

DeFi and the Future of Finance:

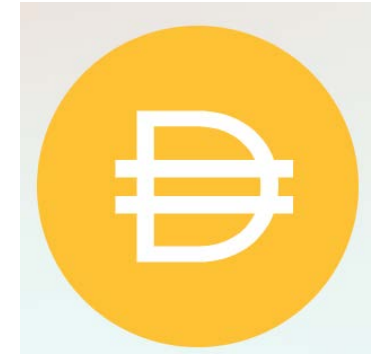
5. DeFi Deep Dive

Campbell R. Harvey
Duke University and NBER

Outline

- Credit/Lending
 - MakerDAO; Compound; Aave
- Decentralized Exchange
 - Uniswap
- Derivatives
 - Yield protocol, dYdX, Synthetix
- Tokenization
 - Set protocol, wBTC

Credit/Lending: MakerDAO



Background

- As the name suggests, MakerDAO is a decentralized autonomous organization.
- The primary value-add is the creation of a crypto-collateralized stablecoin, pegged to USD called DAI. This means the system can run completely from within the Ethereum blockchain without relying on outside centralized institutions to back, vault and audit the stablecoin.
- Two token model: DAI = stablecoin and MKR = governance token

Credit/Lending: MakerDAO

Mechanics of DAI

- DAI is generated as follows. A user can deposit ETH or other supported ERC-20 assets into a *Vault*.
- A Vault is a smart contract that escrows collateral and keeps track of the USD-denominated value of the collateral.
- The user can then mint DAI up to a certain collateralization ratio on their assets.
- This creates a “debt” in DAI that must be paid back by the Vault holder.

Credit/Lending: MakerDAO

Mechanics of DAI

- The DAI is the corresponding asset that can be used any way the Vault holder wishes.
 - Example 1: user can sell the DAI for cash
 - Example 2: user can use DAI to buy more of the collateral asset, and repeat the process, to create a levered position.
- Due to the volatility of ETH and most collateral types, the collateralization requirement is far in excess of 100% and usually in the 150-200% range.

Credit/Lending: MakerDAO

Collateralized debt position (CDP)

- The basic idea is not new; a homeowner in need of some liquidity can pledge their house as collateral to a bank and receive a mortgage loan structured to include a cash takeout.
- The price volatility of ETH is much greater than for a house and, as such, collateralization ratios for the ETH-DAI contract are higher.
- In addition, no centralized institution is necessary as everything happens within the Ethereum blockchain.

Credit/Lending: MakerDAO

Example

- Suppose an ETH owner needs liquidity but does not want to sell her ETH because she thinks it will appreciate.
- The situation is analogous to the homeowner who needs liquidity but does not want to sell her house.

Credit/Lending: MakerDAO

Example

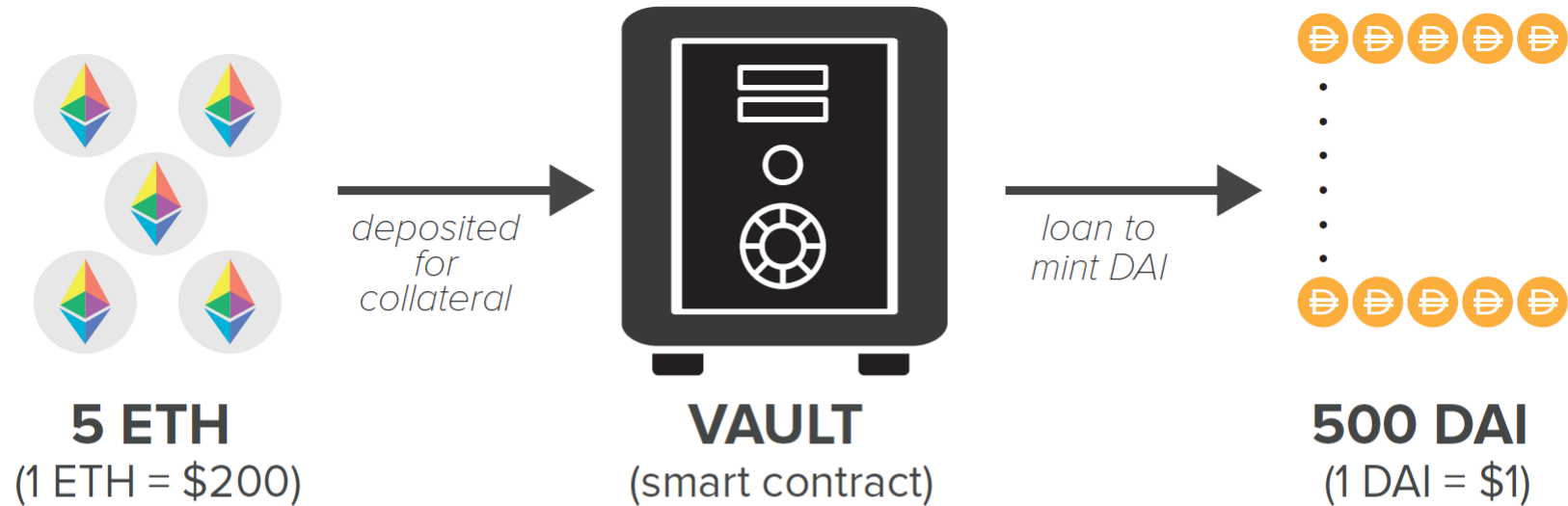
- Let's say an investor has 5 ETH at a market price of \$200 (total value of \$1,000).
- If the collateralization requirement is 150%, then the investor can mint up to 667 DAI ($\$1,000/1.5$ with rounding).
- The collateralization ratio is set high to reduce the probability that the loan debt exceeds the collateral value, and for the DAI token to be credibly pegged to the USD, the system needs to avoid the risk that the collateral is worth less than \$1=1 DAI.

Credit/Lending: MakerDAO

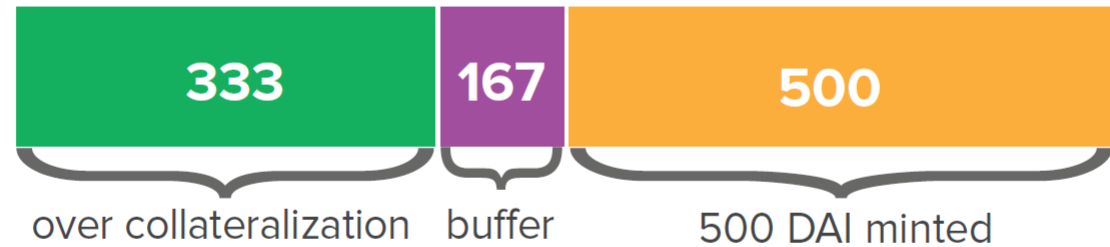
Example

- Given the collateralization ratio of 1.5, it would be unwise to mint the 667 DAI because if the ETH ever dropped below \$200, the contract would be undercollateralized, the equivalent of a “margin call”.
- We are using traditional finance parlance, but in DeFi there is no communication from your broker about the need to post additional margin or to liquidate the position and also no grace period.
- Liquidation can happen immediately.

Credit/Lending: MakerDAO



VALUE of COLLATERAL (5 ETH) = \$1000



collateralization factor: **150%**

maximum loan: **$1000/1.5 = 667$ DAI**

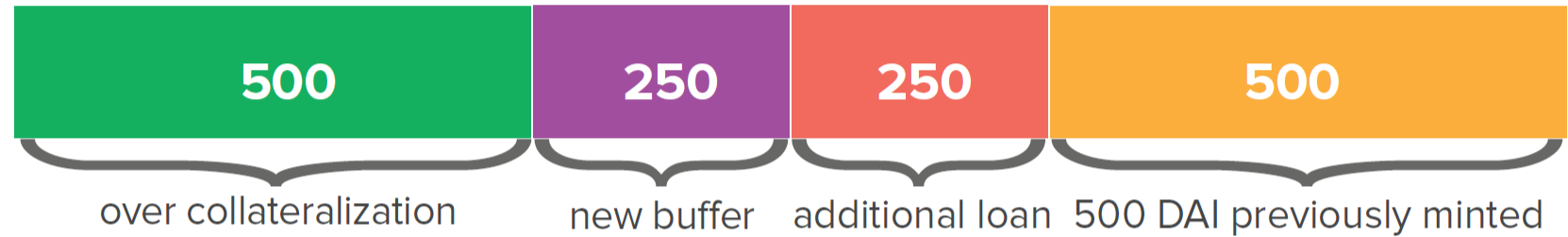
actual loan: **500 DAI**

Credit/Lending: MakerDAO

Scenario 1

ETH appreciates 50% \$200 → \$300

VALUE of COLLATERAL (5 ETH) = \$1500



collateralization factor: **150%**

maximum loan: **$1500/1.5 = 1000$ DAI**

actual loan: **500 DAI** → (ratio now 300%)

additional loan: **250 DAI**

new loan: **750 DAI** → (ratio 200%)

- Suppose ETH rises by 50% so collateral is worth \$1,500.
- The investor can increase the size of her loan.
- To maintain the collateralization of 200%, the investor can mint an extra 250 DAI.

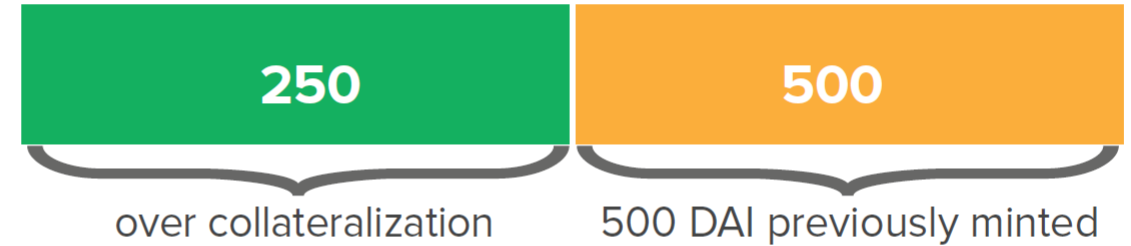
Credit/Lending: Scenario 2

MakerDAO

- Suppose the value of the ETH drops by 25% from \$200 to \$150.
- In this case, the value of the collateral drops to \$750 and the collateralization ratio drops to 1.5 ($\$750/1.5 = 500$).

ETH depreciates 25% \$200 → \$150

VALUE of COLLATERAL (5 ETH) = \$750



collateralization factor: **150%**

maximum loan: **$750/1.5 = 500$ DAI**

actual loan: **500 DAI** → (ratio now 150%)

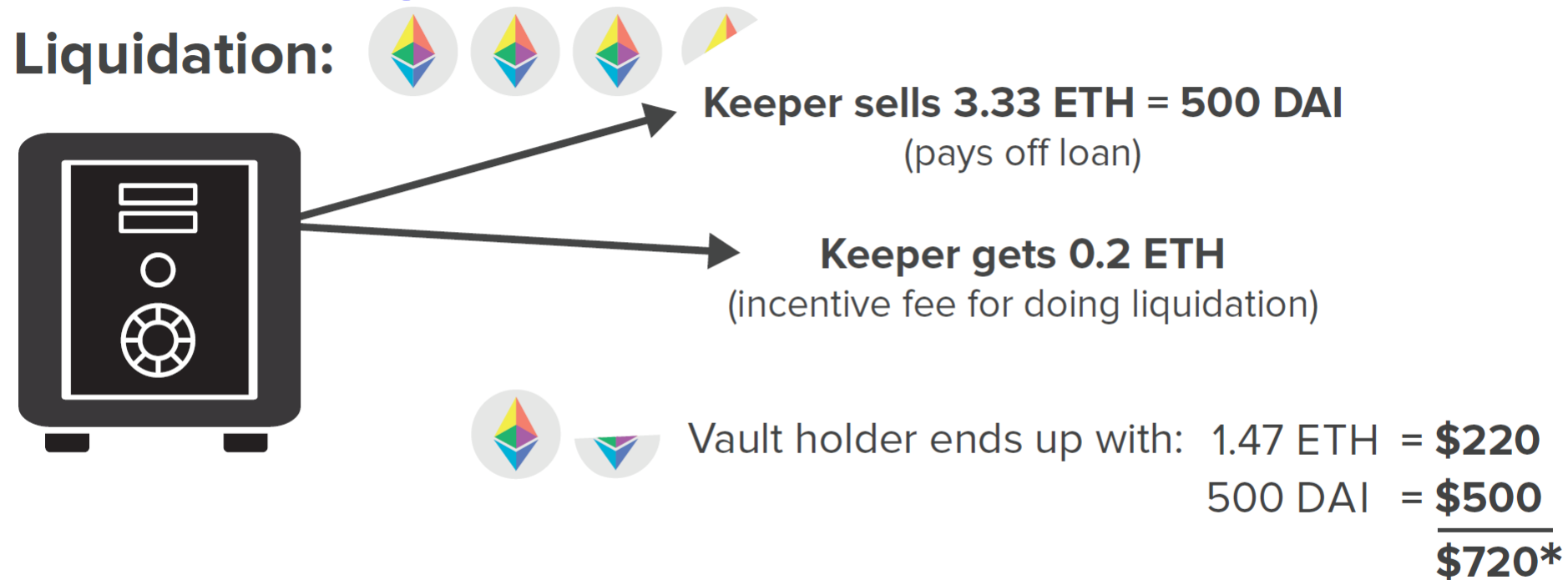
Credit/Lending: MakerDAO

Example

Suppose the value of the ETH drops by 25% from \$200 to \$150.

- The Vault holder faces three scenarios.
 1. She can increase the amount of collateral in the contract (by, for example, adding 1 ETH).
 2. She can use the 500 DAI to pay back the loan and repatriate the 5 ETH. These ETH are now worth \$250 less, but the depreciation in value would have happened irrespective of the loan.
 3. The loan is liquidated by a *keeper* (any external actor).

Credit/Lending: MakerDAO



** Abstracts from gas fees*

- The keeper auctions the ETH for enough DAI to pay off the loan.
- 3.33 ETH are sold and 1.47 ETH returned to the Vault holder.
- Keeper gets incentive fee of 0.2 ETH
- Vault holder has 500 DAI worth \$500 and 1.47 ETH worth \$220.

Credit/Lending: MakerDAO

Stability forces

- Two forces in this process reinforce the stability of DAI.
 1. Overcollateralization.
 2. Market actions. In the liquidation, ETH are sold and DAI are purchased, which exerts positive price pressure on DAI.

Credit/Lending: MakerDAO

Maintaining the Peg

- The viability of the MakerDAO ecosystem critically depends on DAI maintaining a 1:1 peg to the USD.
- Various mechanisms are in place to incentivize demand and supply in order to drive the price toward the peg.
- The primary mechanisms are: the debt ceiling, stability fee, and DAI Savings Rate (DSR).
- These parameters are controlled by holders of the governance token Maker (MKR) and MakerDAO governance.



Credit/Lending: MakerDAO

Stability fee

- The Stability Fee is a variable interest rate paid in DAI by Vault holders on any DAI debt they generate.
- The interest rate can be raised or lowered (even to a negative value) to incentivize the generation or repayment of DAI to drive its price toward the peg.

Credit/Lending: MakerDAO

DAI Savings Rate (DSR)

- The Stability Fee funds the DSR, a variable rate any DAI holder can earn on their DAI deposit.
- The DSR compounds on a per-block basis. The Stability Fee, which must always be greater or equal to the DSR, is enforced by the smart contracts powering the platform.

Credit/Lending: MakerDAO

DAI Debt Ceiling

- Lastly, a smart contract–enforced DAI debt ceiling can be adjusted to allow for more or less supply to meet the current level of demand.
- If the protocol is at the debt ceiling, no new DAI is able to be minted in new Vaults until the old debt is paid or the ceiling is raised.

Credit/Lending: MakerDAO

Liquidation

- When a position is deemed to be under the liquidation ratio, a keeper can initiate an auction (sell some of the ETH collateral) to liquidate the position and close the Vault holder's debt.
- The *Liquidation Penalty* is calculated as a percentage of the debt and is deducted from the collateral in addition to the amount needed to close the position.

Credit/Lending: MakerDAO

Large drops in the value of collateral

- If the collateral drops so far in value that the DAI debt cannot be fully repaid, the position is closed, and the protocol accrues what is known as *Protocol Debt*.
- A buffer pool of DAI exists to cover Protocol Debt, but in certain circumstances the debt can be too great for even the buffer pool to cover.
- The solution involves the governance token MKR and the governance system.

Credit/Lending: MakerDAO

Governance

- The MKR token controls MakerDAO.
- Holders of the token have the right to vote on protocol upgrades, including supporting new collateral types and tweaking parameters such as collateralization ratios.
- MKR holders are expected to make decisions in the best financial interest of the platform.
- Their incentive is that a healthy platform should increase the value of their share in the platform's governance.

Credit/Lending: MakerDAO

Global settlement

- For example, poor governance could lead to a situation where the buffer pool is not sufficient to pay back the Protocol Debt.
- In this case, newly minted MKR tokens are auctioned off in exchange for DAI and the DAI are used to pay back the Protocol Debt.
- This process is *Global Settlement*, a safety mechanism intended for use only when all other measures have failed.
- Global Settlement dilutes the MKR share, which is why stakeholders are incentivized to avoid it and keep Protocol Debt to a minimum.

