Introduction to DeFi

" Decentralized Finance aims to provide the same financial services as traditional banking without any central authority or intermediaries. Without a central authority, DeFi allows everyone to engage with financial services like payments, lending, borrowing or investing with high autonomy and fewer barriers. "

Areas

- Exchanges
- Asset management
- Stablecoins
- Lending / Borrowing
- Remittance

According to DeFi Pulse before summer 2020 the TVL was about $950 million
It now stands at about $77 billion
It has dropped over the last few months

#	NAME	CHAIN	SECTOR	TVL (USD) ⌄	1 Day %
1 🏆	Ｍ Maker	Ethereum	Lending	$14.52B	0.99%
2 🥈	Aave	Multichain	Lending	$11.33B	3.15%
3 🥉	Curve Finance	Ethereum	DEXes	$10.32B	0.29%
4	C Convex Finance	Ethereum	Assets	$9.64B	0.06%
5	Uniswap	Ethereum	DEXes	$7.04B	3.76%
6	Compound	Ethereum	Lending	$6.39B	0.96%
7	InstaDApp	Ethereum	Lending	$5.13B	1.57%
8	yearn.finance	Ethereum	Assets	$2.48B	0.15%
9	Balancer	Ethereum	DEXes	$2.19B	-1.68%
10	Bancor	Ethereum	DEXes	$1.84B	-0.05%

DeFi recent milestones

- Pre 2020

  - ` First DEXs `

  - ` Uniswap `

- Early 2020

  - Synthetix
  - Aave - Flash loans
  - Ampleforth

    - ` Compound `

  - Yearn.finance

- Summer 2020

  - ` YAM `

  - ` Food coins `

  - ` Sushi swap `

- Autumn 2020

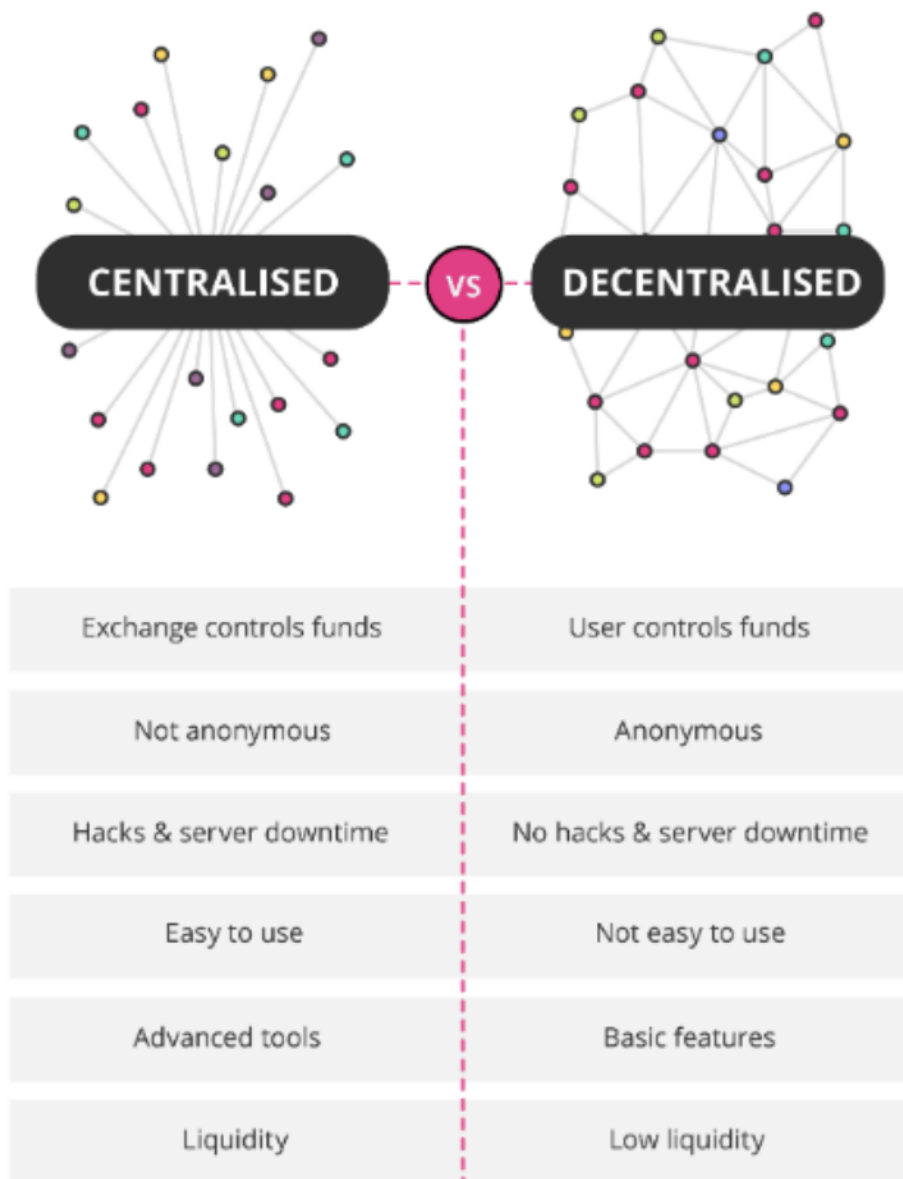 - Area cools
  - NFTs increasingly popular

