CS251 Fall 2021

(cs251.stanford.edu)

DeFi Lending Systems

Dan Boneh

HW#3 posted later tonight.   Please fill out the feedback form on Ed.

By popular request …

A few words on WorldCoin

Where we are in the course

- How consensus protocols work
- **Bitcoin**: the UTXO model, and the Bitcoin scripting language
- **Ethereum** (the blockchain computer): the EVM and Solidity

Current topic: **decentralized finance**

on-chain: exchanges, stablecoins, today: lending

Next: privacy on the blockchain, scaling the blockchain, and interoperability across blockchains

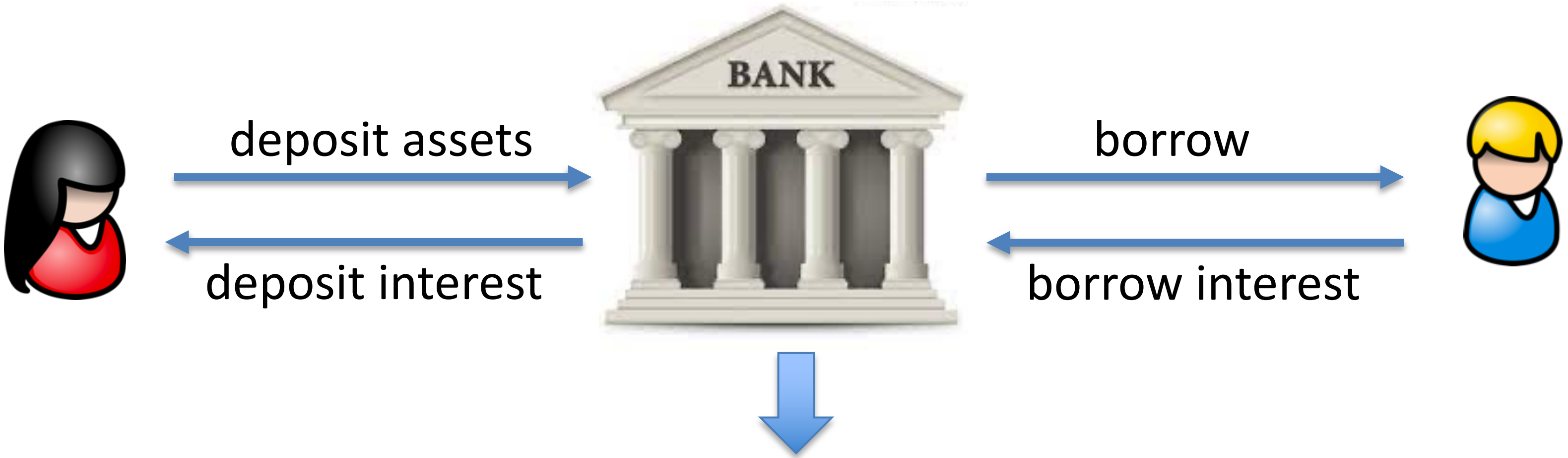
DeFi Lending Protocols

Goal: explain how decentralized lending works

This is not investment or financial advice

The role of banks in the economy

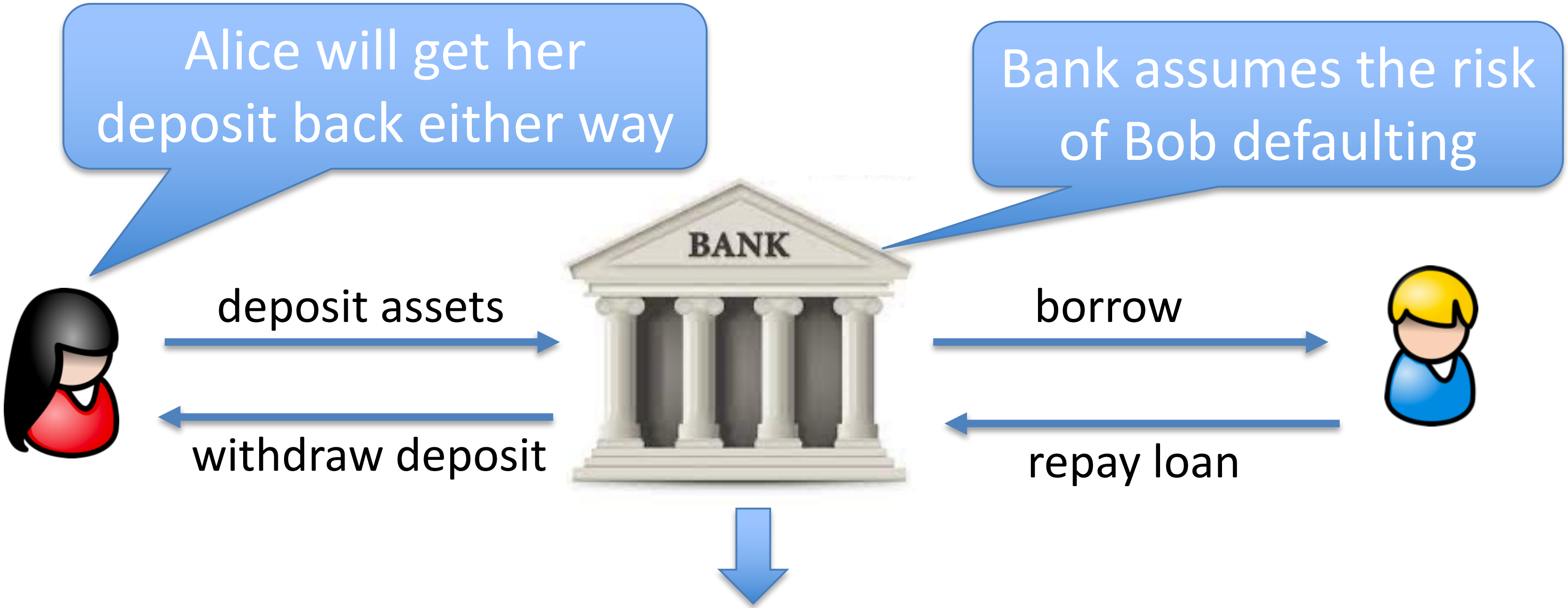
Banks bring together lenders and borrowers



bank spread

(borrow interest – deposit interest)

The role of banks in the economy



bank spread

(borrow interest – deposit interest)

Crypto: CeFi lending (e.g., Blockfi, Nexo, …)

Same as with a traditional bank:

Centralized Finance institution

Alice gives her assets to the CeFi institution to lend out to Bob

The role of collateral

(1 ETH = 100 UNI)

CeFi's concern: what if Bob defaults on loan?

