Machine Translated by Google

CS251 Mùa thu năm 2023

(cs251.stanford.edu)

(1) Giá trị trích xuất tối đa, (2) Thị trư ờng NFT

Dan Boneh

Bài tập về nhà số 3 đã đăng

Machine Translated by Google

Chúng ta đang ở đâu trong khóa học

• Giao thức đồng thuận hoạt động như

thế nào • Bitcoin: mô hình UTXO và ngôn ngữ lập trình Bitcoin • Ethereum

(máy tính blockchain): EVM và Solidity

Chủ đề hiện tại: tài chính phi tập trung

on-chain: sàn giao dịch, stablecoin, hôm nay: MEV

Tiếp theo: quyền riêng tư trên blockchain, mở rộng quy mô blockchain,

và khả năng tư ơ ng tác giữa các blockchain

Machine Translated by Google

Tài chính phi tập trung (DeFi)

- Không cần xin phép: bất kỳ công cụ tài chính nào cũ ng có thể đư ợc triển khai và triển khai với một vài dòng mã Solidity

(một hệ thống tập trung có thể từ chối triển khai một dịch vụ cạnh tranh)

- Minh bạch: Mã Dapp và trạng thái Dapp là công khai

  Bất kỳ ai cũ ng có thể kiểm tra và xác minh

- Có thể cấu hình: Các Dapp có thể gọi nhau

  Tiêu chuẩn ERC-20 cho phép khả năng tư ơ ng tác (6 chức năng)

Machine Translated by Google

Tại sao lại là DeFi? Thất bại của hệ thống tài chính hiện tại

- Hiệu quả xuyên biên giới kém:

  gửi 10 đô la đến Nam Mỹ phí 36%

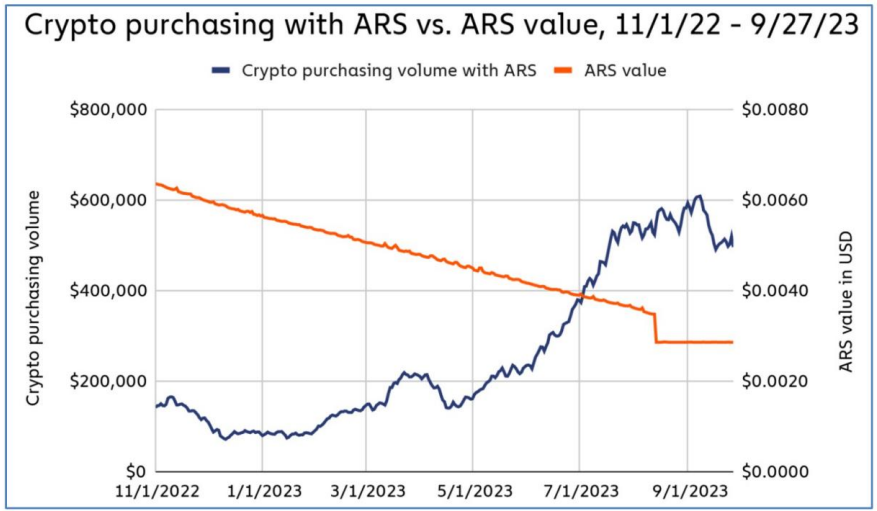
- Chi phí cao của việc nghèo đói ở Mỹ: Năm 2019,

  5,4 phần trăm hộ gia đình ở Hoa Kỳ không có tài khoản ngân hàng

- Nền kinh tế có tiền tệ fiat không ổn định

Machine Translated by Google

Tại sao lại là DeFi? Thất bại của hệ thống tài chính hiện tại



Khối lư ợng mua USDC/USDT hàng ngày tại Argentina trong thời kỳ lạm phát

> "Khi việc áp dụng tiền điện tử ngày càng phát triển, rất nhiều ngư ời [ở Argentina] hiện sẽ nhận tiền lư ơ ng của họ và ngay lập tức chuyển vào USDT hoặc USDC."
>
> Alfonso Martel Seward, Tiền mặt chanh

https://www.chainalysis.com/blog/latin-america-cryptocurrency-adoption/

Machine Translated by Google

Giá trị chiết xuất tối đa (MEV)

Machine Translated by Google

Ngư ời tìm kiếm

Ethereum tạo ra một loại hình kinh doanh mới: ngư ời tìm kiếm

- Trọng tài: Tỷ giá hối đoái Uniswap DAI/USDC là 1,001 trong
  khi tại Sushiswap tỷ giá là 1,002
  ngư ời tìm kiếm đăng Tx để cân bằng thị trư ờng và lợi nhuận

- Thanh lý: giả sử có cơ hội thanh lý trên Aave ngư ời tìm kiếm đăng
  giao dịch thanh lý và lợi nhuận

- Nhiều ví dụ khác.thư ờng sử dụng một chuỗi Tx (một bó)

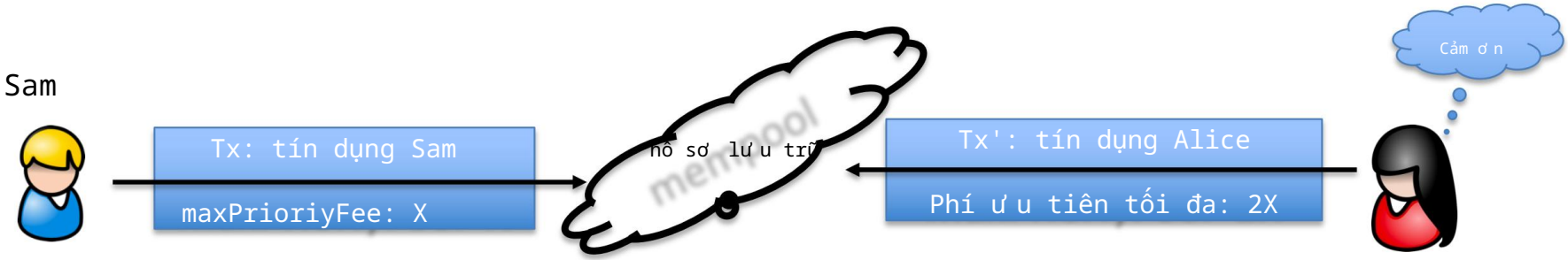
Machine Translated by Google

Vấn đề MEV

Điều gì xảy ra khi ngư ời tìm kiếm đăng một Tx lên mempool?