- 2021

  - ` NFTs / Games `

Decentralised Exchanges

Decentralised Exchanges are a protocol to provide asset exchange without the platform holding the users assets
Vitalik "centralised exchanges go burn in hell as much as possible"

CENTRALISED	DECENTRALISED
Exchange controls funds	User controls funds
Not anonymous	Anonymous
Hacks & server downtime	No hacks & server downtime
Easy to use	Not easy to use
Advanced tools	Basic features
Liquidity	Low liquidity

Early Exchanges
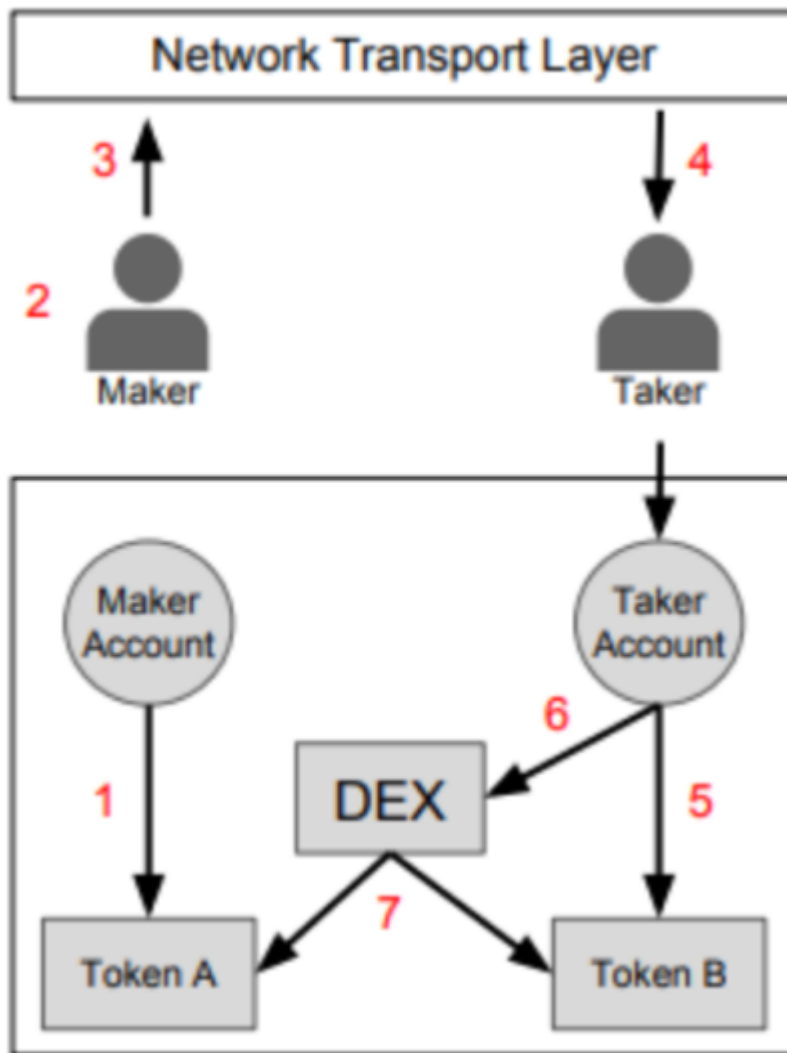
1. Maker approves the decentralized exchange (DEX) contract to access their balance of Token A.