Credit/Lending: MakerDAO

Decisions of MKR holders

- Votes by the MKR holders can change any of the parameters available on the platform, e.g., supporting new collateral types for Vaults
- MKR holders could also vote to pay themselves a dividend funded by the spread between the interest payments paid by Vault holders and the DAI Savings Rate.
- The reward of receiving this dividend would need to be weighed against any negative community response that might decrease the value of the protocol and the MKR token.

Credit/Lending: MakerDAO

Why DAI is attractive

- Importantly, users can purchase and utilize DAI without having to go through the process of generating it in a Vault—they can simply purchase DAI on an exchange.
- Therefore, users do not need to know the underlying mechanics of how DAI are created.

Credit/Lending: MakerDAO

Why DAI is attractive

- Holders can easily earn the DAI Savings Rate by using the protocol.
- More technologically and financially sophisticated users can use the MakerDAO web portal to generate Vaults and create DAI to get liquidity from their assets without having to sell them.
- It is easy to sell DAI and purchase an additional amount of the collateral asset to get leverage.

Credit/Lending: MakerDAO

Drawback of DAI

- DAI supply is always constrained by demand for ETH-collateralized debt.
- No clear arbitrage loop exists to maintain the peg.
- For example, the stablecoin USDC is always redeemable by Coinbase for \$1, with no fees. Arbitrageurs have a guaranteed (assuming solvency of Coinbase) strategy in which they can buy USDC at a discount or sell it at a premium elsewhere and redeem on Coinbase.
- This is not true for DAI. Irrespective of any drawbacks, the simplicity of DAI makes it an essential building block for other DeFi applications.

Credit/Lending: MakerDAO

Traditional Finance Problem	MakerDAO Solution
<i>Centralized Control:</i> Interest rates are influenced by the US Federal Reserve and access to loan products controlled by regulation and institutional policies.	MakerDAO platform is openly controlled by the MKR holders.
<i>Limited Access:</i> Obtaining loans is difficult for a large majority of the population.	Open ability to take out DAI liquidity against an overcollateralized position in any supported ERC-20 token. Access to a competitive USD-denominated return in the DSR.
<i>Inefficiency:</i> Acquiring a loan involves costs of time and money.	Instant liquidity at the push of a button with minimal transaction costs.
<i>Lack of Interoperability:</i> Cannot trustlessly use USD or USD-collateralized token in smart contract agreements.	Issuance of DAI, a permissionless USD-tracking stablecoin backed by cryptocurrency. DAI can be used in any smart contract or DeFi application.
<i>Opacity:</i> Unclear collateralization of lending institutions.	Transparent collateralization ratios of vaults visible to entire ecosystem.

Credit/Lending: Compound



What is Compound?

- Compound is a lending market that offers several different ERC-20 assets for borrowing and lending.
- All the tokens in a single market are pooled together so every lender earns the same variable rate and every borrower pays the same variable rate.

Credit/Lending: Compound

Overcollateralization

- The concept of a credit rating is irrelevant, and because Ethereum accounts are pseudonymous, enforcing repayment in the event of a loan default is virtually impossible.
- For this reason, all loans are overcollateralized in a collateral asset different from the one being borrowed.
- If a borrower falls below their collateralization ratio, their position is liquidated to pay back their debt.
- The debt can be liquidated by a keeper. The keeper receives a bonus.

Credit/Lending: Compound

Collateralization ratios and factors

- The collateralization ratio is calculated via a *collateral factor*.
- Each ERC-20 asset on the platform has its own collateral factor ranging from zero to 90.
- A collateral factor of zero means an asset cannot be used as collateral.
- The required collateralization ratio for a single collateral type is calculated as 100 divided by the collateral factor.

Credit/Lending: Compound

Collateralization ratios and factors

- Volatile assets generally have lower collateral factors, which mandate higher collateralization ratios due to increased risk of a price movement that could lead to undercollateralization.
- An account can use multiple collateral types at once, in which case the collateralization ratio is calculated as 100 divided by the weighted average of the collateral types by their relative sizes (denominated in a common currency) in the portfolio.

Credit/Lending: Compound

Collateralization ratio is like a reserve multiplier

- The collateralization ratio is similar to a reserve multiplier in traditional banking, constraining the amount of “borrowed” dollars that can be in the system relative to the “real” supply.
- For instance, there is occasionally more DAI in Compound than is actually supplied by MakerDAO, because users are borrowing and resupplying or selling to others who resupply.
- Importantly, all MakerDAO supply is ultimately backed by real collateral and there is no way to borrow more collateral value than has been supplied.

Credit/Lending: Compound

Example

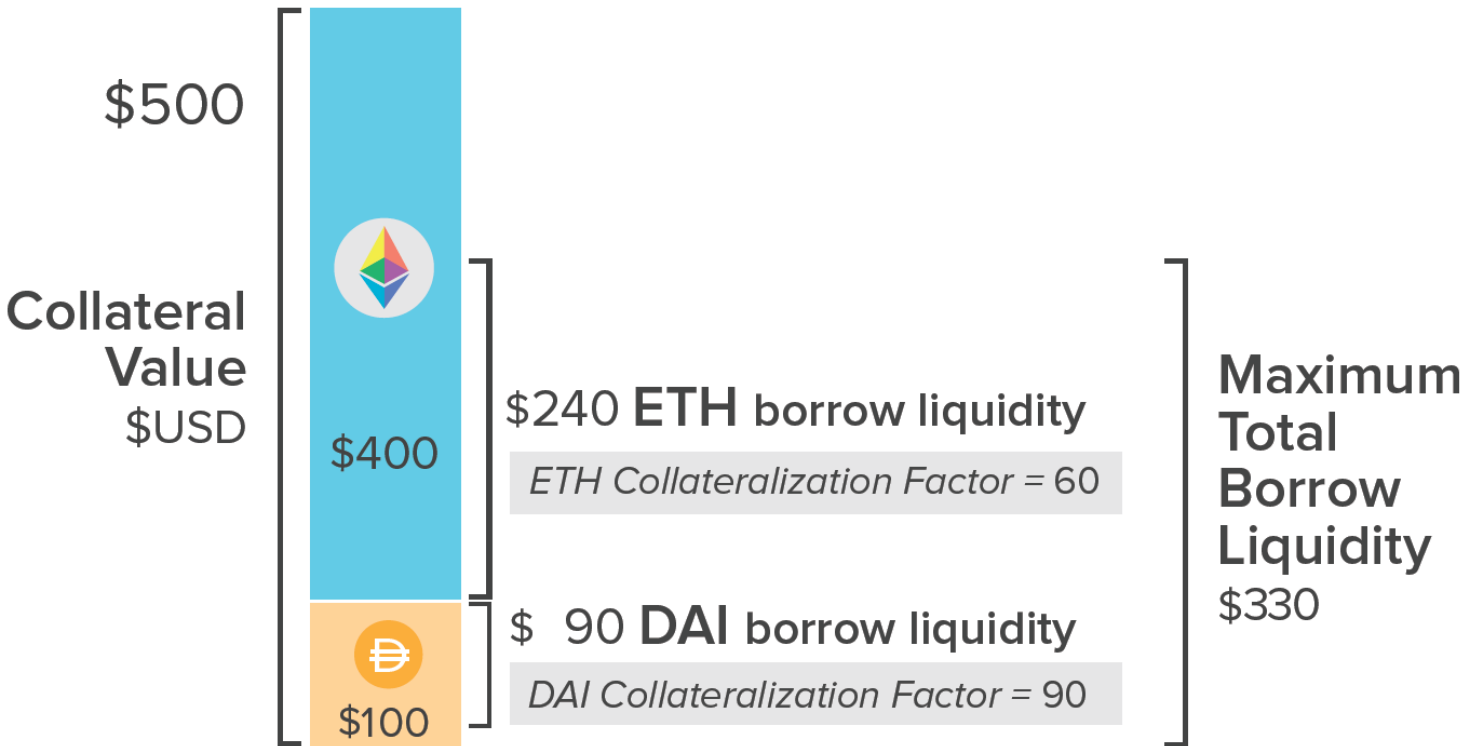
- An investor deposits 100 DAI with a collateral factor of 90.
- This transaction alone corresponds to a required collateralization ratio of 111%.
- Assuming 1 DAI = \$1, the investor can borrow up to \$90 worth of any other asset in Compound.

Credit/Lending: Compound

Example

- If she borrows the maximum, and the price of the borrowed asset increases at all, the position is subject to liquidation.
- Suppose she also deposits two ETH with a collateral factor of 60 and a price of \$200/ETH.
- The total supply balance is now \$500, with 80% being ETH and 20% being DAI. The required collateralization ratio is $100 / (0.8 * 60 + 0.2 * 90) = 151\%$.

Credit/Lending: Compound



Collateralization Ratio

$$= \frac{\$500 \text{ collateral}}{\$330 \text{ borrow liquidity}} = 151\%$$

Also calculated as
 $100 / (0.8 \times 60 + 0.2 \times 90)$

Credit/Lending: Compound

Supply and borrow rates

- The supply and borrow interest rates are compounded every block (approximately 15 seconds on Ethereum producing approximately continuous compounding) and are determined by the utilization percentage in the market.
- Utilization is calculated as total borrow/total supply.
- The utilization rate is used as an input parameter to a formula that determines the interest rates.
- The remaining parameters are set by *Compound Governance*.

Credit/Lending: Compound

Borrow rate formula

- The formula for the borrow rate generally is an increasing linear function with a y-intercept known as the *base rate* that represents the borrow rate at 0% borrow demand and a *slope* representing the rate of change of the rates.
- These parameters are different for each ERC-20 asset supported by the platforms.

Credit/Lending: Compound

Borrow rate formula

- Some markets have more advanced formulas that include a *kink*. A kink is a utilization ratio beyond which the slope steepens.
- These formulas can be used to reduce the cost of borrowing up to the kink and then increase the cost of borrowing after the kink to incentivize a minimum level of liquidity.

Credit/Lending: Compound

Supply interest rate formula

- Supply interest rate = (borrow interest rate x utilization ratio)
so borrow payments can fully cover the supplier rates.
- The reserve factor is a percentage of the borrow payments not given to the suppliers and instead set aside in a reserve pool that acts as insurance in that case a borrower defaults.
- In an extreme price movement, many positions may become undercollateralized in that they have insufficient funds to repay the suppliers. In the event of such a scenario, the suppliers would be repaid using the assets in the reserve pool.

Credit/Lending: Compound

Example

- In the DAI market, 100 million is supplied and 50 million is borrowed.
- Suppose the base rate is 1% and the slope is 10%.
- At 50 million borrowed, utilization is 50%.
- The borrow interest rate is then calculated to be $0.5 * 0.1 + 0.01 = 0.06$ or 6%.
- The maximum supply rate (assuming a reserve factor of zero) would simply be $0.5 * 0.06 = 0.03$ or 3%.

Credit/Lending: Compound

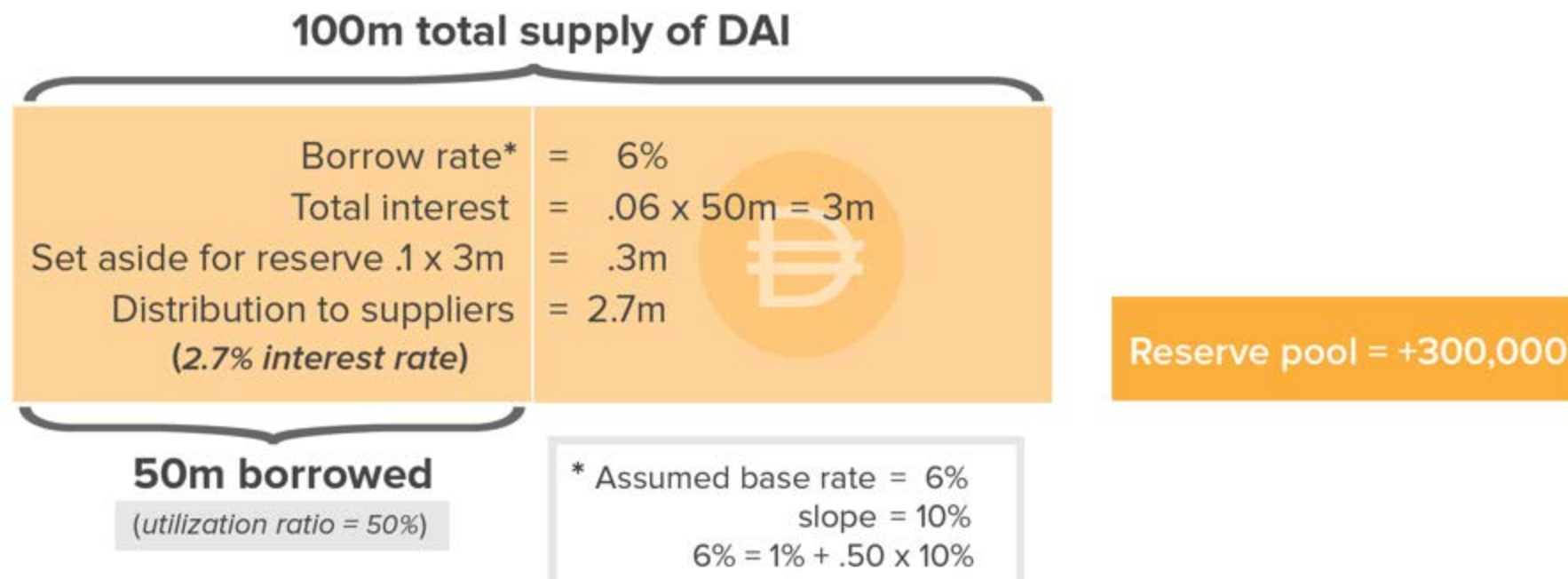
Example

- The borrow rate is not a marginal rate – it is a rate for all borrowers.
- For example, suppose an initial borrower does \$25 million. The rate would be $.25 * 0.1 + 0.01 = 3.5\%$.
- Then suppose another borrower enters the market with another \$25 million loan.
- The rate increases to 6% for all borrowers.

Credit/Lending: Compound

Example

- If the reserve factor is set to 10, then 10% of the borrow interest is diverted to a DAI reserve pool, lowering the supply interest rate to 2.7%. $0.5 * 0.06 * (1 - 0.10) = 0.027$ or 2.7%.



Credit/Lending: Compound

Example

- Another way to think about the supply interest rate is that the 6% borrow interest of 50 million is equal to 3 million of borrow payments.
- Distributing 3 million of payments to 100 million of suppliers implies a 3% interest rate to all suppliers. With 10% diverted (300,000), then there is on 2.7 million of payments

Credit/Lending: Compound

Example with kink

- Suppose 100 million DAI is supplied and 90 million DAI is borrowed, a 90% utilization.
- The kink is at 80% utilization, before which the slope is 10% and after which the slope is 40%, which implies the borrow rate will be much higher if the 80% utilization is exceeded.

Credit/Lending: Compound

Example with kink

- The base rate remains at 1%.
- The borrow interest rate = 0.01 (base) + $0.8 * 0.1$ (pre-kink) + $0.1 * 0.4$ (post-kink) = 13%.
- The supply rate (assuming a reserve factor of zero) is $0.9 * 0.13 = 11.7\%$.

Credit/Lending: Compound

Advantages of Compound

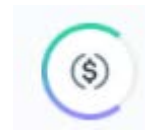
- Unlock value of asset without selling it – like a HELOC
- Easily engineer levered long or short positions
- Suppose you are bearish on price of ETH
 - Deposit stablecoin like USDC or DAI
 - Borrow ETH
 - Sell ETH for stablecoin
 - If price of ETH falls, you can use your stablecoin to buy (cheap) ETH to pay off debt

Credit/Lending: Compound

Advantages of Compound

- Levered positions are possible too
- Suppose you are bearish on price of ETH
 - Deposit stablecoin like USDC or DAI
 - Borrow ETH
 - Sell ETH for stablecoin
 - Deposit additional stablecoin from your sale
 - Borrow more ETH
 - Sell additional ETH for stablecoin
 - If price of ETH falls, you can use your stablecoin to buy (cheap) ETH to pay off debt

Credit/Lending: Compound



cTokens

- The Compound protocol must escrow tokens as a depositor in order to maintain that liquidity for the platform itself and to keep track of each person's ownership stake in each market.
- A naive approach would be to keep track of the number inside a contract.
- A better approach would be to tokenize the user's share.
- Compound does this using a cToken, and this is one of the platform's important innovations.

Credit/Lending: Compound

cTokens are minted and burned

- Compound's cToken is an ERC-20 in its own right that represents an ownership stake in the underlying Compound market.
- For example, cDAI corresponds to the Compound DAI market and cETH corresponds to the Compound ETH market.
- Both tokens are minted and burned in proportion to the funds added and removed from the underlying market as a means to track the amount belonging to a specific investor.

Credit/Lending: Compound

cTokens can be traded

- Given interest payments continually accrue to suppliers, these tokens are always worth more than the underlying asset.
- cTokens can be traded on their own like a normal ERC-20 asset.
- Other protocols can seamlessly integrate with Compound simply by holding cTokens and allows users to deploy their cTokens directly into other opportunities, such as using a cToken as collateral for a MakerDAO Vault.
- Instead of using ETH only as collateral, an investor can use cETH and earn lending interest on the ETH collateral.

