

CS251 Fall 2022
(cs251.stanford.edu)



DeFi Lending Systems

Dan Boneh

HW#3 posted later tonight.

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

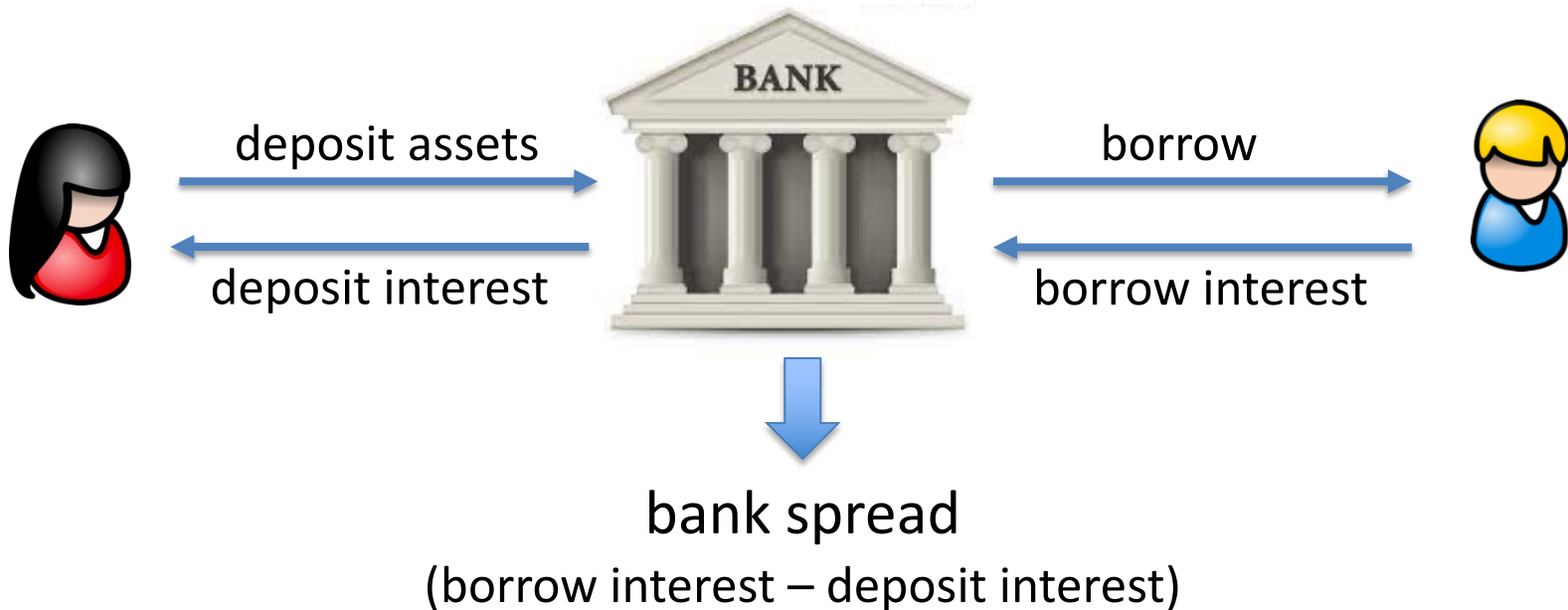
DeFi Lending Protocols

Goal: explain how decentralized lending works

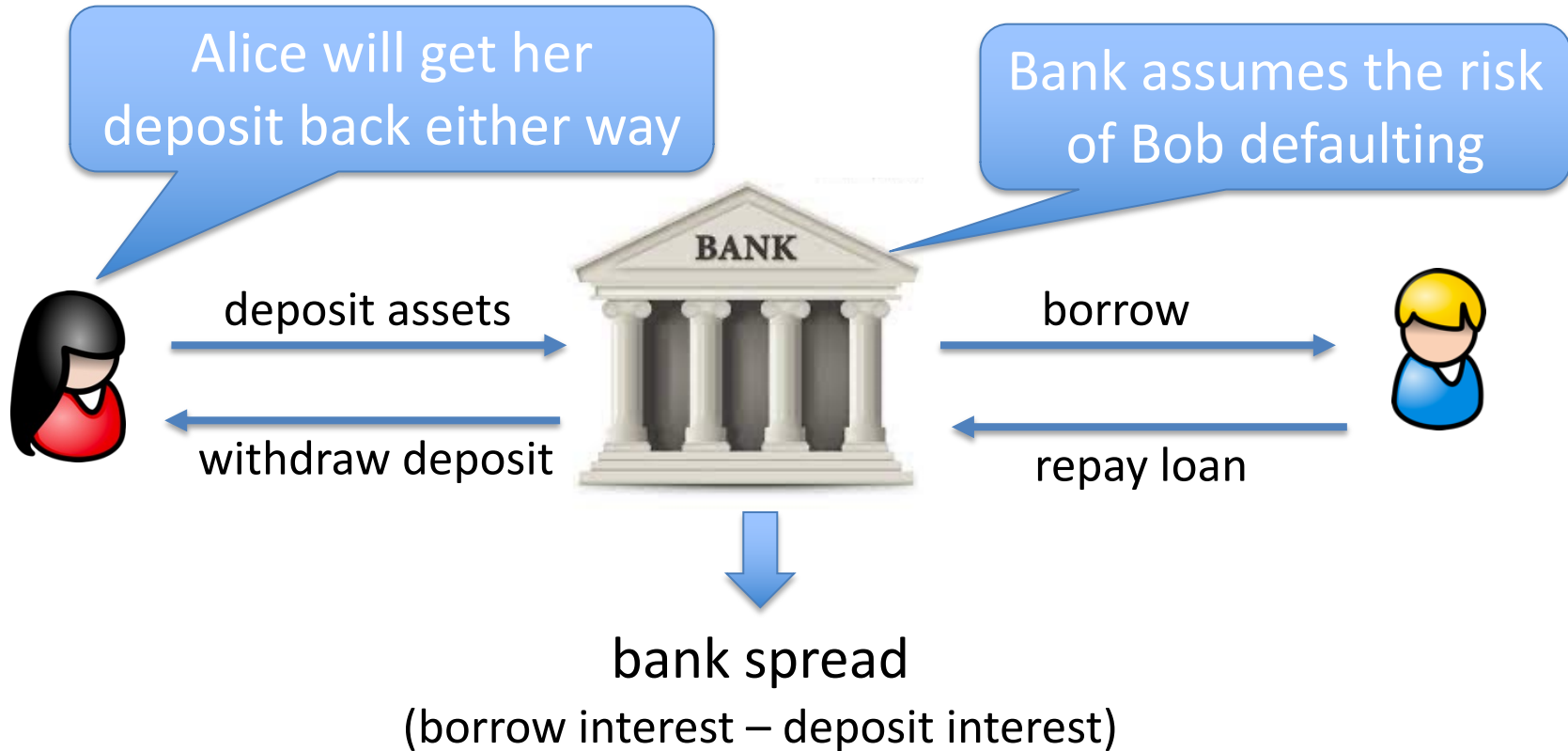
This is not investment or financial advice

