Machine Translated by Google

CS251 Mùa thu năm 2023

(cs251.stanford.edu)

Sàn giao dịch phi tập trung

Dan Boneh

Machine Translated by Google

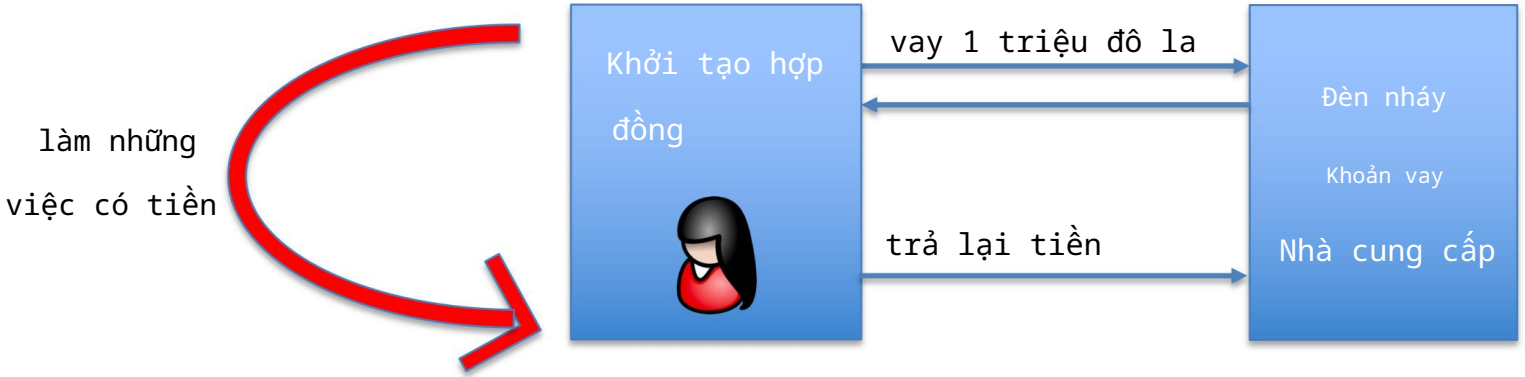
. như ng trư ớc tiên, hãy cho vay nhanh

Machine Translated by Google

Khoản vay nhanh là gì?

Khoản vay nhanh được thực hiện và hoàn trả trong một giao dịch duy nhất

không có rủi ro cho người cho vay người vay không cần thế chấp



(Tx chỉ có hiệu lực nếu tiền được trả lại bằng cùng một Tx)

"Tấn công hệ sinh thái DeFi bằng các khoản vay nhanh để giải trí và kiếm lợi nhuận"

Machine Translated by Google

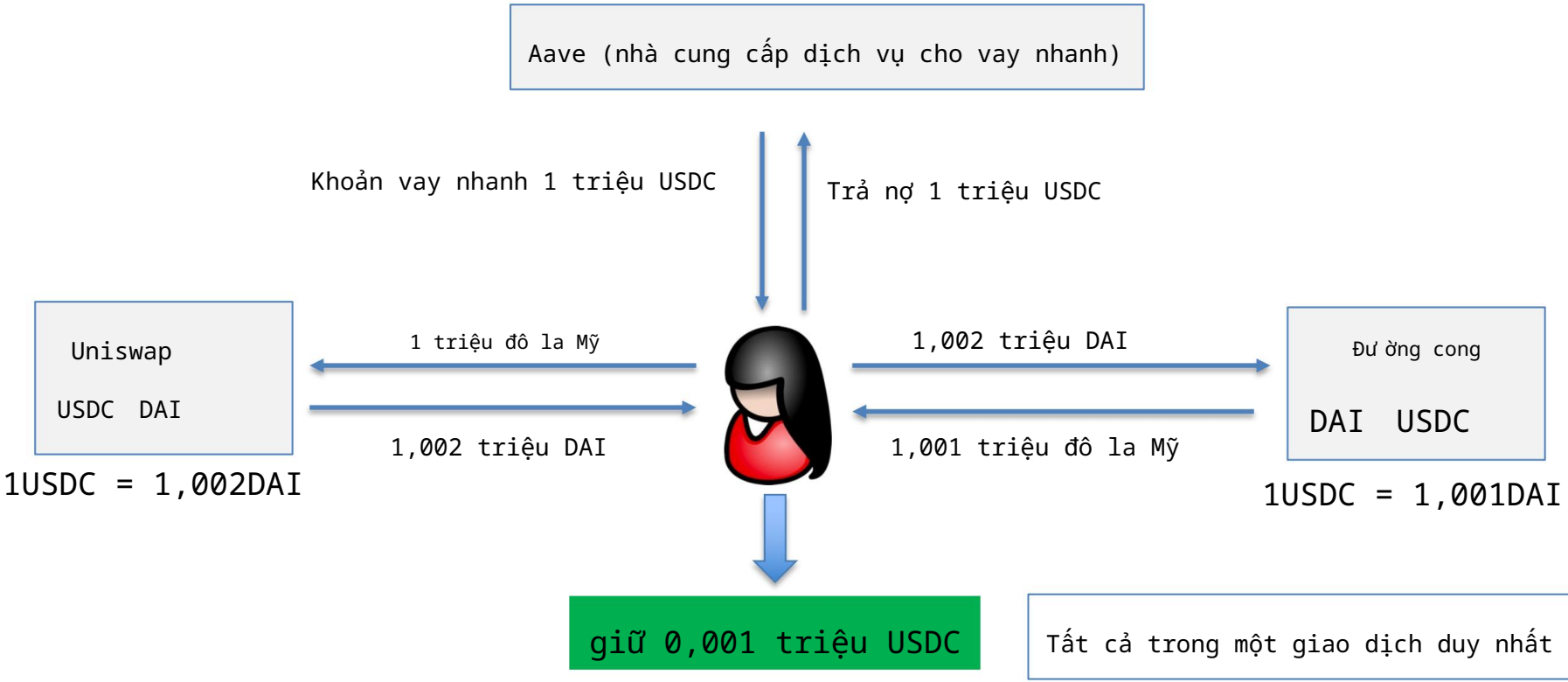
Các trư ờng hợp sử dụng

- Trọng tài không rủi ro
- Hoán đổi tài sản thế chấp
- Các cuộc tấn công DeFi: thao túng giá oracle