Credit/Lending: Compound

Example

- Assume there are 2,000 DAI in the Compound DAI market and a total 500 cDAI represents the ownership in the market; this ratio of cDAI to DAI is not determinative and could just as easily be 500,000 cDAI.



Credit/Lending: Compound

Example

- If a trader comes in and deposits 1,000 DAI, the supply increases by 50% (and Compound mints 50% or 250 cDAI)



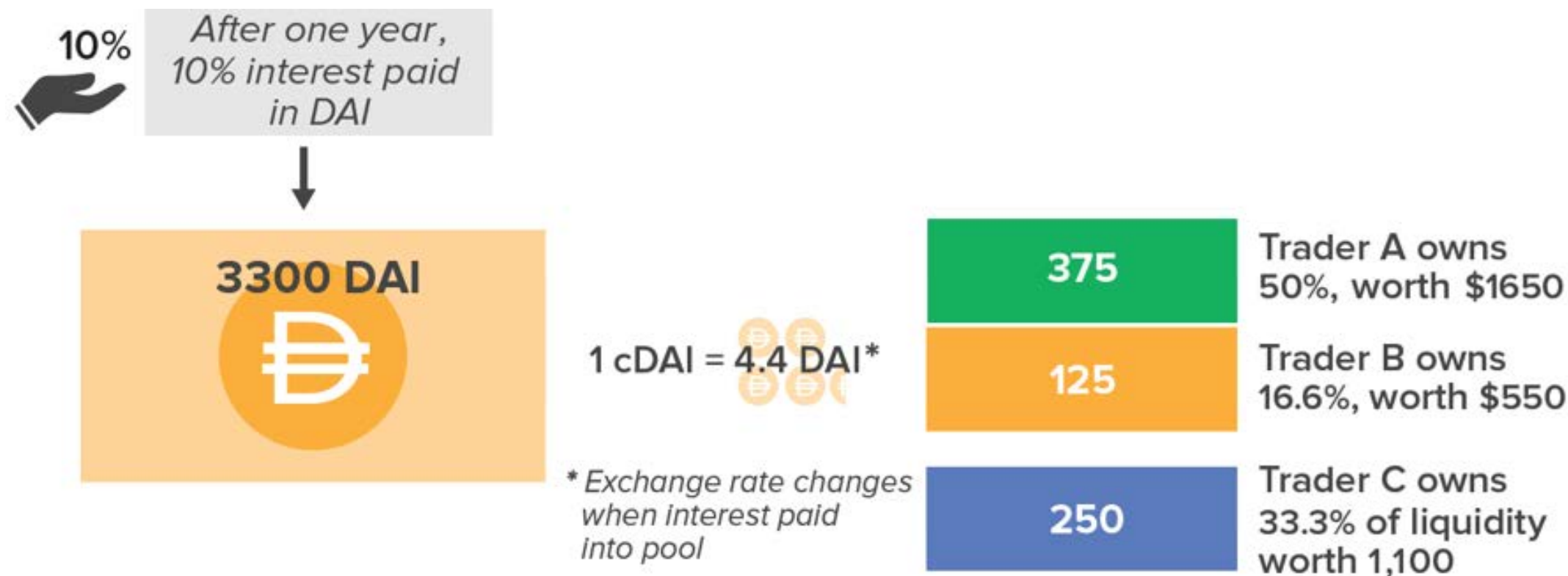
1 cDAI = 4 DAI



Credit/Lending: Compound

Example

- Currently, 1 cDAI = 4 DAI, but after interest accrues the ratio will change. Let interest = 10%, at year end, 3,300 DAI. Trader redeems 250 cDAI for 1,100 DAI



Credit/Lending: Compound

Example

- Note that the trader can deploy cDAI in the place of DAI so the DAI is not sitting idle but earning interest via the Compound pool.
- For example, the trader could deploy cDAI as the necessary collateral to open a perpetual futures position on dYdX or she could market make on Uniswap using a cDAI trading pair (discussed later).

Credit/Lending: Compound

Governance parameters

- The many different parameters of Compound's functionality, such as the *collateral factor*, *reserve factor*, *base rate*, *slope*, and *kink*, can all be tuned.
- The entity capable of tuning these parameters is *Compound Governance*.
- Compound Governance has the power to change parameters, add new markets, freeze the ability to initiate new deposits or borrows in a market, and even upgrade some of the contract code itself.

Credit/Lending: Compound

Governance

- Importantly, Compound Governance cannot steal funds or prevent users from withdrawing.
- In the early stages of Compound's growth, governance was controlled by developer admins, similar to any tech startup.
- Technically, this meant that the first version of Compound was not fully decentralized

Credit/Lending: Compound



Governance parameters

- A strong development goal of Compound, as with most DeFi protocols, was to remove developer admin access and release the protocol to the leadership of a DAO via a governance token.
- The token allowed shareholders and community members to collectively become Compound Governance and propose upgrades or parameter tuning.
- A quorum agreement is required for any change to be implemented.
- The quorum rule is a majority of users each of whom holds with a minimum of 400,000 COMP (~4% of total eventual supply)

Credit/Lending: Compound

COMP token

- Compound implemented this new governance system in May 2020 via the COMP token.
- COMP is used to vote on protocol updates such as parameter tuning, adding new asset support, and functionality upgrades (similar to MKR for MakerDAO).
- On June 15, 2020, the [7th governance proposal](#) passed which provided for distributing COMP tokens to users of the platform based on the borrow volume per market.

Credit/Lending: Compound

COMP token

- The proposal offered an experience akin to a tech company giving its own stock to its users.
- The COMP token is distributed to both suppliers and borrowers, and acts as a subsidization of rates.

Credit/Lending: Compound

COMP token

- With the release of the token on public markets, COMP's market cap spiked to over \$2 billion.
- The price point of the distribution rate is so high that borrowing in most markets turned out to be profitable.
- This arbitrage opportunity attracted considerable volume to the platform, and the community governance has made and passed several proposals to help manage the usage.

Credit/Lending: Compound

Other platforms use Compound

- The Compound protocol can no longer be turned off and will exist on Ethereum as long as Ethereum exists.
- Other platforms can easily escrow funds in Compound to provide additional value to their users or enable novel business models.
- Easy, instant access to yield or borrow liquidity on different Ethereum tokens makes Compound an important platform in DeFi.

Credit/Lending: Compound

Fair lotteries

- [PoolTogether](#) is a no-loss lottery that deposits all user's funds into Compound, but pays the entire pool's earned interest to a single random depositor at fixed intervals.
- In most lotteries, 30-50% of the lottery sales are tagged for administrative costs and government or charitable use; hence, the expected value of investing \$1.00 in a lottery is \$0.50-\$0.70.
- In a no-loss lottery, all sales are paid out and the expected value is \$1.00.

Credit/Lending: Compound

Traditional Finance Problem	Compound Solution
<i>Centralized Control:</i> Borrowing and lending rates are controlled by institutions.	Compound rates are determined algorithmically and gives control of market parameters to COMP stakeholders incentivized to provide value to users.
<i>Limited Access:</i> Difficulty in accessing high-yield USD investment opportunities or competitive borrowing.	Open ability to borrow or lend any supported assets at competitive algorithmically determined rates (temporarily subsidized by COMP distribution).
<i>Inefficiency:</i> Suboptimal rates for borrowing and lending due to inflated costs.	Algorithmically pooled and optimized interest rates.
<i>Lack of Interoperability:</i> Cannot repurpose supplied positions for other investment opportunities.	Tokenized positions via cTokens can be used to turn static assets into yield-generating assets.
<i>Opacity:</i> Unclear collateralization of lending institutions.	Transparent collateralization ratios of borrowers visible to entire ecosystem.

Credit/Lending: Aave



What is Aave?

- Aave, launched in 2017, is a lending protocol similar to Compound.
- More tokens to supply and borrow are offered
- Importantly, the Aave lending and variable borrowing rates are more predictable, because unlike the volatile COMP token in Compound, no subsidy is involved.

Credit/Lending: Aave

Two markets

- The first is for more-conventional ERC-20 tokens similar to those of Compound, supporting assets such as ETH, USDC, and DAI.
- The second is specific to Uniswap UNI LP tokens (discussed later).
- For example, when a user deposits collateral into a Uniswap market, she receives an LP token as a *Liquidity Provider* that represents her ownership in the market.
- The LP tokens can be deposited in the Uniswap market on Aave to generate additional returns.

Credit/Lending: Aave

Flash loans

- Aave charges a fee of 9 basis points (bps) on the loan amount to execute a flash loan.
- The fee is paid to the asset pool and provides an additional return on investment to suppliers, because they each own a pro rata share of the pool.
- An important use case for flash loans is that they allow users quick access to capital as a means to refinance positions.

Credit/Lending: Aave

Example

- Assume the price of ETH is 200 DAI.
- A user supplies 100 ETH in Compound and borrows 10,000 DAI to lever up and purchase an additional 50 ETH, which the user also supplies to Compound.
- Suppose the borrow interest rate in DAI on Compound is 15% on Aave is 5%.
- The goal is to refinance the borrowing to take advantage of the lower rate offered on Aave, which is analogous to refinancing a mortgage, a long and costly process in centralized finance.

Credit/Lending: Aave

Example

- One option is to manually unwind each trade on Compound and re-do both trades on Aave to reconstruct the levered position, but this option is wasteful in terms of exchange fees and gas fees.
- A flash loan provides an attractive alternative

Credit/Lending: Aave

Example



- Take out a flash loan from Aave for 10,000 DAI,
- Use it to pay the debt on Compound,
- Withdraw the full 150 ETH from Compound
- Resupply to Aave, and (at 5% APR) against that collateral to repay the flash loan.
- The latter approach effectively skips the steps of exchanging ETH for DAI to unwind and rewind the leverage.

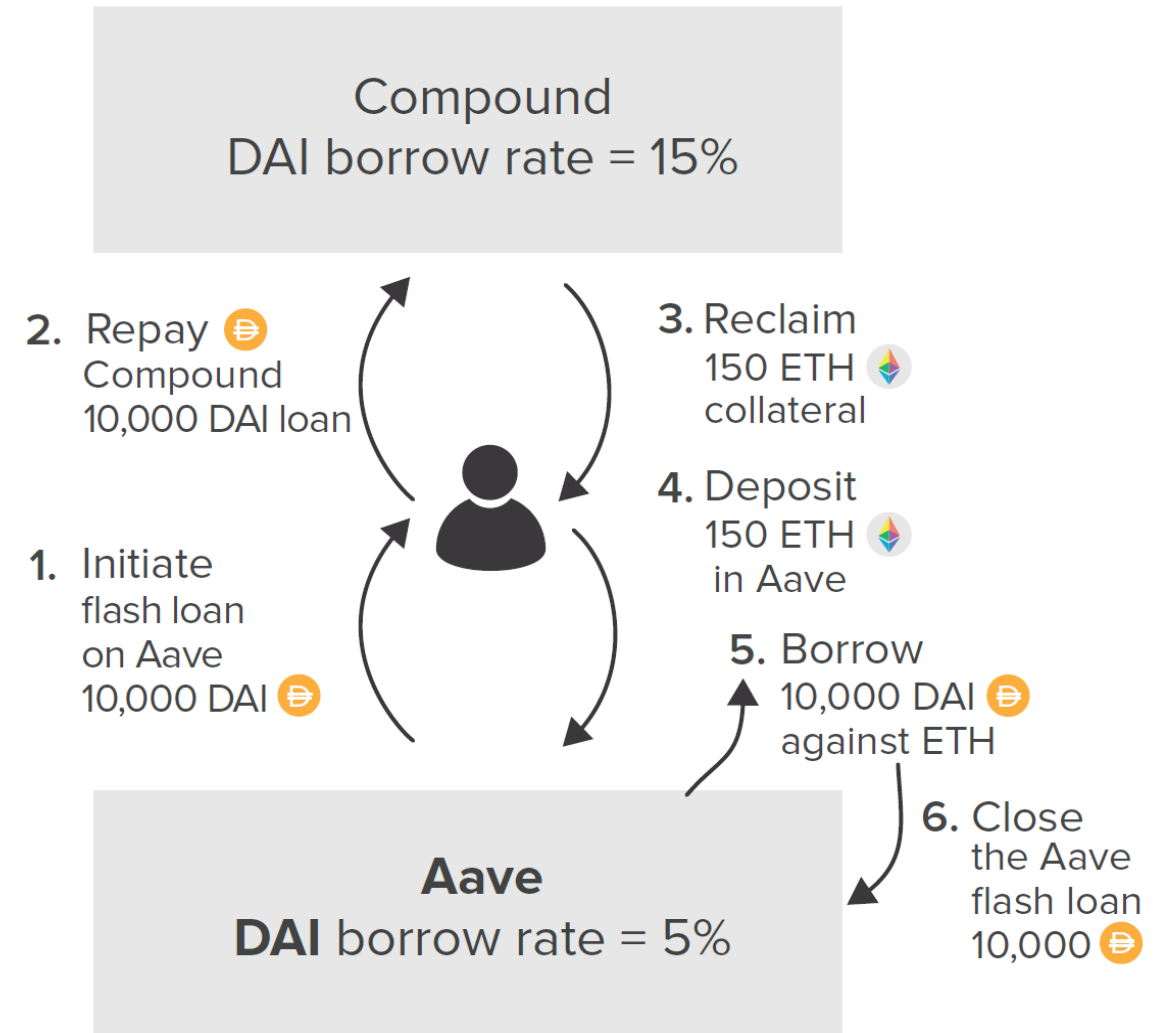
Credit/Lending: Aave

Example



- The flash loan is a single transaction
- A flash loan used to refinance a position allows for DeFi client applications that let users migrate a levered position from one dApp to another with the single push of a button.

Before

+ 150 ETH (collateral) 
– 10,000 DAI (loan)  at 15% interest



After

+ 150 ETH (collateral) 
– 10,000 DAI (loan)  at 5% interest

Credit/Lending: Aave

Stable loan rate

- An Aave innovation (and as of this writing only available on Aave) is a “stable” rate loan.
- The choice of “stable” intentionally avoids the use of “fixed rate.”
- A borrower has the option to switch between the variable rate and the current stable rate.

Credit/Lending: Aave

Supply rate is not stable

- The supply rate is always variable, because under certain circumstances, such as if all borrowers left the market, it would be impossible to fund a fixed supply rate.
- The suppliers always collectively earn the sum of the stable and variable borrow interest payments minus any fees to the platform.

Credit/Lending: Aave

Stable rate is not a fixed rate

- The stable rate is not a fixed rate, because the rate is adjustable in extreme liquidity crunches and can be refinanced to a lower rate if market conditions allow.
- Also, some constraints exist around how much liquidity can be removed at a specific stable rate.
- Algorithmic stable borrowing rates provide value to risk-averse investors who wish to take on leverage without the uncertainty of a variable-rate position.

Credit/Lending: Aave

Credit delegation

- Aave is developing a *Credit Delegation* feature in which users can allocate collateral to potential borrowers who can use it to borrow a desired asset.
- The process is unsecured and relies on trust.
- This process allows for uncollateralized loan relationships, such as in traditional finance, and potentially opens up new sources of liquidity.
- The credit delegation agreements will likely have fees and credit scores to compensate for the risk of unsecured loans.

Credit/Lending: Aave

Credit delegation

- The delegator has sole discretion to determine who is an eligible borrower and what contract terms are sufficient.
- Credit delegation terms can be mediated by a smart contract.
- The delegated liquidity can be given to a smart contract, and the smart contract can use the liquidity to accomplish its intended function.
- The underlying benefit of credit delegation is that all loans in Aave are ultimately backed by collateral, regardless of whose collateral it is.

Credit/Lending: Aave

Example

- A supplier has a balance of 40,000 DAI in Aave earning interest.
- The supplier wants to increase their expected return via an unsecured delegation of their collateral to a trusted counterparty.
- The supplier likely knows the counterparty through an off-chain relationship, perhaps it is a banking client.

Credit/Lending: Aave

Example

- The counterparty can proceed to borrow, for instance, 100 ETH with the commitment to repay the asset to the supplier plus an agreed-upon interest payment.
- The practical impact is that the external relationship is unsecured because no collateral is available to enforce payment; the relationship is based essentially on trust.

Credit/Lending: Aave

Summary

- Aave flash loans offer extra returns to suppliers (incentives liquidity)
- Attracts arbitrageurs and other applications that require flash liquidity
- Stable borrow rates are compelling
- Credit delegation allows loan providers to take their own collateral in the form of nonfungible Ethereum assets, perhaps tokenized art or real estate not supported by the main Aave protocol.

Credit/Lending: Aave

Traditional Finance Problem	Aave Solution
<i>Centralized Control:</i> Borrowing and lending rates controlled by institutions.	Aave interest rates are controlled algorithmically.
<i>Limited Access:</i> Only select groups have access to large quantities of money for arbitrage or refinancing.	Flash loans democratize access to liquidity for immediately profitable enterprises.
<i>Inefficiency:</i> Suboptimal rates for borrowing and lending due to inflated costs.	Algorithmically pooled and optimized interest rates.
<i>Lack of Interoperability:</i> Cannot monetize or utilize excess collateral in a lending position.	Credit delegation allows parties to use deposited collateral when they do not need borrowing liquidity.
<i>Opacity:</i> Unclear collateralization of lending institutions.	Transparent collateralization ratios of borrowers visible to the entire ecosystem.