The role of banks in the economy

Banks bring together lenders and borrowers

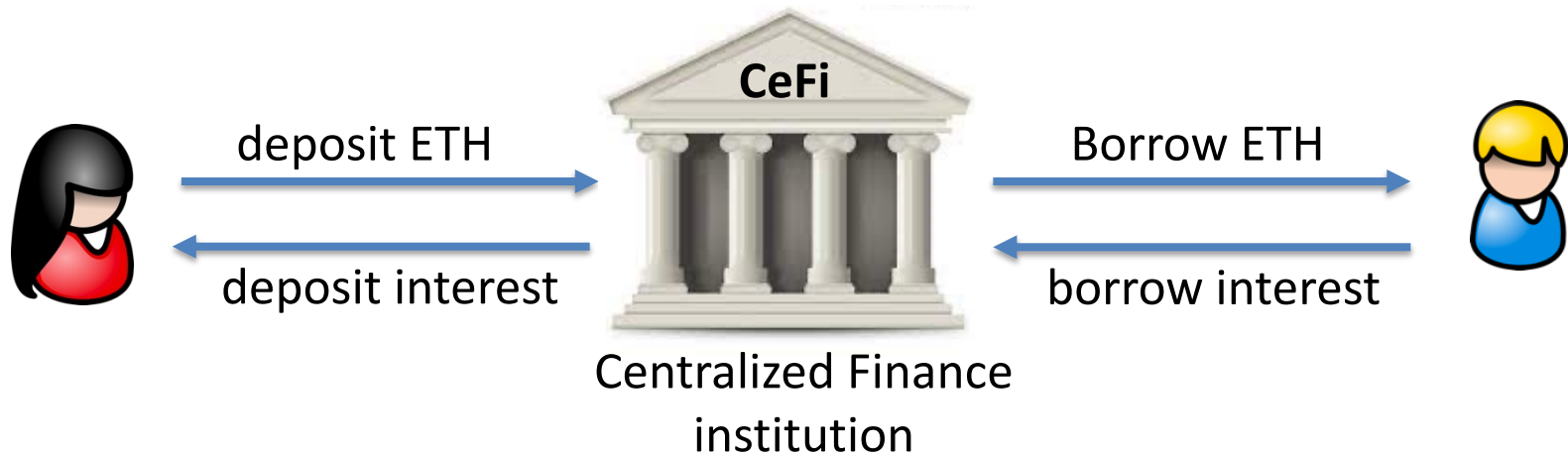


The role of banks in the economy



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

Same as with a traditional bank:



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?

⇒ CeFi will absorb the loss

Solution: require Bob to lock up collateral

collateral



deposit 500 UNI

Borrow 1 ETH



debt position:

+ 500 UNI
- 1 ETH

interest deducted from collateral

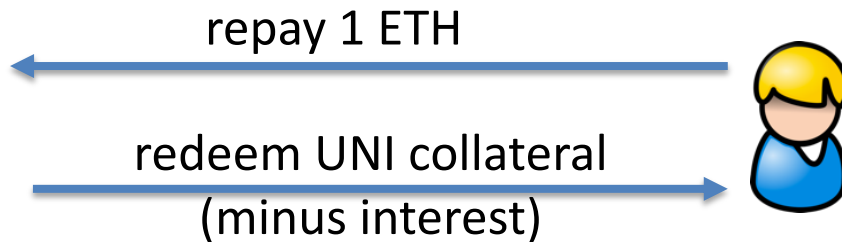
over collateralized loan

The role of collateral

Several things can happen next:

(1 ETH = 100 UNI)

(1) Bob repays loan



debt position:

~~+ 50 UNI
- 1 ETH~~

The role of collateral

Several things can happen next:

(1) Bob repays loan

(2) Bob defaults on loan

(1 ETH = 100 UNI)

Ok, I'll keep
(100 + penalty) UNI



I can't repay 1 ETH

redeem remaining UNI collateral
(400 - interest - penalty) UNI



debt position:

~~+ 500 UNI
- 1 ETH~~

The role of collateral

Several things can happen next:

(1 ETH = 400 UNI)

(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 = 20 UNI)



debt position:

+ 80 UNI
- 0 ETH

lender needs to liquidate **before** $\text{value}(\text{debt}) > \text{value}(\text{collateral})$