Machine Translated by Google

Trọng tài không rủi ro

Alice tìm thấy sự chênh lệch giá USDC/DAI trong hai nhóm



Machine Translated by Google

Hoán đổi thế chấp

bắt đầu:

Alice @Hợp chất

mục tiêu cuối cùng:

Alice @Hợp chất

-1000 DAI

+1 cETH

Vay khoản vay flash 1000 DAI

Trả nợ 1000 DAI (@Compund)

Đổi 1 cETH (từ Compound)

Đổi 1 cETH lấy 1500 cUSDC

Gửi 1500 cUSDC làm tài sản thế chấp

Vay 1000 DAI

Trả lại khoản vay flash 1000 DAI

-1000 DAI

+1500 đô la Mỹ

đã vay DAI bằng cách sử dụng

ETH làm tài sản thế chấp

(một giao dịch Ethereum duy nhất)

mư ợn DAI sử dụng

USDC làm tài sản thế chấp

Machine Translated by Google

Triển khai Aave v1

```
hàm flashLoan(địa chỉ _receiver, uint256 _amount) {
   .
   // chuyển tiền cho ngư ời nhận
   core.transferToUser(_reserve, userPayable, _amount);

   // thực hiện hành động của bộ
   thu receiver.executeOperation(_reserve, _amount, amountFee, _params);
   .
   // hủy bỏ nếu khoản vay không
   đư ợc trả lại require( availableLiquidityAfter == availableLiquidityBefore.add(amountFee),
        "cân bằng không nhất quán");
}
```

Machine Translated by Google

Số tiền vay nhanh trên Aave (năm 2021)

Top 5 Days - Loan Amount

Date	FALSHLOAN_USD
May 22	624.5M
May 5	520.9M
May 21	515.0M
May 19	265.7M
Aug 3	163.7M

Machine Translated by Google

Sàn giao dịch phi tập trung

(Khéo léo)

Machine Translated by Google

Trao đổi là gì?

Nhiều loại token ERC-20 trên Ethereum: • WETH: ETH đư ợc đóng gói dư ới dạng ERC-20, • USDC, USDT, DAI: Đồng tiền ổn định USD • Token quản trị (ví dụ: GTC cho Gitcoin), • Token chơ i game

stETH: ETH đã đư ợc đặt cọc

•

Một sàn giao dịch: đư ợc sử dụng để chuyển đổi một mã thông báo này sang mã thông báo khác (ví dụ: USDC GTC) • Tỷ giá hối đoái là bao nhiêu? • Làm thế nào để kết nối ngư ời bán và ngư ời mua?

Machine Translated by Google

Cách tiếp cận đầu tiên: một sàn giao dịch tập trung (CeX)

Tôi muốn đổi 2 ETH lấy USDC

Tỷ giá hối đoái: 1600 USDC/ETH

Ok. Gửi 2 ETH để trao đổi

Gửi 3200 USDC cho Bob

X-X

5ETH

1000: ETH
10000: USDC
10: GTC

Kho bạc

Machine Translated by Google

Cách tiếp cận đầu tiên: một sàn giao dịch tập trung (CeX)

Tôi muốn đổi 2 ETH lấy USDC

Tỷ giá hối đoái: 1600 USDC/ETH

Ok. Gửi 2 ETH để trao đổi

Gửi 3200 USDC cho Bob

X-X

3: ĐẠI HỌC

1600: USDC

1002: ETH

6800: USDC

10: GTC

Kho bạc

Machine Translated by Google

Cách tiếp cận đầu tiên: một sàn giao dịch tập trung (CeX)

Nhiều loại lệnh

Ví dụ: Lệnh giới hạn:

Tôi sẵn sàng mua

1 ETH cho tối đa 1700 USDC

[trong vòng 24 giờ tới]

X-X

Sàn giao dịch có thể "hoàn thành" lệnh hoặc không.

Danh sách các lệnh mua/bán như vậy được gọi là sổ lệnh

Machine Translated by Google

Một số vấn đề .

Tỷ giá hối đoái đư ợc xác định như thế nào?

- Theo cung và cầu tại sàn giao dịch (không minh bạch) • Cạnh tranh với các sàn giao dịch khác (trải nghiệm ngư ời dùng kém)

Bảo mật: Điều gì sẽ xảy ra nếu exch. lấy 2 ETH của Bob như ng không bao giờ gửi USDC?

Kiểm duyệt: Điều gì sẽ xảy ra nếu sàn giao dịch từ chối làm ăn với Bob?

Machine Translated by Google

Một giải pháp đáng tin cậy hơ n: DeX

DEX là gì?

- một thị trư ờng nơ i các giao dịch diễn ra trực tiếp giữa những ngư ời tham gia, không có trung gian đáng tin cậy

Thuộc tính: •

Có thể lập trình: có thể đư ợc sử dụng như một dịch vụ bởi các hợp đồng khác

- Minh bạch: mã có sẵn để mọi ngư ời có thể xem
- Không cần xin phép: bất kỳ ai cũ ng có thể sử dụng
- Không giam giữ

Machine Translated by Google

Làm thế nào để xây dựng một DeX?

Ý tưởng đầu tiên: sổ lệnh trên chuỗi

- Nhà cung cấp thanh khoản đặt lệnh mua/bán trên chuỗi
- Người dùng điền chúng vào chuỗi

Vấn đề: gas không hiệu quả. • Các lệnh tốn gas: khi đặt, khi hoàn tất, khi hủy. • Việc khớp lệnh mua với lệnh bán tốn rất nhiều gas (nhưng hãy xem tại đây) • Có thể thực hiện trên các chuỗi có khí giá rẻ

Machine Translated by Google

Làm thế nào để xây dựng một DeX?

Ý tưởng tiếp theo: sổ lệnh ngoài chuỗi

- Nhà cung cấp thanh khoản ký lệnh mua/bán ngoài chuỗi
    - Đăng đơn hàng lên trang web tập trung
- Người dùng ký lệnh muốn thực hiện và gửi lệnh đó lên chuỗi.
- Ví dụ: 0x Protocol, OpenSea

Vấn đề: sổ lệnh không thể truy cập được vào hợp đồng (dAPP)

Machine Translated by Google

Làm thế nào để xây dựng một DeX?

