CS251 Mùa thu năm 2023

(cs251.stanford.edu)

Stablecoin và giao thức cho vay

Dan Boneh

Tóm tắt: Sự vững chắc

Mọi thứ đều là hợp đồng:

• Hợp đồng quản lý các biến trạng thái

• Hợp đồng có các hàm có thể được gọi bên ngoài • Có thể kế thừa mã từ các hợp đồng khác (hợp đồng A là B,C) • Các loại hợp đồng: hợp đồng, giao diện, trừu tượng, thư viện

Đối tượng toàn cục: block, msg, tx

Ví dụ: Mã thông báo ERC20

- https://github.com/ethereum/EIPs/blob/master/EIPS/eip-20.md

- Một API chuẩn cho các mã thông báo có thể thay thế. (ERC-721 dành cho các mã thông báo không thể thay thế)

- Mã thông báo ERC20 tự nó là một hợp đồng thông minh duy trì tất cả số dư của người dùng:

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

- Một giao diện chuẩn cho phép các hợp đồng khác tương tác với

  mọi token ERC20. Không cần logic đặc biệt cho từng token.

Giao diện mã thông báo ERC20

```
hàm chuyển (địa chỉ _đến, giá trị _uint256) trả về bên ngoài (bool);

hàm transferFrom(địa chỉ _from, địa chỉ _to, giá trị uint256) trả về bên ngoài (bool);

hàm approve(địa chỉ _spender, uint256 _value) trả về bên ngoài (bool);


hàm totalSupply() chế độ xem bên ngoài trả về (uint256);

hàm balanceOf(địa chỉ _owner) chế độ xem bên ngoài trả về (uint256);

hàm allowance(địa chỉ _owner, địa chỉ _spender) trả về chế độ xem bên ngoài (uint256);
```

Một ví dụ .

Hãy xem xét hai mã thông báo ERC-20: chẳng hạn như USDC và WETH

• USDC là hợp đồng duy trì ánh xạ _balances[] • WETH là hợp đồng khác cũ ng duy trì _balances[]

Giả sử Bob sở hữu 5 USDC và 2 WETH. Điều này được ghi lại như sau:

Trong hợp đồng USDC: _balances[Địa chỉ của Bob] == 5

Trong hợp đồng WETH: _balances[Địa chỉ của Bob] == 2

Phần mềm ví hiển thị tất cả các đồng tiền liên quan đến địa chỉ của Bob

Bất kỳ ai cũng có thể đọc ERC20 _balances[]

Mã băm giao dịch: 0x6b85ca95e484d94503d1276456bfc32cc55f6fdb8bb231ff83..

Yêu cầu hợp đồng USDC chuyển 10.010,00 USDC từ tài khoản Circle
tới 0x7656159E42209A95b77aD374d.

Storage Address: 0x4d3e7741e6c98c0c469419fcfe58fa7ec622d7b26345802d22d17415768760f8

Before: Hex → 0x0000000000000000000000000000000000000000000000000000000000000000

After: Hex → 0x0000000000000000000000000000000000000000000000000000002540be400

mục nhập của người nhận

Storage Address: 0x57d18af793d7300c4ba46d192ec7aa095070dde6c52c687c6d0d92fb8532b305

Before: Hex → 0x000000000000000000000000000000000000000000000000000266988cda8061

After: Hex → 0x0000000000000000000000000000000000000000000000002669638ce9c61

Vòng tròn lối vào

(Số dư của vòng tròn sau)

(etherscan.io)

Gọi các hợp đồng khác

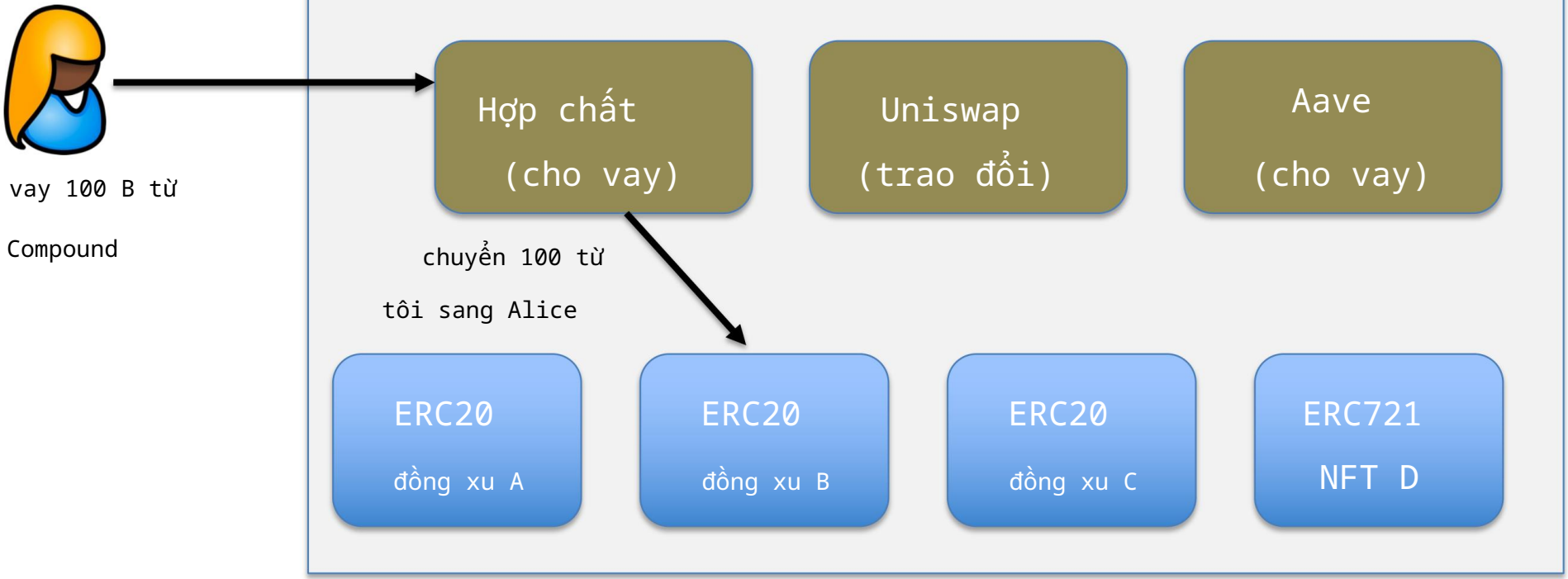
Địa chỉ có thể được chuyển thành loại hợp đồng.

```
địa chỉ _usdc = 0x7656159E42209A95b77aD374d.;
ERC20Token usdcContract = ERC20Token(_usdc);
```