$\Longrightarrow$ CeFi will absorb the loss

Solution: require Bob to lock up collateral

collateral

deposit 500 UNI

Borrow 1 ETH

interest deducted from collateral

over collateralized loan

debt position:

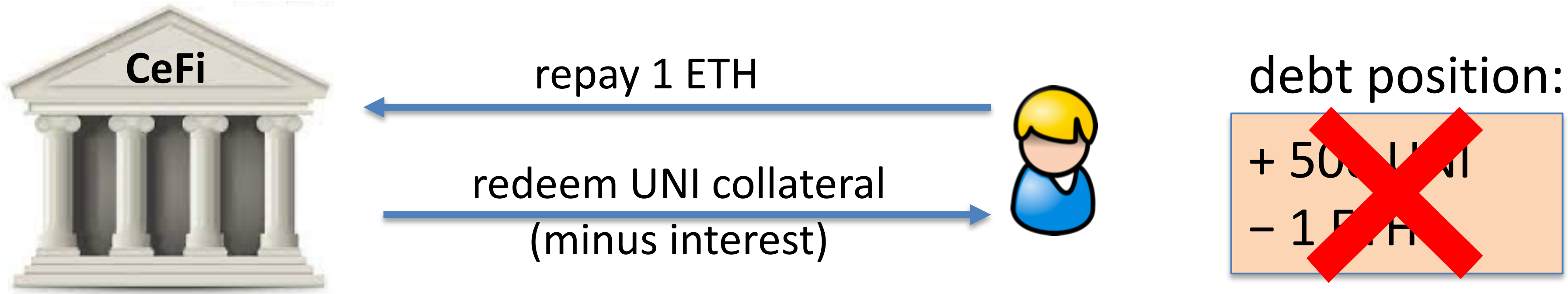
+ 500 UNI
− 1 ETH

The role of collateral

(1 ETH = 100 UNI)

Several things can happen next:

(1) Bob repays loan



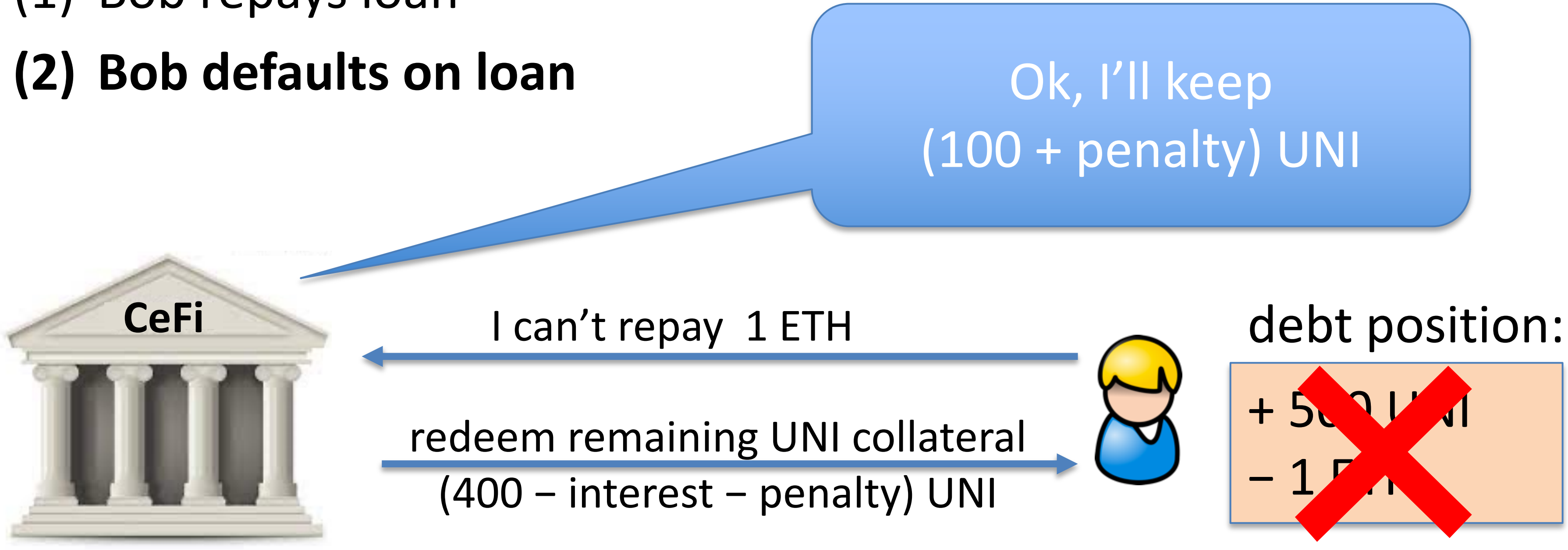
The role of collateral

(1 ETH = 100 UNI)

Several things can happen next:

(1) Bob repays loan

(2) Bob defaults on loan



The role of collateral

(1 ETH = 400 UNI)