Terminology

Collateral: assets that serve as a security deposit

Over-collateralization: borrower has to provide
 $value(collateral) > value(loan)$

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

Liquidation:

if $value(debt) > 0.6 \times value(collateral)$

then collateral is liquidated until inequality flips

(liquidation reduces both sides of the inequality)

collateral factor

Collateral factor

CollateralFactor $\in [0,1]$

- Max value that can be borrowed using this collateral
- High volatility asset \implies low collateral factor
- Relatively stable asset \implies higher collateral factor

Examples: (on Compound)

ETH, DAI: 83%,

UNI: 75%,

MKR: 73%

Health of a debt position

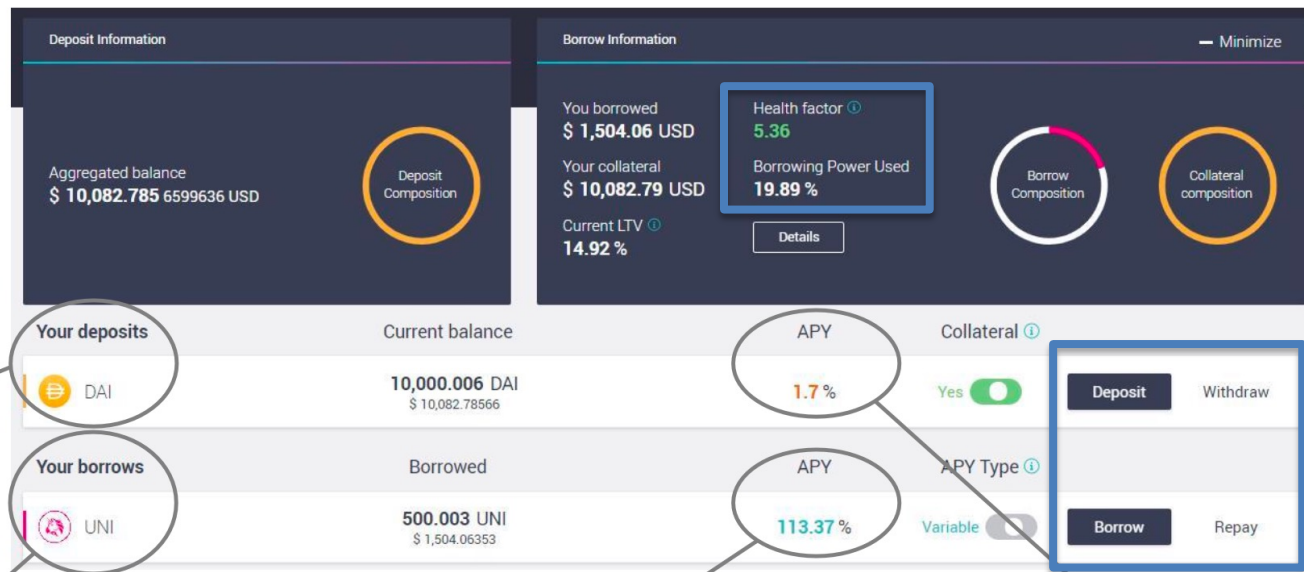
$$\text{BorrowCapacity} = \sum_i \text{value}(\text{collateral}_i) \times \text{CollateralFactor}_i$$

(in ETH)

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

health < 1 \Rightarrow triggers liquidation until (health \geq 1)

Example: Aave dashboard (a DeFi lending Dapp)



DAI is deposited as collateral

UNI is borrowed

The borrowing interests the borrower needs to pay

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

Why borrow ETH?

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

- Bob may need ETH (e.g., to buy in-game assets), 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?

⇒ no central trusted parties

⇒ code available on Ethereum for inspection

A first idea: an order book Dapp

Order Book Protocol

LENDERS



(large institutions, banks)