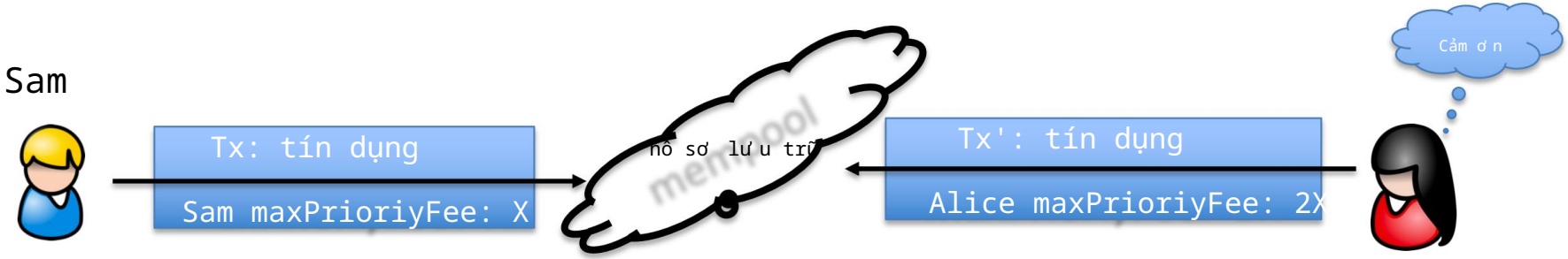
- Trình xác thực: tạo một Tx' mới với chính nó là ngư ời thụ hư ởng và đặt nó trư ớc Tx của Sam trong khối đư ợc đề xuất
- Ngư ời tìm kiếm khác: tạo một Tx' mới với chính nó là ngư ời thụ hư ởng và đăng nó với maxPrioriyFee cao hơ n

hành động này hiện nay chủ yếu đư ợc tự động hóa bằng các bot sao chép-dán



Machine Translated by Google

Vấn đề MEV



Machine Translated by Google

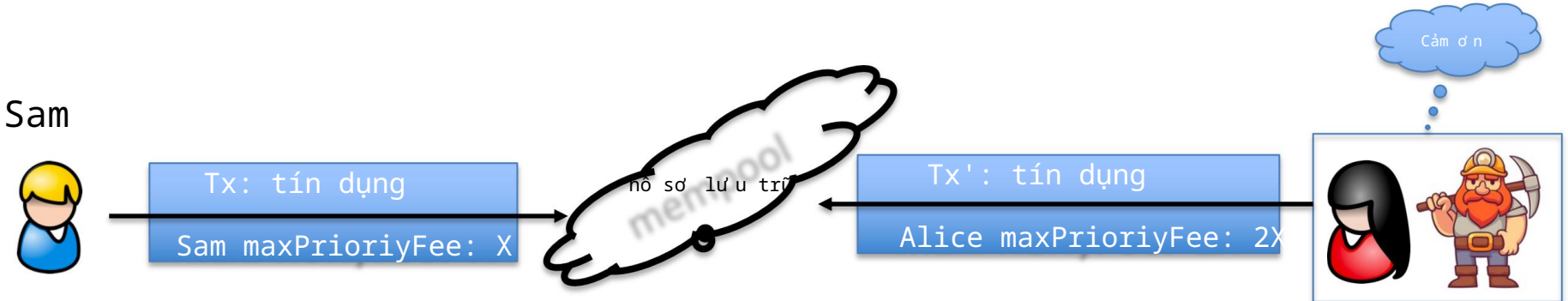
Kết quả gây hại cho ngư ời dùng trung thực

Đấu giá giá khí đốt (PGA): nhiều ngư ời tìm kiếm

cạnh tranh • Liên tục gửi một Tx với maxPriorityFee ngày càng

cao cho đến khi ngư ời xác thực chọn một . xảy ra trong vòng vài gi

gây tắc nghẽn (nhiều Tx trong mempool) và phí gas cao

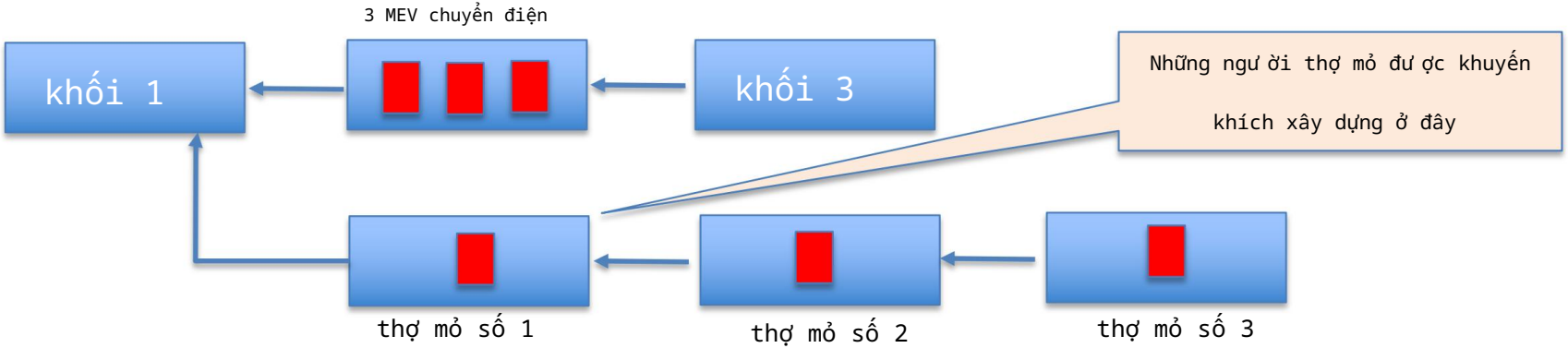


Machine Translated by Google

Kết quả gây tổn hại đến sự đồng thuận

Tấn công phá hoại sự đồng thuận của chuỗi dài nhất (không phải Ethereum):

Thợ mỏ hợp lý: có thể gây ra sự tái tổ chức bằng cách lấy một MEV Tx cho chính nó và để lại hai cho những người khai thác khác



Vấn đề: MEV Tx tạo ra doanh thu bổ sung cho thợ đào, cao hơn phần thưởng khối

Machine Translated by Google

Kết quả gây ra sự tập trung hóa

Ngư ời xác thực có thể đánh cắp MEV Tx từ ngư ời tìm kiếm

Mempool riêng tư

Ngư ời tìm kiếm chỉ gửi Tx đến ngư ời xác thực mà họ tin tư ởng

(có quan hệ kinh doanh với)