Decentralized exchange: Uniswap

What is Uniswap?

- Prime example of Automated Market Maker on Ethereum
- Constant product rule, $k=x*y$ where x is the balance of asset A , and y the balance of asset B .
- The product k is the *invariant* and is required to remain fixed at a given level of liquidity. To purchase (withdraw) some x , some y must be sold (deposited). The implied price is x/y and is the *risk-neutral* price, because the contract is equally willing to buy or sell at this rate as long as invariant k is constant.

Decentralized exchange: Uniswap

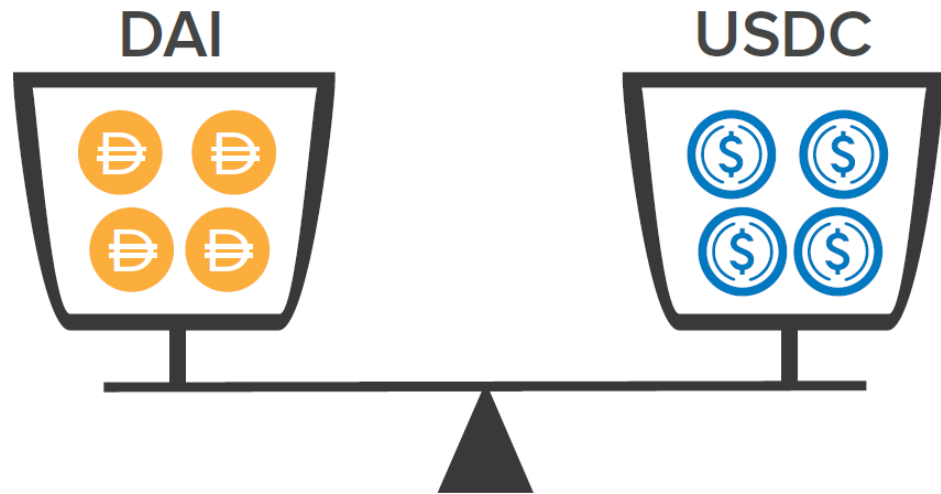
What is Uniswap?

- $k = x * y$ where x is the balance of asset A , and y the balance of asset B .
- To purchase (withdraw) some x , some y must be sold (deposited).
- The implied price is x/y and is the *risk-neutral* price, because the contract is equally willing to buy or sell at this rate as long as invariant k is constant.



Decentralized exchange: Uniswap

Example

- Investor in the Uniswap USDC/DAI market has 4 DAI (Asset A) and 4 USDC (Asset B). This sets the instantaneous exchange rate at 1 DAI:1 USDC and the invariant at 16 ($= x * y$).



Uniswap USDC/DAI Market

Instantaneous
exchange rate = 1  = 1 

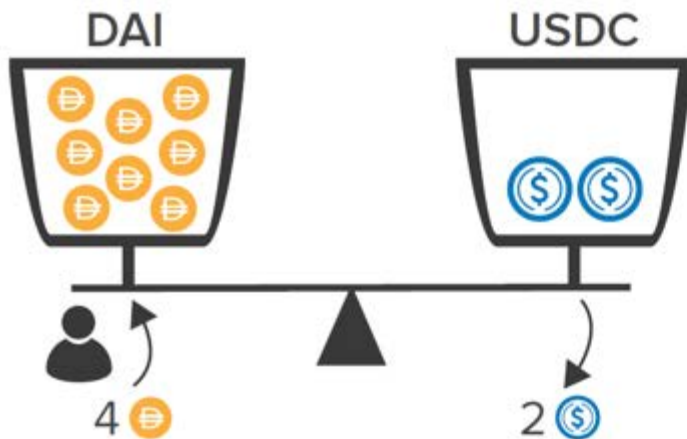
Invariant (K) = 4  x 4  = 16

Decentralized exchange: Uniswap

Example

- To sell 4 DAI for USDC, the investor deposits 4 DAI to the contract and withdraws 2 USDC. Now the USDC balance is $4 - 2 = 2$ and the DAI balance is $4 + 4 = 8$. Invariant remains at 16.

Exchange 4 DAI



Invariant = $K = 8 \text{ DAI} \times 2 \text{ USDC} = 16$

Hence, 4 DAI exchanged for 2 USDC

Decentralized exchange: Uniswap

Example

- Notice that the effective exchange rate was 2 DAI: 1 USDC.
- The change in the exchange rate is due to slippage because of the low level of liquidity in the market.
- The magnitude of the invariant determines the amount of slippage.

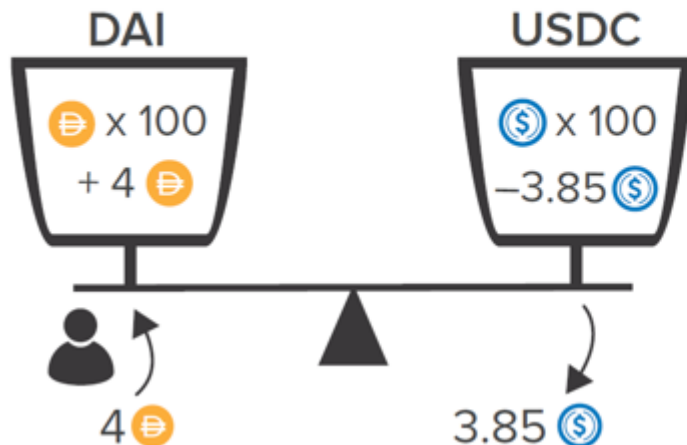
Decentralized exchange: Uniswap



Example

- Assume balance is 100 DAI and 100 USDC; $k=10,000$
- If investor sells 4 DAI for USDC, now 3.85 USDC can be withdrawn so much lower slippage at an effective rate of 1.04 DAI: 1 USDC.

Exchange 4 DAI



but contract has more liquidity, 100 DAI, 100 USDC



Instantaneous
exchange rate = 1  = 1 

Before $K = 100 \times 100 = 10,000$

After $K = 104 \times 96.15 = 10,000$

Implied price = 1.04  = 1 

Decentralized exchange: Uniswap

Importance of liquidity

- Deep liquidity helps minimize slippage.
- Therefore, Uniswap incentivizes depositors to supply capital to a given market.
- Anyone can become a liquidity provider by supplying assets on both sides of a market at the current exchange rate.
- A liquidity provider adds to both sides of the market, thereby increasing total market liquidity. If a user exchanges one asset for another, the total liquidity of the market as measured by the invariant does not change.

Decentralized exchange: Uniswap

Importance of liquidity

- Supplying both sides increases the product of the amount of assets held in the trading pair (i.e., increases the invariant).
- Higher invariants lead to lower slippage and therefore an increase in effective liquidity.
- The invariant as a direct measure of liquidity.
- In summary, liquidity providing increases the invariant with no effect on price, whereas trading against a market impacts the price with no effect on the invariant.

Decentralized exchange: Uniswap

Importance of liquidity

- Each trade in a Uniswap market has an associated 0.3% fee that is paid back into the pool.
- Liquidity providers earn these fees based on their pro rata contribution to the liquidity pool.
- They therefore prefer high-volume markets.
- This mechanism of earning fees is identical to the *cToken* model of Compound. The ownership stake is represented by a similar token called a *Uni* token. For example, the token representing ownership in the DAI/ETH pool is Uni DAI/ETH.

Decentralized exchange: Uniswap

Impermanent loss

- Liquidity providers in Uniswap essentially earn passive income in proportion to the volume on the market they are supplying.
- Upon withdrawal, however, the exchange rate of the underlying assets will almost certainly have changed.
- This raises the possibility of impermanent loss.

Decentralized exchange: Uniswap

Impermanent loss

- Impermanent loss is the amount of money the liquidity provider would have made if she just held the pair rather than invested in Uniswap pool.
- The fees earned from trading volume must exceed impermanent loss in order for liquidity providing to be profitable.
- Consequently, stablecoin trading pairs such as USDC/DAI are attractive for liquidity providers because the high correlation of the assets minimizes the impermanent loss.

Decentralized exchange: Uniswap

Pair correlation

- Uniswap's $k = x * y$ pricing model works well if the correlation of the underlying assets is unknown.
- The model calculates the exact same slippage at a given liquidity level for any two trading pairs. In practice, however, we would expect much lower slippage for a stablecoin trading pair than for an ETH trading pair, because we know by design that stablecoin's price should be close to \$1.

Decentralized exchange: Uniswap

Pair correlation

- The Uniswap pricing model leaves money on the table for arbitrageurs on high correlation pairs such as stablecoins, because it does not adjust default slippage lower, as would be expected; the profit is subtracted from the liquidity providers.
- For this reason, competitor AMMs, such as [Curve](#), that specialize in high-correlation trading pairs may cannibalize liquidity in these types of Uniswap markets.

Decentralized exchange: Uniswap

Any ERC-20 pair is possible on Uniswap

- Anyone can start an ERC-20/ERC-20 or ETH/ERC-20 trading pair on Uniswap, if the pair does not already exist, by simply supplying capital on both sides.
- ETH, although fungible, is not an ERC-20 token.
- Many platforms, including Uniswap, instead use [WETH](#), an ERC-20-wrapped version of ETH to get around this.
- Uniswap allows a user to directly supply and trade with ETH and it converts to WETH behind the scenes.

Decentralized exchange: Uniswap

Router contracts

- The user determines the initial exchange rate, and arbitrageurs should drive that price to the true market price if it deviates at all.
- Users of the platform can effectively trade any two ERC-20 tokens supported by using *router contracts* that determine the most efficient path of swaps in order to get the lowest slippage, if no direct trading pair is available.

Decentralized exchange: Uniswap

Front running

- A drawback of the AMM model is that it is particularly susceptible to front-running.
- This should not be confused with illegal front running that sometimes occurs in centralized finance (e.g., a company gets a big buy order and places some of their own trades before the buy order to benefit from the price appreciation from the market impact).
- All information is public in DeFi. So best thought of as “legal” front running.

Decentralized exchange: Uniswap

Front running

- When an Ethereum user posts a transaction to the memory pool, it is publicly visible to all Ethereum nodes.
- Front-runners can see this transaction and post a higher gas-fee transaction to trade against the pair before the user's transaction is added to a block, and then immediately trade in the reverse direction against the pair.
- This strategy allows a user to easily profit from large transactions, especially in illiquid markets with high slippage.

Decentralized exchange: Uniswap

Maximum slippage

- Uniswap allows users to set a maximum slippage as a clause in the transaction. If the level of slippage is exceeded, the trade will fail to execute.
- This is a smart contract level check.

Decentralized exchange: Uniswap

Maximum slippage

- In other words, before finalizing the trade, the contract checks the total slippage from the initially posted price to the effective execution price (which could have changed if other transactions made it in first like the described front running attempt).
- If this slippage exceeds the pre-defined user tolerance, the entire trade is cancelled and the contract execution fails.
- This provides a limit to the profit front-runners can make, but does not completely remove the problem.

Decentralized exchange: Uniswap

Arbitrageurs

- Another drawback is that arbitrage profits go only to arbitrageurs, who do not have a vested interest in the platform.
- The arbitrageurs profit at the expense of liquidity providers.
- Competing platforms, such as [Mooniswap](#), propose to solve this issue by supplying virtual prices that slowly approach the true price, leaving tighter time windows and lower spreads for arbitrageurs to capitalize on.
- The additional spread remains in the pool for the liquidity providers.

Decentralized exchange: Uniswap

Flash swap

- In a flash swap, the contract sends the tokens *before* the user pays for them with assets on the other side of the pair.
- A flash swap unlocks many opportunities for arbitrageurs.
- The user can deploy this instant liquidity to acquire the other asset at a discount on another exchange before repaying it; the corresponding amount of the alternate asset must be repaid in order to maintain the invariant.

Decentralized exchange: Uniswap

Flash swap

- This flexibility in a flash swap is different from the provision in a flash loan, which requires that repayment occur with the same asset.
- A key aspect of a flash swap is that all trades must take place during a single Ethereum transaction and that the trade must be closed with the corresponding amount of the complementary asset in that market.

Decentralized exchange: Uniswap

Example

- Consider this example in the DAI/USDC market with a supply of 100,000 each.
- This implies a 1:1 exchange rate and an invariant of 10 billion.
- A trader who has no starting capital spots an arbitrage opportunity to buy DAI on a DEX for 0.95 USDC.

Decentralized exchange: Uniswap

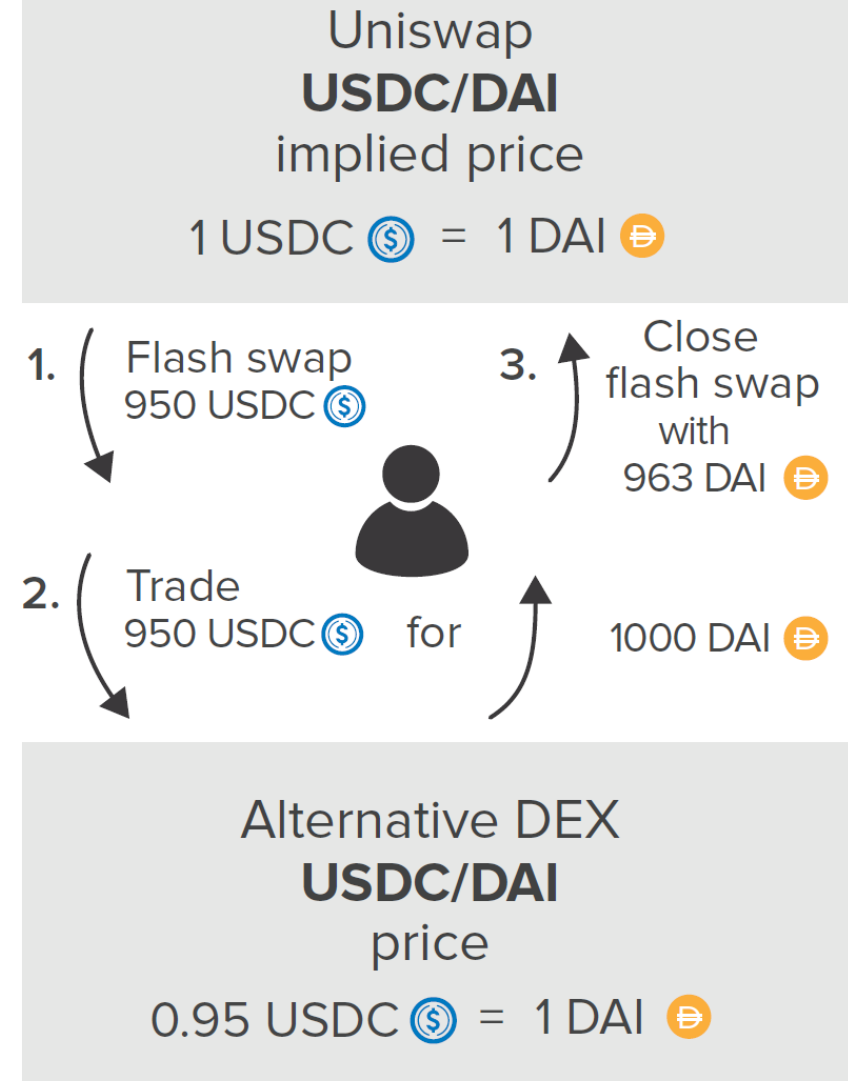
Example

- The trader can capitalize on this arbitrage via a flash swap by withdrawing 950 USDC of flash liquidity (liquidity derived from a flash loan) from the DAI/USDC market, purchase 1,000 DAI via the described arbitrage trade, and repay 963 DAI for a profit of 37 DAI—all consummated with no initial capital.
- The figure of 963 is calculated as 960 (with rounding for ease of illustration) to maintain the 10 billion invariant, and to account for some slippage, plus a $0.30\% \times 960 = 3$ DAI transaction fee.

Decentralized exchange: Uniswap

Example

- The 30bp fee is paid into the pool owned by the liquidity providers.



1. Slippage = 10 DAI, so 960 DAI
Fee = $.003 \times 960 = 3$ DAI
Swap done at $960 + 3 = 963$ DAI
Profit = $1000 - 963 = 37$ DAI

Decentralized exchange: Uniswap



Governance

- Lastly, an important point about Uniswap is the release of a governance token in September 2020 called UNI.
- Like COMP, the Compound governance token, UNI is distributed to users to incentivize liquidity in key pools including ETH/USDC and ETH/DAI.



Decentralized exchange: Uniswap

Governance

- The UNI governance even has some control over its own token distribution because 43% of the supply will be vested over four years to a treasury controlled by the UNI governance.
- Importantly, each unique Ethereum address that had used Uniswap before a certain cutoff date (over 250,000 addresses) was given 400 UNI tokens as a free airdrop.
- At the same time as the airdrop, UNI was released on Uniswap and the Coinbase Pro exchange for trading.