BORROWERS



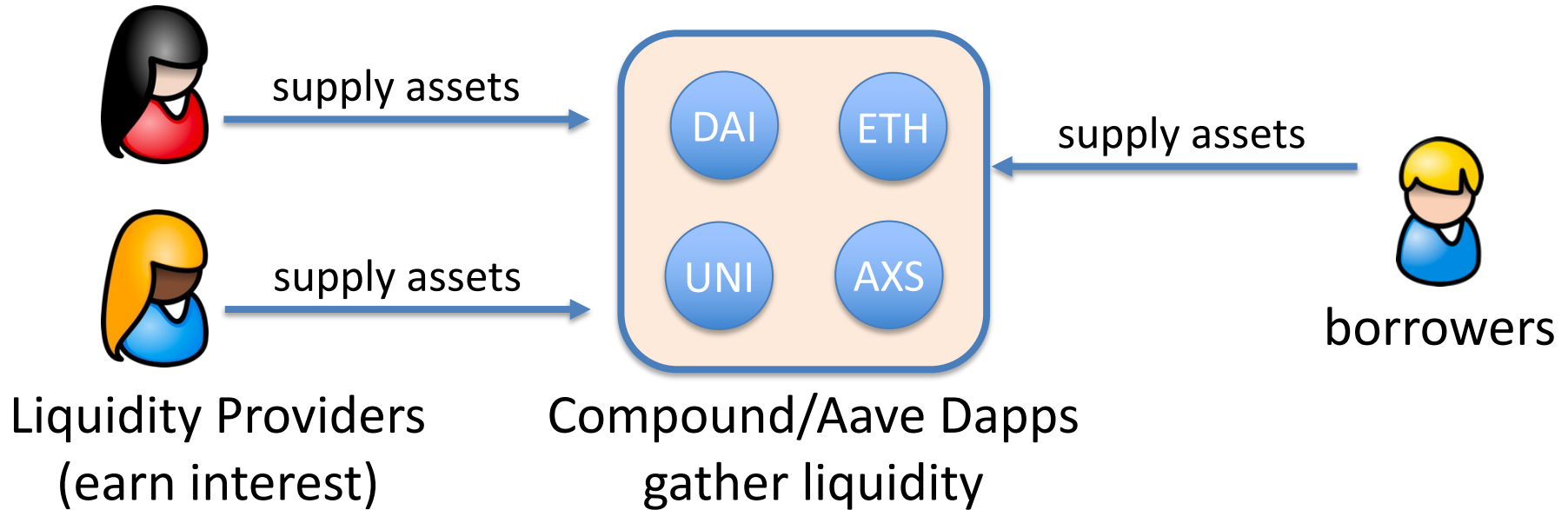
Credit: Eddy Lazzarin

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

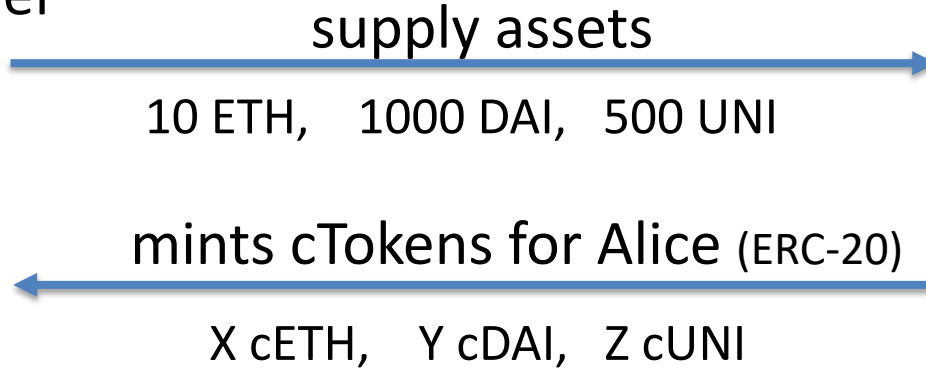
A better approach: liquidity pools

Over-collateralized lending: Compound and Aave

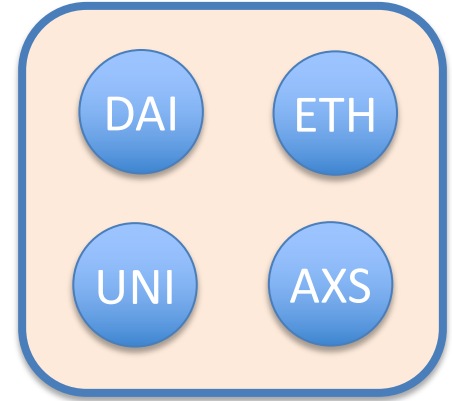


Example: Compound cTokens

Liquidity Provider



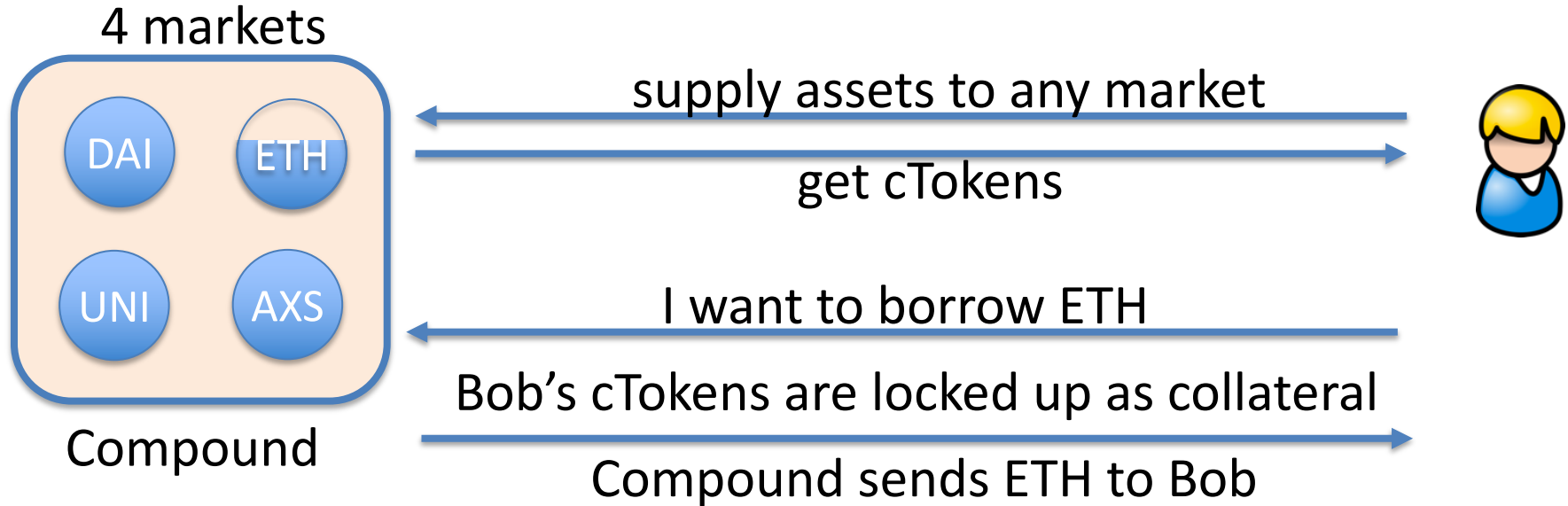
4 markets



Compound

Value of X, Y, Z is determined by the current exchange rate:
Token to cToken exchange rate is calculated every block

Borrowers



Bob's accrued interest increases ETH/cETH exchange rate

⇒ 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 $\text{totalBorrowBalance}_{\text{ETH}}$