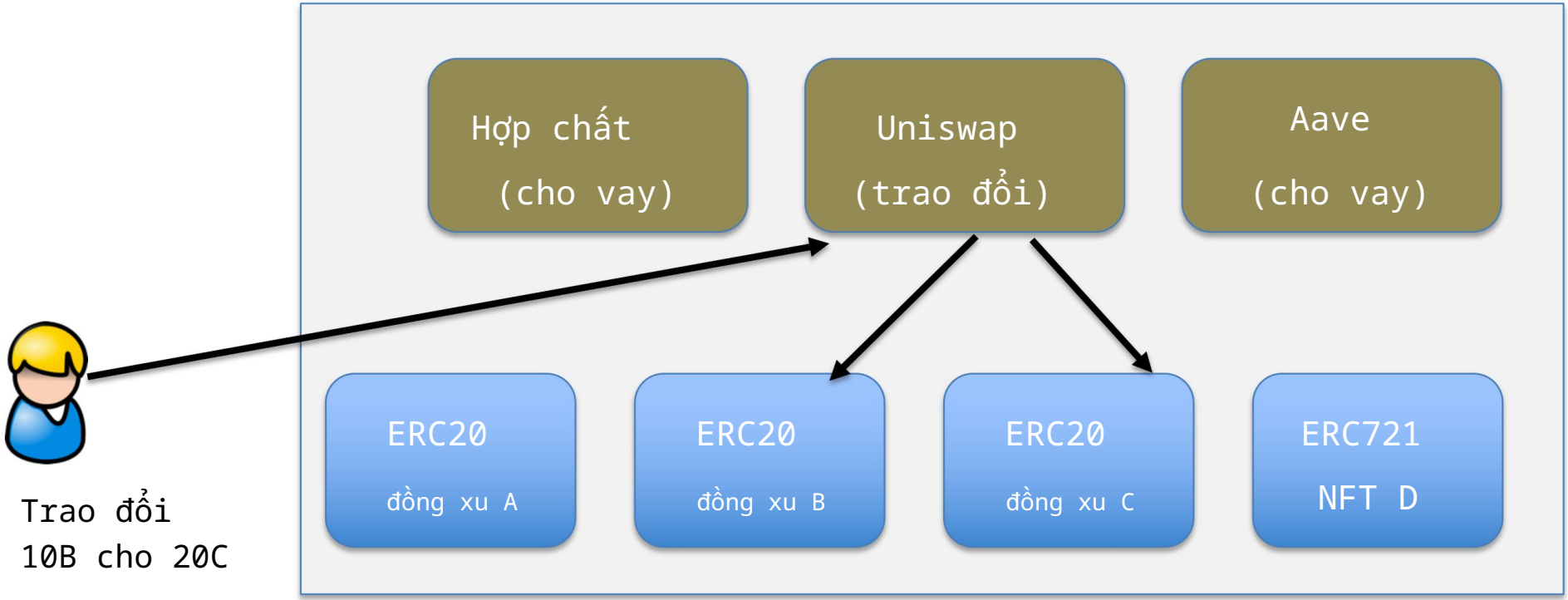
Để gọi hàm “chuyển” của hợp đồng tại địa chỉ _usdc:

```
usdcContract.chuyển nhượng(_đến, _giá trị);
```

Thế giới DeFi



Thế giới DeFi



Ứng dụng DeFi số 1: Stablecoin

Tiền xu ổn định

Một loại tiền điện tử được thiết kế để giao dịch ở mức giá cố định

- Ví dụ: 1 xu = 1 USD, 1 xu = 1 EUR, 1 xu = 1 USDX

Mục tiêu:

- Tích hợp các loại tiền tệ thực tế vào các ứng dụng trên chuỗi

- Cho phép những người không dễ dàng tiếp cận USD nắm giữ và giao dịch tài sản tương đương USD

Các loại tiền ổn định

	tập trung	thuật toán
được thế chấp	giám hộ đồng tiền ổn định (Tiền USD)	tổng hợp (DAI, RAI)
Có thế chấp	tiền tệ của ngân hàng trung ương (kỹ thuật số)	Stablecoin không có thế chấp

Tiền ổn định lưu ký: đúc tiền

100 đô la Mỹ

35 đô la Mỹ

Người bảo vệ

triển khai hợp đồng ERC-20

bạc hà (Bob, 100)

bạc hà (Alice, 35)

tình trạng

Bob: 100

Alice: 35

_cân bằng

100 đô la Mỹ

\+ 35 đô la Mỹ

Tiền ổn định lưu ký: chuyển khoản

trả cho Carol 15$:

chuyển nhượng (Bob Carol, 15)

(và phí xăng)

Việc chuyển tiền được thực hiện trên chuỗi (bên giám sát không tham gia)

135 đô la Mỹ

Bob: 80

Alice: 35

Hát mừng: 15

_cân bằng

Tiền ổn định lưu ký: rút tiền

rút 60 USD

60 đô la Mỹ

đốt cháy (Bob, 60)

Người bảo vệ

1375 đô la Mỹ

Bob: 85

Alice: 35

Hát mừng: 15

_cân bằng

Hai ví dụ

	Tiền xu phát hành	khối lượng 24h
USDC	25,3 tỷ	4,6B
USDT	83,7 tỷ	20,8 tỷ

Một số vấn đề

Người lưu ký giữ kho bạc trong một ngân hàng truyền thống

• Phải được kiểm toán để đảm bảo kho bạc có sẵn • Kiếm lãi từ tiền gửi

Người giám hộ có quyền hạn mạnh mẽ: •

Có thể đóng băng tài khoản / từ chối yêu cầu rút tiền • Người giám hộ có thể rút tiền khỏi số dư của người dùng

Stablecoin phi tập trung được thế chấp

Mục tiêu: một đồng tiền ổn định không có bên nào đáng tin cậy

Ví dụ: DAI, RAI và các ví dụ khác.