2. Maker creates an order to exchange Token A for Token B, specifying a desired exchange rate, expiration time (beyond which the order cannot be filled), and signs the order with their private key.

3. Maker broadcasts the order over any arbitrary communication medium.

4. Taker intercepts the order and decides that they would like to fill it.

5. Taker approves the DEX contract to access their balance of Token B.

6. Taker submits the makers signed order to the DEX contract. 7. The DEX contract authenticates makers signature, verifies that the order has not expired, verifies that the order has not already been filled, then transfers tokens between the two parties at the specified exchange rate.
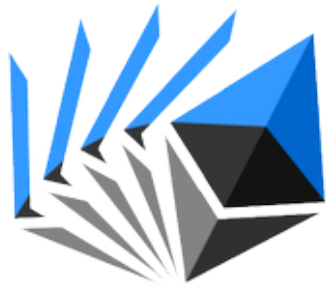
December 2017 Ether Delta is attacked

The DNS for Ether Delta is redirected to a fake site
Many people send tokens to this site thinking it is genuine
308 ETH stolen

EtherDelta @EtherDelta · 15 Aug 2018

Hello EtherDelta users, we have heard multiple reports of a false website claiming to promote an EtherDelta Token V2.0. This site has no affiliation with the real EtherDelta platform or team.

Uniswap

The first ideas came from Vitalik, Nick Johnson and Martin Koppelmann in 2016 in a Reddit post

It was followed by an implementation from Hayden Adams and launched in Nov 2018

- Launched in 2018, Uniswap is a DEX featuring an AMM
- Solves the problem of illiquid assets since anyone can set up a liquidity pool

Total value locked in Uniswap as of 27 August 2020 (source: DeFi Pulse)
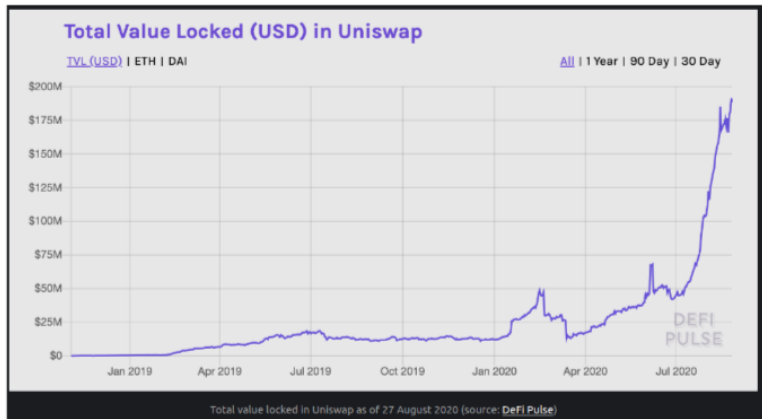
- Truly Decentralised
- Allows swap between any ERC20 pairs
- The code is robust

V2 Launched May 2020 allowing direct token swaps - halving gas fees

It solved many of the problems of the initial exchanges such as lack of incentives to provide liquidity for rarely traded assets.
It relies on a smart contract acting as an automatic market maker (AMM)

Incentivising Users

- Users deposit funds into a liquidity pool, for example ETH and USDT
- This pool (a token pair) allows users to exchange tokens
- Interacting with the exchange incurs fees
- These fees are paid to the liquidity providers

The AMM is more specifically a constant function market maker.