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

⇒ As $\text{totalBorrowBalance}$ increases so does ExchangeRate

The interest rate: constantly updates

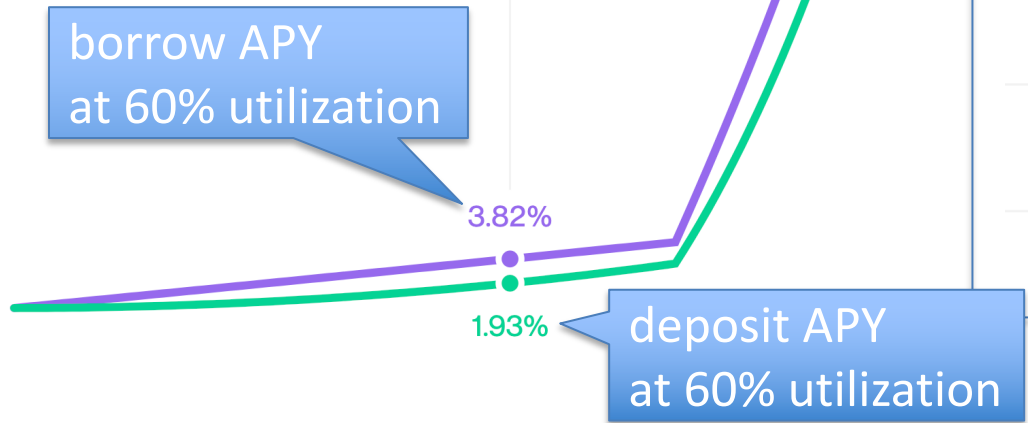
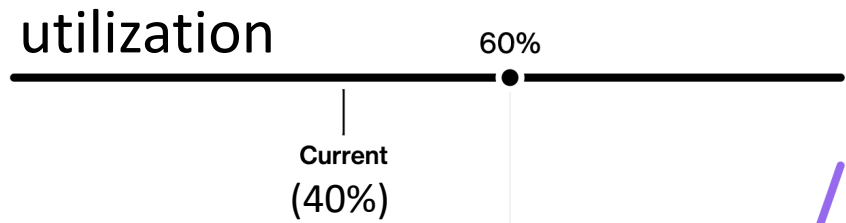
Key idea: determined by demand for asset vs. asset market size

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

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

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

Example: Compound DAI market



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

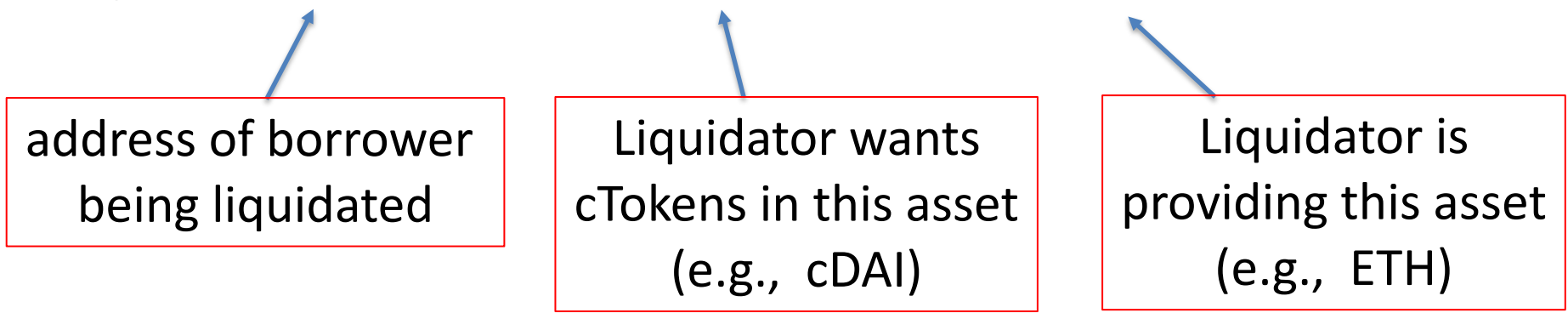
(Oct. 2022)

Liquidation: $\text{debt} > \text{BorrowCapacity}$

If user's health < 1 then 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: $\text{debt} > \text{BorrowCapacity}$

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

Liquidator is repaying the user's ETH debt
and getting the user's cDAI

[at a discounted exchange rate -- penalty for user]

(e.g., cDAI)

(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):

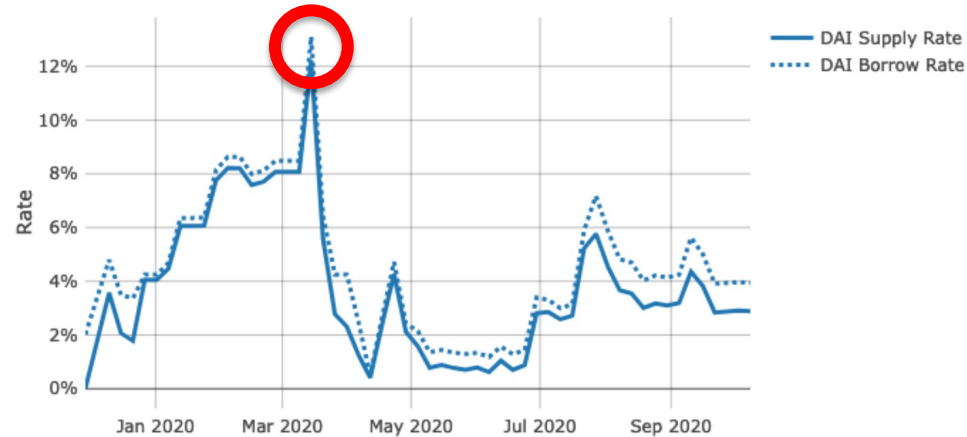
Demand for DAI spikes

⇒ price of DAI spikes

⇒ user's debt shoots up

⇒ user's health drops

⇒ liquidation ...