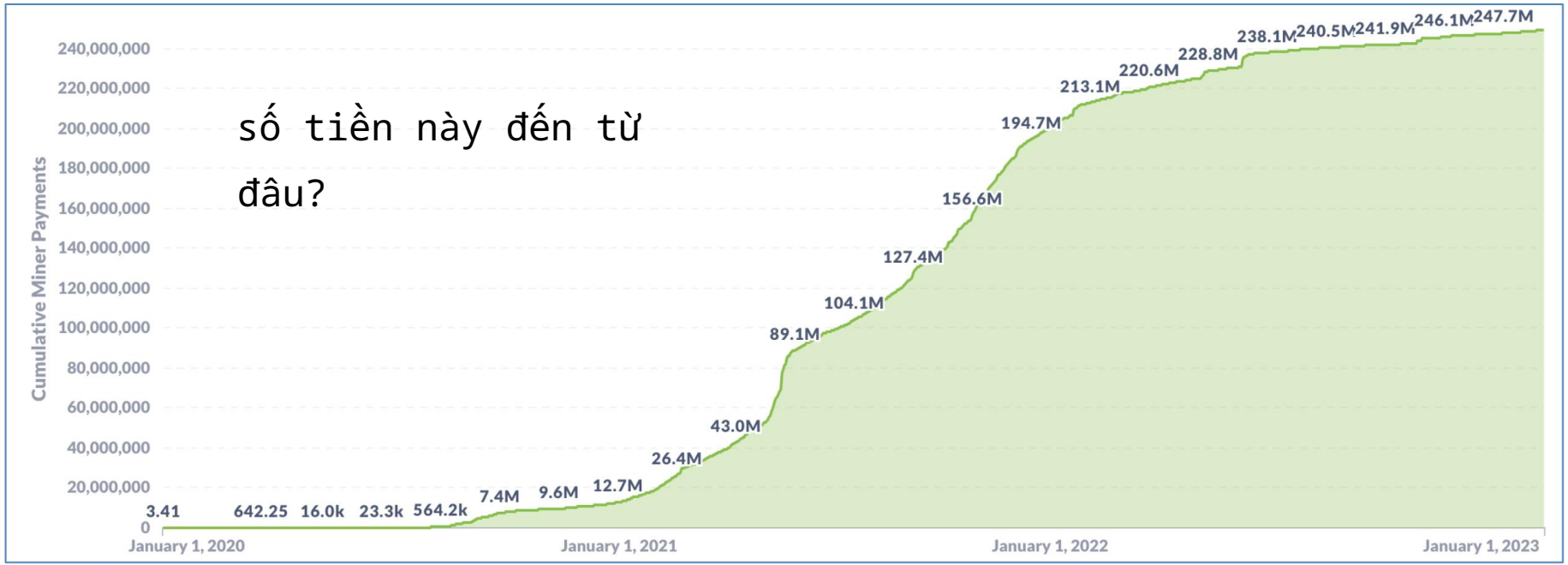
Các trình xác thực này không truyền Tx đến mạng mà tự đặt chúng vào các khối

Về lâu dài: một số trình xác thực sẽ xử lý phần lớn tất cả các Tx

Machine Translated by Google

Phần thưởng MEV lớn đến mức nào?

Tổng số tiền thanh toán MEV cho người xác thực kể từ tháng 11 năm 2020: (247 triệu đô la)

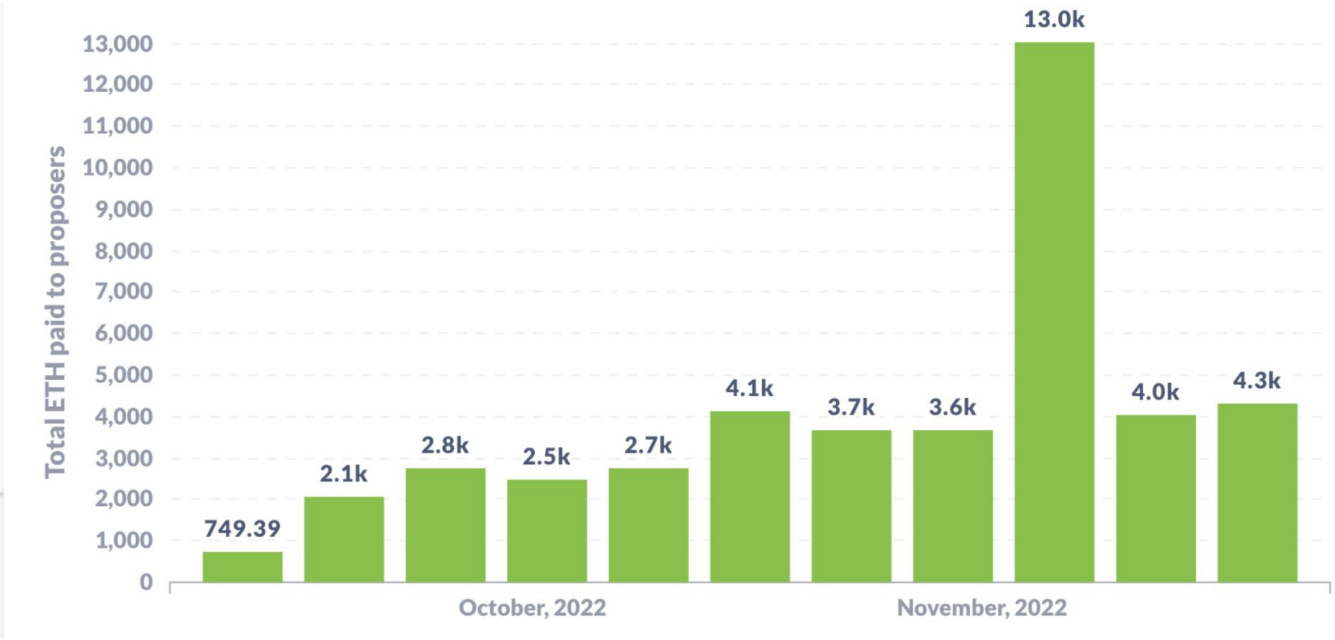


nguồn: explore.flashbots.net

Machine Translated by Google

Phần thưởng MEV lớn đến mức nào?

Số tiền MEV hàng tuần được trả cho người xác thực (bằng ETH):



nguồn: transparency.flashbots.net

Machine Translated by Google

Phải làm gì đây?