Several things can happen next:

(1) Bob repays loan

(2) Bob defaults on loan

(3) Liquidation: value of loan increases relative to collateral

I need to liquidate your collateral (and charge a penalty)

debt position:

+ 100 UNI
− 0 ETH

lender needs to liquidate **before** value(debt) > value(collateral)

Terminology

Collateral: assets that serve as a security deposit

Over-collateralization: borrower has to provide

value(collateral) > value(loan)

Under-collateralization: *value(collateral) < value(loan)*

collateral factor

Liquidation:

if value(debt) > 0.6 × value(collateral)

then collateral is liquidated until inequality flips

(liquidation reduces both sides of the inequality)

Collateral factor

CollateralFactor $\in$ [0,1]

- Max value that can be borrowed using this collateral

- High volatility asset $\Longrightarrow$ low collateral factor
- Relatively stable asset $\Longrightarrow$ higher collateral factor

<u>Examples:</u> (on Compound)

ETH, DAI: 75%, UNI: 60%, YFI: 35%

Health of a debt position

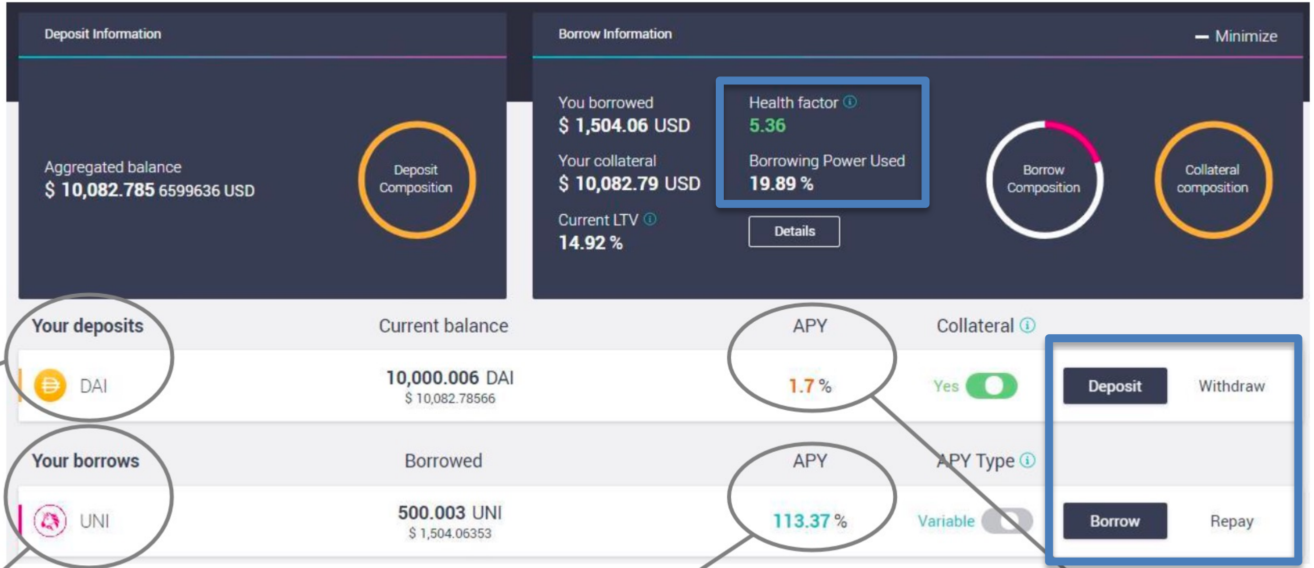
$$\text{BorrowCapacity} = \sum_i \text{value}(\text{collateral}_i) \times \text{CollateralFactor}_i$$

(in ETH)

$$\boxed{\text{health} = \frac{\text{BorrowCapacity}}{\text{value}(\text{TotalDebt})}}$$

helath < 1 $\implies$ triggers liquidation until (health ≥ 1)

Example: Aave dashboard (a DeFi lending Dapp)



DAI is deposited as collateral

actions

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.

Credit: Arthur Gervais

Why borrow ETH?

If Bob has collateral, why can't he just buy ETH?

- Bob may need ETH (e.g., to buy in-game Axies),
  but he might not want to sell his collateral (e.g., an NFT)

- As an investment strategy: using UNI to borrow ETH gives Bob exposure to both

The problem with CeFi lending

Users must trust the CeFi institution:

- Not to get hacked, steal assets, or miscalculate
- This is why traditional finance is regulated

- Interest payments go to the exchange, not liquidity provider Alice

- CeFi fully controls spread (borrow interest – deposit interest)