Một ý tưởng rất thanh lịch: Nhà tạo lập thị trường tự động (AMM)

- Nhà cung cấp thanh khoản gửi tài sản vào một nhóm trên chuỗi
- Người dùng giao dịch với nhóm trên chuỗi
    - tỷ giá hối đoái được xác định theo thuật toán
- Ví dụ: Uniswap, Balancer, Bancor, .

Lợi ích: Tiết kiệm khí đốt, dễ dàng ký hợp đồng, dễ dàng khởi nghiệp

Hơn 90% khối lượng DeX trên Ethereum

Machine Translated by Google

Nhà tạo lập thị trư ờng tự động

Mục tiêu: Mọi ngư ời muốn trao đổi USDC WETH

ổn định

dễ bay hơ i

Nhà cung

cấp thanh khoản

USDC, WETH

USDC, WETH

(kiếm đư ợc lãi suất)

Uniswap

Nhóm USDC-WETH

(dAPP)

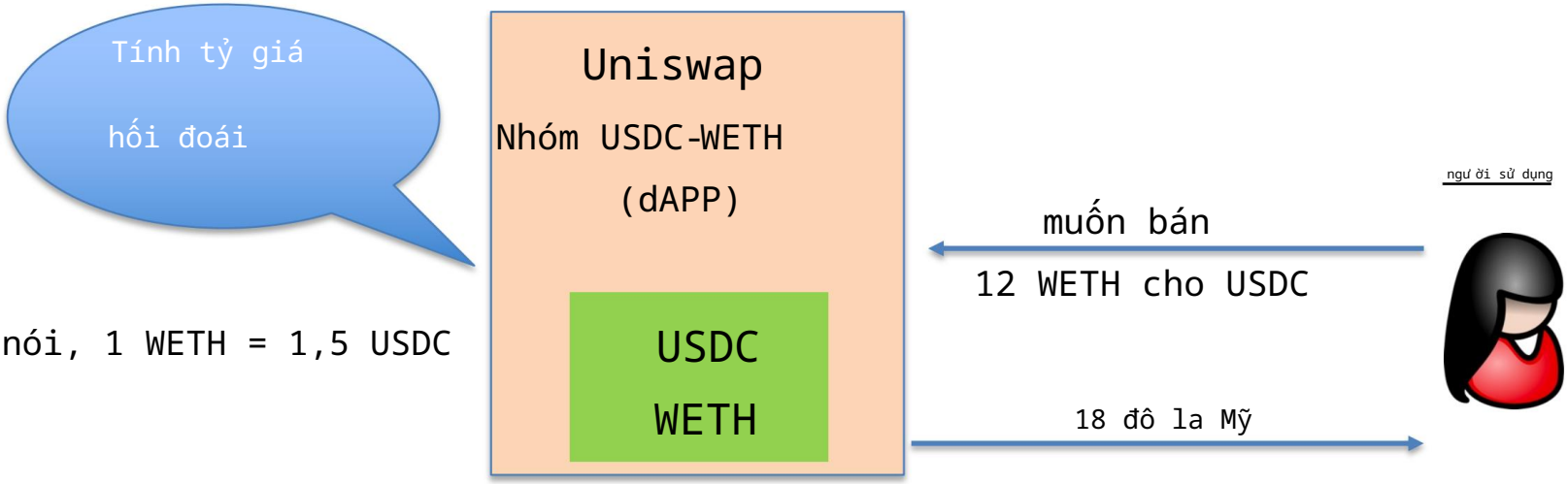
USDC

WETH

Machine Translated by Google

Nhà tạo lập thị trư ờng tự động

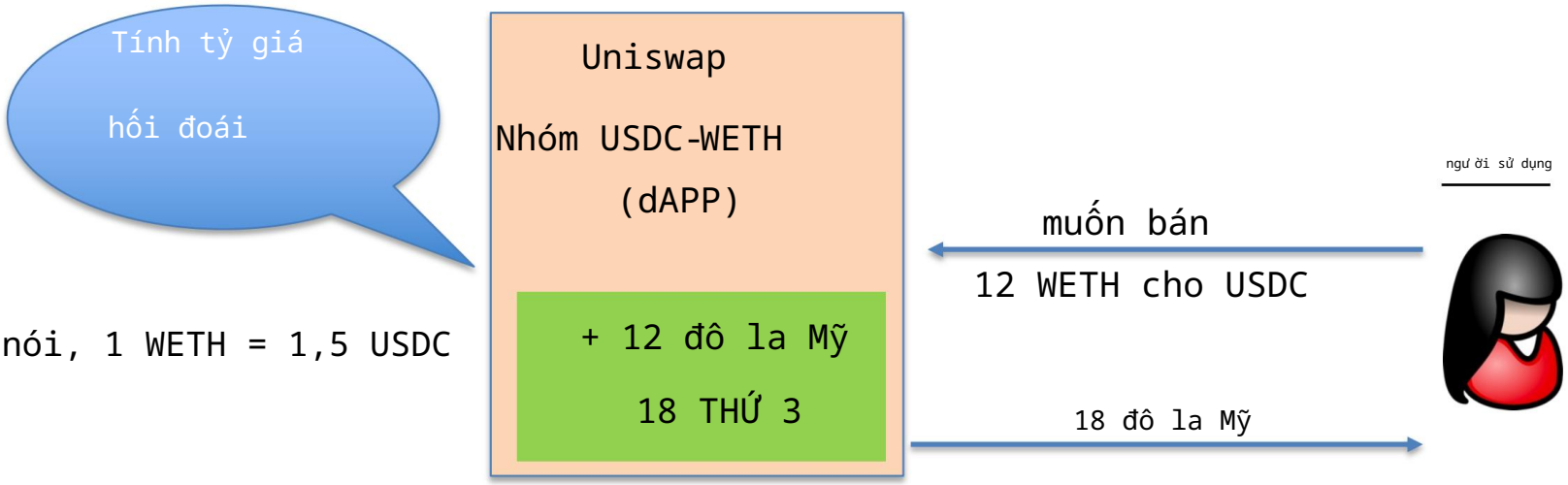
Mục tiêu: Mọi ngư ời muốn trao đổi USDC WETH



Machine Translated by Google

Nhà tạo lập thị trư ờng tự động

Mục tiêu: Mọi ngư ời muốn trao đổi USDC WETH



Machine Translated by Google

Làm thế nào để xác định tỷ giá hối đoái?

