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
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

- Deposit assets
- Deposit interest
- Borrow
- Borrow interest

Bank spread
(borrow interest – deposit interest)
The role of banks in the economy

Alice will get her deposit back either way

Bank assumes the risk of Bob defaulting

deposit assets
withdraw deposit

borrow
repay loan

bank spread
(borrow interest – deposit interest)
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

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

⇒ CeFi will absorb the loss

Solution: require Bob to lock up collateral

Borrow 1 ETH

CeFi deposits 500 UNI collateral

Interest deducted from collateral

Over collateralized loan

(1 ETH = 100 UNI)

debt position:

+ 500 UNI

− 1 ETH
The role of collateral

Several things can happen next:

1. **Bob repays loan**

   - **CeFi** repays 1 ETH
     - 1 ETH = 100 UNI
     - Debt position:
       - + 500 UNI
       - − 1 ETH

   - Redeem UNI collateral (minus interest)
The role of collateral

Several things can happen next:

(1) Bob repays loan
(2) Bob defaults on loan

CeFi

I can’t repay 1 ETH

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

(1 ETH = 100 UNI)

Ok, I’ll keep
(100 + penalty) UNI

debt position:
+ 500 UNI
− 1 ETH
The role of collateral

Several things can happen next:

1. Bob repays loan
2. Bob defaults on loan
3. Liquidation: value of loan increases relative to collateral

CeFi

I need to liquidate your collateral (and charge a penalty = 20 UNI)

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

Debt position:
+ 80 UNI
− 0 ETH

(1 ETH = 400 UNI)
**Terminology**

**Collateral**: assets that serve as a security deposit

**Over-collateralization**: borrower has to provide

\[value(\text{collateral}) > value(\text{loan})\]

**Under-collateralization**: \[value(\text{collateral}) < value(\text{loan})\]

**Liquidation**: if \[value(\text{debt}) > 0.6 \times value(\text{collateral})\] then collateral is liquidated until inequality flips (liquidation reduces both sides of the inequality)
Collateral factor

**CollateralFactor** ∈ [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

\[ \text{BorrowCapacity} = \sum_{i} \text{value(collaral}_{i}) \times \text{CollateralFactor}_{i} \]  
(in ETH)

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

\[ \text{health} < 1 \Rightarrow \text{triggers liquidation until (health} \geq 1) \]
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.

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 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)
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

Supply Assets ➔ Receive Interest

Supply Assets ➔ Receive Interest

Supply Assets ➔ Receive Interest

BORROWERS

Supply Collateral ➔ Borrow Assets ➔ Pay Interest

Supply Collateral ➔ Borrow Assets ➔ Pay Interest

Supply Collateral ➔ Borrow Assets ➔ Pay Interest

(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

Liquidity Providers (earn interest) → supply assets → Compound/Aave Dapps gather liquidity → supply assets → borrowers

Supply assets: DAI, ETH, UNI, AXS
Example: Compound cTokens

Liquidity Provider

supply assets

10 ETH, 1000 DAI, 500 UNI

mints cTokens for Alice (ERC-20)

X cETH, Y cDAI, Z cUNI

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

4 markets

DAI
ETH
UNI
AXS

Compound
Borrowers

4 markets

- DAI
- ETH
- UNI
- AXS

Bob’s accrued interest increases ETH/cETH exchange rate

⟹ benefit cETH token holders (ETH liquidity providers)

I want to borrow ETH

Bob’s cTokens are locked up as collateral

Compound sends ETH to Bob

supply assets to any market

get cTokens

Compound
Consider the ETH marker:

- **Supplying ETH:** adds to \(\text{UnderlyingBalance}_{\text{ETH}}\)
- **Borrowing ETH:** adds to \(\text{totalBorrowBalance}_{\text{ETH}}\)
- **Interest:** added repeatedly to \(\text{totalBorrowBalance}_{\text{ETH}}\)

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

\[\implies \text{As } \text{totalBorrowBalance} \text{ increases so does } \text{ExchangeRate}\]
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

interestRate\_ETH = BaseRate\_ETH + U\_ETH \times \text{slope\_ETH}

higher \( U_{ETH} \in [0,1] \)
Example: Compound DAI market

- **Current Utilization:** 60%
- **borrow APY at 60% utilization:** 3.82%
- **deposit APY at 60% utilization:** 1.93%

<table>
<thead>
<tr>
<th>Market Liquidity</th>
<th>377,443,771 DAI</th>
</tr>
</thead>
<tbody>
<tr>
<td># of Suppliers</td>
<td>18,468</td>
</tr>
<tr>
<td># of Borrowers</td>
<td>2,750</td>
</tr>
<tr>
<td>Collateral Factor</td>
<td>83%</td>
</tr>
<tr>
<td>cDAI Minted</td>
<td>26,810,077,978</td>
</tr>
<tr>
<td>Exchange Rate</td>
<td>1 DAI = 45.26986803778856 cDAI</td>
</tr>
</tbody>
</table>

(Oct. 2022)
**Liquidation:** debt > 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: debt > 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]

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:

**Compund outstanding debt**

(Oct. 2022) $802M
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

“Attacking the DeFi Ecosystem with Flash Loans for Fun and Profit”
Use cases

• Risk free arbitrage
• Collateral swap
• DeFi attacks: price oracle manipulation
Alice finds a USDC/DAI price difference in two pools

Risk free arbitrage

Aave (flash loan provider)

Flash loan 1M USDC

Uniswap
USDC → DAI

1USDC = 1.002DAI

1M USDC → 1.002M DAI

1.002M DAI → 1.001M USDC

Rely 1M USDC loan

Curve
DAI → USDC

1USDC = 1.001DAI

1.002M DAI → 1.001M USDC

keep 0.001M USDC

All in a single transaction
Collateral swap

start:
Alice @Compound

borrowed DAI using ETH as collateral
-1000 DAI
+1 cETH

end goal:
Alice @Compound

borrowed DAI using USDC as collateral
-1000 DAI
+3000 cUSDC

(a single Ethereum transaction)

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
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");
}
## Top 5 Days - Loan Amount

<table>
<thead>
<tr>
<th>Date</th>
<th>FLASHLOAN_USD</th>
</tr>
</thead>
<tbody>
<tr>
<td>May 22</td>
<td>624.5M</td>
</tr>
<tr>
<td>May 5</td>
<td>520.9M</td>
</tr>
<tr>
<td>May 21</td>
<td>515.0M</td>
</tr>
<tr>
<td>May 19</td>
<td>265.7M</td>
</tr>
<tr>
<td>Aug 3</td>
<td>163.7M</td>
</tr>
</tbody>
</table>
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)

3. **DAOs**: decentralized organizations
Digital assets (NFTs)

Example digital assets: (ERC-721)
- Digital art: opensea, foundation
- Collector items: NBA top shots
- Game items: horses (zed.run), axies, ...
- Metaverse: plots in a virtual land

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)
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  
<table>
<thead>
<tr>
<th></th>
<th></th>
</tr>
</thead>
<tbody>
<tr>
<td>CryptoPunks</td>
<td>1,017.69</td>
</tr>
<tr>
<td>CreatureToadz</td>
<td>916.15</td>
</tr>
<tr>
<td>CyberKongz</td>
<td>892.68</td>
</tr>
<tr>
<td>Doodles</td>
<td>730.72</td>
</tr>
</tbody>
</table>

## 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)

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

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