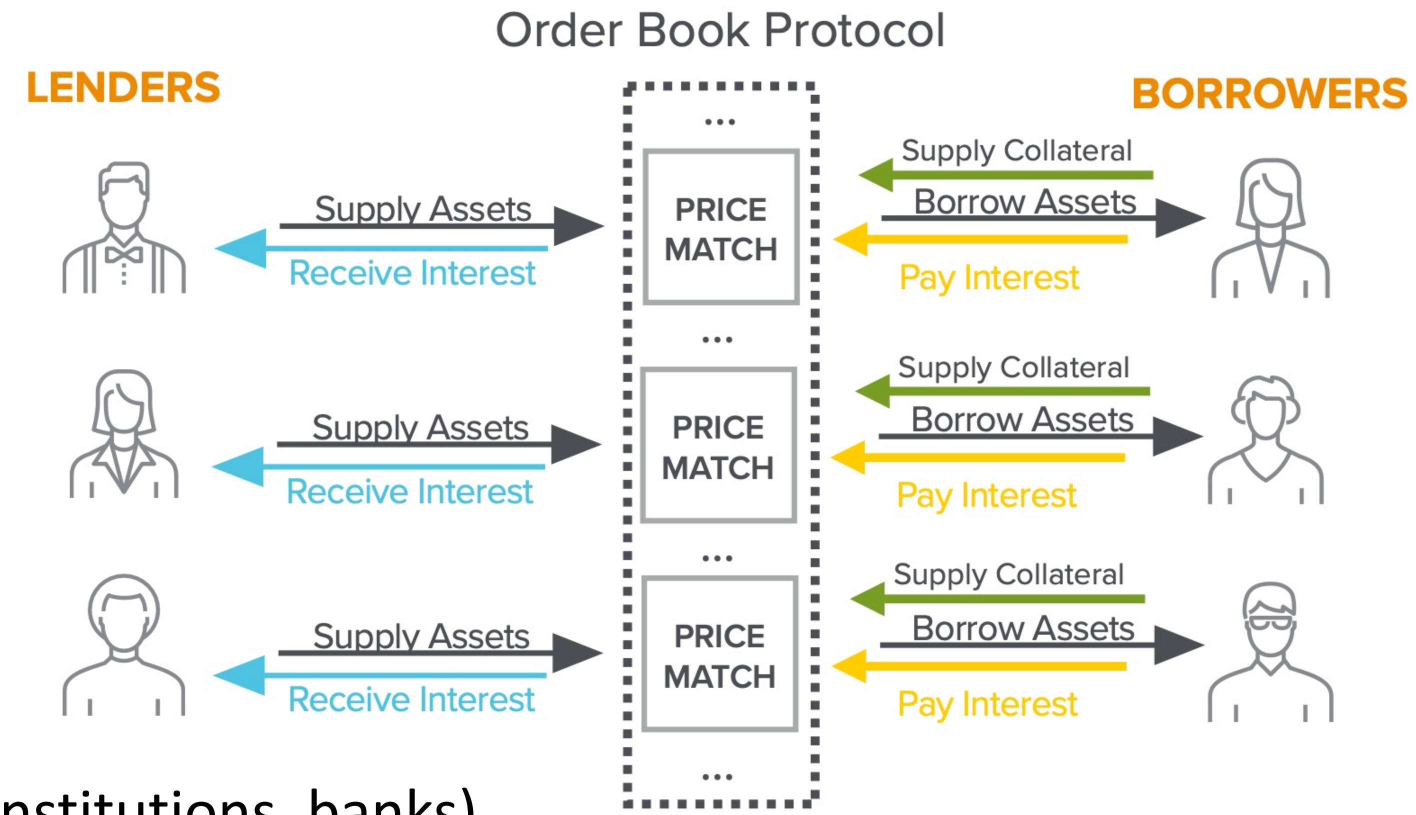
DeFi Lending

Can we build an on-chain lending Dapp?

$\Longrightarrow$ no central trusted parties

$\Longrightarrow$ code available on Ethereum for inspection

A first idea: an order book Dapp



(large institutions, banks)