Bể có (x đơn vị của X) và (y đơn vị của Y)

Định nghĩa: giá cận biên.

Giả sử Alice gửi một lượng X (vô cùng nhỏ) vào nhóm;

và hồ bơi được gửi trở lại lượng Y.

(, sự thay đổi trong X là dương; , sự thay đổi trong Y là âm)

Sau đó giá biên được xác định là = / (>0)

Giá của một lượng nhỏ Y theo đơn vị X

Machine Translated by Google

Làm thế nào để xác định tỷ giá hối đoái?

Mục tiêu hợp lý mà nhóm cần duy trì:

(giá trị của X trong nhóm) = (giá trị của Y trong nhóm)

Chúng ta hãy sử dụng giá biên để ước tính giá trị tài sản trong nhóm:

• (giá trị của X trong nhóm) theo đơn vị của *

Y: • (giá trị của Y trong nhóm) theo đơn vị của Y:

Vì vậy, mục tiêu trên yêu cầu: * = = /

Cắm def vào sẽ cho kết quả:

$$\frac{!"}{!\#} = /$$

Machine Translated by Google

Làm thế nào để xác định tỷ giá hối đoái?

Phư ơ ng trình vi phân. $\frac{}{} = /$ có một giải pháp độc đáo:

$= \frac{+}{,}$, đối với hằng số $\mathbb{R}$ (

thực vậy:

$$\frac{"\#}{"\$} = \frac{\%}{\$!} = \frac{\&}{\$} * \frac{\%}{\$} = \frac{\#}{\$} \quad)$$

hoặc tư ơ ng đư ơ ng, nhóm phải duy trì: $* =$

. công thức tích hằng số nổi tiếng

Machine Translated by Google

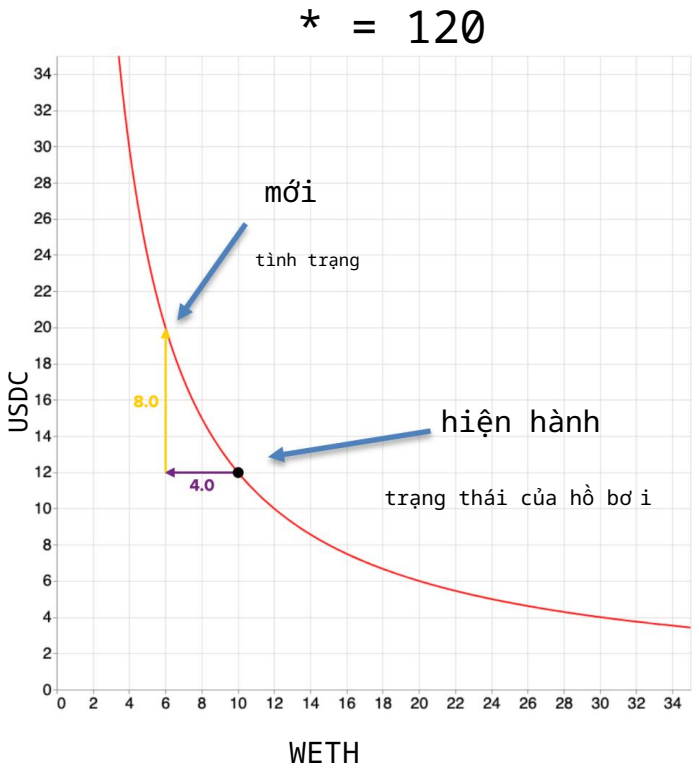
Vậy " = có nghĩa là gì ??

Nhà tạo lập thị trư ờng sản phẩm liên tục:

- Nói: = 10 WETH, = 12 USDC 10 × 12 = 120
- Alice muốn mua 4 WETH từ nhóm 4 = 6

Để duy trì = 120 Alice cần gửi 8

USDC vào nhóm + 8 = 20



Machine Translated by Google

Tổng quát hơn: Uniswap v2

* = ; Alice muốn mua (0,) từ nhóm.

Cô ấy nên trả bao nhiêu ?

( ) * (+) = =

$$\frac{\#' \ \$}{\$) \ \$}$$

(giải cho và đơn giản hóa)

Nhưng các nhà cung cấp thanh khoản (LP) lấy một khoản phí [0,1] (nói =0,97)

Alice trả : nhóm nhận được , LP nhận được (1)

vậy: ( ) * (+) = =

$$\frac{\&}{,} * \frac{\#' \ \$}{\$) \ \$}$$

Machine Translated by Google

Phương trình mua và bán

Selling x for y ( )

$$\Delta y = \frac{y\phi\Delta x}{x + \phi\Delta x}$$

```
41
42      // given an input amount of an asset and pair reserves, returns the maximum output amount of the other asset
43      function getAmountOut(uint amountIn, uint reserveIn, uint reserveOut) internal pure returns (uint amountOut) {
44          require(amountIn > 0, 'UniswapV2Library: INSUFFICIENT_INPUT_AMOUNT');
45          require(reserveIn > 0 && reserveOut > 0, 'UniswapV2Library: INSUFFICIENT_LIQUIDITY');
46          uint amountInWithFee = amountIn.mul(997);
47          uint numerator = amountInWithFee.mul(reserveOut);
48          uint denominator = reserveIn.mul(1000).add(amountInWithFee);
49          amountOut = numerator / denominator;
50      }
51
```