Không được sử dụng rộng rãi như stablecoin tập trung

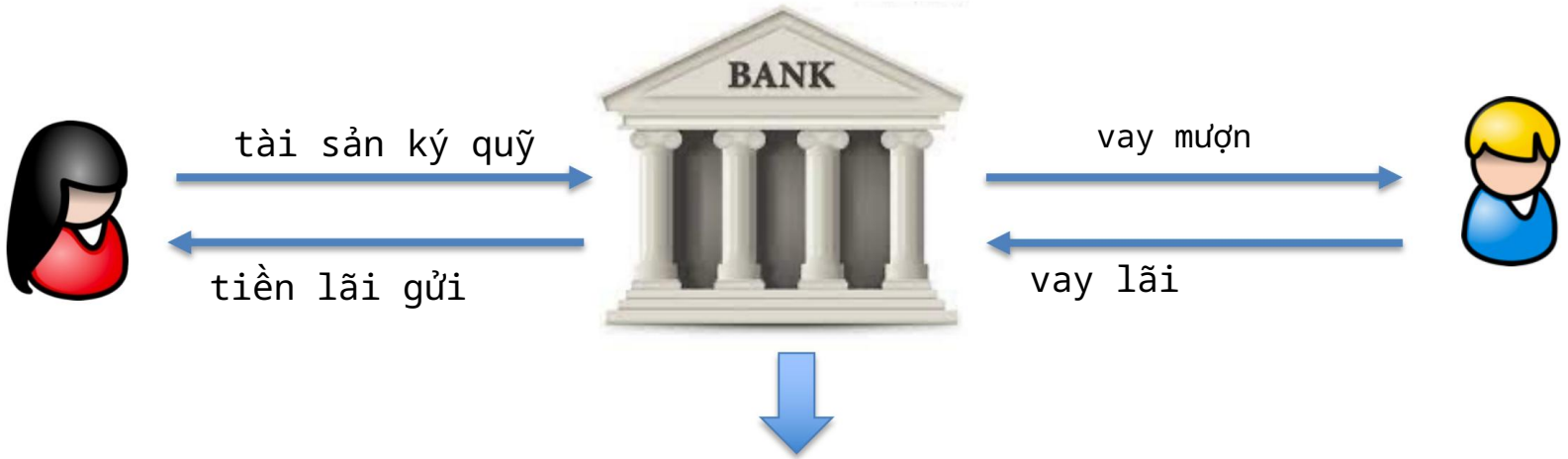
Ứng dụng DeFi số 2: Giao thức cho vay

Mục tiêu: giải thích cách thức hoạt động của cho vay phi tập trung

Đây không phải là lời khuyên về đầu tư hoặc tài chính

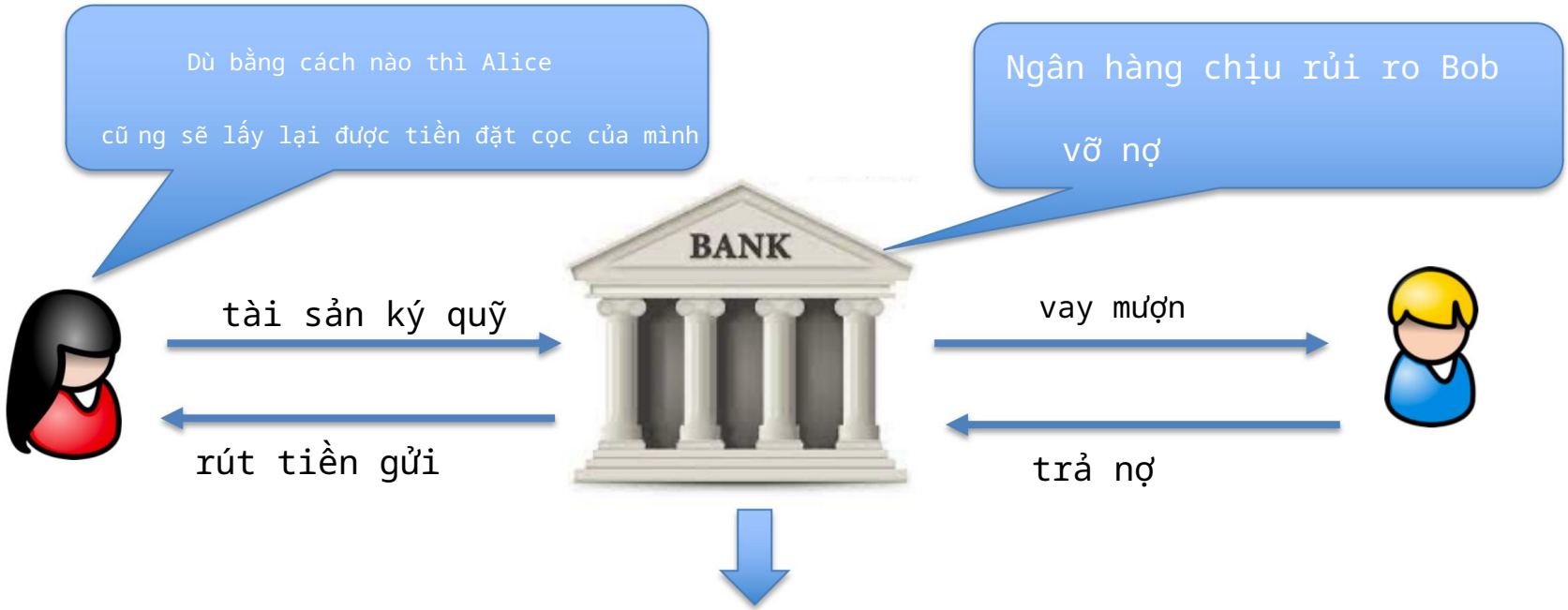
Vai trò của ngân hàng trong nền kinh tế

Ngân hàng tập hợp người cho vay và người đi vay



(lãi vay - lãi gửi)

Vai trò của ngân hàng trong nền kinh tế



chênh lệch ngân hàng

(lãi vay - lãi gửi)

Tiền điện tử: Cho vay CeFi (ví dụ: Blockfi, Nexo, .)

Giống như ngân hàng truyền thống:

Alice đưa tài sản của mình cho tổ chức CeFi để cho Bob vay

Vai trò của tài sản thế chấp

(1 ETH = 100 UNI)

Mối quan ngại của CeFi: Điều gì sẽ xảy ra nếu Bob vỡ nợ?

CeFi sẽ hấp thụ khoản lỗ

Giải pháp: yêu cầu Bob khóa tài sản thế chấp

thế chấp

gửi 500 UNI

Vay 1 ETH

lãi suất khấu trừ từ tài sản thế chấp

cho vay thế chấp

tình hình nợ:

+ 500 ĐÔ LA MỸ

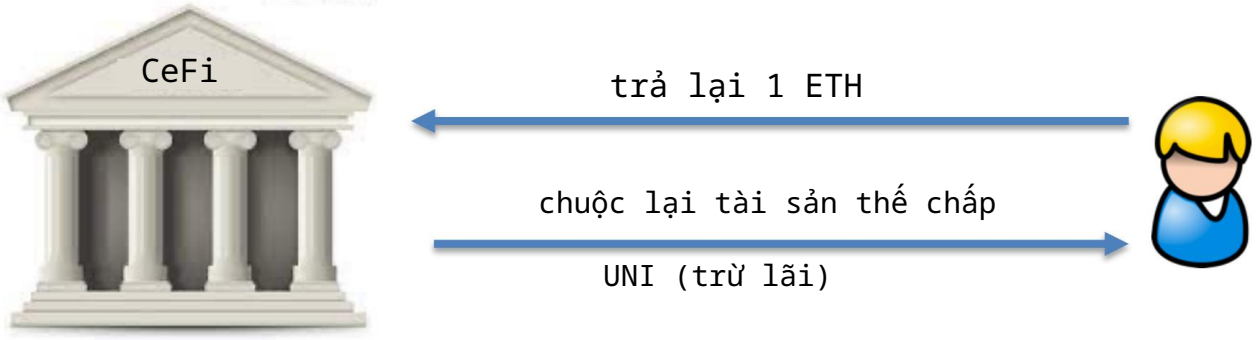
1ETH

Vai trò của tài sản thế chấp

(1 ETH = 100 UNI)