Machine Translated by Google

Hai lựa chọn

Lựa chọn 1:

- Chấp nhận MEV là điều không thể tránh khỏi; giảm thiểu tác hại của nó đối với hệ sinh thái Flashbot

Tùy chọn 2:

- Cố gắng ngăn ngừa một số MEV, bằng cách loại bỏ lựa chọn của ngư ời đề xuất khối trong việc sắp xếp Tx trong một khối. (chủ yếu trong các bài báo nghiên cứu)

Machine Translated by Google

Tùy chọn 1: Tách biệt ngư ời xây dựng đề xuất (PBS)

Mục tiêu:

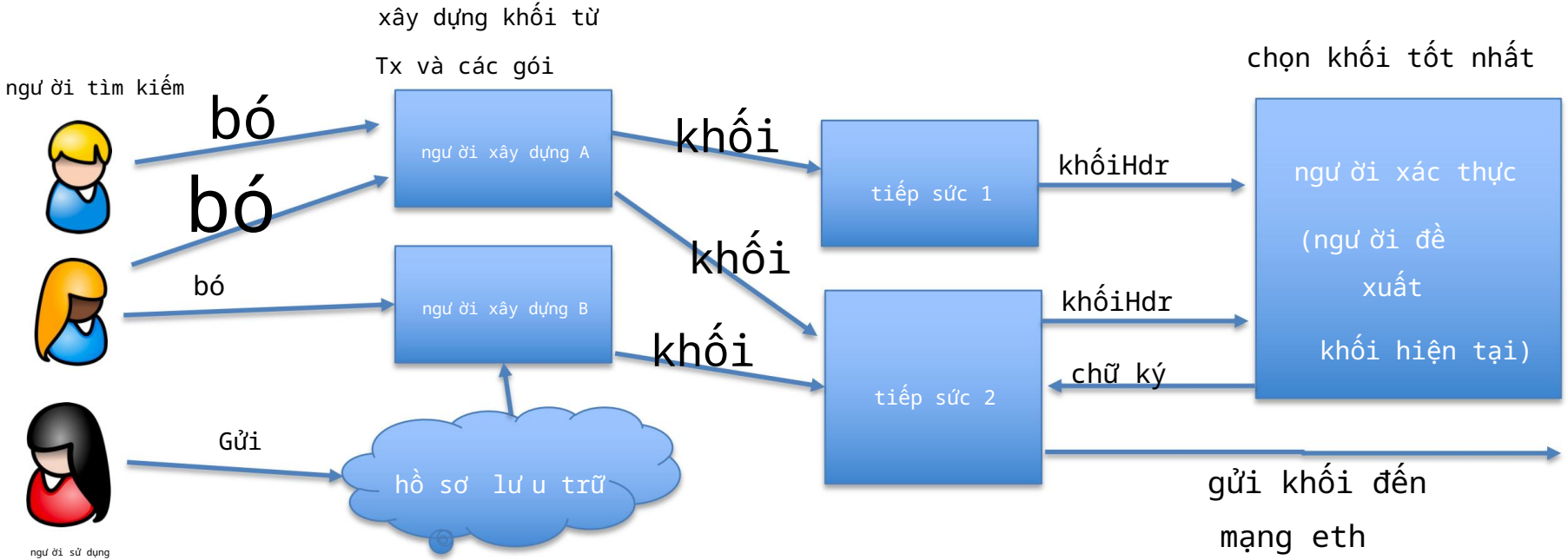
- Loại bỏ giá đấu giá khí đốt trong mempool công cộng
    - Thay vào đó, hãy tạo ra một thị trư ờng ngoài chuỗi để ngư ời tìm kiếm cạnh tranh về vị trí của các bó của chúng trong một khối
- Ngăn chặn sự tập trung của trình xác thực: tạo điều kiện cho mọi trình xác thực kiếm đư ợc khoản thanh toán MEV từ ngư ời tìm kiếm

Triển khai PBS hiện tại: MEV-boost

Machine Translated by Google

Những ngư ời tham gia PBS (như trong MEV-boost)

Ngư ời dùng có Tx và ngư ời tìm kiếm có các gói (chuỗi Tx) • ngư ời tìm kiếm muốn gói của mình đư ợc đăng trong một khối không sửa đổi



Machine Translated by Google

Tăng cường MEV

Người xây dựng: thu thập các bó và Tx, xây dựng một khối (≈300 bó/khối)

• bao gồm một đề nghị MEV cho người xác thực (feeRecipient)

Rơ le: thu thập các khối, chọn khối có giá trị MEV tối đa • gửi

tiêu đề khối (và giá trị MEV) cho người đề xuất khối • Không thể

tiết lộ Tx trong khối cho người đề xuất (người đề xuất có thể đánh cắp Tx)

Người đề xuất: chọn lời đề nghị tốt nhất và ký tiêu đề với khóa đặt cược

của mình Sau đó, Relay gửi khối đến mạng, công khai khối đó

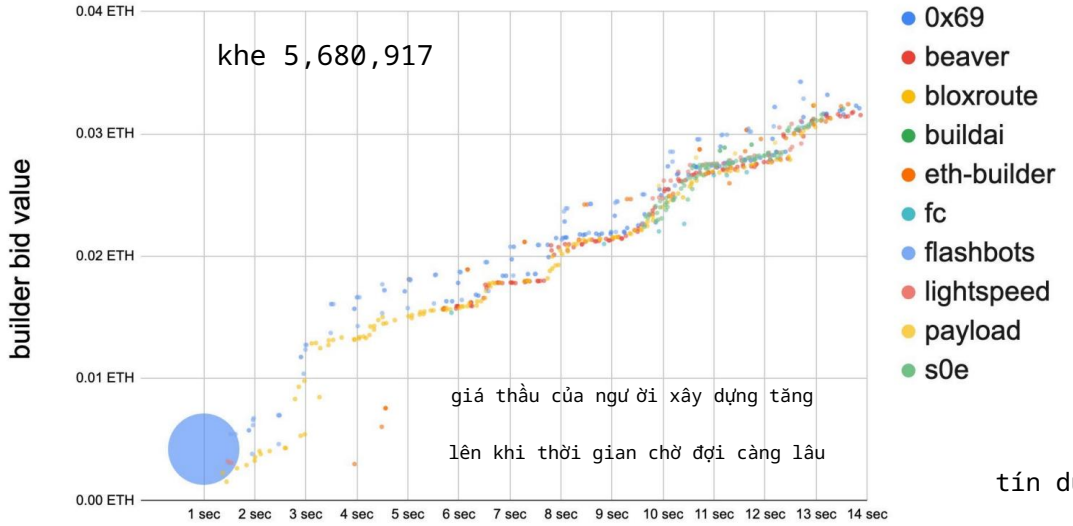
Bây giờ, người đề xuất không thể đánh cắp MEV (sẽ bị lộ thông tin)

https://writings.flashbots.net/searching-post-merge

Machine Translated by Google

Nhiều tùy chọn khối cho mỗi khe

Một rơ le có thể nhận 500 khối cho mỗi ô từ ngư ời xây dựng • Mỗi ngư ời xây dựng có thể gửi 20 khối cho rơ le cho một ô • Tại sao? Ngư ời xây dựng càng chờ lâu thì càng có nhiều cơ hội MEV



tín dụng: Justin Drake và Shea Ketsdever

Machine Translated by Google

Rơ le hoạt động

Flashbots: Lọc ra các địa chỉ đư ợc OFAC chấp thuận, nhằm mục đích tối đa hóa khoản thanh toán cho ngư ời xác thực (để nhiều ngư ời xác thực sẽ làm việc với nó)