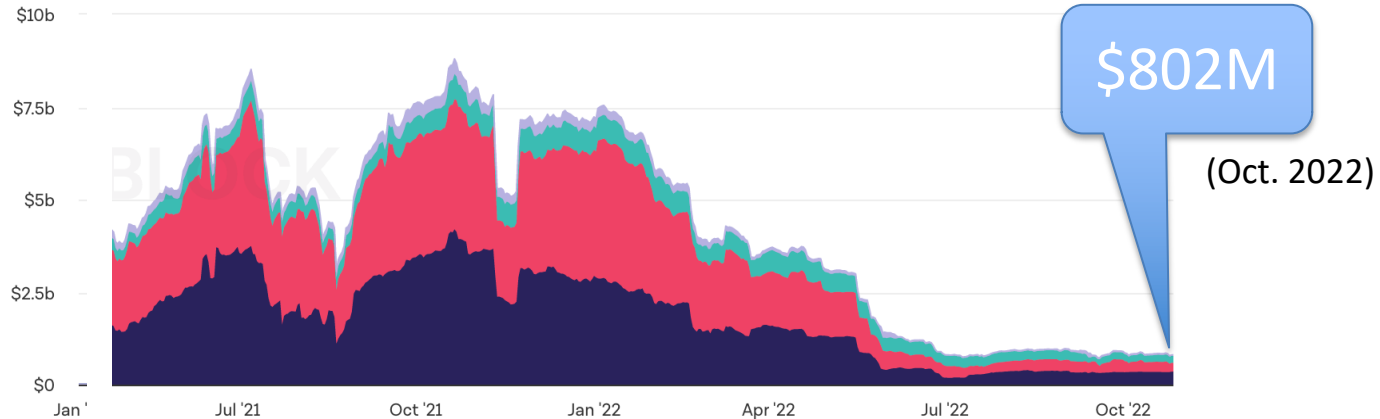


To use Compound, borrower must constantly monitor APY and quickly repay loans if APY goes too high (can be automated)

Summary & stats

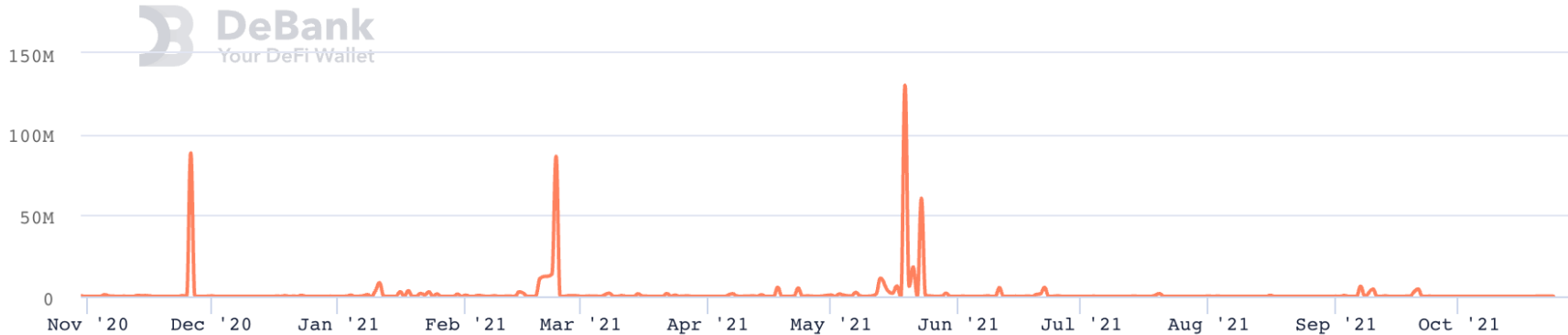
- Liquidity providers can earn interest on their assets
- DeFi lending is being used quite a bit:

Compound outstanding debt



Summary & stats

Compound liquidation statistics:



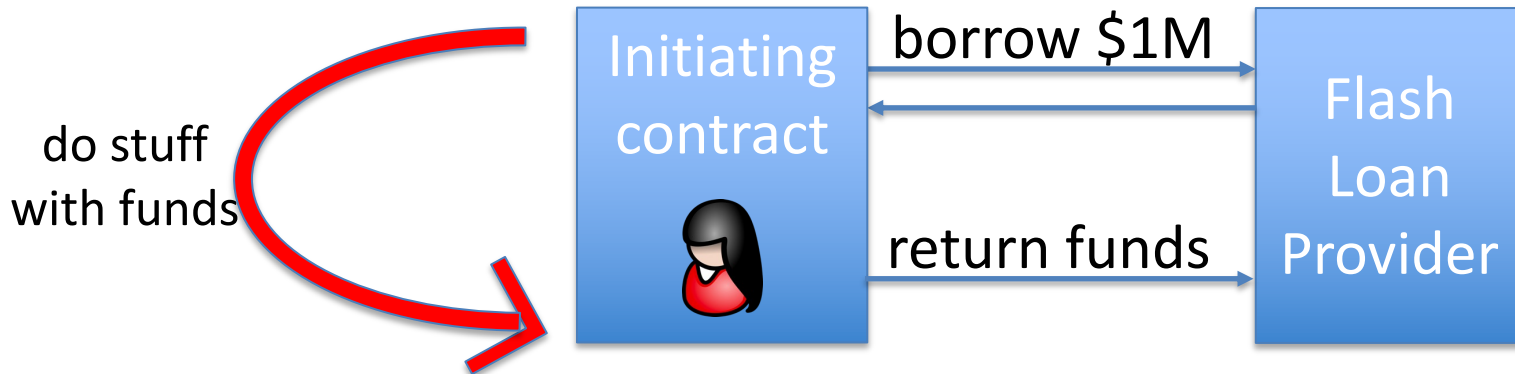
Caused by collateral price drops or debt APY spikes

Flash loans

What is a flash loan?