Một số điều có thể xảy ra tiếp theo:

(1) Bob trả nợ



tình hình nợ:

+ 500 ĐÔ LA MỸ

1ETH

Vai trò của tài sản thế chấp

(1 ETH = 100 UNI)

Một số điều có thể xảy ra tiếp theo:

(1) Bob trả nợ

(2) Bob vỡ nợ

Được thôi, tôi sẽ

giữ lại (100 + hình phạt) UNI

Tôi không thể trả lại 1 ETH

chuộc lại số tiền thế chấp UNI còn

lại (400 lãi suất tiền phạt) UNI

tình hình nợ:

+ 500 Đ LA

1ET

Vai trò của tài sản thế chấp

(1 ETH = 400 UNI)

Một số điều có thể xảy ra tiếp theo:

(1) Bob trả nợ

(2) Bob vỡ nợ

(3) Thanh lý: giá trị khoản vay tăng lên so với tài sản thế chấp

Tôi cần thanh lý tài sản thế chấp của bạn (và tính phí phạt = 20 UNI)

tình hình nợ:

+ 500 ĐÔ LA MỸ

0ETH

người cho vay cần thanh lý trước giá trị (nợ) > giá trị (tài sản thế chấp)

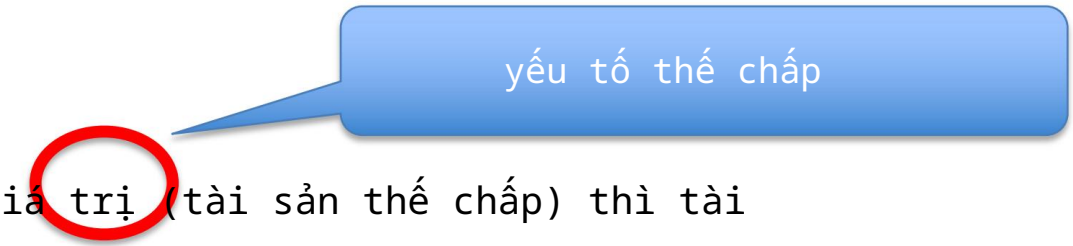
Thuật ngữ

Tài sản thế chấp: tài sản dùng làm tiền đặt cọc

Thế chấp quá mức: người vay phải cung cấp

giá trị(thế chấp) > giá trị(vay)

Thiếu thế chấp: giá trị (thế chấp) < giá trị (vay)



Thanh lý: nếu

giá trị (nợ) > 0,6 × giá trị (tài sản thế chấp) thì tài sản thế chấp sẽ được thanh lý cho đến khi bất bình đẳng đảo ngược

(thanh lý làm giảm cả hai vế của bất đẳng thức)

Yếu tố thế chấp

Hệ số thế chấp [0,1]

- Giá trị tối đa có thể được vay bằng tài sản thế chấp này

- Tài sản có tính biến động cao hệ số thế chấp thấp
- Tài sản tương đối ổn định hệ số thế chấp cao hơn

Ví dụ: (trên Compound)

ETH, DAI: 83%, ĐẠI HỌC: 75%, MKR: 73%

Sức khỏe của một vị thế nợ

Khả năng vay = Giá trị X (tài sản thế chấp) Yếu tố tài sản thế chấp

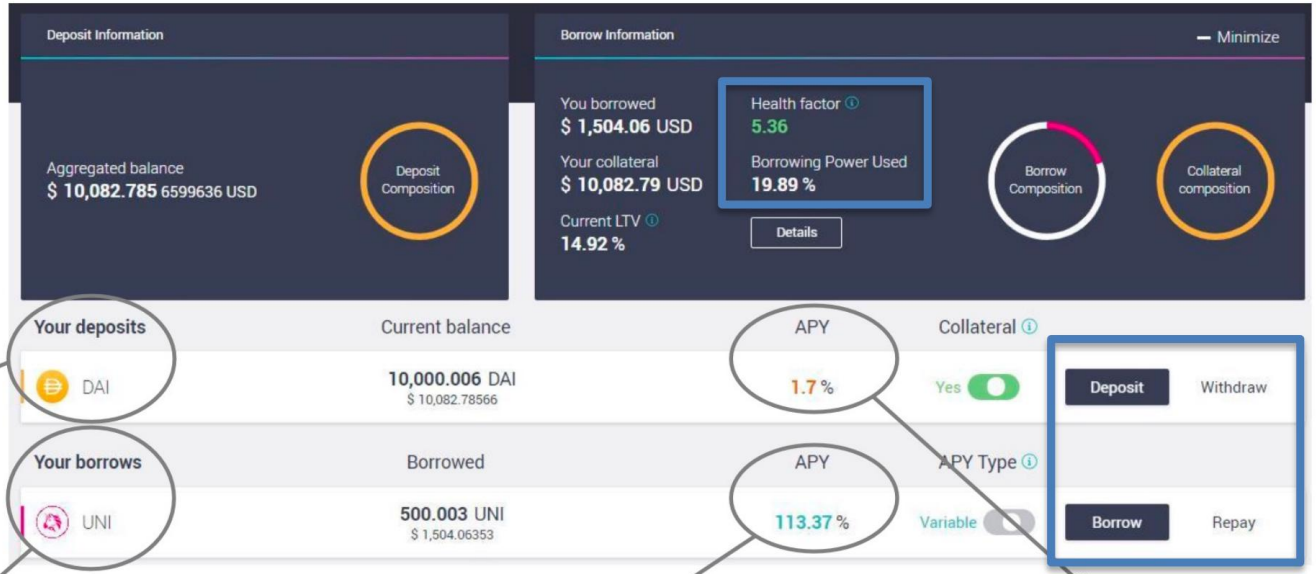
(bằng ETH)

Tôi

$$= \text{giá trị} \quad \frac{\text{Sức khỏe khả năng vay}}{\text{(Tổng nợ)}}$$

helath < 1 kích hoạt thanh lý cho đến khi (health ≥ 1)

Ví dụ: Bảng điều khiển Aave (một Dapp cho vay DeFi)



DAI is deposited as collateral

UNI is borrowed

The borrowing interests the borrower needs to pay

In Aave, the collteral is also lent out. Hence the borrower can also earn interests.

hành động

Tín dụng: Arthur Gervais

Tại sao lại vay ETH?

Nếu Bob có tài sản thế chấp, tại sao anh ta không thể mua ETH?