BloXroute: không kiểm duyệt, nhằm mục đích tối đa hóa khoản thanh toán của ngư ời xác thực

UltraSound: không vì lợi nhuận, không kiểm duyệt

Machine Translated by Google

Một ví dụ: flashbots relay

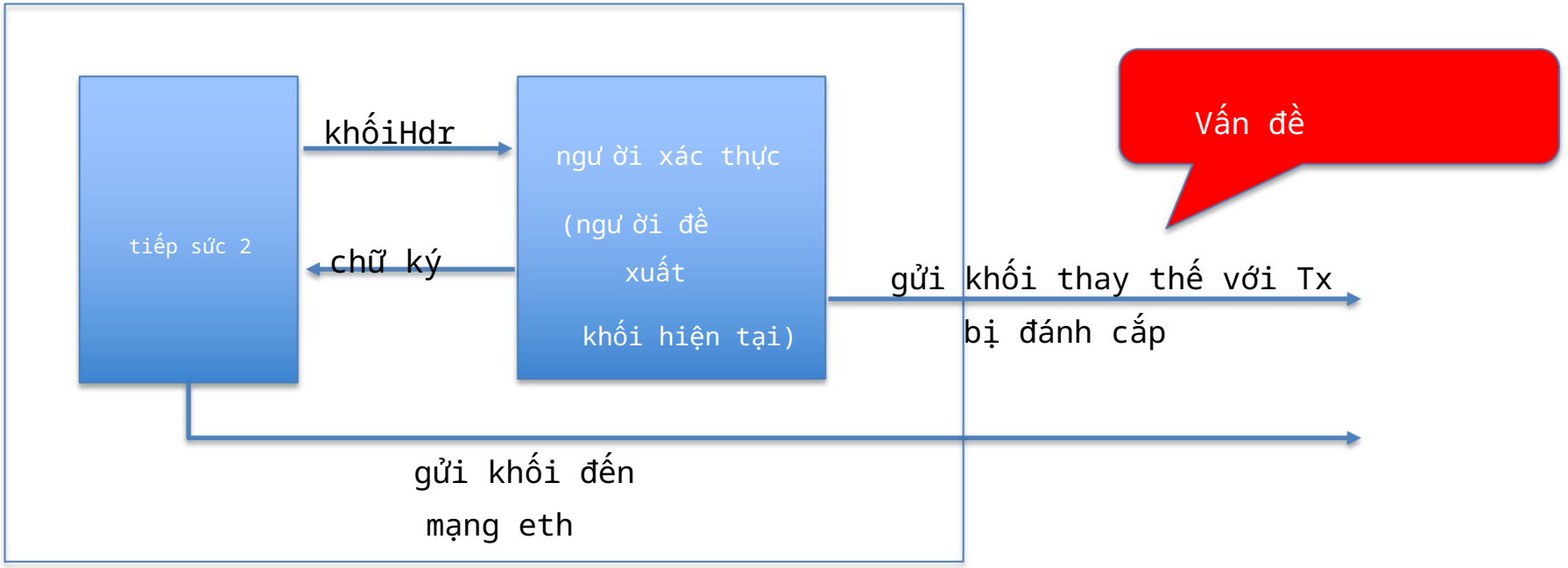
Recently Delivered Payloads

phí cho người xác thực

Epoch	Slot	Block number	Value (ETH)	Num tx
165,046	5,281,503	16,115,184	0.0759673152	186
165,046	5,281,501	16,115,182	0.05098935853	142
165,046	5,281,499	16,115,180	0.1902791095	167
165,046	5,281,498	16,115,179	0.103438972	295
165,046	5,281,496	16,115,177	0.07159735143	199
165,046	5,281,495	16,115,176	0.04034671944	125

Machine Translated by Google

Vấn đề chủng tộc



Ngư ời đề xuất khối sẽ bị cắt giảm (tại sao?) Mất 1 ETH.

như ng có thể kiếm đư ợc nhiều hơ n từ MEV bị đánh cắp.

Machine Translated by Google

Chúng ta xong chưa? Chưa hẳn...

Tập trung xây dựng: ba người xây dựng 75% tổng số khối !!

- Tập trung rõ ràng vào thị trường xây dựng
- Cho phép kiểm duyệt bởi các nhà xây dựng

(builder0x69,beaverbuild,Flashbots)

Người đề xuất nắm giữ toàn bộ quyền lực (đấu giá giá đầu tiên giữa các nhà xây dựng)

Hầu hết lợi nhuận của MEV chảy vào những người đề xuất chặn

MEV-boost không được thiết kế cho MEV chuỗi chéo • Đối với

chênh lệch giá chuỗi chéo, không đảm bảo tính nguyên tử cho bó

Machine Translated by Google

Bư ớc tiếp theo: SUAVE

Mục tiêu:

- Giao dịch phải đư ợc bảo mật (đư ợc mã hóa) cho đến khi đư ợc ngư ời đề xuất khối ký