Decentralized exchange: Uniswap

Governance

15	 Uniswap UNI	\$11.52	▲ 2.86%	▲ 23.65%	\$3,275,199,138
16	 Aave AAVE	\$252.80	▲ 1.75%	▲ 33.65%	\$3,071,258,380

Decentralized exchange: Uniswap

Summary

- Uniswap is critical infrastructure for DeFi applications; it is important to have exchange operational whenever it is needed.
- Uniswap offers a unique approach for generating yield on users' assets by being a liquidity provider.
- The platform's flash swap functionality aids arbitrageurs in maintaining efficient markets and unlocks new use cases for users. Users can access any ERC-20 token listed, including creating completely new tokens through an IDO.

Decentralized exchange: Uniswap

Traditional Finance Problem	Uniswap Solution
<i>Centralized Control:</i> Exchanges that control which trading pairs are supported.	Allows anyone to create a new trading pair if it does not already exist and automatically routes trades through the most efficient path if no direct pair exists.
<i>Limited Access:</i> The best investment opportunities and returns from liquidity providing are restricted to large institutions.	Anyone can become a liquidity provider and earn fees for doing so. Any project can list its token on Uniswap to give anyone access to an investor.
<i>Inefficiency:</i> Trades generally require two parties to clear.	An AMM that allows constant access for trading against the contract.
<i>Lack of Interoperability:</i> Ability to exchange assets on one exchange is not easily used within another financial application.	Any token swap needed for a DeFi application can utilize Uniswap as an embedded feature.
<i>Opacity:</i> Unknown if the exchange truly owns all user's entire balance.	Transparent liquidity levels in the platform and algorithmic pricing.

Decentralized Exchange: Balancer

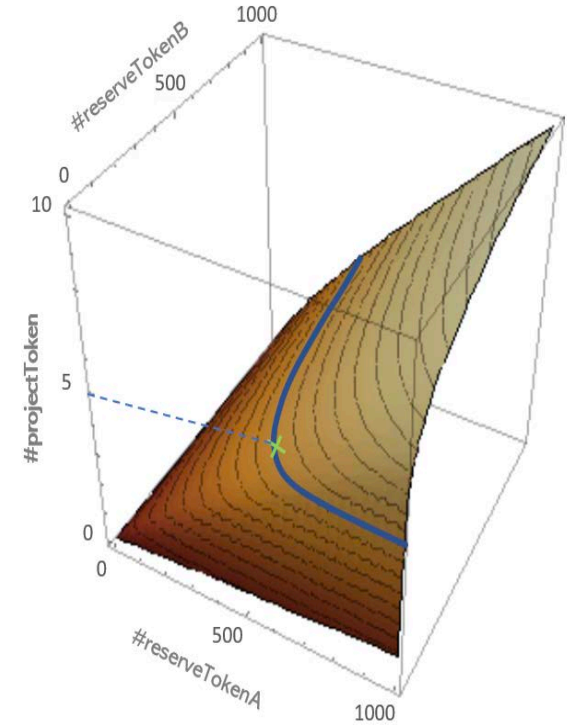
Overview

- Balancer is a decentralized exchange with an Automated Market Maker and is similar to Uniswap
 - Up to 8 assets (ERC-20 Tokens or ETH) can be supported in a single liquidity pool
 - Assets can be weighed arbitrarily and do not need to be weighted 50:50 in value like in Uniswap
 - Liquidity pool controller (creator) sets transaction fees
 - Liquidity pools can be finalized (public), controlled (private), or smart (controlled by a smart contract)

Decentralized Exchange: Balancer

Bonding Surfaces

- To allow up to 8 assets in a single Liquidity pool, Balancer uses bonding surfaces, which generalizes Uniswap's $x*y=k$ formula to n dimensions
- The Bonding Surface is given by $V = \prod_{t=0}^n B_t^{W^t}$
 - V is the value function (analogous to k in a bonding curve)
 - n is the number of tokens in the pool
 - B is the balance of token t in the pool
 - W is the normalized weight of token t



Decentralized Exchange: Balancer

Token Price and Pool Value

- The effective price between a single pair of tokens is given by the ratio of the token balances normalized by their weights: $EP_y^x = \frac{A_y}{A_x}$
 - Where A_x is the amount of token x being bought and A_y is the amount of token y being sold

Decentralized Exchange: Balancer

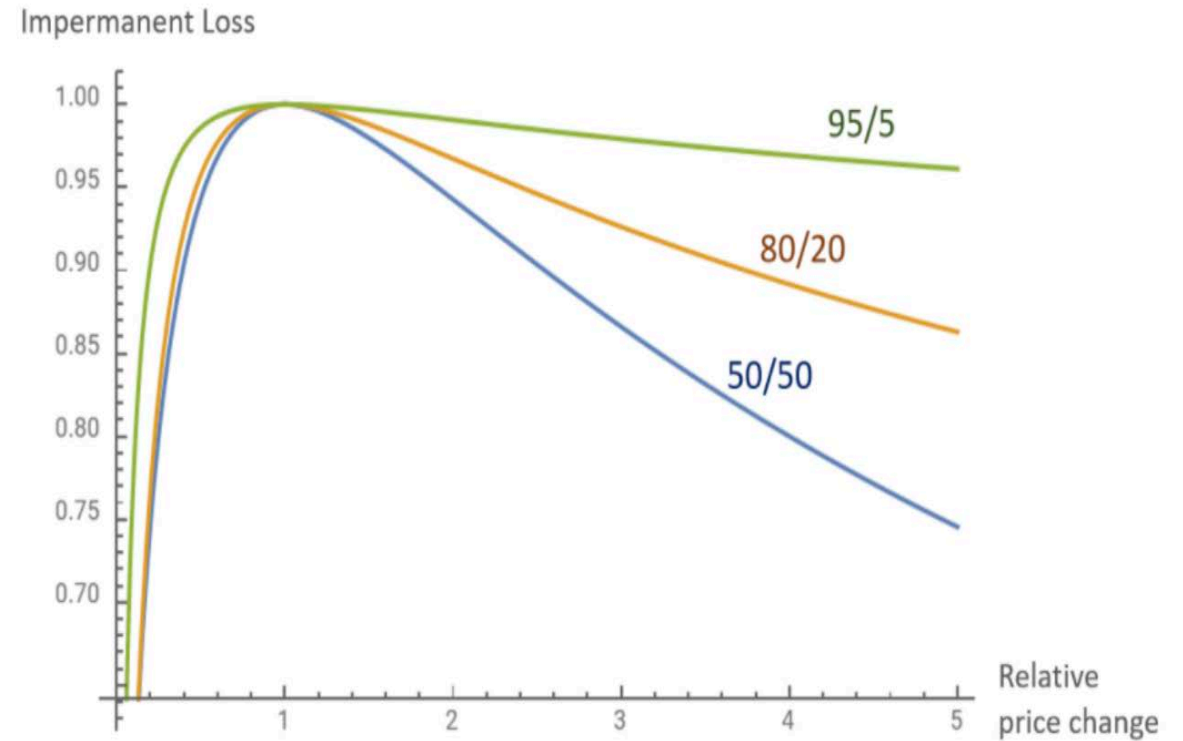
Swap Fees and Limits

- A user can only swap in up to 50% of the current balance of a token *into* a pool
- A user can swap out up to 33.3% of the current balance of a token *out* of a pool
- Liquidity pool controllers set transaction fees between 0.0001% and 10%

Decentralized Exchange: Balancer

Impermanent Loss

- Impermanent loss can be higher or lower in Balancer depending on the weighting of tokens
- Two tokens weighted 50/50 and a 5x increase in the token valuation results in an impermanent loss of 25.5%. However, two tokens weighted 95/5 and the same increase results in an impermanent loss of just 3.88%
- If a pool creator is confident in a token, they can create more uneven pools to offer themselves selective exposure and earn transaction fees



Impermanent Loss for different combinations of Balancer pool weights

Decentralized Exchange: Balancer

Slippage and Smart Order Router

- Equal token weights in a pool have the lowest slippage, while uneven pools have higher slippage, which disincentivizes traders from using the pool and results in less trading volume and lower transaction fees generated for the pool
- Smart Order Router (SOR) is an off-chain price optimizer that searches across all Balancer pools to find the best price

Decentralized Exchange: Balancer

Governance

- BAL is the Balancer Governance Protocol Token
- Total supply of BAL is capped at 100M BAL
 - 25M to founders, advisors, and investors
 - 5M to Balancer Ecosystem Fund and 5M to fundraising fund
 - 65M to liquidity providers with 145,000 BAL per week distributed to providers
 - Community will have to decide whether to continue distributing after 100M cap has been reached
- BAL is distributed to liquidity miners as a function of the total amount of liquidity contributed relative to the total liquidity on Balancer

Decentralized Exchange: Balancer

Native Pools

- Finalized Pool: Weights, ratios, fees, and tokens are fixed
- Controlled Pool: Weights, ratios, fees, and tokens are controlled by the pool creator. Fees can be updated any number of times
 - This is ideal for index funds
 - Liquidity providers can be restricted in a controlled pool

Decentralized Exchange: Balancer

Smart Pools and Use Cases

- Smart pools are controlled by smart contracts whose parameters change based on factors codified in the contract
- Investor Consortiums: Dynamically update/restrict liquidity providers to a defined group of addresses
- Automated Swap Fee Adjustment (i.e., Surge pricing): The smart pool can adjust swap fees based on trading volatility

Decentralized Exchange: Balancer

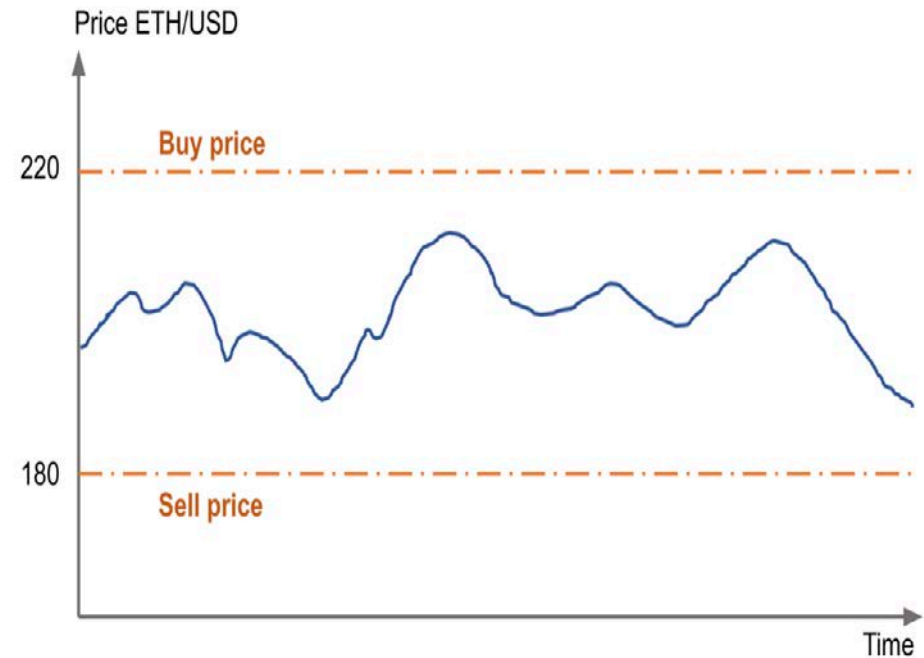
Smart Pools: Liquidity Bootstrapping

- If a team creates a new token, the capital requirements for preventing slippage become expensive
- With a smart pool, a team can start with a weight of 80/20 of Token X/ETH and slowly adjust the weights over time as certain price thresholds are hit enable more efficient price discovery (this is analogous to a Dutch Auction)
 - Adjustment can be based on linear or exponential curves and a new token can be priced against multiple assets in the pool

Decentralized Exchange: Balancer

Example: Swing Trading

- Assume we have 50/50 ETH/DAI pool has 1000 ETH and 200,000 DAI. A 1% fee would result in the buy price of 1 ETH being 202 DAI and the sell price being 198 DAI. If the price of 1ETH goes outside of these two values, an arbitrageur has an incentive to make a profit
- If the fees are higher (e.g., 10%), the pool will effectively act as a holding strategy

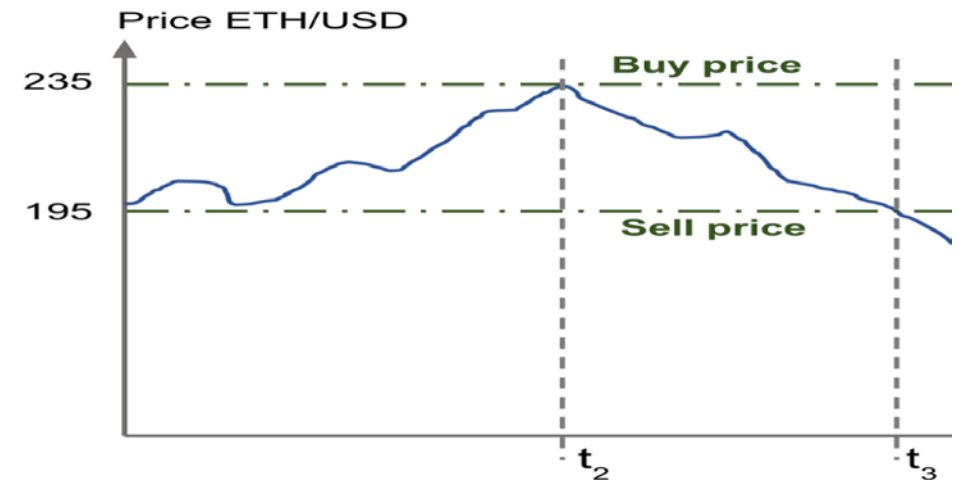
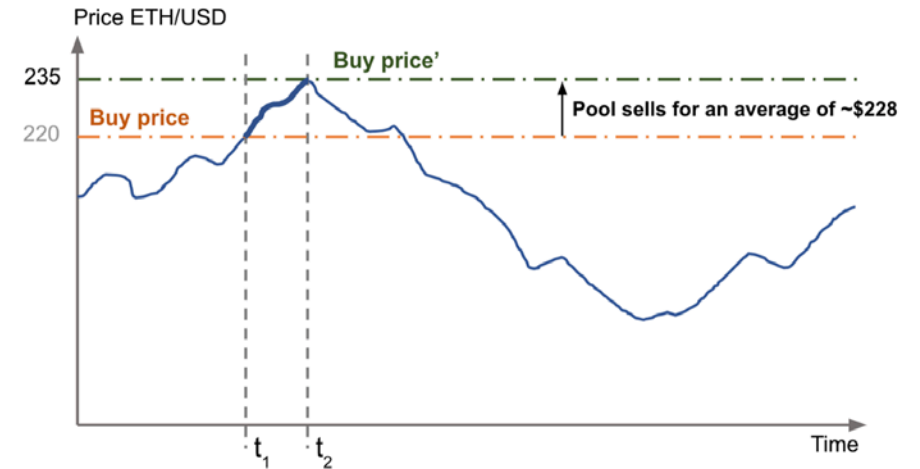


As long as the ETH price stays between the buy and sell prices of the Balancer pool no arbitrage trades will happen and the pool will behave identically to a holding strategy

Decentralized Exchange: Balancer

Example: Swing Trading

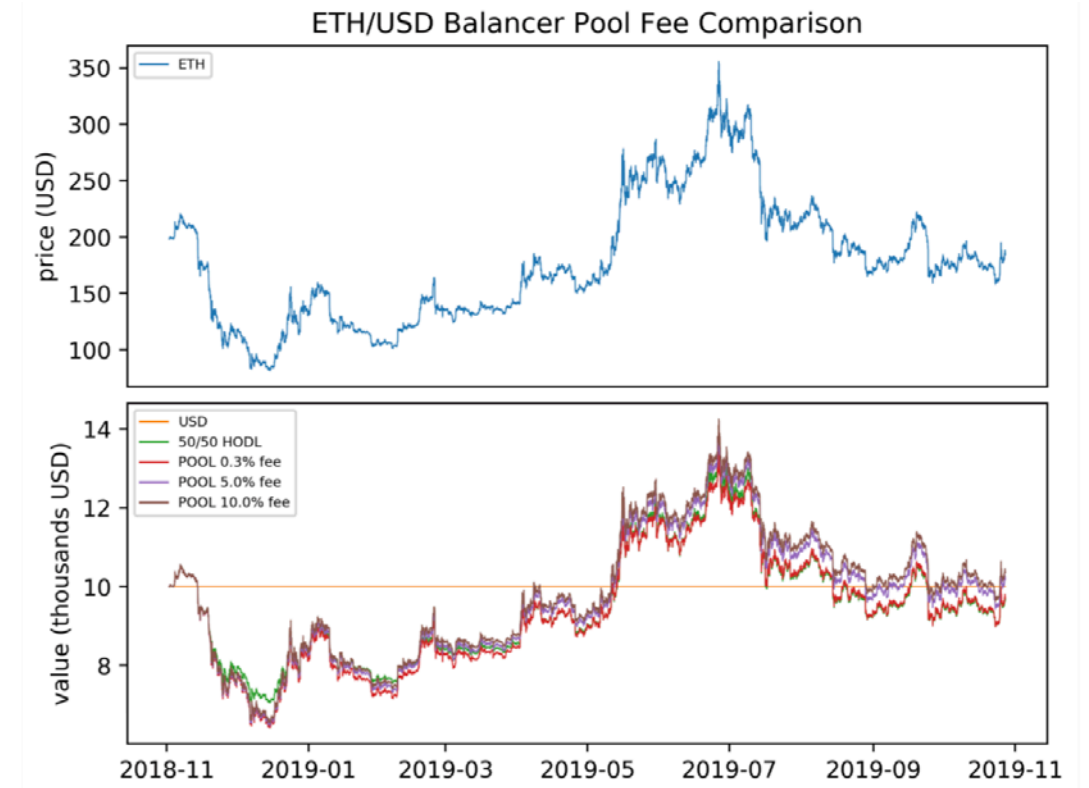
- If prices move above the price of 220 DAI, the arbitrageur is incentivized to buy from the Balancer pool and sell externally
- Here, arbitrageurs will continue buying from the pool until the price of 1 ETH hits 235 DAI
- The new buy and sell prices become 235 DAI and 195 DAI respectively



Decentralized Exchange: Balancer

Example: Swing Trading

- The pool continues to oscillate between different buy/sell bands
- Pools with 10% fees can generate better returns than those with lower fees when only arbitrage trades are considered. Simulated returns:
 - 0.3% Fee: \$9639
 - 5% Fee: \$10,135
 - 10% Fee: \$10,361



Value of ETH (top) and value of a Balancer pool with different fees compared with holding a 50/50 portfolio with initial total value of \$10,000

Derivatives: Yield protocol

What is Yield protocol?