- Bob có thể cần ETH (ví dụ, để mua tài sản trong trò chơi),
  nhưng anh ta có thể không muốn bán tài sản thế chấp của mình (ví dụ: NFT)

- Là một chiến lược đầu tư: sử dụng UNI để vay ETH
  cho Bob tiếp xúc với cả hai

Vấn đề với việc cho vay CeFi

Người dùng phải tin tưởng vào tổ chức CeFi:

- Không bị hack, đánh cắp tài sản hoặc tính toán sai
- Đây là lý do tại sao tài chính truyền thống được quản lý

- Các khoản thanh toán lãi suất được chuyển đến sàn giao dịch, không phải nhà cung cấp thanh khoản Alice

- CeFi kiểm soát hoàn toàn chênh lệch (lãi vay – lãi tiền gửi)

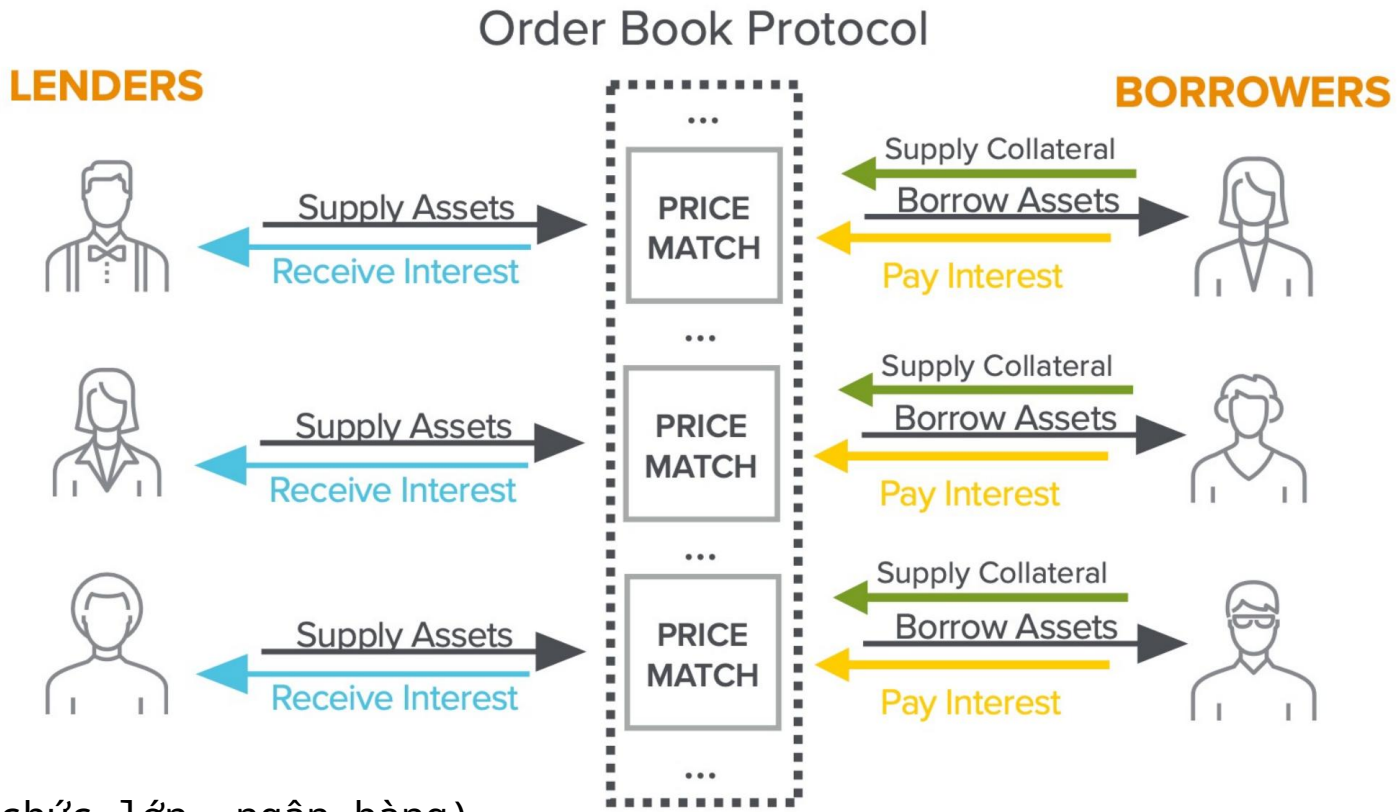
Cho vay DeFi

Chúng ta có thể xây dựng một Dapp cho vay trên chuỗi không?

không có bên trung tâm đáng tin cậy

mã có sẵn trên Ethereum để kiểm tra

Ý tưởng đầu tiên: một Dapp sổ lệnh



(các tổ chức lớn, ngân hàng)

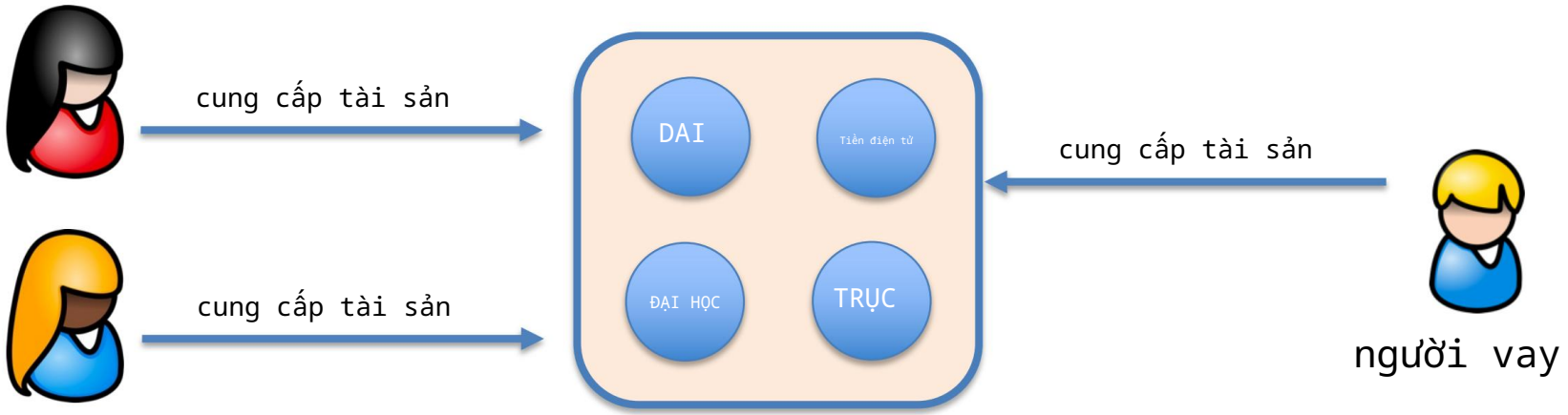
Tín dụng: Eddy Lazzarin

Thách thức

- Tốn kém về mặt tính toán: việc kết nối người vay với người cho vay đòi hỏi nhiều giao dịch cho mỗi người (đăng giá thầu, rút lại nếu thị trường thay đổi, lặp lại)
- Rủi ro tập trung: người cho vay phải chịu rủi ro vỡ nợ từ đối tác trực tiếp của họ
- Rút tiền phức tạp: người cho vay phải đợi các bên đối tác trả nợ của họ