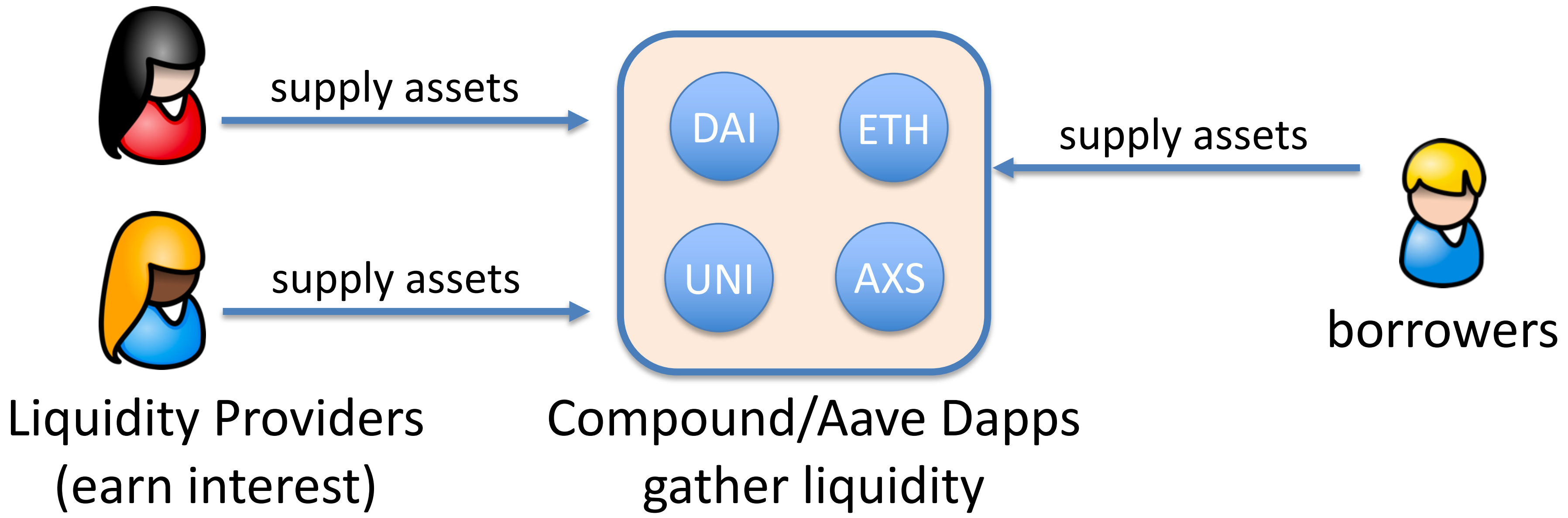
Credit: Eddy Lazzarin

Challenges

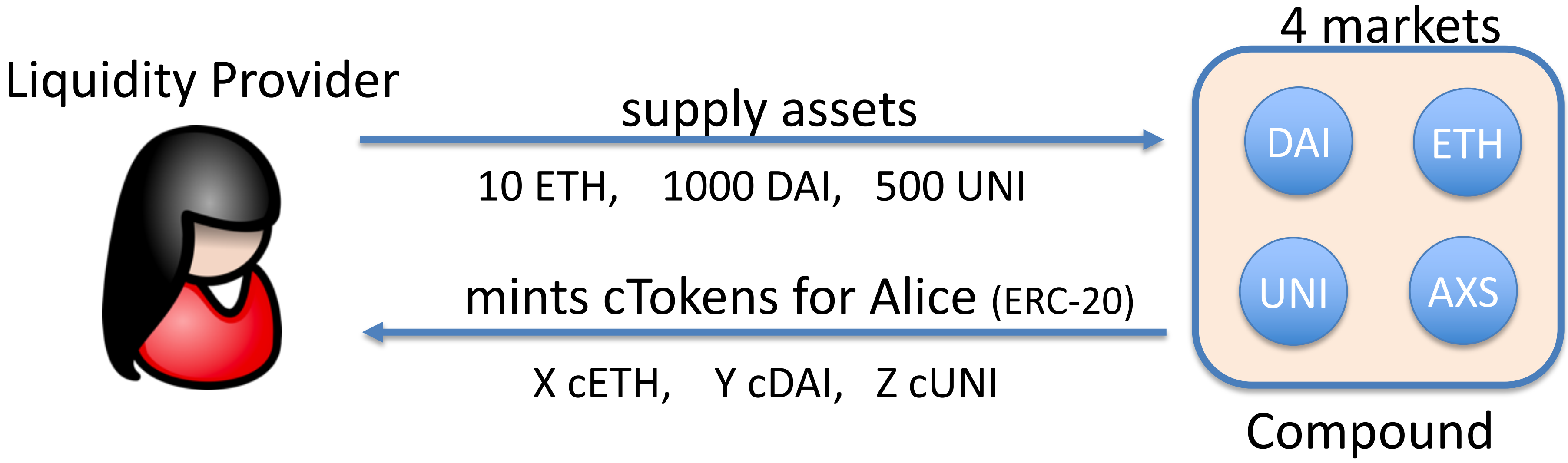
- **Computationally expensive**: matching borrowers to lenders requires many transactions per person (post a bid, retract if the market changes, repeat)
- **Concentrated risk**: lenders are exposed to their direct counterparty defaulting
- **Complex withdrawal**: a lender must wait for their counter-parties to repay their debts

A better approach: liquidity pools

Over-collateralized lending: Compound and Aave



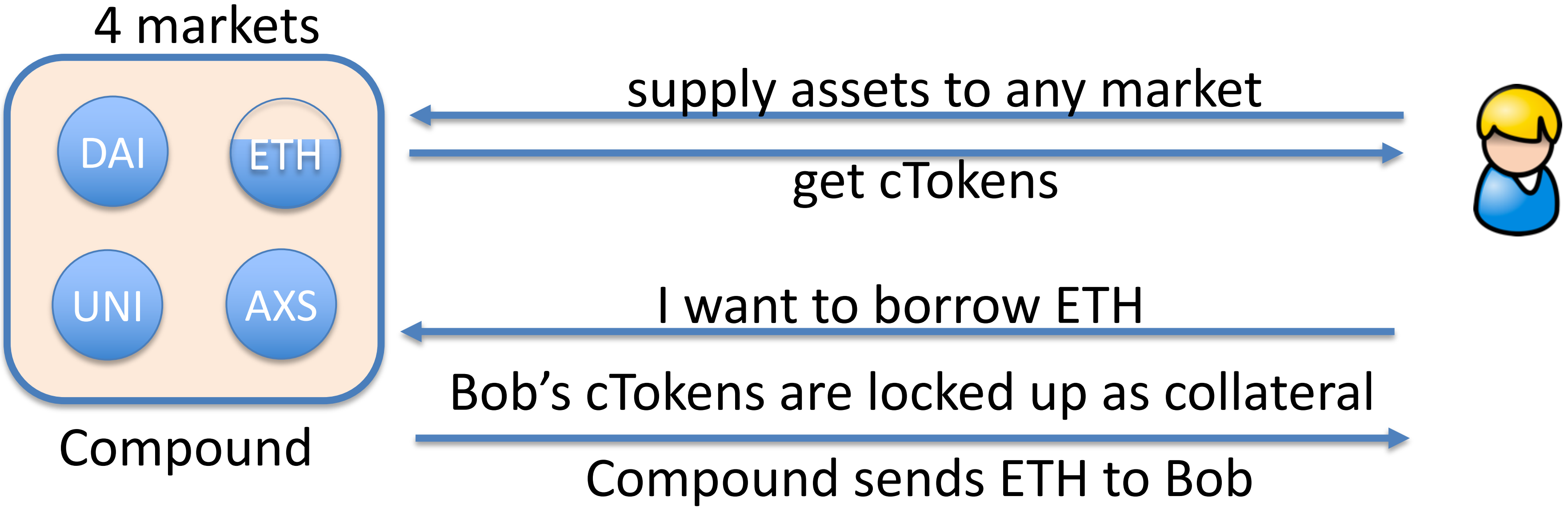
Example: Compound cTokens



Value of X, Y, Z is determined by an exchange rate:

Token to cToken exchange rate is calculated every block

Borrowers



Bob's accrued interest increases ETH/cETH exchange rate

$\Longrightarrow$ benefit cETH token holders (ETH liquidity providers)

The exchange rate

Consider the ETH marker:

Supplying ETH: adds to $\text{UnderlyingBalance}_{\text{ETH}}$

Borrowing ETH: adds to $\text{totalBorrowBalance}_{\text{ETH}}$

Interest: added repeatedly to $\text{totalBorrowBalance}_{\text{ETH}}$

$$\text{ExchangeRate}_{\text{ETH/cETH}} = \frac{\text{UnderlyingBalance}_{\text{ETH}} + \text{totalBorrowBalance}_{\text{ETH}} - \text{reserve}_{\text{ETH}}}{\text{cTokenSupply}_{\text{ETH}}}$$

$\Longrightarrow$ As totalBorrowBalance increases so does ExchangeRate

The interest rate: constantly updates

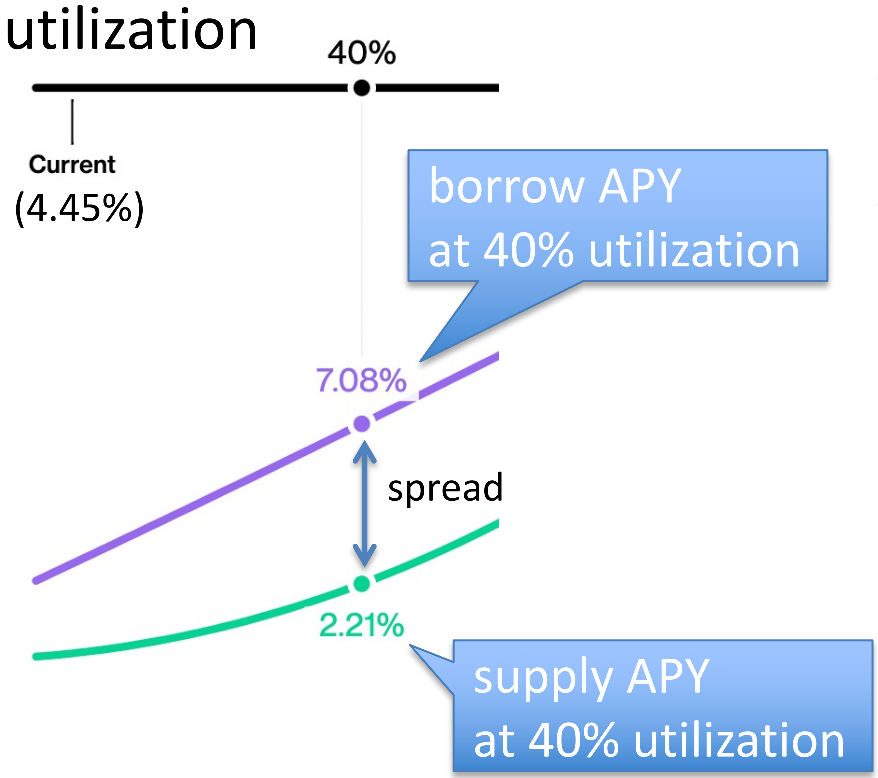
Key idea: determined by demand for asset vs. asset market size

Utilization ratio: $\mathbf{U_{ETH}} = \dfrac{\text{totalBorrowBalance}_{ETH}}{\text{availableBalance}_{ETH} + \text{totalBorrowBalance}_{ETH}}$

higher totalBorrowBalance, or lower availableBalance in contract	⇒	higher $\mathbf{U_{ETH}} \in [0,1]$

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

Example: Compound ETH market



Market Liquidity	1,499,627 ETH
# of Suppliers	68607
# of Borrowers	1260
Collateral Factor	75%
cETH Minted	78,227,475
Exchange Rate	1 ETH = 49.86243030285714 cETH

Liquidation: debt > BorrowCapacity

If user's   health < 1   the **anyone** can call:

liquidate(borrower,   CollateralAsset,   BorrowAsset, uint amount)

address of borrower being liquidated

Liquidator wants cTokens in this asset (e.g., cDAI)

Liquidator is providing this asset (e.g., ETH)

This function transfers liquidator's ETH into ETH market,
and gives the liquidator cDAI from user's collateral

Liquidation: debt > BorrowCapacity

If user's   health < 1   the **anyone** can call:

lic t)

Liquidator is repaying the user's ETH debt
and getting the user's cDAI
[at a discounted exchange rate -- penalty for user]

add
b

(e.g., cDAI)

set
(e.g., ETH)

This function transfers liquidator's ETH into ETH market,
and gives the liquidator cDAI from user's collateral

What is liquidation risk?

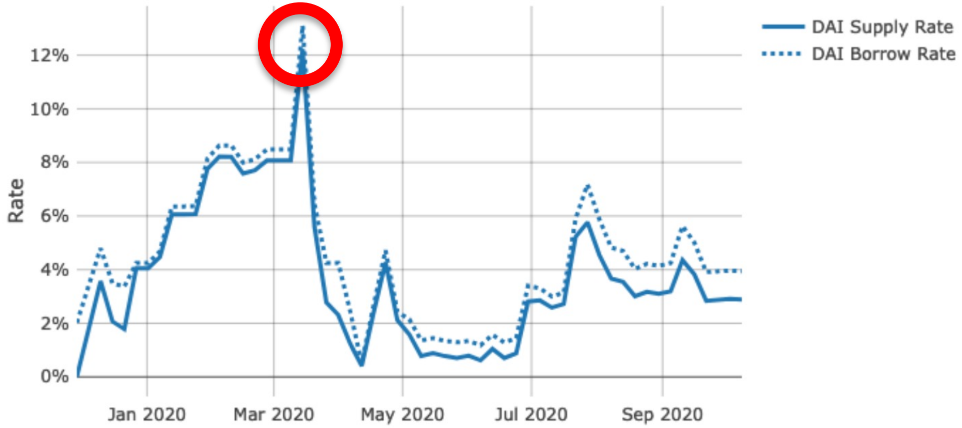
Historical DAI interest rate on Compound (APY):