- Yield Protocol proposes a derivative model for secured, zero-coupon bonds.
- Essentially, the protocol defines a *yToken* to be an ERC-20 (fungible) token that settles in some fixed quantity of a target asset at a specified date.
- The contract will specify that the tokens, which have the same expiry, target asset, collateral asset, and collateralization ratio, are fungible.

The Yield Protocol: On-Chain Lending With Interest Rate Discovery

Dan Robinson

dan@paradigm.xyz

Allan Niemerg

allan@yield.is

April 2020

WORKING DRAFT, rev. 1

Abstract

This paper presents a sketch of a new building block for decentralized finance: yTokens. yTokens are like zero-coupon bonds: on-chain obligations that settle on a specific future date based on the price of some target asset, and are secured by collateral in another asset. By buying or selling yTokens, users can synthetically lend or borrow the target asset for a fixed term. yTokens are fungible and trade at a floating price, which means their “interest rates” are determined by the market. The prices of yTokens of varying maturities can be used to infer interest rates, and even to construct a yield curve. Depending on the target asset, yTokens can settle through “cash-settlement” using an on-chain price oracle, through “physical settlement” in the target ERC20 token, or by synthetically issuing or borrowing the target ERC20 token on another platform.

Derivatives: Yield protocol

What is Yield protocol?

- The tokens are secured by the collateral asset and have a required maintenance collateralization ratio similar to, for example, MakerDAO, as well as to other DeFi platforms we have discussed.
- If the collateral's value dips below the maintenance requirement, the position can be liquidated with some or all of the collateral sold to cover the debt.

Derivatives: Yield protocol

Cash settlement

- The mechanism for yToken settlement is still undecided, but one proposed solution is “cash” settlement, which means paying an equivalent amount of the collateral asset worth the specified amount of the target asset.
- For example, if the target asset is 1 ETH secured by 300 DAI, and at expiry $1 \text{ ETH} = 200 \text{ DAI}$, a cash settlement would pay out 200 DAI and return the 100 DAI excess collateral to the seller of the yToken.

Derivatives: Yield protocol

Physical settlement



- The other commonly proposed solution is “physical” settlement, which automatically sells collateral for the target asset upon expiry (perhaps on Uniswap) to pay out in the target asset.
- Using the same numbers as in the previous example, the owner of the yToken would receive 1 ETH and the seller would receive slightly less of the remaining collateral, likely around 95 DAI, after subtracting exchange fees

Derivatives: Yield protocol

Example

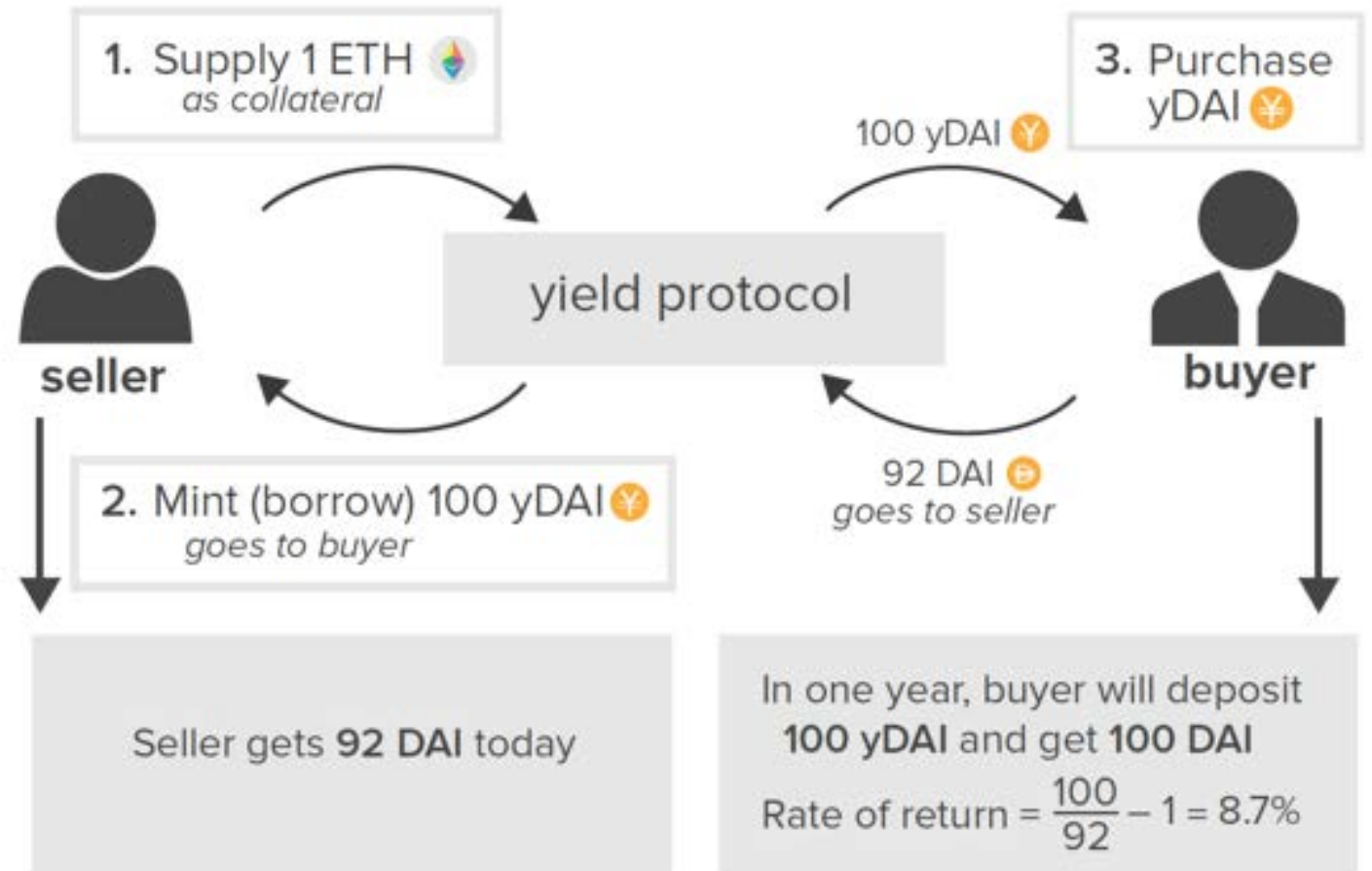
- The yToken effectively allows for fixed-rate borrowing and lending, using the implied return on the discounted price of the token versus the target amount.
- We can illustrate as follows: assume a user has a yToken with the target asset of 1 DAI backed by ETH. The maturity date is one year ahead and the yToken is trading at 0.92 DAI. A purchase of the yToken effectively secures an 8.7% fixed interest rate, even in the case of a liquidation $[(0.08/0.92) - 1]$.

Derivatives: Yield protocol

1 ETH  = 200 DAI 
collateralization ratio: **125%**

Example

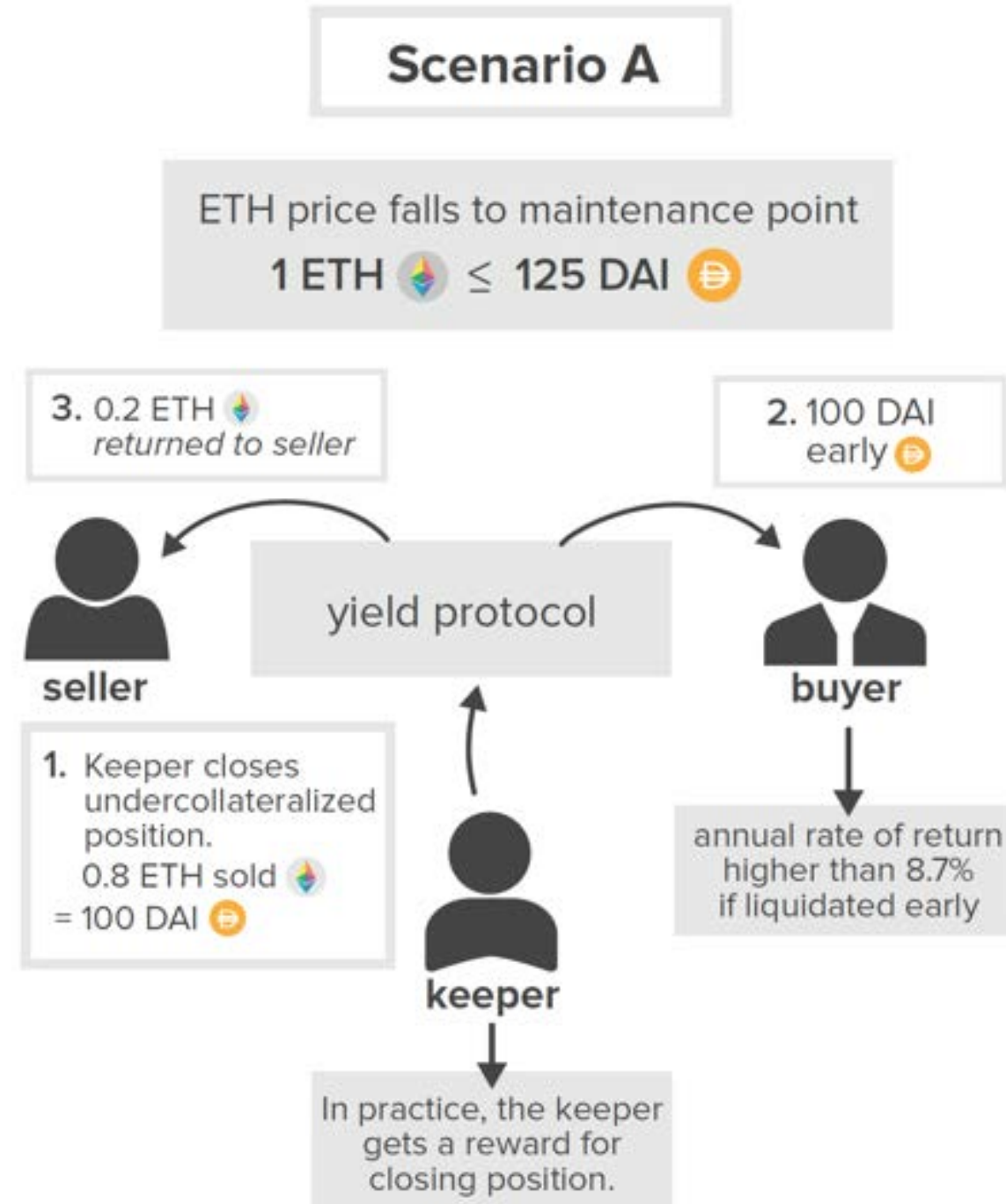
- The buyer of yDAI locks in a 8.7% return



Derivatives: Yield protocol

Example

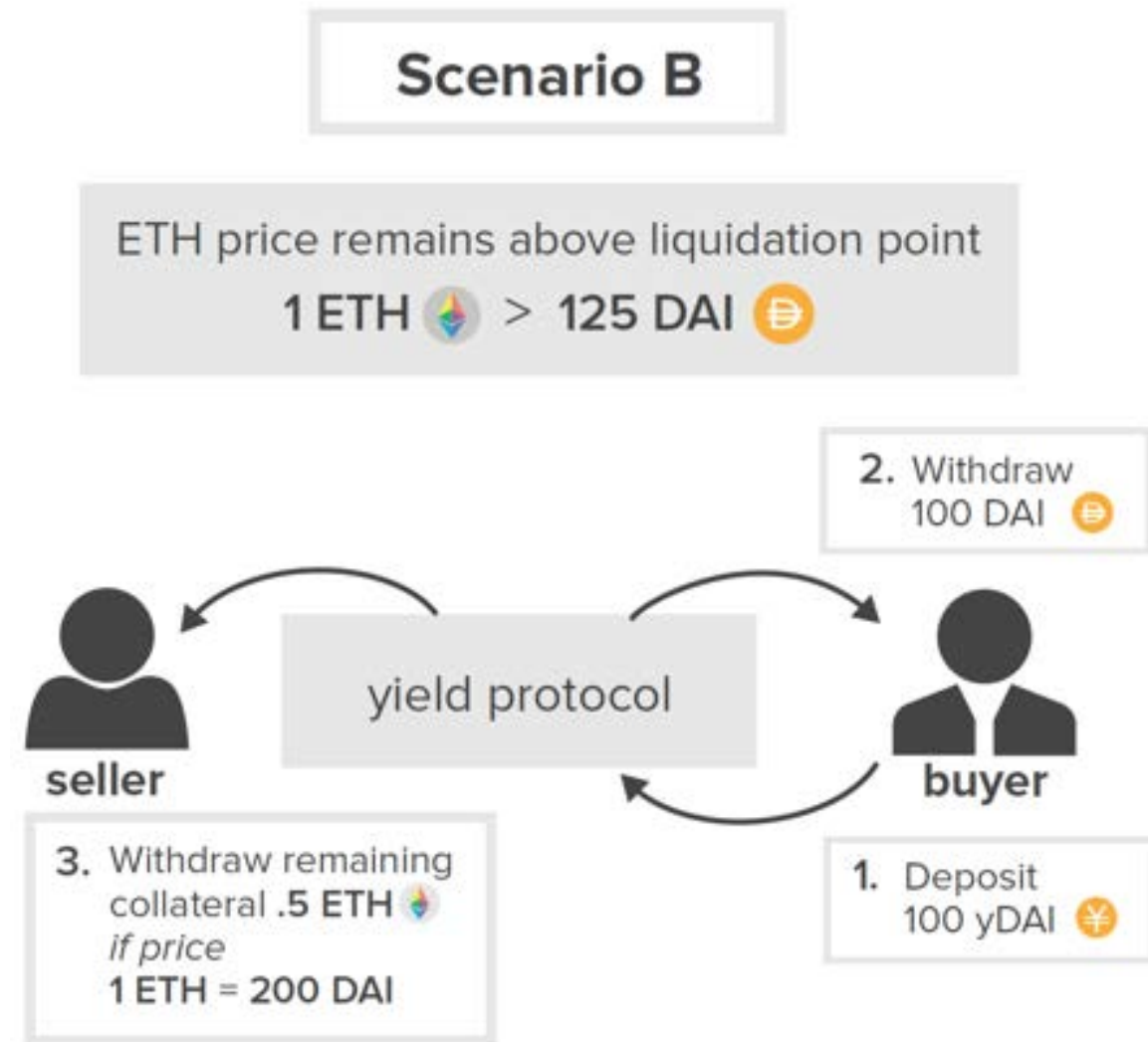
- Keeper triggers liquidation if ETH price falls below maintenance point



Derivatives: Yield protocol

Example

- Seller ends up with the original 92 DAI plus the excess collateral.



Derivatives: Yield protocol

Synthetic settlement

- An investor can purchase yTokens to synthetically lend the target asset.
- The investor would be paying X amount of the asset now to purchase the yTokens.
- Upon settlement, the investor receives $X + \text{interest}$.
- This financial transaction in total is functionally a lend of the target asset.

Derivatives: Yield protocol

Synthetic settlement

- Note that the interest is implied in the pricing and not a directly specified value.
- Alternatively one can mint and sell yTokens to synthetically borrow the target asset.
- By selling a yToken, you are receiving X amount of the asset now (the face value) and promising to pay $X + \text{interest}$ in the future.
- This financial transaction is functionally a borrow of the target asset.

Derivatives: Yield protocol

Floating yields

- Consider a perpetual product on top of yTokens that maintains a portfolio of different maturities and rolls short-term profits into long term yToken contracts.
- E.g., the portfolio may include 3-month, 6-month, 9-month, and 1-year maturity yTokens. When the 3-month tokens mature, the smart contract reinvests the balance into 1-year maturity yTokens.
- Token holders in this fund would experience a floating rate yield on the underlying asset with rate updates every three months.