Một cách tiếp cận tốt hơn: nhóm thanh khoản

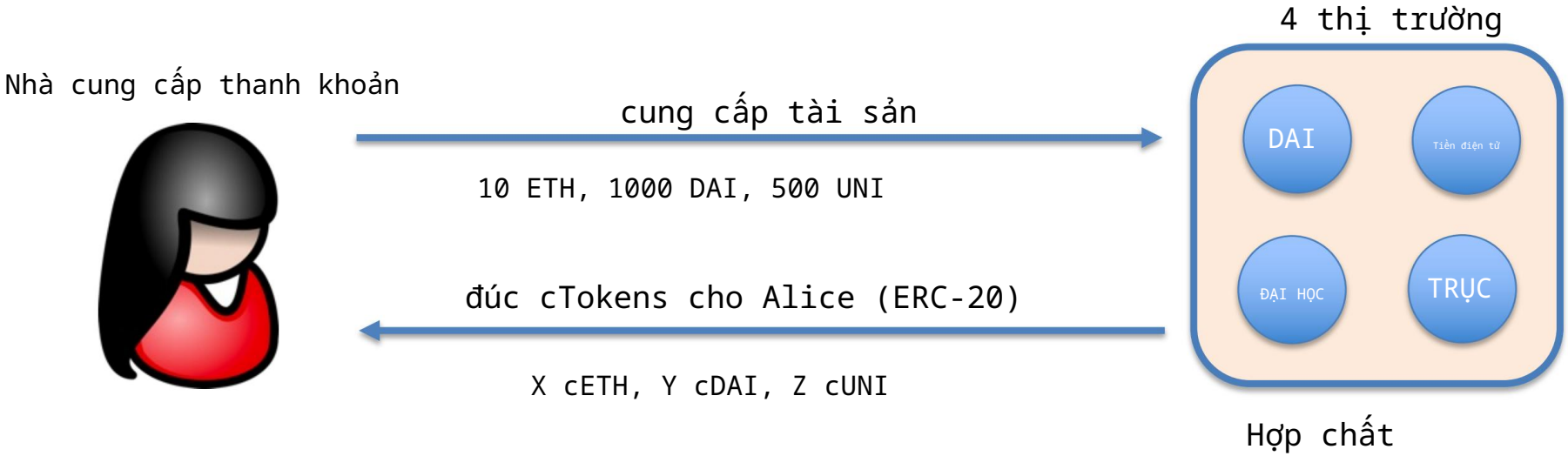
Cho vay thế chấp quá mức: Compound và Aave



Nhà cung cấp thanh khoản (kiếm lãi)

Dapps Compound/Aave thu thập thanh khoản

Ví dụ: Hợp chất cTokens

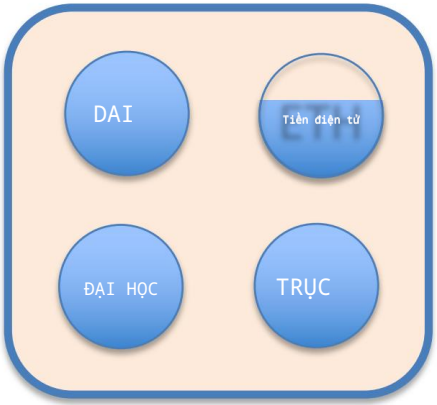


Giá trị của X, Y, Z được xác định bởi tỷ giá hối đoái hiện tại:

Tỷ giá trao đổi Token sang cToken được tính toán sau mỗi khối

Người vay

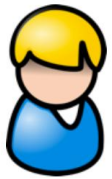
4 thị trường



Hợp chất

cung cấp tài sản cho bất kỳ thị trường nào

nhận cTokens



Tôi muốn vay ETH

cToken của Bob bị khóa làm tài sản thế chấp

Compound gửi ETH cho Bob

Lãi suất tích lũy của Bob làm tăng tỷ giá hối đoái ETH/cETH

lợi ích cho người nắm giữ token cETH (nhà cung cấp thanh khoản ETH)

Tỷ giá hối đoái

Hãy xem xét thị trường ETH:

Cung cấp ETH: thêm vào UnderlyingBalanceETH

Vay ETH: được thêm vào totalBorrowBalanceETH

Quan tâm: thêm nhiều lần vào totalBorrowBalanceETH

$$\text{Tỷ giá hối đoái}_{ETH/cETH} = \frac{\text{Số dư cơ sở}_{ETH} + \text{tổng số dư vay}_{ETH} - \text{dự trữ}_{ETH}}{\text{cTokenSupply}_{ETH}}$$

Khi totalBorrowBalance tăng thì ExchangeRate cũ ng tăng

Lãi suất: liên tục cập nhật

Ý tưởng chính: được xác định bởi nhu cầu về tài sản so với quy mô thị trường tài sản

Tỷ lệ sử dụng:

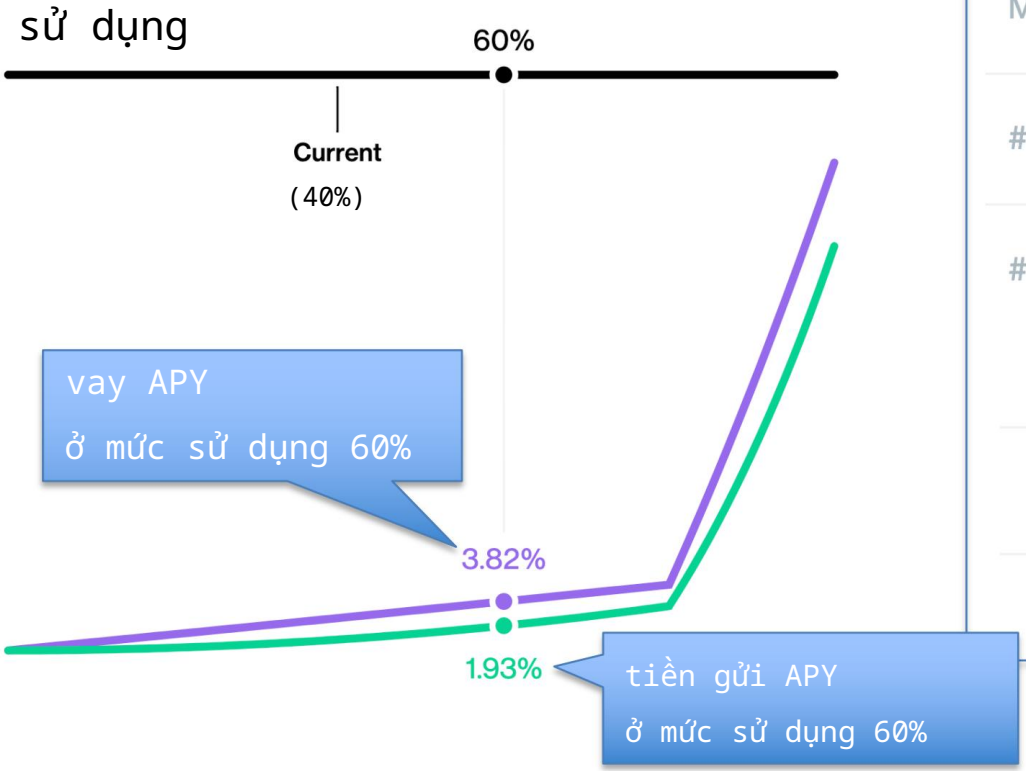
$$U_{ETH} = \frac{\text{tổng số dư vayETH}}{\text{Số dư khả dụng ETH} + \text{Tổng số dư vay ETH}}$$