Buying x for y (+)

$$\Delta y = \frac{1}{\phi} \cdot \frac{y\Delta x}{x - \Delta x}$$

```
51
52      // given an output amount of an asset and pair reserves, returns a required input amount of the other asset
53      function getAmountIn(uint amountOut, uint reserveIn, uint reserveOut) internal pure returns (uint amountIn) {
54          require(amountOut > 0, 'UniswapV2Library: INSUFFICIENT_OUTPUT_AMOUNT');
55          require(reserveIn > 0 && reserveOut > 0, 'UniswapV2Library: INSUFFICIENT_LIQUIDITY');
56          uint numerator = reserveIn.mul(amountOut).mul(1000);
57          uint denominator = reserveOut.sub(amountOut).mul(997);
58          amountIn = (numerator / denominator).add(1);
59      }
60
```

UniswapV2Library.sol

tính toán hiệu quả sử dụng khí

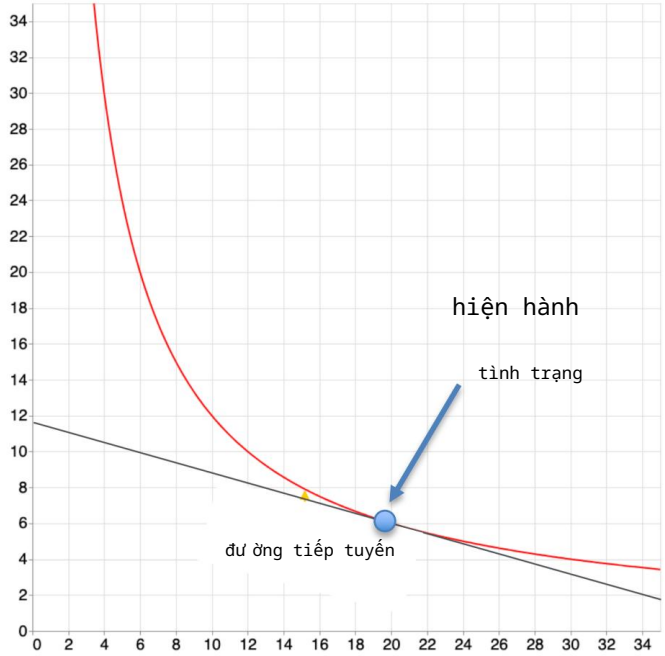
Machine Translated by Google

Giá cận biên như một tiếp tuyến

* = = /

Giá cận biên: = $\frac{"\#}{"\$} = \frac{\bullet}{/}$

là độ dốc của tiếp tuyến tại trạng thái hiện tại



Machine Translated by Google

Một tính năng: tự động phát hiện giá (giả sử =1)

Thm: giá biên / hội tụ về tỷ giá hối đoái thị trư ờng

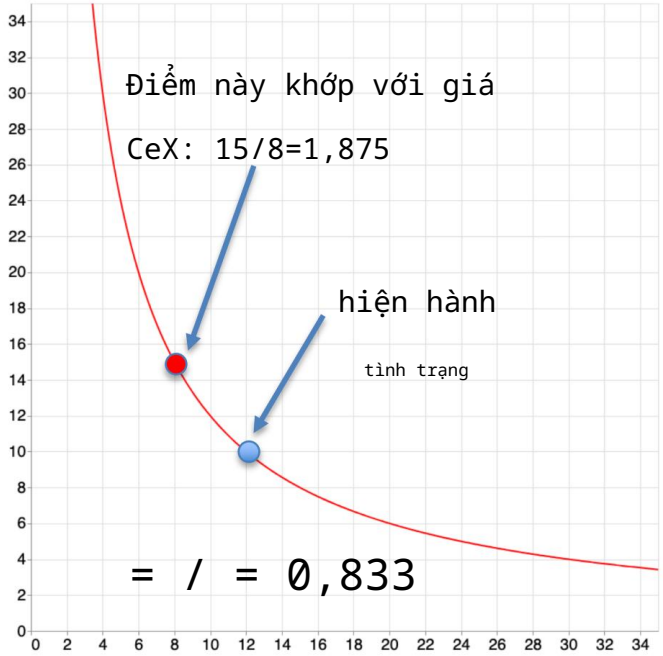
Chứng minh bằng ví dụ: giả sử, = 12, = 10

giá biên = / = 0,833

Giả sử một CeX cung cấp một mức giá khác =

012%34 1,875

cơ hội kiếm lời chênh lệch giá!

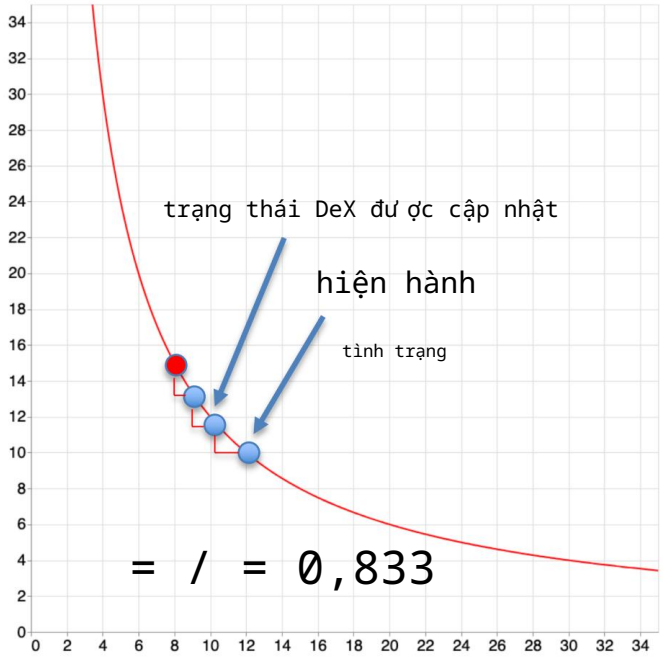


Machine Translated by Google

Một tính năng: tự động phát hiện giá (giả sử =1)

Thm: giá biên / hội tụ về tỷ giá hối đoái thị trư ờng

Ngư ời kinh doanh chênh lệch giá sẽ thực hiện: • mư ợn 1 token loại Y từ Compound • gửi 1 Y đến DeX, nhận lại 0,77 X token • gửi 0,77 X đến CeX, nhận 077×1,875 = 1,44 Y • trả lại 1 Y cho Compound, giữ lại 0,44 Y !!



Lặp lại cho đến khi giá biên DeX = giá CeX Arb. đang cung cấp dịch vụ và tạo ra lợi nhuận

Con số 0,44 Y đến từ đâu? Ai đã mất tiền?