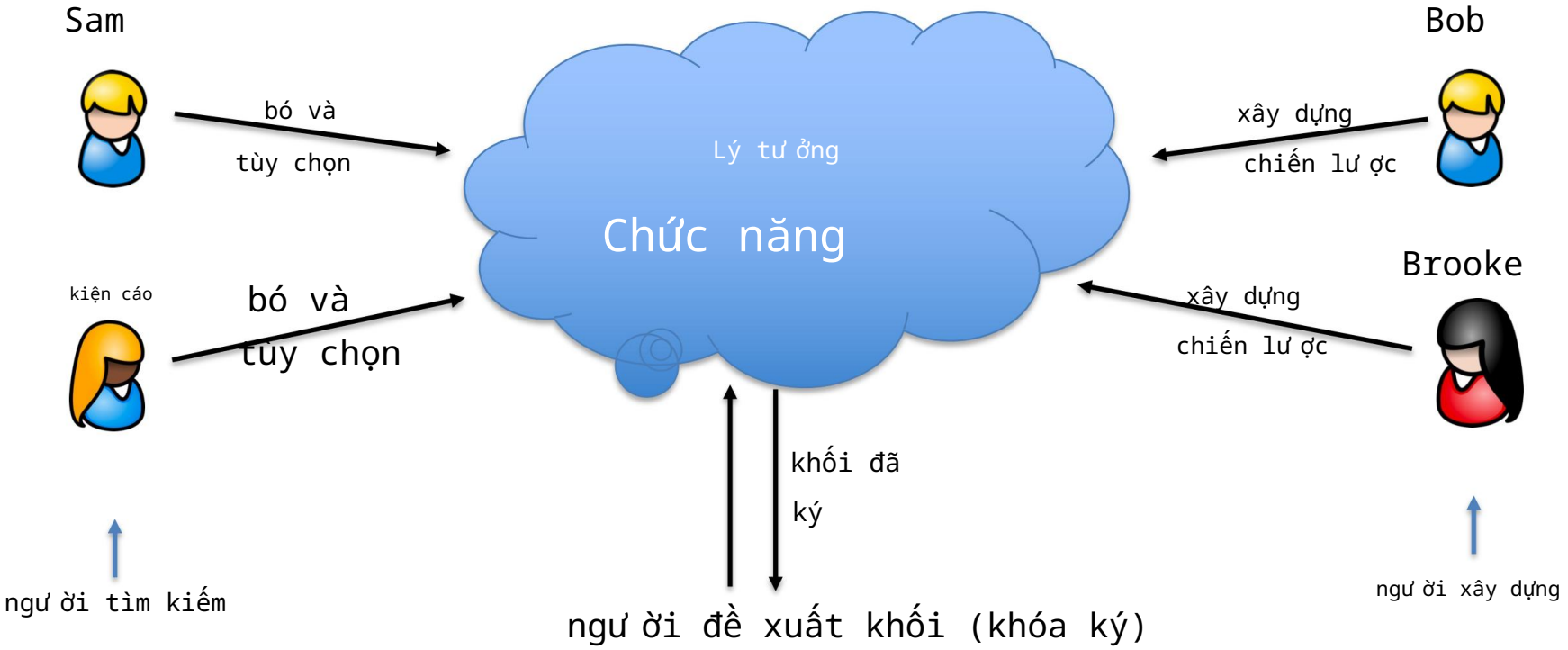
  ... như ng phải có sẵn cho tất cả ngư ời xây dựng khối để xây dựng khối

Có vẻ mâu thuẫn! tiền điện tử sẽ giải cứu:

yêu cầu một MPC lớn hoặc vùng bảo mật HW an toàn

Machine Translated by Google

Tính toán đa phư ơ ng SUAVE



Machine Translated by Google

Lựa chọn 2:

Sắp xếp giao dịch công bằng

Machine Translated by Google

Chúng ta có thể giảm MEV không?

1. Ngẫu nhiên hóa các giao dịch trước khi thực hiện Nhược điểm: spam với giao dịch trích xuất giống hệt nhau

2. Công bằng theo thứ tự thời gian

3. Lệnh mù-Công bằng

4. Môi trường thực hiện đáng tin cậy (TEE) để đặt hàng giao dịch
   Nhược điểm: giả định về phần cứng

5. Bạn còn ý tưởng nào nữa không? Ý tưởng của bạn ở đây .

Machine Translated by Google

Aequitas: Công bằng theo thứ tự thời gian

Ý tưởng cơ bản: nếu hầu hết trình xác thực nhận được tx1 trước tx2, thì tx1 phải đi trước tx2 trong thứ tự cuối cùng.

Bài toán chu trình Condorcet: • trình xác thực số 1: [tx1, tx2, tx3] • trình xác thực số 2: [tx2, tx3, tx1] • trình xác thực số 3: [tx3, tx1, tx2]

Hai lần nhận được (tx1 trước tx2) VÀ hai lần nhận được (tx2 trước tx3) VÀ hai lần nhận được (tx3 trước tx1) Không có thứ tự !!

Một giải pháp khả thi: từ chối toàn bộ chu kỳ nếu Tx trong chu kỳ xung đột.

[Kelkar-Zhang-Goldfeder-Juels 2020]

Machine Translated by Google

Aequitas: Công bằng theo thứ tự thời gian

Giao thức Block-Fair-Ordering :

1. Ngư ời khai thác phát đi lệnh ư u tiên của họ.
2. Xây dựng biểu đồ giao dịch:
   a. Đỉnh = giao dịch có mặt trong một số lư ợng lớn thứ tự, b. Cạnh(tx1 tx2) nếu tx1 đứng trư ớc tx2 trong hầu hết các thứ tự.
3. Thu gọn các thành phần đư ợc kết nối chặt chẽ thành một đỉnh duy nhất.
4. Sắp xếp các đỉnh theo cấu trúc tôpô.
5. Cuối cùng là một lệnh sắp xếp theo thứ tự.

[Kelkar-Zhang-Goldfeder-Juels 2020]

Machine Translated by Google

Nhiều giao thức công bằng theo thứ tự dựa trên thời gian hơn

- Vấn đề: Ưu điểm của người tìm kiếm có kết nối tốt hơn
- Giao tiếp cao: ( ).

Themis: cùng mục tiêu với Aequitas, nhưng chỉ ( ) giao tiếp.

"Themis: Nhanh chóng, Mạnh mẽ Trật tự-Công bằng trong Sự đồng thuận của Byzantine" bởi Kelkar-Deb-Long-Juels-Kannan 2021

Machine Translated by Google

Một cách tiếp cận khác: trật tự mù quáng-công bằng

Công bằng trong lệnh mù: ba giai đoạn:

- Cam kết giao dịch:

  ngư ời dùng gửi cam kết cho giao dịch của họ

  (Dữ liệu Tx vẫn đư ợc ẩn khỏi ngư ời đề xuất khối)

- Cam kết đơ n hàng:

  ngư ời đề xuất khối đặt hàng các cam kết vào một khối.

- Tiết lộ giao dịch:

  khi khối đư ợc hoàn tất, các cam kết sẽ đư ợc tiết lộ (bởi ngư ời xác thực hoặc “tự động”). Quá muộn để đánh cắp MEV.

