium.com/nayuta-inc/taro-ed6b93b09a75
- https://river.com/learn/what-is-taro-in-bitcoin/
- https://github.com/Roasbeef/bips/blob/bip-taro/bip-taro.mediawiki

Tài liệu tham khảo②

Diamond Hands

DID

- https://github.com/decentralized-identity/ion
- https://developer.tbd.website/projects/web5/

Decentralized Social Social Media

- https://nostr.com

DLCs

- https://bitcoinops.org/en/topics/discreet-log-contracts/
- https://river.com/learn/terms/d/discreet-log-contract-dlc/

Stablesats

- https://stablesats.com/

Liquid

- https://blockstream.com/liquid/