A flash loan is taken and repaid in a single transaction

⇒ zero risk for lender ⇒ borrower needs no collateral



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

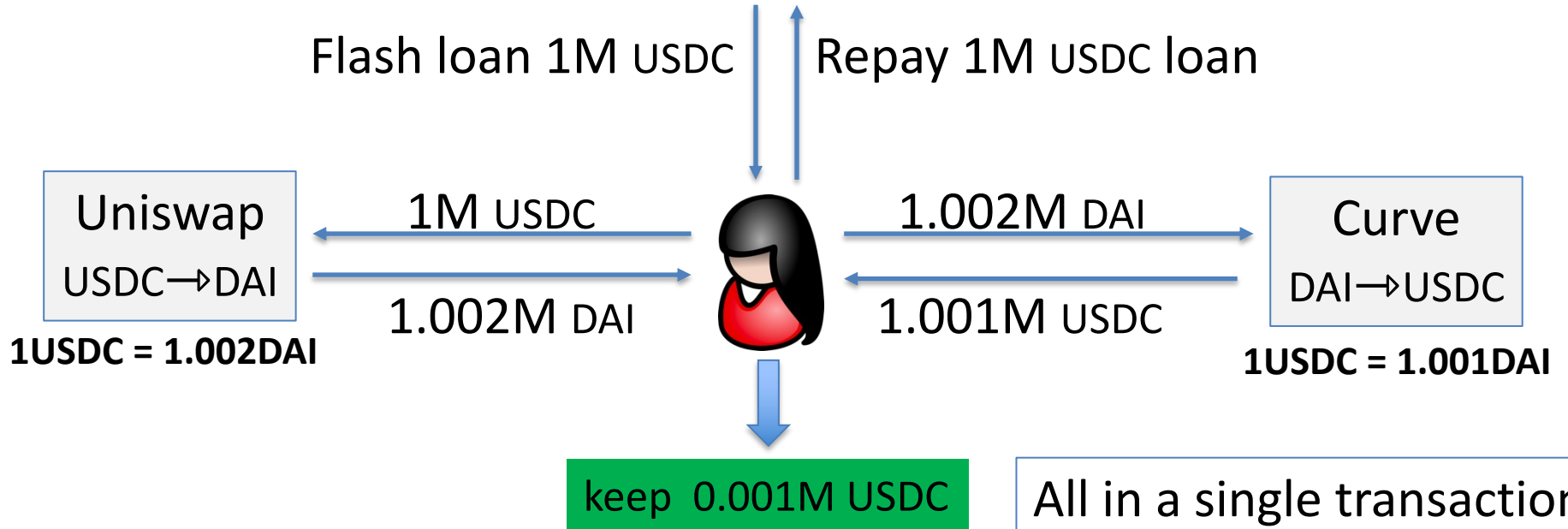
Use cases

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

Risk free arbitrage

Alice finds a USDC/DAI price difference in two pools

Aave (flash loan provider)



Collateral swap

start:

Alice @Compound



end goal:

Alice @Compound

-1000 DAI
+1 cETH

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

-1000 DAI
+3000 cUSDC

borrowed DAI using
ETH as collateral

(a single Ethereum transaction)

borrowed DAI using
USDC as collateral

Aave v1 implementation

```
function flashLoan(address _receiver, uint256 _amount) {
    ...
    // transfer funds to the receiver
    core.transferToUser(_reserve, userPayable, _amount);

    // execute action of the receiver
    receiver.executeOperation(_reserve, _amount, amountFee, _params);
    ...
    // abort if loan is not repaid
    require( availableLiquidityAfter == availableLiquidityBefore.add(amountFee),
        "balance inconsistent");
}
```

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

Recall the main application areas

1. Finance (DeFi):

- new financial instruments, exchanges, lending, ...

2. Managing digital assets (NFTs)



CryptoPunk #2890

3. DAOs: decentralized organizations



◆ 30

Digital assets (NFTs)

Example digital assets: (ERC-721)

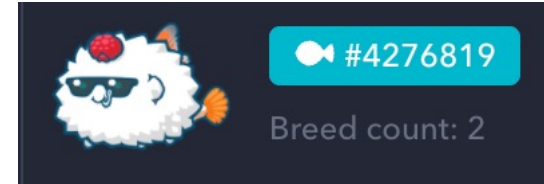
- Digital art: opensea, foundation
- Collector items: NBA top shots
- Game items: horses (zed.run), axes, ...
- Metaverse: plots in a virtual land



#8857



NBA



Why manage on a blockchain? Why not manage centrally?

- Blockchain ensures long-term ownership, until sale.
- Provides a trusted record of provenance (forgeries are evident)

ERC-721 (subset)

mapping (uint256 => address) internal **idToOwner**;