Trả lời: LP đã mất. chúng ta sẽ xem tại sao

Machine Translated by Google

Một tính năng: tự động phát hiện giá (giả sử =1)

Thm: giá biên / hội tụ về tỷ giá hối đoái thị trư ờng

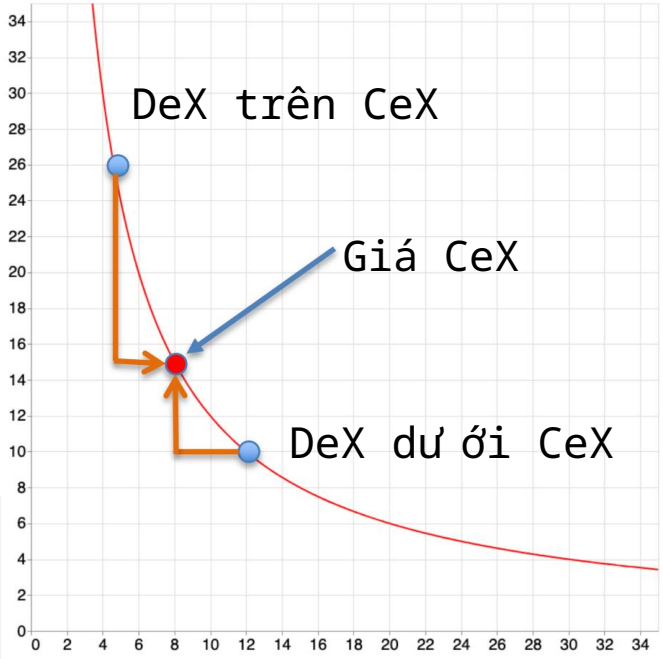
Tóm lại:

- Trạng thái DeX thấp hơ n giá thị trư ờng

  những ngư ời kinh doanh chênh lệch giá sẽ đư a DeX lên cao

- Trạng thái DeX cao hơ n giá thị trư ờng

  những ngư ời kinh doanh chênh lệch giá sẽ di chuyển DeX xuống



Giá biên của DeX khớp với giá thị trư ờng
mà không cần phải thông báo giá thị trư ờng!!

Machine Translated by Google

Vấn đề 1: Trư ợt

Trư ợt giá:

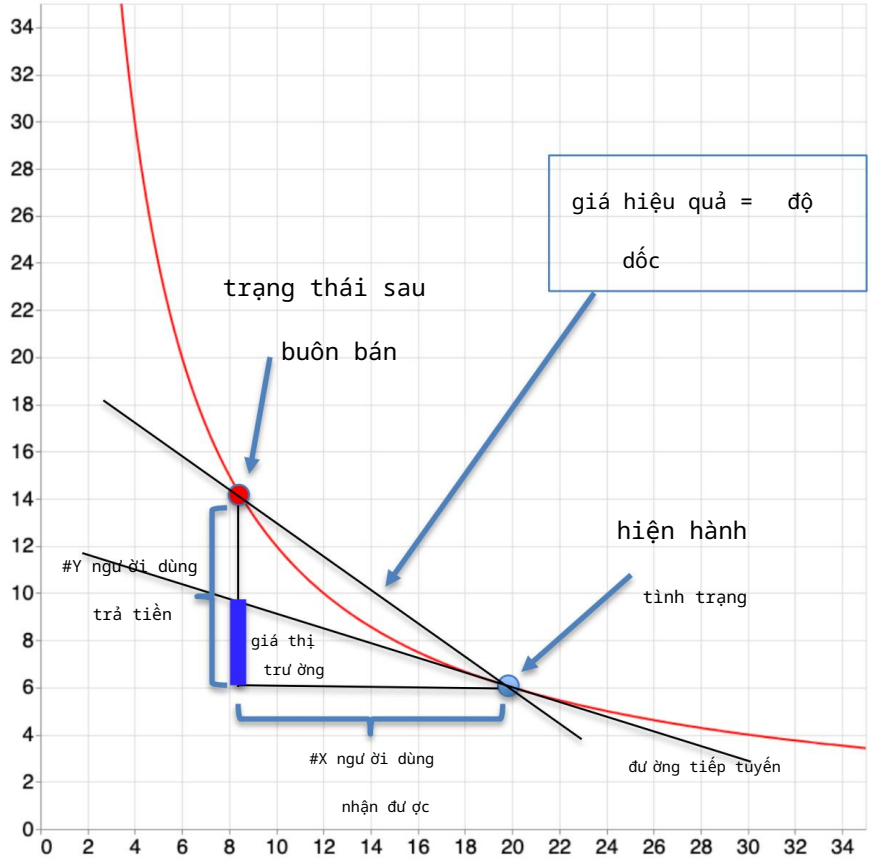
- giao dịch càng lớn, tỷ
  giá hối đoái càng bất lợi cho
  ngư ời dùng

giá thị trư ờng = độ dốc tang

Ngư ời dùng #Y phải trả = dòng màu xanh

. như ng ngư ời dùng phải trả nhiều hơ n

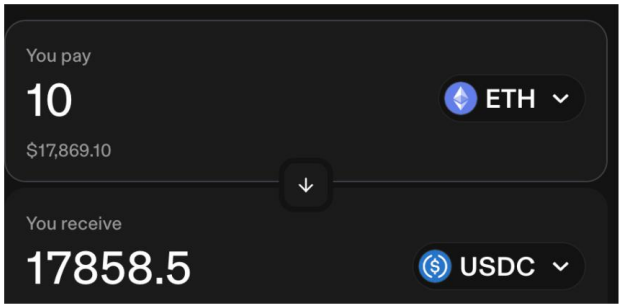
(trư ợt giới hạn uniswap ở mức 0,5%)

