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

- 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

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)

Collateral

Debt position:

+ 500 UNI

− 1 ETH
The role of collateral

Several things can happen next:

(1) Bob repays loan

CeFi

repay 1 ETH

redeem UNI collateral (minus interest)

(1 ETH = 100 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

I can’t repay 1 ETH
redeem remaining UNI collateral
(400 - interest - penalty) UNI

CeFi

I’ll keep (100 + penalty) UNI

(1 ETH = 100 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)

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

(1 ETH = 400 UNI)

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

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

**Liquidation**: if \[
\text{value(debt)} > 0.6 \times \text{value(collateral)}
\]
then collateral is liquidated until inequality flips
(liquidation reduces both sides of the inequality)
Collateral Factor $\in [0,1]$

- 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: 75%,
- UNI: 60%,
- YFI: 35%
Health of a debt position

BorrowCapacity = \sum_i \text{value}(\text{collateral}_i) \times \text{CollateralFactor}_i
\quad \text{(in ETH)}

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

health < 1 \implies \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 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)
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

**BORROWERS**
- 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) -> Compound/Aave Dapps gather liquidity

supply assets

DAI ETH UNI AXS

supply assets

borrowers
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 an exchange rate:
Token to cToken exchange rate is calculated every block

4 markets

DAI  ETH

UNI  AXS

Compound
Borrowers

I want to borrow ETH

Bob’s cTokens are locked up as collateral

Compound sends ETH to Bob

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 UnderlyingBalance_{ETH}
Borrowing ETH: adds to totalBorrowBalance_{ETH}
Interest: added repeatedly to totalBorrowBalance_{ETH}

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

⇒ As 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 \( U_{ETH} \in [0,1] \)

\( \text{interestRate}_{ETH} = \text{BaseRate}_{ETH} + U_{ETH} \times \text{slope}_{ETH} \)
Example: Compound ETH market

- Borrow APY at 40% utilization: 4.45%
- Supply APY at 40% utilization: 2.21%

<table>
<thead>
<tr>
<th>Market Liquidity</th>
<th>1,499,627 ETH</th>
</tr>
</thead>
<tbody>
<tr>
<td># of Suppliers</td>
<td>68607</td>
</tr>
<tr>
<td># of Borrowers</td>
<td>1260</td>
</tr>
<tr>
<td>Collateral Factor</td>
<td>75%</td>
</tr>
<tr>
<td>cETH Minted</td>
<td>78,227,475</td>
</tr>
<tr>
<td>Exchange Rate</td>
<td>1 ETH = 49.86243030285714 cETH</td>
</tr>
</tbody>
</table>
**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:

```
liquidate(address of borrower, CollateralAsset, BorrowAsset, uint amount)
```

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

[at a discounted exchange rate -- penalty for user]
What is liquidation risk?

Historical DAI interest rate on Compound (APY):

APY shoots up temporarily
→ 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:
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
Risk free arbitrage

Alice finds a USDC/DAI price difference in two pools

Aave (flash loan provider)

Flash loan 1M USDC

Repay 1M USDC loan

Uniswap
USDC→DAI

1USDC = 1.002DAI

1M USDC

1.002M DAI

1.001M USDC

Curve
DAI→USDC

1USDC = 1.001DAI

keep 0.001M USDC

All in a single transaction
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)

<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>
Next lecture: U.S. blockchain regulations