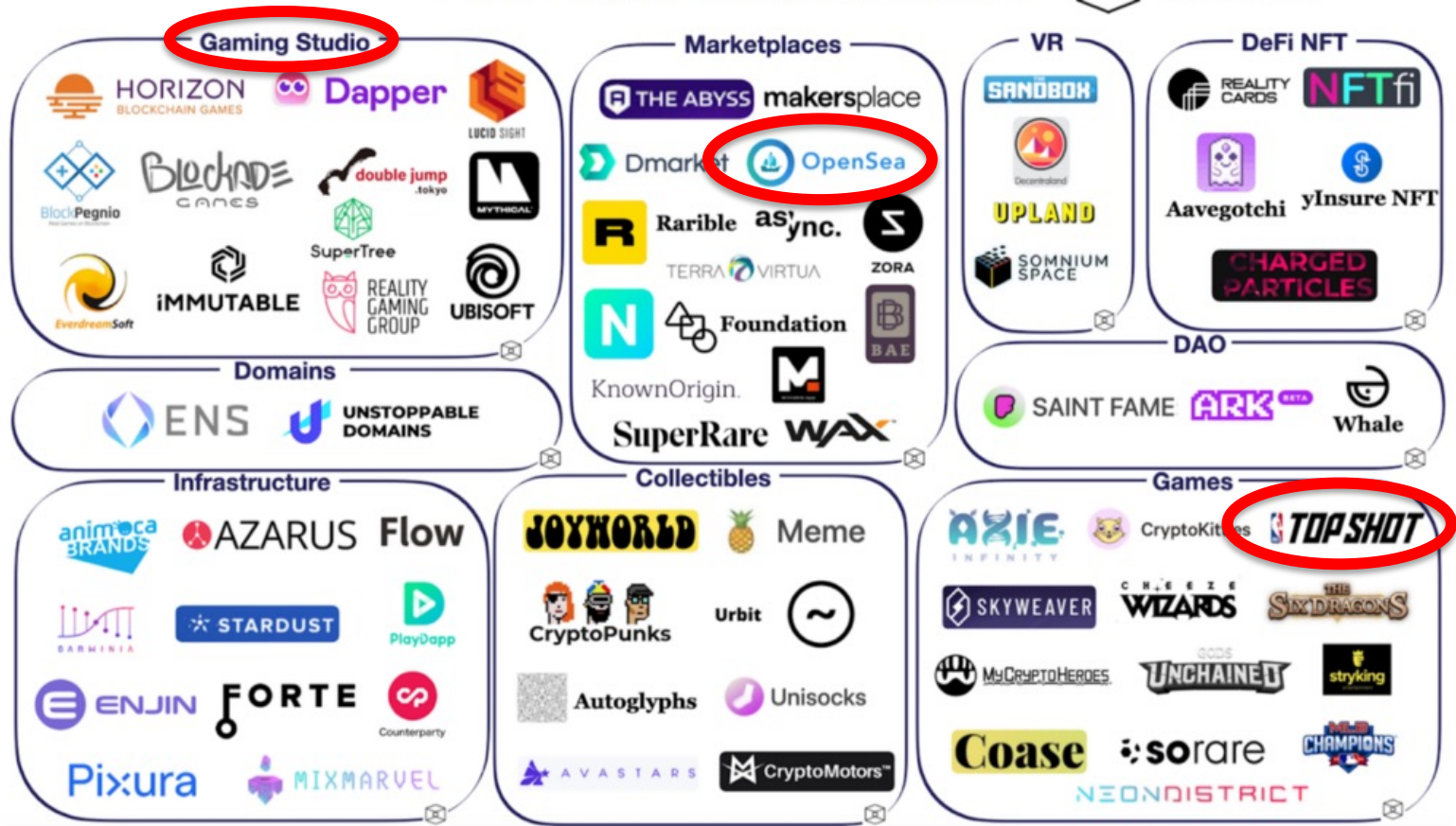
function **safeTransferFrom**(
 address _from, address _to, uint256 _tokenId, bytes data)

function **approve**(address _approved, uint256 _tokenId)

function **setApprovalForAll**(address _operator, bool _approved)





function **ownerOf**(uint256 _tokenId) returns (address);

The non-fungible token (NFT) ecosystem










(Sep. 2020, out of date)

OpenSea 24h volume

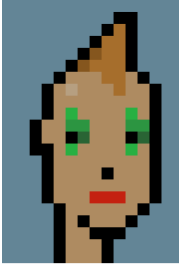
Collection	Volume ▾
1  CryptoPunks	◆ 1,017.69
2  CreatureToadz	◆ 916.15
3  CyberKongz	◆ 892.68
4  Doodles	◆ 730.72

OpenSea categories

 Art
 Music
 Domain Names
 Virtual Worlds
 Trading Cards
 Collectibles
 Sports

Example: CryptoPunks (generated in 2017)

10,000 total CryptoPunks. Managed by contract at Ethereum address 0xb47e3cd8DF8... (250 lines of solidity)



#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	gr8wxi	0x84c920	21Ξ (\$31,117)	Mar 05, 2021
Offered			21Ξ (\$31,117)	Mar 05, 2021
Sold	0x02751f	gr8wxi	0.30Ξ (\$67)	Aug 03, 2017
Offered			0.30Ξ (\$59)	Jul 30, 2017
Claimed		0x02751f		Jun 23, 2017

← buy offer

← sold!

← sell offer

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

digital assets: where is this going?

What does ownership mean?

- Who receives royalties on item: owner or creator?
- Where is item stored? Where can it be displayed?

... depends on NFT code.

NFTs and DeFi: asset-based DeFi:

- Use NFT as collateral in loans
- Fractional ownership of NFT assets
- NFT-based futures market

Decentralized orgs (DAO)

What is a DAO?

- A Dapp deployed on-chain at a specific address
- Anyone (globally) can send funds to DAO treasury
- Anyone can submit a proposal to DAO
⇒ participants vote



Examples:

art collector DAOs, charity DAOs, investment DAOs

Examples

Creating a DAO is quite simple: syndicate.io

... cheaper than creating a real-world U.S. partnership

Example DAOs:

- **PleasrDAO**: invests in digital art (NFTs),
30 pieces collected, treasury of \$26M
- **Gitcoin**: DAO to fund open source projects (\$36M sent)
- Investment DAOs: many

Regulation? Next lecture ...