Machine Translated by Google

Mù lệnh-Công bằng

Xây dựng #1: mã hóa ngư ỡng (Chuỗi thẩm thấu):

- Thiết lập: trình xác thực tạo ra, ngư ỡng chia sẻ khóa bí mật
- Cam kết (tx): ngư ời dùng gửi Mã hóa(, Tx)
- Tiết lộ (bởi ngư ời xác thực): sau khi khối đư ợc hoàn tất:

  Các trình xác thực cùng nhau giải mã: Tx Giải mã(,)

Reiter-Birman, 1994

Cachin-Kursawe-Petzold-Shoup, 2001

Machine Translated by Google

Mù lệnh-Công bằng

Xây dựng #2: cam kết theo thời gian

- Commit (tx): ngư ời dùng gửi TimeCommit(Tx)

- Tiết lộ (bởi bất kỳ ai):
  - Bất kỳ ai cũ ng có thể mở cam kết bằng cách sử dụng mư ời phút tính toán tuần tự. khi đó khối sẽ đư ợc hoàn tất.

Lư u ý: cần cam kết thời gian hàng loạt để tránh mất 10 phút cho mỗi Tx!

Machine Translated by Google

Cần thêm nhiều ý tưởng hơn!

Một lĩnh vực nghiên cứu đang hoạt động

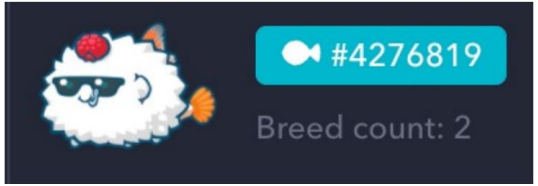
Machine Translated by Google

Chủ đề mới: Thế giới NFT

Machine Translated by Google

Tài sản kỹ thuật số (NFT)

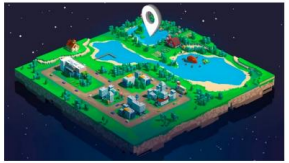
Ví dụ về tài sản kỹ thuật số: (ERC-721)



- Tài sản trò chơi: axies, DFK Heroes, .
- Thành viên: Proof tập thể (truy cập vào các sự kiện)
- Tên miền: ENS

Những cú đánh đỉnh cao của NBA

- Đồ sưu tầm thể thao: Những cú đánh đỉnh cao của NBA
- Thế giới ảo: các lô đất trong một vùng đất ảo



- Nghệ thuật

Machine Translated by Google

Tài sản kỹ thuật số (NFT)

Không có hai NFT nào giống hệt nhau: chúng không thể hoán đổi cho nhau

• NFT được xác định bởi: lịch sử, tiện ích, giao diện, v.v.

Tại sao không quản lý trong một DB

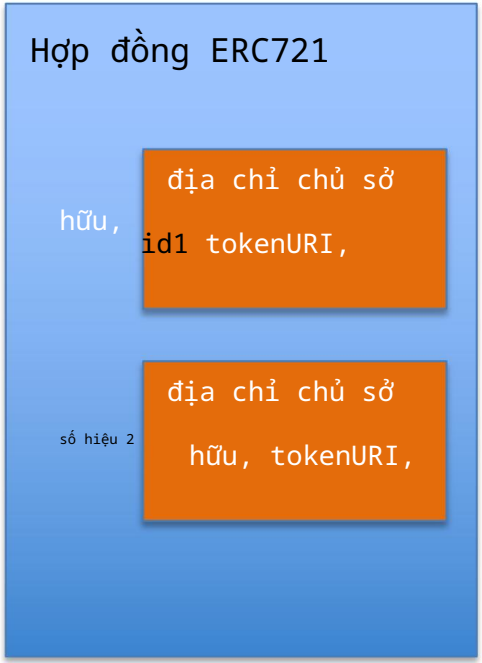
trung tâm? • Blockchain đảm bảo quyền sở hữu lâu dài, cho

đến khi bán. • Cung cấp hồ sơ xuất xứ đáng tin cậy (có bằng chứng làm giả)

Machine Translated by Google

Tiêu chuẩn ERC-721

Bộ sưu tập NFT



Một bộ sưu tập NFT khác

Bộ sưu tập NFT

Machine Translated by Google

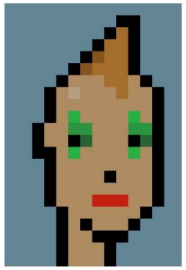
Tiêu chuẩn ERC-721 (tập hợp con)

```
ánh xạ (uint256 => địa chỉ) idToOwner nội bộ;

chức năng safeTransferFrom(
    địa chỉ _từ, địa chỉ _đến, uint256 _tokenId, byte dữ liệu)

chức năng phê duyệt(địa chỉ _đã phê duyệt, uint256 _tokenId)

hàm setApprovalForAll(địa chỉ _operator, bool _approved)

hàm ownerOf(uint256 _tokenId) trả về (địa chỉ);
```

Machine Translated by Google

Ví dụ: CryptoPunks (2017, trước ERC-721)

Tổng cộng 10.000 CryptoPunks. Được quản lý theo hợp đồng tại địa chỉ Ethereum 0xb47e3cd8DF8. (250 dòng độ rắn chắc) thị trường trên chuỗi:



#7610

Bid	beautifu...	visa	150Ξ ($497,239)	Aug 24, 2021
Sold	gmoney	0xa04e64	49.50Ξ ($149,939)	Aug 18, 2021
Bid	0xa04e64		49.50Ξ ($149,024)	Aug 18, 2021
Sold	gr8wxl	0x84c920	21Ξ ($31,117)	Mar 05, 2021
Offered			21Ξ ($31,117)	Mar 05, 2021
Sold	0x02751f	gr8wxl	0.30Ξ ($67)	Aug 03, 2017
Offered			0.30Ξ ($59)	Jul 30, 2017
Claimed		0x02751f		Jun 23, 2017

mua cung cấp

đã bán!

bán chào hàng

https://www.larvalabs.com/cryptopunks/details/7610

Machine Translated by Google

Hệ sinh thái NFT

Quyền sở hữu theo phần: mua một phần NFT với một nhóm lớn • chẳng hạn như tài sản chơi game đắt tiền (tàu vũ trụ) • kiểm soát nó với nhóm (quản trị, làm việc hợp tác)

Cho vay/mượn NFT: (được kích hoạt bằng phần mở rộng cho ERC-721)

• Cho mượn NFT chơi game hoặc tên miền để ai đó sử dụng • Trải nghiệm dùng thử trước khi mua

Sử dụng NFT làm tài sản thế chấp cho khoản vay (cần ước tính giá liên tục)