tổng số dư nợ vay cao hơn, hoặc
số dư khả dụng thấp hơn trong hợp đồng

U_{ETH} cao hơn [0,1]

$$\text{interestRate}_{ETH} = \text{BaseRate}_{ETH} + U_{ETH} \times \text{slope}_{ETH}$$

Ví dụ: Thị trường DAI hợp chất



Market Liquidity	377,443,771 DAI
# of Suppliers	18468
# of Borrowers	2750
Collateral Factor	83%
cDAI Minted	26,810,077,978
Exchange Rate	1 DAI = 45.26986803778856 cDAI

(Tháng 10 năm 2022)

Thanh lý: nợ > Khả năng vay

Nếu sức khỏe của người dùng < 1 thì bất kỳ ai cũng có thể gọi:

thanh lý(người vay, Tài sản thế chấp, Tài sản vay, số tiền uint)

địa chỉ của người vay đang được thanh lý

Người thanh lý muốn có cToken trong tài sản này (ví dụ: cDAI)

Người thanh lý đang cung cấp tài sản này (ví dụ: ETH)

Chức năng này chuyển ETH của người thanh lý vào thị trường ETH và cung cấp cho người thanh lý cDAI từ tài sản thế chấp của người dùng

Thanh lý: nợ > Khả năng vay

Nếu sức khỏe của người dùng < 1 thì bất kỳ ai cũng có thể gọi:

```
thanh lý(người vay, Tài sản thế chấp, Tài sản vay, số tiền uint)
```

Người thanh lý đang trả nợ ETH của người dùng và nhận cDAI

của người dùng Người thanh lý muốn Người

địa chỉ của người vay thanh lý đang [ở mức tỷ giá hối đoái được chiết

khấu -- hình phạt cho người dùng] cung cấp tài sản này cToken trong tài

cDAI) lý (ví dụ: ETH) (ví dụ: sản này đang được thanh

Chức năng này chuyển ETH của người thanh lý vào thị trường ETH và cung cấp cho người thanh lý cDAI từ tài sản thế chấp của người dùng

Rủi ro thanh lý là gì?

Lãi suất DAI lịch sử trên Compound (APY):

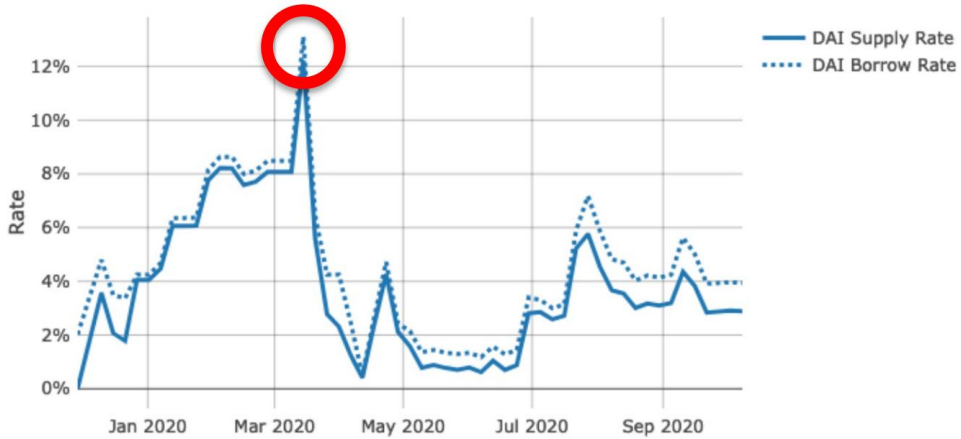
Nhu cầu về DAI tăng đột

biến giá DAI tăng đột

biến nợ của người dùng tăng

vọt sức khỏe của người

dùng giảm sút thanh lý .

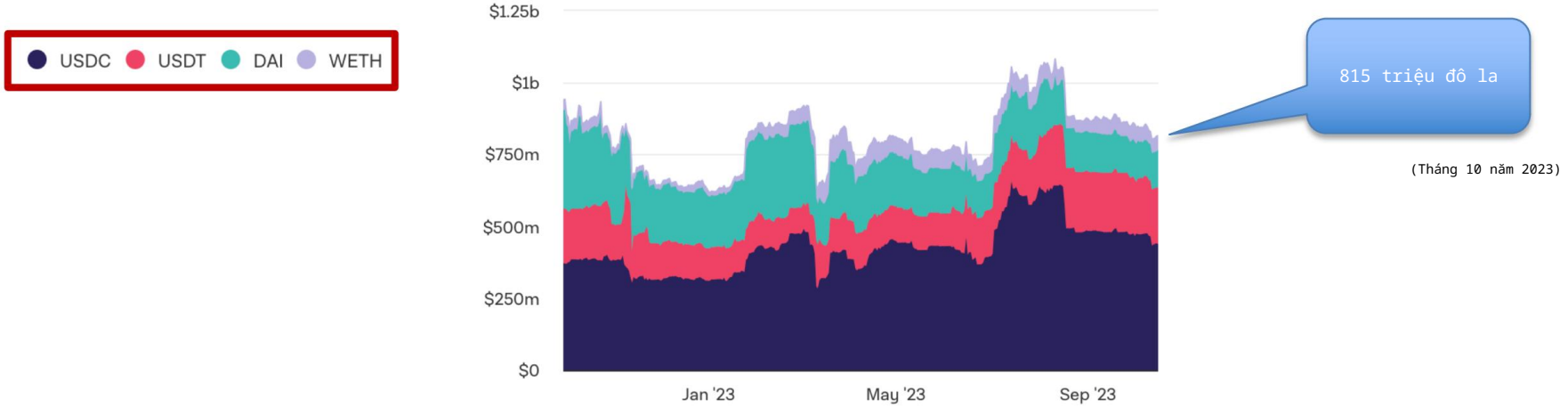


Để sử dụng Compound, người vay phải liên tục theo dõi APY và nhanh chóng trả nợ nếu APY tăng quá cao (có thể tự động hóa)