APY shoots up temporarily

$\Longrightarrow$ user's debt shoots up

$\Longrightarrow$ user's health drops

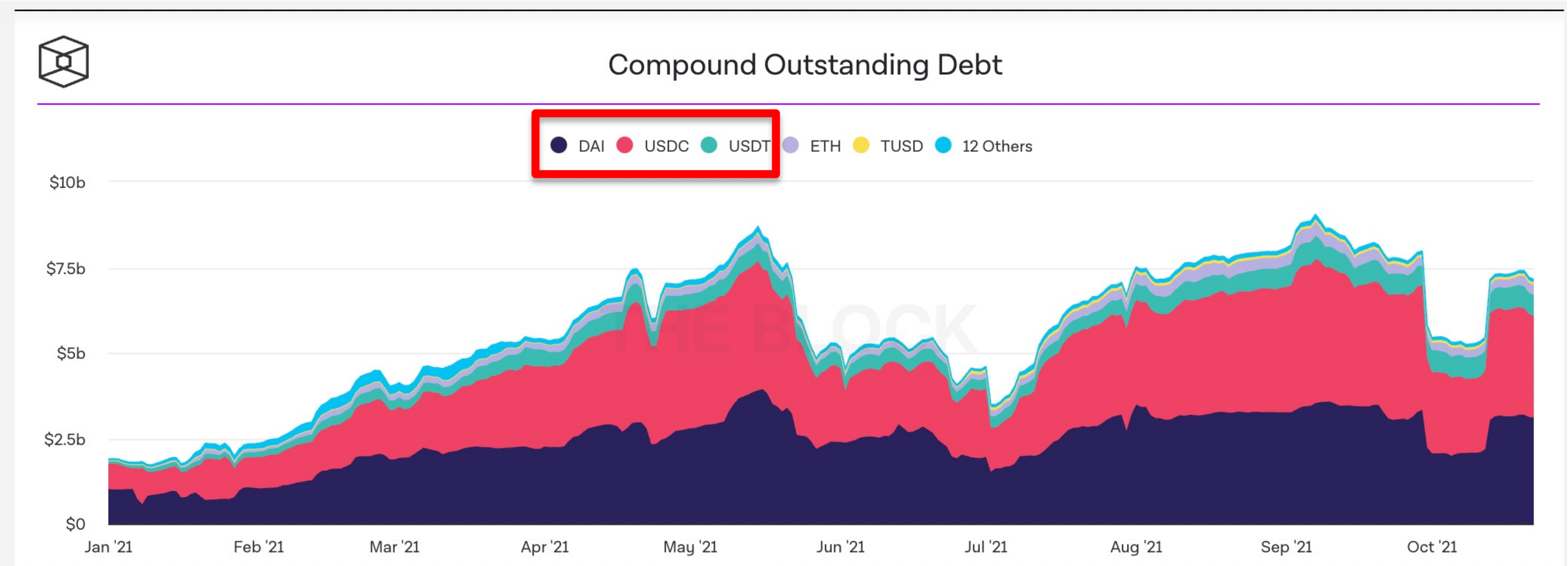
$\Longrightarrow$ liquidation …



To use Compound borrower must constantly monitor APY and quickly repay loans if APY goes too high (can be automated)

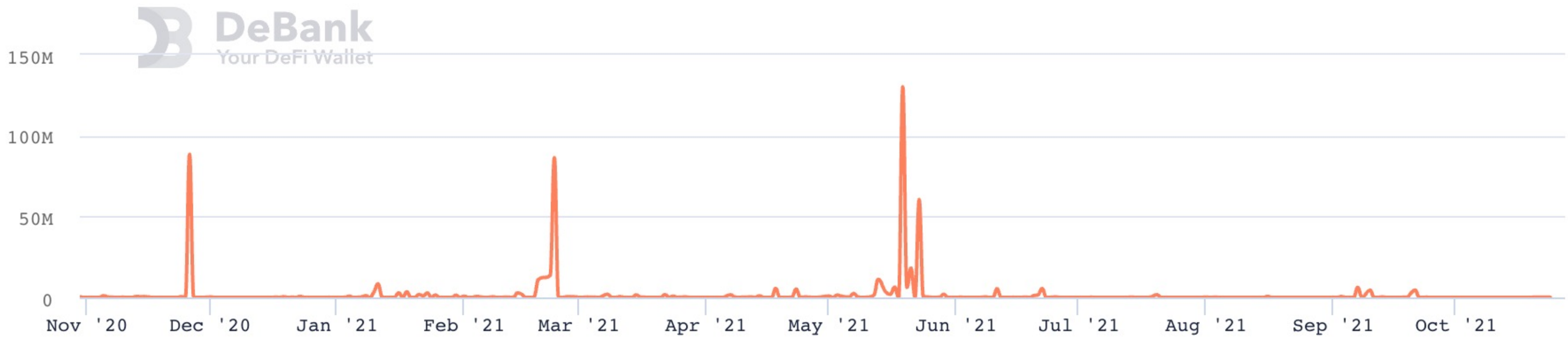
Summary & stats

- Liquidity providers can earn interest on their assets
- DeFi lending is being used quite a bit:



Summary & stats

Compound liquidation statistics:



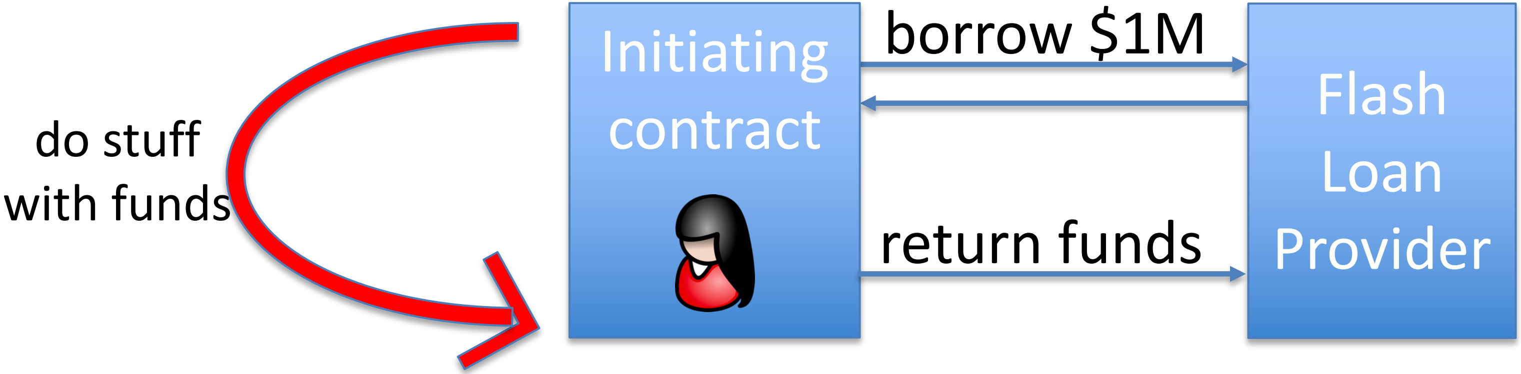
Caused by collateral price drops or debt APY spikes

Flash loans

What is a flash loan?

A flash loan is taken and repaid in a single transaction

$\Longrightarrow$ zero risk for lender $\quad\Longrightarrow$ borrower needs no collateral



(Tx is valid only if funds are returned in same Tx)

"Attacking the DeFi Ecosystem with Flash Loans for Fun and Profit"

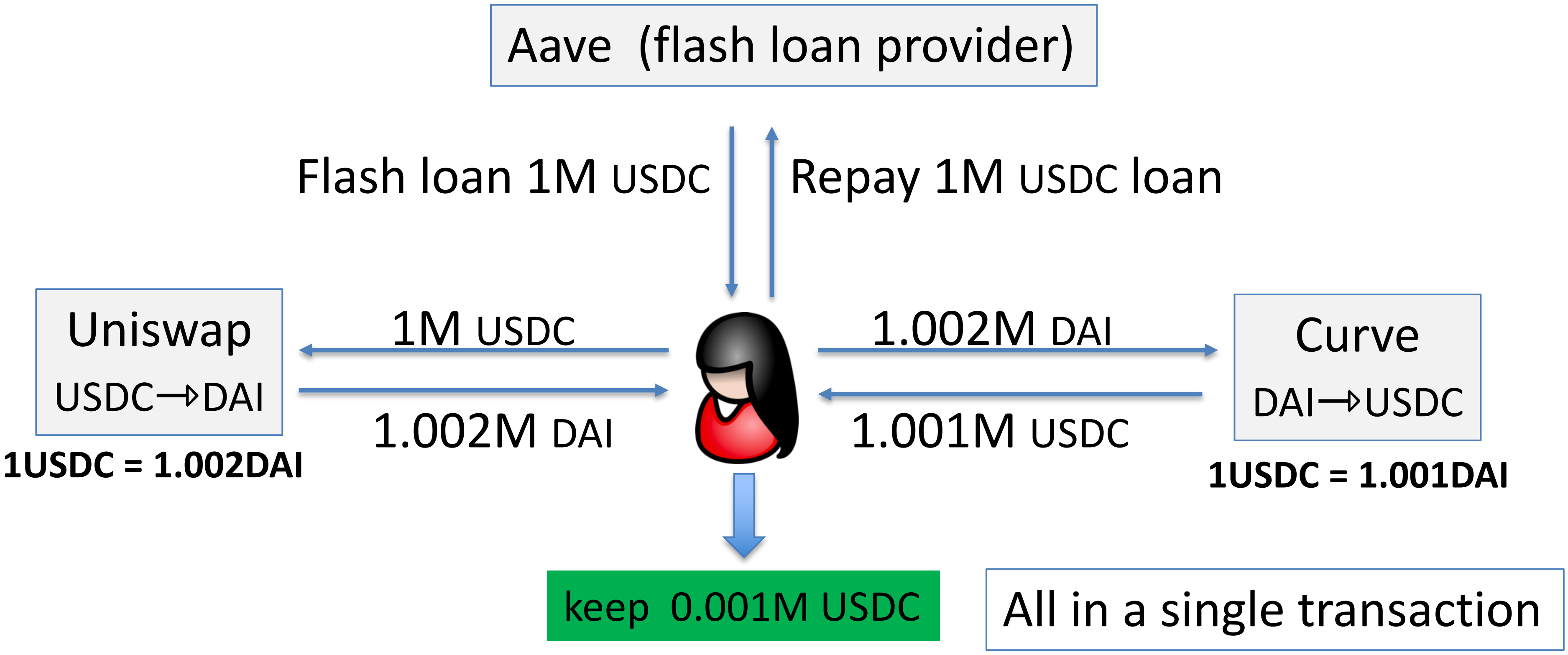
Use cases

- Risk free arbitrage
- Collateral swap
- DeFi attacks: price oracle manipulation

⋮

Risk free arbitrage

Alice finds a USDC/DAI price difference in two pools



Collateral swap

Alice @Compound

-1000 DAI
+1 cETH

borrowed DAI using ETH as collateral

Take 1000 DAI flash loan
Repay 1000 DAI debt
Redeem 1 cETH
Swap 1 cETH for 3000 cUSDC
Deposit 3000 cUSDC as collateral
Borrow 1000 DAI
Repay 1000 DAI flash loan

(a single Ethereum transaction)

Alice @Compound

-1000 DAI
+3000 cUSDC

borrowed DAI using USDC as collateral

Flash loans amounts on Aave (in 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

END OF LECTURE

Next lecture: U.S. blockchain regulations