Derivatives: Yield protocol

Yield curves

- The yTokens also allow for the construction of yield curves by analyzing the implied yields of short and longer term contracts.
- This can allow observers to get insights into investor sentiment among the various supported target assets.

Derivatives: Yield protocol

Betting on rates

- The Yield Protocol can be used to speculate on interest rates.
- There exist a few DAI derivative assets that represent a variable interest rate (Compound cDAI, Aave aDAI, [Chai](#)).
- One can imagine a seller of yDAI using one of these DAI derivative assets as collateral. The effect of this transaction is that the seller is paying the fixed rate on the yDAI while receiving the variable rate on the collateral. This is a bet that rates will increase.
- Likewise purchasing yDAI (of any collateral type) is a bet that variable rates will NOT increase beyond the fixed rate received.

Derivatives: Yield protocol

Summary

- Yield is an important protocol that supplies fixed rate products to Ethereum.
- It can be tightly integrated with other protocols like MakerDAO and Compound to create robust interest-bearing applications for investors.
- Demand for fixed income components will grow as mainstream investors begin adopting DeFi with portfolios in need of these types of assets.

Derivatives: Yield protocol

Traditional Finance Problem	Yield Solution
<i>Centralized Control:</i> Fixed income instruments largely restricted to governments and large corporations.	Yield protocol is open to parties of any size.
<i>Limited Access:</i> Many investors have limited access to buy or sell sophisticated fixed income investments.	Yield allows any market participant to buy or sell a fixed income asset that settles in a target asset of their choosing.
<i>Inefficiency:</i> Fixed income rates are lower due to layers of fat in traditional finance.	Lean infrastructure running on Ethereum allows for more competitive rates and diverse liquidity pools.
<i>Lack of Interoperability:</i> Fixed income instruments generally settle in cash which the investor must determine how to allocate.	yTokens can settle in any Ethereum target asset and even settle synthetically into a floating-rate lending protocol to preserve returns.
<i>Opacity:</i> Risk and uncertainty of counterparty in traditional agreements.	Clear collateralization publicly known on Ethereum blockchain backing the investment.

Derivatives: dYdX

What is dYdX?

- [dYdX](#) is a company that specializes in margin trading and derivatives.
- The margin trading protocol supports USDC, DAI, and ETH.
- The company has a spot DEX that allows investors to exchange these assets against the current bid–ask on the order book.

Derivatives: dYdX

Order processing

- The DEX uses a hybrid on–off chain approach.
- Essentially dYdX stores *signed* or pre-approved orders without submitting to Ethereum.
- These orders use cryptography to guarantee they are only used to exchange funds for the desired asset at the desired price.
- The DEX supports limit orders and a *maximum slippage* parameter for market orders in an effort to mitigate the slippage associated with price moves or front running.

Derivatives: dYdX

Order processing

- Allowing dYdX to match the orders holds little or no risk that the company could steal user funds, because the signed orders can only be used as intended per the smart contract.
- When the orders are matched, they are submitted to the Ethereum blockchain, where the smart contract facilitates settlement.

Derivatives: $dYdX$

Leverage

- Levered long or short position are possible using margined collateral.
- The maximum leverage $dYdX$ allows is 10 times.
- The positions can be isolated so that a single collateral deposit is used or cross-margined so that all of the investor's balances are pooled to serve as collateral.

Derivatives: dYdX

Keepers

- As in other protocols, dYdX has a maintenance margin requirement that if not maintained triggers liquidation of the collateral to close the position.
- The liquidations can be performed by external keepers who are paid to find and liquidate underwater positions, similar to the process followed by MakerDAO.

Derivatives: dYdX

Lending/borrowing

- dYdX offers borrowing and lending similar to Compound and Aave.
- The dYdX markets also feature flash loans.
- Unlike Aave, the flash loans are free, so that dYdX is a popular choice for DAI, ETH, and USDC flash liquidity.

Derivatives: $dYdX$

Free flash loans

- In the world of open smart contracts, it makes sense that flash loans rates would be driven to zero given that they are near risk free.
- Lending rates are determined by the loan's duration and default risk.
- For flash loans, repayment is algorithmically enforced and time is infinitesimal: in a single transaction, only the user can make any function calls or transfers.
- No other Ethereum users can move funds or make any changes while a particular user's transaction is in flight, resulting in no opportunity cost for the capital.

Derivatives: dYdX

Flash loans and arbitrage

- A market participant offering free flash loans will attract more usage to their platform.
- Because flash loans do not require any upfront capital, they democratize access to funds for various use cases.
- In the Aave example, we showed how flash loans can be used to refinance a loan.
- We will now illustrate the use of flash loans to capitalize on an arbitrage opportunity.

Derivatives: dYdX

Example

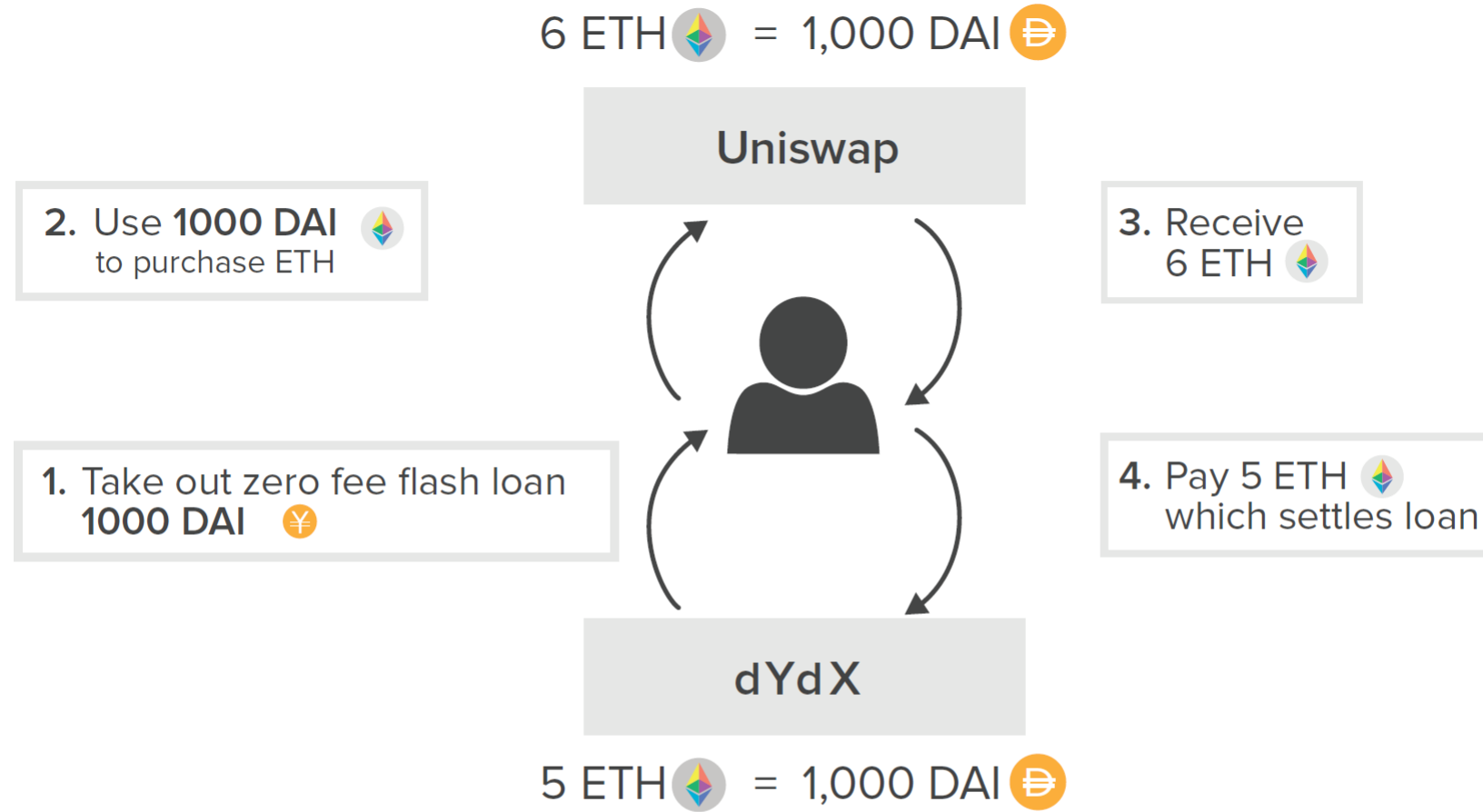
- Suppose the effective exchange rate for 1,000 DAI for ETH on Uniswap is 6 ETH/1,000 DAI. (The instantaneous exchange rate would be different, due to slippage.)
- Also, suppose the dYdX DEX has a spot ask price of 5 ETH for 1,000 DAI (i.e., the ETH are much more expensive on dYdX than Uniswap).

Derivatives: dYdX

Example

- Arbitrage opportunity, (without any capital beyond the gas fee):
 1. Execute a flash loan to borrow 1,000 DAI,
 2. Exchange it on Uniswap for 6 ETH, and
 3. Use 5 of those ETH to trade for 1,000 DAI on dYdX.
 4. Repay the flash loan with the 1,000 DAI and
 5. Pocket the 1 ETH profit.
- All of this happens in a single transaction.

Derivatives: dYdX



All of this is a single transaction, so flash loan has minimal risk.

Profit = 1 ETH
(received 6 ETH from Uniswap and paid back loan with 5 ETH)

(abstracts from gas fees)

Derivatives: dY/dX

BTC perpetual futures

- Perpetual futures are a popular derivative product similar to traditional futures but without a settlement date.
- By entering into a perpetual futures contract, the investor is simply betting on the future price of an asset.
- The contract can be long or short, with or without leverage.

Derivatives: dYdX

BTC perpetual futures

- The perpetual futures contract uses an Index Price based on the average price of the underlying asset across the major exchanges.
- BTC-USD Perpetual uses the MakerDAO BTCUSD Oracle V2, an oracle that reports in on-chain fashion the bitcoin prices from the cryptocurrency exchanges of Binance, Bitfinex, Bitstamp, Bittrex, Coinbase Pro, Gemini, and Kraken.

Derivatives: $dYdX$

BTC perpetual futures

- The investor deposits margin collateral and chooses a direction and amount of leverage.
- The contract can trade at a premium or discount to the Index Price depending on whether more traders are long or short the underlying, in this case BTC.

Derivatives: dY/dX

Futures funding rate

- A funding rate, paid from one side to the other, keeps the futures price close to the Index.
- If the futures contract is trading at a premium to the Index, the funding rate would be positive, and longs would pay shorts.
- The magnitude of the funding rate is a function of the difference in price compared to the Index.
- Likewise, if the contract is trading at a discount, the shorts pay the long positions.

Derivatives: dYdX

Futures funding rate

- The funding rate incentivizes investors to take up the opposing side from the majority in order to keep the contract price close to the Index.
- Each protocol in DeFi can only update balances when a user interacts with the protocol.
- In the example of Compound, the interest rate is fixed until supply enters or leaves the pool which changes the utilization.
- The contract simply keeps track of the current rate and the last timestamp when the balances updated.

Derivatives: dYdX

Futures funding rate

- When a new user borrows or supplies, that transaction updates the rates for the entire market.
- Similarly, whereas the dYdX's Funding Rate is updated every second, it is only applied at the time a user opens, closes, or edits a position.
- The contract calculates the new values based on what the rates were and how long the futures position has been open.

Derivatives: $dYdX$

Margins

- Like a traditional futures contract, the perpetual futures contract has two margins: initial and maintenance.
- Suppose the initial margin is 10%. This means the investor needs to post collateral (or equity) worth 10% of the underlying asset.
- A long futures contract allows the investor to buy the asset at a set price in the future.
- If the market price rises, the investor can buy the asset at a price cheaper than the market price and the profit is the difference between the market price and the contract price.

Derivatives: $dYdX$

Margins

- Like a traditional futures contract, the perpetual futures contract has two margins: initial and maintenance.
- Suppose the initial margin is 10%. This means the investor needs to post collateral (or equity) worth 10% of the underlying asset.

Derivatives: dY/dX

Long futures

- A long futures contract allows the investor to buy the asset at a set price in the future.
- If the market price rises, the investor can buy the asset at a price cheaper than the market price and the profit is the difference between the market price and the contract price.

Derivatives: dY/dX

Short futures

- A short position works similarly except that the investor agrees to sell the asset at a fixed price.
- If the market price falls, the investor can purchase the asset in the open market and sell at the higher price stipulated in the contract.
- The profit is the difference between the contract price and the market price.

Derivatives: $dYdX$

Futures risk

- The risk is that the price moves against the investor.
- For example, if the investor is long with a 10% margin and the market price drops by 10%, the collateral is gone because the difference between purchasing at the contract price and selling in the open market (at a loss) wipes out the value of the collateral.

Derivatives: dY/dX

Futures are not options

- If the underlying asset's price moves the wrong way in an option contract, the option holder can walk away: The exercise of the option is discretionary—that's why it is called an option—and no trader would exercise an option to guarantee a loss.
- Futures, however, are obligations.
- As such, traditional exchanges have mechanisms that seek to minimize the chance the contract holder does not default on a losing position.

Derivatives: $dYdX$

Maintenance margin

- The maintenance margin is the main tool to minimize default.
- Suppose the maintenance margin is 5%.
- On a traditional futures exchange, if the price drops by 5% the investor is required to replenish the collateral to bring it back up to 10%.
- If the investor fails to do this, the exchange liquidates the position.

Derivatives: dYdX

Maintenance margin

- A similar mechanism exists on dYdX, but with important differences.
 1. If any position falls to 5%, keepers will trigger liquidation. If any collateral remains, they may keep it as a reward.
 2. The liquidation is almost instantaneous.
 3. No centralized exchange exists.
 4. dYdX contracts are perpetual, whereas traditional exchange contracts usually have a fixed maturity date.

Derivatives: dY/dX

Mechanics

- Suppose the BTC price index is 10,000 USDC/BTC.
- An investor initiates a long position by depositing 1,000 USDC as margin (collateral), creating a levered bet on the price of BTC.
- If the price rises by 5%, the profit is 500.
- Given the investor has only deposited 1,000, the investor's rate of return is 50%, or $(1,000 - 500)/1,000$.

Derivatives: $dYdX$

Mechanics

- We can also think about the mechanics another way.
- Taking a long position at 10,000, the investor is committing to buying at 10,000 and the obligation is 10,000.
- Think of the obligation as a “negative balance” because the investor must pay 10,000 according to the contract.
- The investor has already committed collateral of 1,000 and owes 9,000.

Derivatives: $dYdX$

Mechanics

- On the other side, the investor has committed those funds to purchase an asset, 1 BTC.
- The investor thus has a positive balance of 10,000, the current price.
- The collateralization ratio is $10,000/9,000 = 111\%$, which is a margin percentage of 11% and is nearly the maximum amount of allowed leverage (10% margin).

Derivatives: $dYdX$

Mechanics

- This intuition works similarly for a short position.
- The investor has committed to sell at 10,000, which is a positive balance and is supplemented by the margin deposit of 1,000 (so total of 11,000).
- The investor's negative balance is the obligation to buy 1 BTC, currently worth 10,000.
- The collateralization ratio is $11,000/10,000$, which corresponds to a margin of 10%.

Derivatives: dY/dX

Short position when underlying price rises

- Suppose the underlying asset (BTC) increases in value by 5%.
- If the price of BTC increases to 10,500 (a 5% increase), the margin percentage becomes $(11,000/10,500) - 1 = 4.76\%$ and the short position becomes subject to liquidation.
- The paper net balance of the position is \$500, the incentive for the liquidator to close the position collect the balance.



Derivatives: dYdX



Long position

- Long 1 BTC
- 1 BTC=10,000



Open long position of
1 BTC at 10,000 **USDC**
Offer 1,000 **USDC** as margin

1 BTC  = 10,000 **USDC** 
initial margin = **10%**
maintenance margin = **5%**

Long Balance (what you will get)	Short Balance (what you owe)	Margin $\frac{10,000}{9,000} - 1 = 11\%$
10,000 1 BTC 	10,000 - 1,000 = 9,000 USDC 	

Derivatives: dYdX

Long position

- Long 1 BTC
- Price increases by 10%


Scenario A

BTC ↑ by 10% to 11,000

Long Balance	Short Balance
10,000 1 BTC 	9,000

$$\text{Margin} \quad \frac{11,000}{9,000} - 1 = 22.2\%$$



- Trader can withdraw USDC to bring margin towards **10%**
- Trader can close position with **1000 USDC**  profit, which is a ROI of **100%**

Derivatives: dYdX

Long position

- Long 1 BTC
- Price decreases by -7.5%

Scenario B

BTC ↓ by -7.5% to 9,250

Long Balance	Short Balance
9,250 1 BTC ⓑ	9,000

Margin $\frac{9,250}{9,000} - 1 = 2.8\%$



- Position is below 5% maintenance margin requirement
- Keeper liquidates position by selling **1 BTC** and paying back **9,000**
- Keeper keeps **\$250 USDC** Ⓢ as reward

Derivatives: dYdX

Summary

- The dYdX BTC perpetual futures contract allows investors to access BTC returns natively on the Ethereum blockchain, while being able to supply any ERC-20 asset as collateral.
- Perpetual futures are rising in popularity, and this functionality may continue to attract liquidity over time.