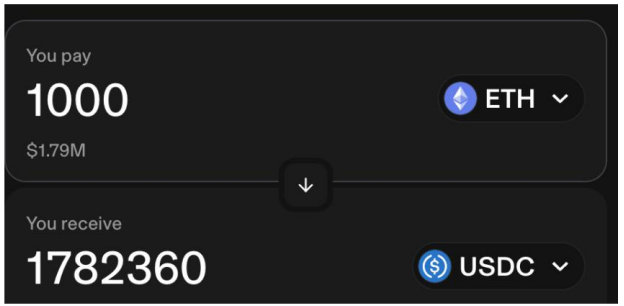


Machine Translated by Google

Trượt: một ví dụ

$$= \frac{*}{\quad\quad}$$





1785,5 USDC/ETH > 1782,36 USDC/ETH

Lưu ý: nếu = (Alice muốn mua toàn bộ nhóm) thì giá là ∞

Pool sẽ không bao giờ hết token X hoặc Y.

https://app.uniswap.org/swap

Machine Translated by Google

Vấn đề 2: Tấn công kiểu bánh sandwich

Hãy xem xét nhóm WETH-USDC :

• Ngư ời dùng Alice gửi một Tx để bán USDC vào nhóm. • Thông thư ờng, cô ấy nhận lại = /( ) WETH

Sam theo dõi mempool và thấy Tx của Alice.

Ông ta ngay lập tức nộp hai bản Tx của mình:

• Tx1: Sam bán 5 USDC cho nhóm, lấy lại WETH (tiền boa cao)

• Tx2: Sam bán WETH cho nhóm, lấy lại USDC (tiền boa thấp)

Machine Translated by Google

Vấn đề 2: Tấn công kiểu bánh sandwich

Bây giờ, Alice quay lại $' = \frac{(!"\#)\ \%}{(\%'()"\ \%} <$ WETH

cô ấy nhận được tỷ giá hối đoái tệ hơn vì Sam's Tx1

Dành cho Sam, > 5 vì vậy anh ấy đã làm (' 5) USDC ngoài Alice

Đây là một cuộc tấn công tiên phong:

- Cũng xảy ra ở các thị trường tài chính thông thường (xem flash boys).
- Chúng ta sẽ quay lại vấn đề này khi thảo luận về MEV.

Machine Translated by Google

Ưu đãi cho các nhà cung cấp thanh khoản

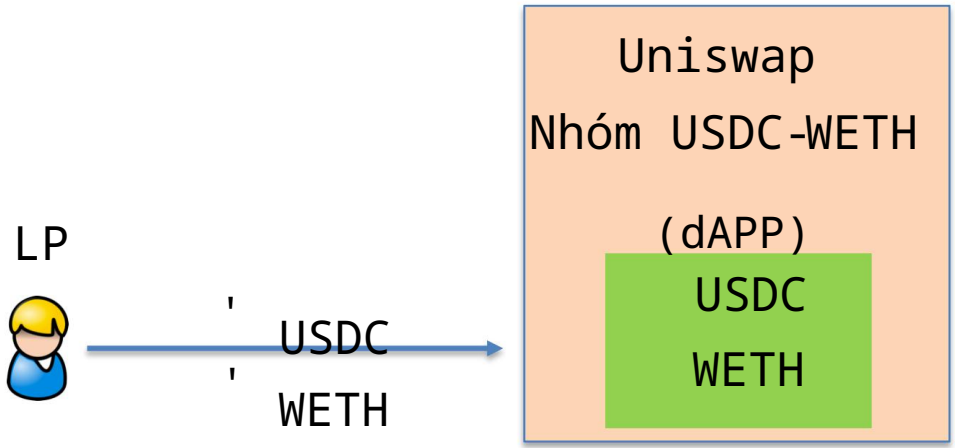
Machine Translated by Google

Nhắc lại: nhà cung cấp thanh khoản (LP)

Khi LP đóng góp vào nhóm: $\frac{>}{/}$ $\frac{>}{/}$ = /

không làm thay đổi giá biên của hồ bơi, cụ thể là $\frac{\#?\#"}{"\$?\$"} = \frac{\#}{\$}$

LP "sở hữu" $\frac{\$>}{"\$?\$"}$ của hồ bơi



Machine Translated by Google

Nhắc lại: nhà cung cấp thanh khoản (LP)

Khi LP đóng góp vào nhóm: ˃/ ˃ = /

không làm thay đổi giá biên của hồ bơi, cụ thể là #?#" = #
"$?$" $

LP "sở hữu" nhóm $˃
"$?$"

lưu ý: Đóng góp LP thay đổi hằng số:

(+ ˃)(˃) = ˃ token UNI mới

LP nhận được được đúc,

chỉ ra quyền sở hữu một phần của nhóm

LP

USDC

WETH

Uniswap

Nhóm USDC-WETH

(dAPP)

USDC

WETH

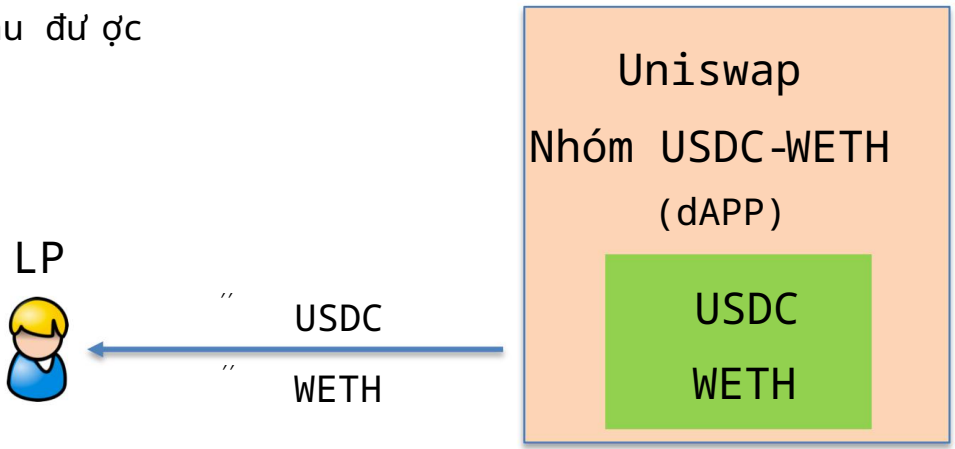
Machine Translated by Google

Rút LP

(,) là trạng thái hiện tại của nhóm. LP sở hữu một phần của nhóm.