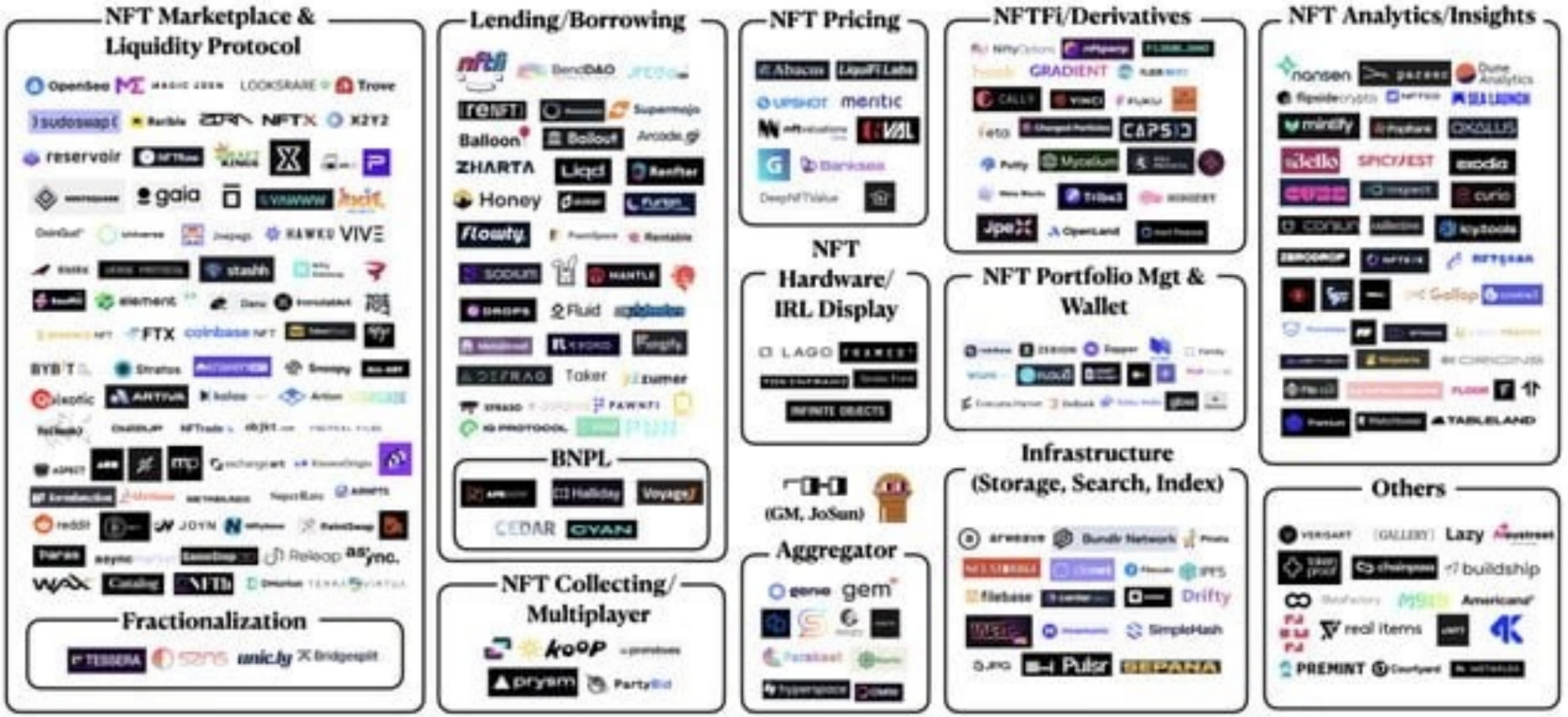
Thị trường phái sinh NFT, dịch vụ định giá NFT

Machine Translated by Google

The NFTFi Ecosystem

GBV

@oxminion
@alexgedevani



Caveats:

- Not all encompassing. Does not include a few big verticals that also touch NFTs: Photography, Music, Fashion, Metaverse, Reputation/Identity
- Some products overlap in multiple areas but are only listed once. Some in stealth are adding competing products in adjacent markets
- Have not mapped all chains supported. Ethereum leads in activity but most products will go multichain

Aug 2022

Machine Translated by Google

Tiền bản quyền

Với ERC-721, việc mã hóa bất kỳ kế hoạch trả tiền bản quyền nào cũ ng khá dễ dàng:

• Ví dụ: đối với mỗi lần bán tài sản, hãy gửi 1% tiền bản quyền cho ngư ời sáng tạo.

(nghĩ đến: NBA Top Shots)

Vấn đề: không khó để bỏ qua chính sách này.

• Thị trư ờng lư u ký sở hữu tài sản hiển thị trên trang web của mình rằng tài sản thuộc về Bob

• Khi Bob bán tài sản cho Carol, thị trư ờng sẽ cập nhật trang web của mình. Không có Tx trên chuỗi không có tiền bản quyền trả cho ngư ời sáng tạo

Machine Translated by Google

Hội chơi game

Các tổ chức tài chính liên trò chơi (Yield Guild Games)

Đó là gì:

Nguồn vốn từ LP (bằng cách phát hành token)

Mua các vùng đất ảo và vật phẩm trong trò chơi,

Tạo doanh thu bằng cách cho thuê tài sản cho người chơi, Trả cổ tức cho LP, Tích lũy lãi vốn từ tài sản cơ sở.

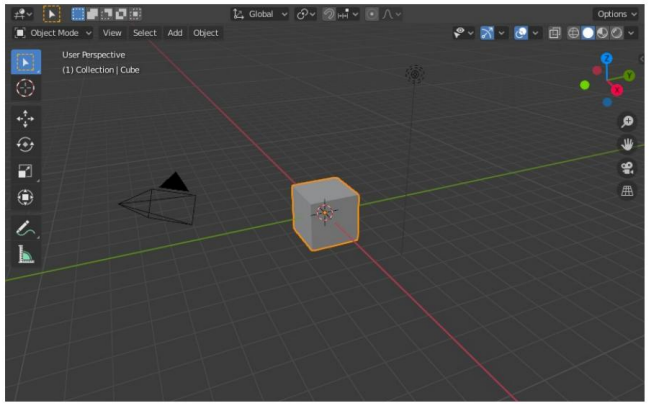
Machine Translated by Google

Phát triển đất ảo?

Các nền tảng thành công tận dụng sự sáng tạo của ngư ời dùng (UGC)

• NFT cho phép ngư ời sáng tạo sở hữu, duy trì và kiểm soát các sáng tạo của họ

Thử thách dành cho mọi ngư ời: biến khối lập phư ơ ng thành thành phố kỹ thuật số.



=>

Machine Translated by Google

KẾT THÚC BÀI GIẢNG

Bài giảng tiếp theo: Bối cảnh pháp lý