The term "constant function" refers to the fact that any trade must change the reserves in such a way that the product of those reserves remains unchanged (i.e. equal to a constant).

Swap   Pool   Vote   Charts↗

Swap   ⚙

ETH ⌄   1
Balance: 0 ETH   ~$ 2,847.34

↓

USDT ⌄   2845.56
Balance: 0 USDT   ~$ 2,850.73 (0.119%)

⤴   1 USDT = 0.0003514 ETH ⓘ

Insufficient ETH balance

Select Pair

◆ ETH ⌄   △ UNI ⌄

0.3% fee tier
1% select   Edit

Deposit Amounts

◆ ETH   1
Balance: 0 ETH **(Max)**   ~$ 2,847.22

△ UNI   36.1374
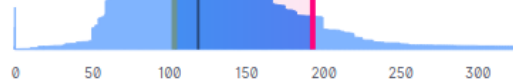Balance: 0 UNI **(Max)**   ~$ 862.921

Set Price Range   ⊕ ⊖

Current Price: 118.94 UNI per ETH

−13%   62%

0   50   100 150 200 250 300

Min Price	Max Price
− 103.94 +	− 192.82 +
UNI per ETH	UNI per ETH

Full Range

Insufficient UNI balance

LP Tokens

Typically the liquidity provider receives LP tokens when they add liquidity, say ETH and USDT

Later they can take liquidity by providing LP tokens to the contract and will receive back ETH and USDT. Ideally they will make a profit