Khi LP rút khỏi nhóm, họ sẽ nhận đư ợc:

- ('', '') của (USDC, WETH) trong đó ’’ / ’’ = / và ''/ = .
- LP cũ ng nhận đư ợc một phần nhỏ phí thu đư ợc



Machine Translated by Google

LP có nên đóng góp vào quỹ không?

Giả sử LP có (• ,) của (USDC, WETH).

LP có nên đóng góp chúng vào quỹ USDC-WETH không?

• Hay có một chiến lược có lợi nhuận cao hơn cho LP?

Chiến lược AMM:

đóng góp , ′) vào nhóm USDC-WETH tại thời điểm , @,

(rút lui (′′) từ nhóm tại thời điểm & > @.

Machine Translated by Google

Mất mát so với Giữ (mất mát phân kỳ)

Chiến lược GIỮ: LP giữ (* , *) của (USDC, WETH) giữa thời gian + Và ,.

Giả sử ( ) là giá thị trường của WETH/USDC tại thời điểm .

Thực tế: nếu (+) = (,) thì tại thời điểm ,, Giá trị danh mục đầu tư của LP là:

Chiến lược GIỮ: t, 3 ( ) * + ′ WETH.

Chiến lược AMM: t, 3 ( ) * + ′ + phí WETH.

Sự thật: Cho = (,)/ + (Tại thời ,, Giá trị danh mục đầu tư của LP:

điểm chiến lược GIỮ: t, ( ) * + ′ WETH.

lược AMM: [t, 3 trong đó ( ) * + ′] 3 (1) + phí WETH, chiến

(0) = 0 và ( ) tăng theo | |.

Thua lỗ so với Giữ

Machine Translated by Google

Mất mát so với Giữ (mất mát phân kỳ)

Chiến lược GIỮ: LP giữ (*, *) của (USDC, WETH) giữa thời gian $_{+}$ Và ,.

(1) Mất mát so với giữ tăng khi = (&) /(@) lệch khỏi 1.

giá thay đổi càng lớn thì tổn thất của LP càng lớn

(1) Chiến lược AMM so với GIỮ chỉ có ý nghĩa nếu phí > Lỗ so với Giữ.

xác định mức phí của nhóm cần thiết để thu hút thanh khoản

(3) Ai sẽ chịu tổn thất của LP? Người kinh doanh chênh lệch giá

Machine Translated by Google

Mất mát so với Tái cân bằng (LVR)

Chiến lược tái cân bằng:

- LP duy trì danh mục đầu tư của mình bên ngoài DeX
- LP thực hiện việc tái cân bằng danh mục đầu tư giống như DeX, nhưng thực hiện bằng cách giao dịch với CeX.

Một chiến lược dự đoán chính xác hơn về khoản lỗ của LP khi cung cấp thanh khoản cho DeX

xác định chính xác hơn mức phí cần thiết để thu hút thanh khoản

https://arxiv.org/pdf/2208.06046.pdf

Machine Translated by Google

Các chức năng khác

Machine Translated by Google

Nhà tạo lập thị trư ờng hàm hằng số (CFMM)

Hồ bơ i duy trì (,) = đối với một số hàm (*, *)

Ví dụ:

giá trị( ) = giá trị( )

- tích hằng số: (,) = *
- tích có trọng số không đổi: (,) = Đ# * Đ$
  - Duy trì danh mục đầu tư mất cân bằng val( )/val( ) = $/ #
- tổng hằng số: (,) = * + đối với một hằng số nào đó.
  - giá biên luôn là / = (không bao giờ thay đổi)
  - đư ợc sử dụng khi tỷ giá hối đoái X-Y không thay đổi

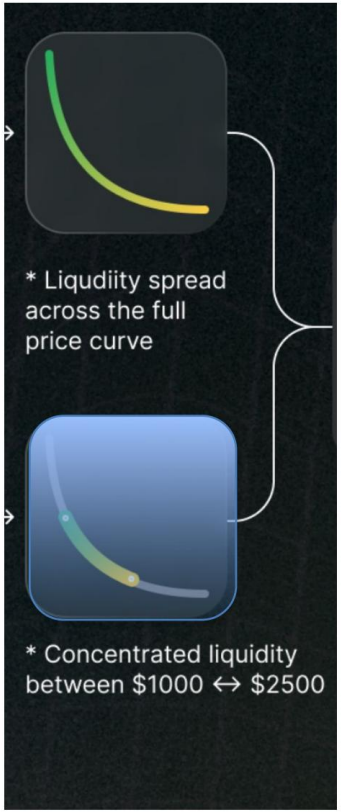
Machine Translated by Google

Uniswap v3: thanh khoản tập trung

Ở v2, tính thanh khoản của LP đư ợc sử dụng trên toàn bộ phạm vi giá.

Trong v3, LP có thể chỉ định phạm vi giá mà tính thanh khoản của họ sẽ đư ợc sử dụng

bảo vệ LP khỏi sự biến động giá. Kết quả là hồ bơ i sâu hơ n khi giá nằm trong phạm vi cho phép.



https://uniswap.org/whitepaper-v3.pdf

Machine Translated by Google

Uniswap v4: móc

Cho phép ngư ời tạo nhóm chỉ định các móc tại thời điểm tạo nhóm: •

mã thực thi tại các thời điểm nhất định trong quá trình

giao dịch: ví dụ, móc BeforeSwap, AfterSwap

Móc cho phép: (thêm ví dụ tại đây) • Phí

giao dịch động ( ) dựa trên trạng thái của nhóm • Lệnh

giới hạn (ví dụ: giá chấp nhận đư ợc trong 24 giờ tới) •

Chiến lư ợc định giá tinh vi hơ n (ví dụ: giá trung bình trong giờ qua)

https://blog.uniswap.org/uniswap-v4

Machine Translated by Google

Tóm tắt: AMM

- AMM đư ợc triển khai như một hợp đồng thông minh đơ n giản (dự án #4)
- Tự động phát hiện giá (không có oracle ngoài chuỗi)
- Không phụ thuộc vào điểm kiểm soát trung tâm
- Có thể kết hợp hoàn toàn với các dAPP khác

Machine Translated by Google

KẾT THÚC BÀI GIẢNG

Bài giảng tiếp theo: MEV