Tóm tắt & số liệu thống kê

• Nhà cung cấp thanh khoản có thể kiếm được lãi suất từ tài sản của họ • Sử dụng cho vay DeFi:

Tổng hợp nợ chưa thanh toán



(Tháng 10 năm 2023)

Tóm tắt & số liệu thống kê

Thống kê thanh lý hợp chất:

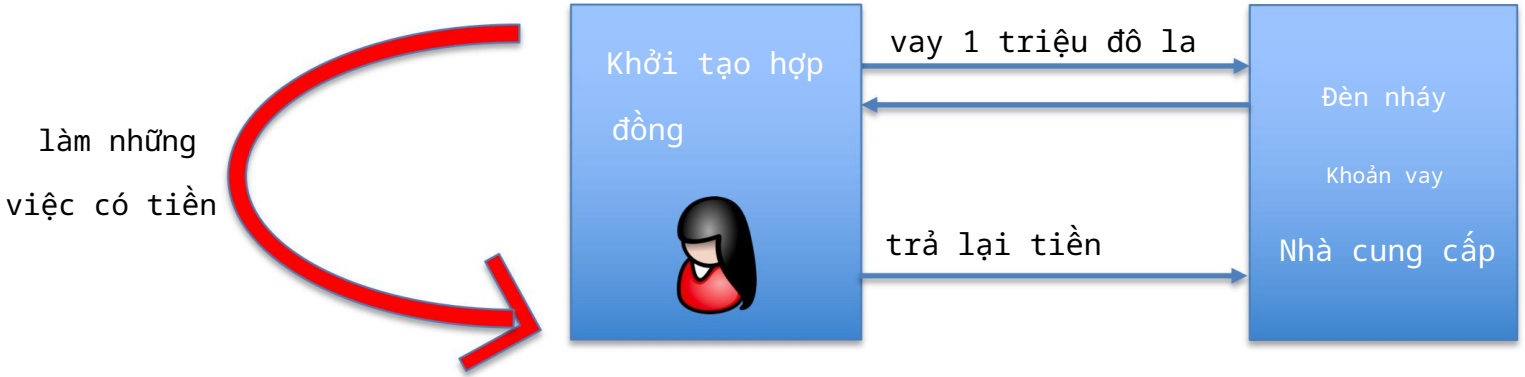
Do giá thế chấp giảm hoặc APY nợ tăng đột biến

Cho vay nhanh

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)

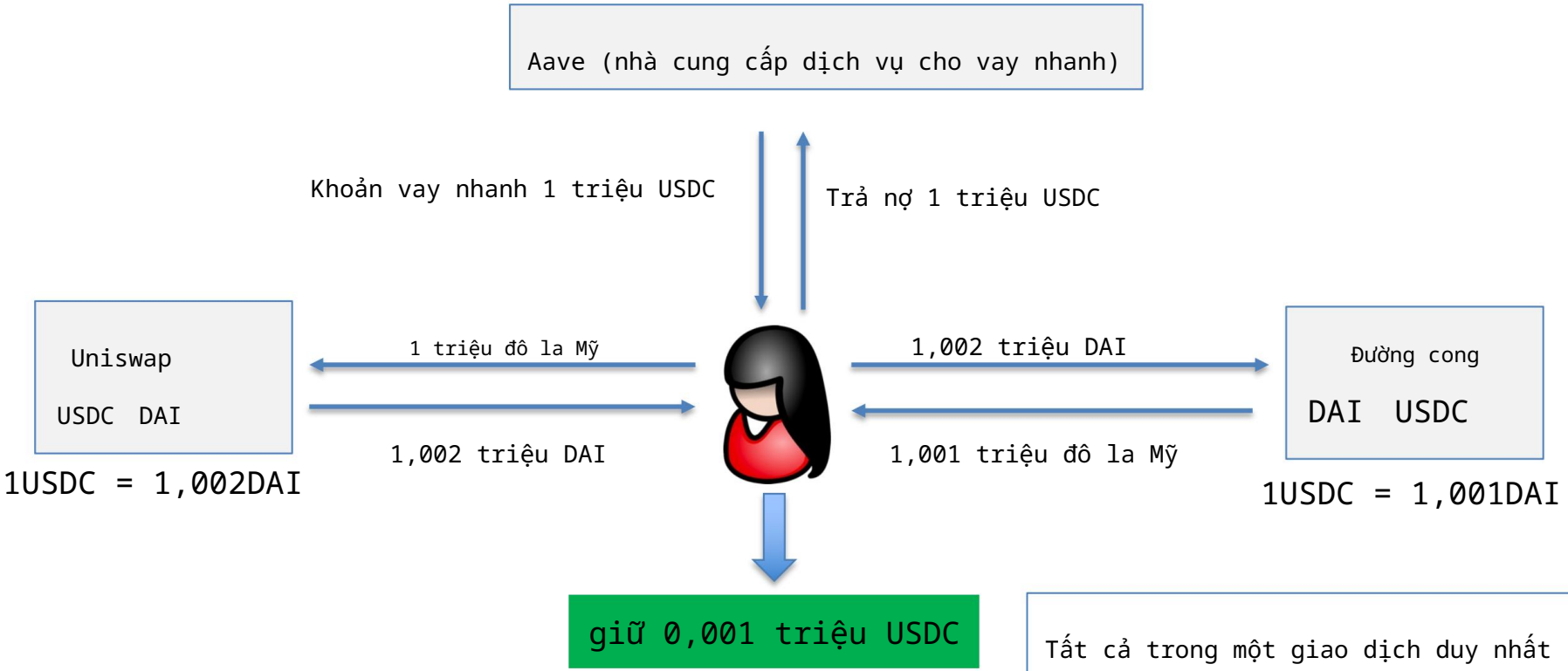
“Tấn công hệ sinh thái DeFi bằng các khoản vay nhanh để giải trí và kiếm lợi nhuận”

Các trường hợp sử dụng

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

Trọng tài không rủi ro

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



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

Đổi 1 cETH

Đổi 1 cETH lấy 3000 cUSDC

Gửi 3000 cUSDC làm tài sản thế chấp

Vay 1000 DAI

Trả lại khoản vay flash 1000 DAI

-1000 DAI

+3000 đô la Mỹ

đã vay DAI bằng cách sử dụng

ETH làm tài sản thế chấp

(một giao dịch Ethereum duy nhất)

mượn DAI sử dụng

USDC làm tài sản thế chấp

Triển khai Aave v1

```
hàm flashLoan(địa chỉ _receiver, uint256 _amount) {
   .
   // chuyển tiền cho người 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
   được trả lại require( availableLiquidityAfter == availableLiquidityBefore.add(amountFee),
        "cân bằng không nhất quán");
}
```

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

KẾT THÚC BÀI GIẢNG

Bài giảng tiếp theo: Sàn giao dịch phi tập trung (DeX)