Risks when providing liquidity

- Slippage
  Large trades can move the price

- Impermanent loss
  As a result of volatility

Losses to liquidity providers due to price variation
Compared to holding the original funds supplied
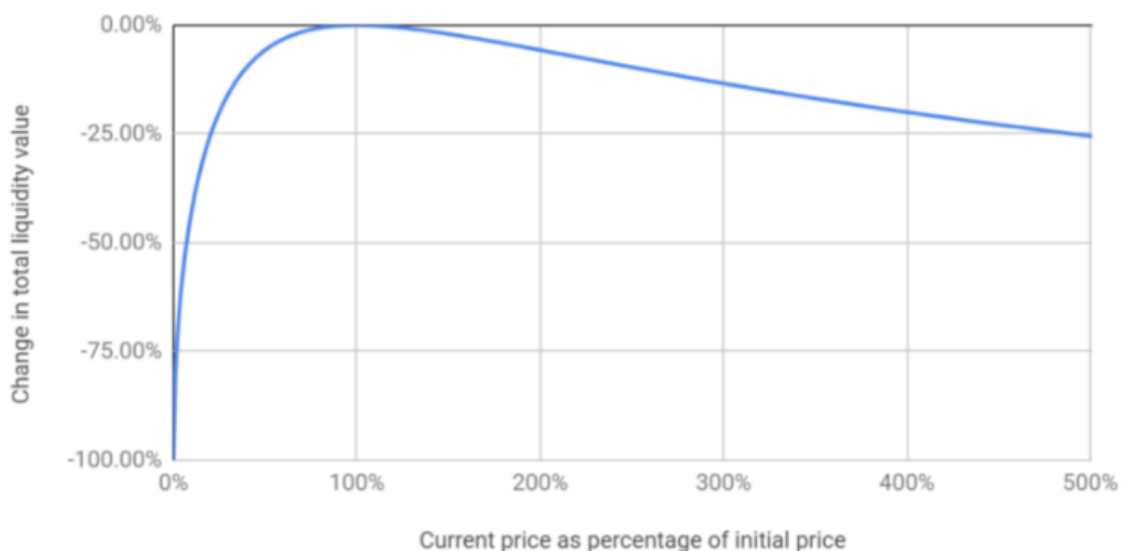
While liquidity providers can use stablecoins, yields, and rewards to help lessen the impact of impermanent loss they can also reduce this by using liquidity pools that use ratios other than 50/50. Balancer is a platform that offers liquidity pools with ratios like 60/40 or 80/20. When ETH is deposited into a pool that is 50/50 the liquidity provider has to have 50% exposure to another token. With an 80/20 pool, they only need 20% exposure to another token. You can see below how three liquidity pool ratios are affected by impermanent loss differently, with the 95/5 pool seeing the least impermanent loss.
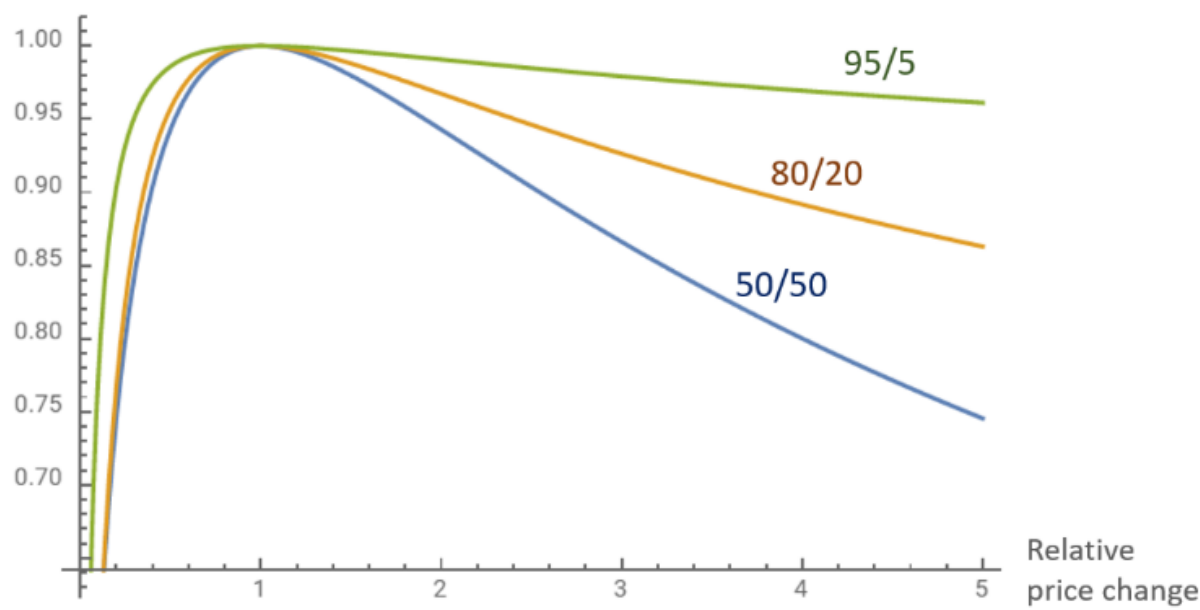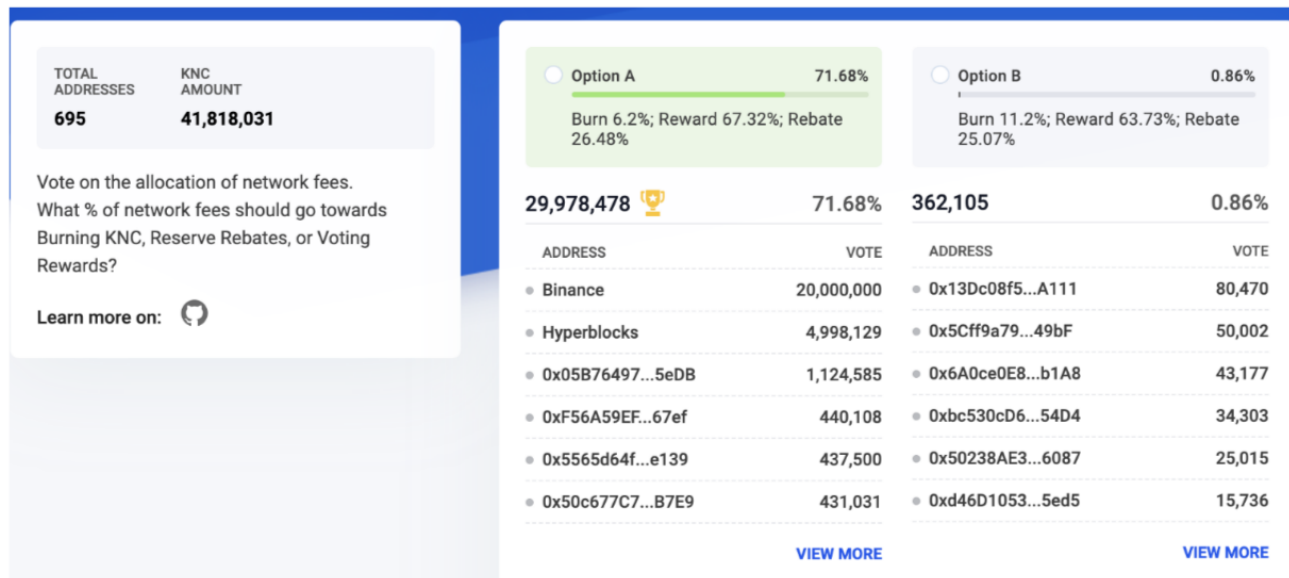
Governance and governance tokens