Derivatives: dYdX

Traditional Finance Problem	dYdX Solution
<i>Centralized Control:</i> Borrowing and lending rates controlled by institutions.	dYdX rates are determined algorithmically.
<i>Limited Access:</i> Difficulty in accessing high yield USD investment opportunities or competitive borrowing as well as futures and derivative products. Access to capital for immediately profitable enterprises is limited.	Open ability to borrow or lend any supported assets at competitive algorithmically determined rates. Includes a perpetual futures contract that could synthetically support any asset. Free flash loans give anyone access to large amounts of capital to capitalize on arbitrage or other profitable opportunities.
<i>Inefficiency:</i> Suboptimal rates for borrowing and lending due to inflated costs.	Algorithmically pooled and optimized interest rates. Free flash loans offered for immediate use cases.
<i>Lack of Interoperability:</i> Difficult to repurpose funds within a financial instrument.	Flash loans can immediately utilize the entirety of the AUM for outside opportunities without risk or loss to investors.
<i>Opacity:</i> Unclear collateralization of lending institutions.	Transparent collateralization ratios of borrowers are visible to the entire ecosystem.

What is Synthetix?

- Many traditional derivative products have a decentralized counterpart.
- DeFi, however, allows new types of derivatives because of smart contracts.
- Imagine creating a derivative cryptoasset, whose value is based on an underlying asset that is neither owned nor escrowed.
- Synthetix is one company whose primary focus is creating a wide variety of liquid synthetic derivatives.

Derivatives: Synthetix

What is Synthetix?

- The company issues *Synths*, tokens whose prices are pegged to an underlying price feed and are backed by collateral.
- MakerDAO's DAI is also a synthetic asset.
- The price feeds come from the [Chainlink](#)'s decentralized oracles.
- Synths can theoretically track any asset, long or short.
- In practice, the main tracked assets are cryptocurrencies, fiat currencies, and gold.

Derivatives: Synthetix

Synthetix tokens


- A long Synth is called an *sToken*, for example, a sUSD or a sBTC.
- The sUSD is a synthetic because its value is based on a price feed.
- A short Synth is called an *iToken*, for example, an iETH.



Derivatives: Synthetix

Synthetix platform token

- Synthetix also has a platform token called SNX. SNX is not a governance token like MKR and COMP, but is a *utility token* or a *network token*, which means it enables the use of Synthetix functionality as its only feature.
- SNX serves as the unique collateral asset for the entire system.

					Market cap	Volume
23	 Synthetix SNX	\$17.19	▲ 9.50%	▲ 5.48%	\$1,955,438,107	\$273,761,997 16,077,853 SNX

Derivatives: Synthetix

Minting synths

- When users mint Synths against their SNX, they incur a debt proportioned to the total outstanding debt denominated in USD.
- They become *responsible* for this percentage of the debt in the sense that to unlock their SNX collateral they need to return the total USD value of their debt.
- The global debt of all Synths is thus shared collectively by the Synth holders based on the USD-denominated percentage of the debt they owned when they opened their positions.

Derivatives: Synthetix

Minting synths

- The total outstanding USD-denominated debt changes when any Synth's price fluctuates, and each holder remains responsible for the same percentage they were responsible for when they minted their Synths.
- Therefore, when a SNX holder's Synths outperform the collective pool, the holder effectively profits, and vice versa, because their asset value (their Synth position) outpaced the growth of the debt (sum of all sUSD debt).

Derivatives: Synthetix




Minting synths

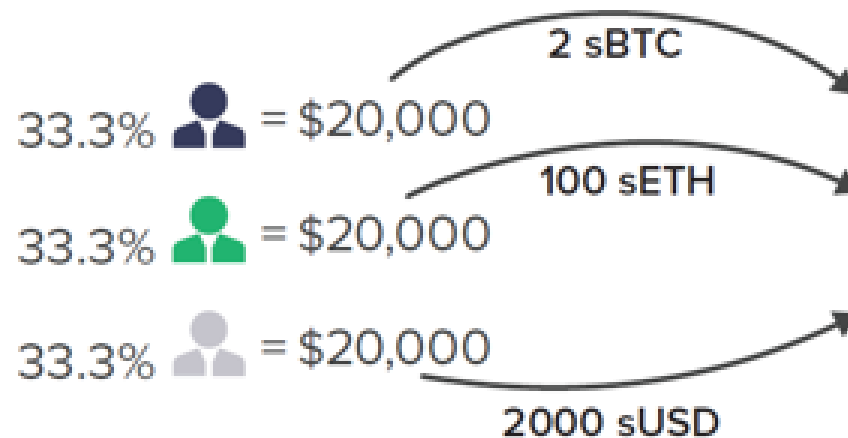
- In any Synthetix position, the trader is effectively “long” his personal portfolio against the entire pool's portfolio.
- In other words, the trader is betting his returns will exceed the pool's returns.
- For example, by holding sUSD only, the trader is effectively shorting the entire composition of all other traders' Synthetix portfolios and betting that USD will outperform all other assets held.
- The trader's goal is to own Synths that he thinks will outperform the rest of the market, because it is the only way to profit.

Derivatives: Synthetix

Example

- As an example, three traders each have \$20,000 for a total debt of \$60,000: one holds 2 sBTC priced at \$10,000 each, one holds 100 sETH priced at \$200 each, and one holds 20,000 sUSD priced at \$1 each. Each has a debt proportion of 33.3%.

	= \$10,000
	= \$200
	= \$1




Synthetix	
	2 x sBTC 
	100 x sETH 
	20,000 x sUSD 


Total Debt = \$60,000

Derivatives: Synthetix


Example


- If the price of BTC doubles to \$20,000 and the price of ETH spikes to \$1,000, the total debt becomes \$160,000 = \$40,000 (sBTC) + \$100,000 (sETH) + \$20,000 (sUSD).
- Because each trader is responsible for 33.3%, about \$53,300, only the sETH holder is profitable even though the price of BTC doubled.


 = \$20,000 (+100%)

 = \$1,000 (+500%)

 = \$ (no change)

33.3%  \$40,000 - \$53,300 = -\$13,300

33.3%  \$100,000 - \$53,300 = \$46,700


33.3%  \$20,000 - \$53,300 = -\$33,300

Debt = \$160,000 / 3 = \$53,300

Synthetix

2 x sBTC  = \$ 40,000

100 x sETH  = \$ 100,000




20,000 x sUSD  = \$ 20,000




Total Debt = \$160,000




Derivatives: Synthetix

Example

- If the price of BTC falls to \$5,000 and ETH to \$100, then the total debt falls to \$40,000 and the sUSD holder becomes the only profiting trader.

 = \$5,000 (-50%)
 = \$100 (-50%)
 = \$1 (no change)

33.3%  \$10,000 - \$13,300 = -\$3,300
33.3%  \$10,000 - \$13,300 = -\$3,300
33.3%  \$20,000 - \$13,300 = +\$6,600
Debt = \$40,000 / 3 = \$13,300

Synthetix
2 x sBTC  = \$10,000
100 x sETH  = \$10,000
20,000 x sUSD  = \$20,000
Total Debt = \$40,000

Derivatives: Synthetix

Platform DEX

- The platform has a DEX native that will exchange any two Synths at the rate quoted by the oracle.
- SNX holders pay the exchange fees to a fee pool redeemable by SNX holders in proportion to their percentage of the debt.
- The contracts enforce that users can only redeem their fees if they maintain a sufficient collateralization ratio relative to their portion of the debt.

Derivatives: Synthetix

Collateralization

- The required collateralization ratio to mint Synths and participate in staking rewards is high, currently 800%.
- The Synthetix protocol also mints new SNX tokens via inflation to reward various stakeholders in the ecosystem for contributing value.
- The protocol distributes the rewards as a bonus incentive for maintaining a high collateralization ratio or increasing the liquidity of SNX.

Derivatives: Synthetix

Collateralization

- Synthetix has branched into products that track real-world equities with the release of sNIKKEI and sFTSE.
- The company is also beginning to offer an options trading interface, further expanding its capabilities.
- The platform could easily gain popularity because there is no slippage against the price feed, however, the pooled liquidity and shared debt models offer interesting challenges.

Derivatives: Synthetix

Traditional Finance Problem	Synthetix Solution
<i>Centralized Control:</i> Assets can generally only be bought and sold on registered exchanges.	Offer synthetic assets in one place that can track any real world asset.
<i>Limited Access:</i> Access to certain assets is geographically limited.	Anyone can access Synthetix to buy and sell Synths.
<i>Inefficiency:</i> Large asset purchases suffer from slippage as traders eat into the liquidity pool.	Synths exchange rates are backed by a price feed, which eliminates slippage.
<i>Lack of Interoperability:</i> Real-world assets such as stocks can't be easily represented directly on a blockchain	Synth representations of real assets are totally compatible with Ethereum and other DeFi protocols.
<i>Opacity:</i>	

Derivatives: Overlay

What is Overlay?

- To be added

Derivatives: Fei Protocol

What is Fei Protocol?

- To be added

Tokenization

What is tokenization?

- Tokenization refers to the process of taking some asset or bundle of assets, either on or off chain, and
 1. representing that asset on chain with possible fractional ownership, or
 2. creating a composite token that holds some number of underlying tokens.
- A token can conform to different specifications based on the type of properties a user wants the token to have.
- The most popular token standard is ERC-20, the fungible token.

Tokenization

What is tokenization?

- ERC-20 defines abstractly how a token, which has units that are non-unique and interchangeable (such as USD), should behave.
- ERC-721 standard defines nonfungible tokens (NFTs). These tokens are unique, such as a token representing ownership of a piece of fine art or a specific digital asset from a game.
- DeFi applications can take advantage of these and other standards to support any token using the standard simply by coding for the single standard.

Tokenization: Set Protocol

What is Set Protocol?

- [Set Protocol](#) offers the “composite token” approach to tokenization.
- Set Protocol combines Ethereum tokens into composite tokens that function more like traditional exchange traded funds (ETFs).
- Set Protocol combines cryptoassets into *Sets*, which are themselves ERC-20 tokens and fully collateralized by the components escrowed in a smart contract.

Tokenization: Set Protocol

Static Sets

- A Set token is always redeemable for its components.
- Sets can be static or dynamic, based on a trading strategy.
- Static Sets are straightforward to understand and are simply bundled tokens the investor cares about; the resulting Set can be transferred as a single unit.

Tokenization: Set Protocol

Dynamic Sets

- Dynamic Sets define a trading strategy that determines when reallocations can be made and at what times.
- Some examples include the “Moving Average” Sets that shift between 100% ETH and 100% USDC whenever ETH crosses its X-day simple or exponentially weighted moving average.
- Similar to normal ETFs, these Set tokens have fees and sometimes performance-related incentives.

Tokenization: Set Protocol

Dynamic Sets

- At the Set's creation, the manager pre-programs the fees, which are paid directly to the manager for that particular Set.
- The available fee options are:
 1. buy fee (front-end load fee),
 2. streaming fee (management fee), and
 3. performance fee (percentage of profits over a high-water mark).
- The Set Protocol currently takes no fee for itself, although it may add a fee in the future.

Tokenization: Set Protocol

Oracle

- The prices and returns for Set Protocol are calculated via MakerDAOs' publicly available oracle price feeds, which are also used by Synthetix.
- The main value-add of dynamic Sets is that the trading strategies are publicly encoded in a smart contract so users know exactly how their funds are being allocated and can easily redeem at any time.

Tokenization: Set Protocol

Social trading

- Set Protocol also has a *Social Trading* feature in which a user can purchase a Set whose portfolio is restricted to certain assets with reallocations controlled by a single trader.
- Because these portfolios are actively managed, they function much more like mutual funds.
- The benefits are similar in that the portfolio manager has a predefined set of assets to choose from, and the users benefit from this contract-enforced transparency.

Tokenization: Set Protocol

Example

- A portfolio manager for a Set has a goal to “buy low and sell high” on ETH.
- The only assets she can use are ETH and USDC, and the only allocations she is allowed are 100% ETH and 100% USDC.
- At her sole discretion, she can trigger a contract function to rebalance the portfolio entirely into one asset or the other; this is the only allocation decision she can make.

Tokenization: Set Protocol

Example

- Assume she starts with 1,000 USDC. The price of ETH dips to 100 USDC/ETH and she decides to buy.
- She can trigger a rebalance to have 10 ETH in the Set.
- If the price of ETH doubles to \$200, the entire Set is now worth \$2,000.
- A shareholder who owns 10% of the Set can redeem her shares for 1 ETH or 200 USDC.

Tokenization: Set Protocol

Summary

- Sets could democratize wealth management in the future by being more peer to peer, allowing fund managers to gain investment exposures through nontraditional channels and giving all investors access to the best managers.
- Many use cTokens, (Compound) earning interest through the Compound protocol.
- This is one example of DeFi platforms being composed (*DeFi Legos*) to create new products and value for investors.

Tokenization: Set Protocol

Traditional Finance Problem	Set Protocol Solution
<i>Centralized Control:</i> Fund managers can control their funds against the will of investors.	Enforces sovereignty of the investor over their funds at the smart contract level.
<i>Limited Access:</i> Talented fund managers often are unable to gain exposures and capital to run a successful fund.	Allows anyone to become a fund manager and display their skills using social trading features.
<i>Inefficiency:</i> Many arising from antiquated practices.	Trading strategies encoded in smart contracts lead to optimal execution.
<i>Lack of Interoperability:</i> Difficult to combine assets into new packages and incorporate the combined assets into new financial products.	Set tokens are ERC-20 compliant tokens that can be used on their own in other DeFi protocols. For example, Aave allows Set token borrowing and lending for some popular Sets.
<i>Opacity:</i> Difficult to know the breakdown of assets in an ETF or mutual fund at any given time.	Total transparency into strategies and allocations of Set tokens.

Tokenization: wBTC



What is wBTC?

- The wBTC application takes the *representing off-chain assets on chain* approach to tokenization, specifically for BTC.
- Wrapped bitcoin or wBTC allows BTC to be included as collateral or liquidity on all of the Ethereum-native DeFi platforms.
- Given that BTC has comparatively low volatility to other cryptocurrencies and is the most well-adopted cryptocurrency by market-cap, this characteristic unlocks a large potential capital pool for DeFi dApps.

Tokenization: wBTC

Stakeholders

- The wBTC ecosystem contains three key stakeholders: users, merchants, and custodians.
- Users are simply the traders and DeFi participants who generate demand for the value proposition associated with wBTC, namely, Ethereum-tokenized BTC.
- Users can purchase wBTC from merchants by transferring BTC and performing the requisite KYC/AML, thus making the entry and exit points of wBTC centralized and reliant on off-chain trust and infrastructure.

Tokenization: wBTC

Stakeholders

- The wBTC ecosystem contains three key stakeholders: users, merchants, and custodians.
- Merchants are responsible for transferring wBTC to the custodians.
- At the point of transfer, the merchant signals to an on-chain Ethereum smart contract that the custodian has taken custody of the BTC and is approved to mint wBTC.

Tokenization: wBTC

Stakeholders

- The wBTC ecosystem contains three key stakeholders: users, merchants, and custodians.
- Custodians use industry-standard security mechanisms to custody the BTC until it is withdrawn from the wBTC ecosystem.
- Once the custodians have confirmed receipt, they can trigger the minting of wBTC that releases wBTC to the merchant.
- Finally, closing the loop, the merchant transfers the wBTC to the user.

Tokenization: wBTC

Stakeholders

- No single participant can control the minting and burning of wBTC, and all BTC entering the system is audited via transaction receipts that verify custody of on-chain funds.
- These safeguards increase the system's transparency and reduce the risk to users that is inherent in the system.
- Because the network consists of merchants and custodians, any fraud is quickly expungable from the network at only a small overall cost versus the cost that would be incurred in a single centralized entity.

Tokenization: wBTC


Governance

- The mechanism by which merchants and custodians enter and leave the network is a multi-signature wallet controlled by the wBTC DAO.
- The DAO does not have a governance token; instead, a set of owners who can add and remove owners controls the DAO.

Tokenization: wBTC

Governance

- The contract currently allows a maximum of 50 owners, with a minimum threshold of 11 to invoke a change.
- The numbers 50 and 11 can be changed, if the number of conditions are met.
- This system is more centralized than other governance mechanisms we have discussed, but is still more decentralized than allowing a single custodian to control all of the wBTC.

☆	14	 Wrapped Bitcoin	WBTC	\$32,465.28	▲ 0.63%	▼ 13.07%	Market cap \$3,700,425,918	Volume \$197,270,245 6,140 WBTC
---	----	---	------	-------------	---------	----------	-------------------------------	---------------------------------------

DeFi risks

Next

- We will do an analysis of the major risks in the DeFi space including: Smart contract risk; Governance risk; Oracle risk; Scaling risk; DEX risk; and Regulatory risk.

Contact: Follow me on LinkedIn

<http://linkedin.com/in/camharvey>

cam.harvey@duke.edu

@camharvey

SSRN: <http://ssrn.com/author=16198>

PGP: E004 4F24 1FBC 6A4A CF31 D520 0F43 AE4D D2B8 4EF4