Holding the token gives the holder the right to vote on aspects of the protocol, typically economic settings, inclusion of assets

The tokens may have a yield

Questions

What are the issues around the governance token having a value ?
Why have a delay between the vote and the implementation ?

Yield Farming

Yield Farming at its simplest is a means of earning rewards for depositing tokens
Users are rewarded for providing liquidity
Different strategies are used by investors to maximise their rewards from the many DeFi projects
Compound and yearn.finance introduced this area to DeFi

The first Yearn product was a lending aggregator. Funds are shifted between dYdX, AAVE, and Compound automatically as interest rates change between these protocols

June 2020 BAT token APY

Assets ▽	Market size ▽	Total borrowed ▽	Deposit APY ▽	Borrow APR Variable ▽	Stable ▼
Basic Attention Token...	1.85M	1.47M	110.63 % 30D 1.51 % Avg.	193.70 % 30D 4.23 % Avg.	199.70 %
WBTC Coin (WBTC)	143.78	127.03	24.17 % 30D 0.76 % Avg.	28.87 % 30D 1.36 % Avg.	38.04 %
sUSD	332.92K	281.76K	14.03 % 30D 6.60 % Avg.	16.58 % 30D 8.07 % Avg.	—
Binance USD (BUSD)	254.55K	216.03K	14.57 % 30D 5.38 % Avg.	17.17 % 30D 6.78 % Avg.	—

Other important projects

Compound

Total Supply		Total Borrow	
$17,916,024,210.00 +0.57%		**$8,139,203,009.09** +0.97%	
Top 3 Markets		Top 3 Markets	
ETH	30.13%	USDC	45.15%
USDC	25.41%	DAI	40.52%
DAI	24.55%	USDT	7.32%
24H Supply Volume	# of Suppliers	24H Borrow Volume	# of Borrowers
$102,132,076.20	295707	$77,972,172.00	8862

All Markets

Market		Total Supply	Supply APY	Total Borrow	Borrow APY
Ether	ETH	$5,397.79M -0.19%	0.10% –	$236.49M -1.60%	2.82% -0.01
USD Coin	USDC	$4,553.05M +2.24%	4.15% -1.04	$3,674.99M +1.00%	5.60% -1.32
Dai	DAI	$4,398.66M +1.52%	2.76% –	$3,297.78M +1.50%	4.37% –
Wrapped BTC	WBTC	$1,858.42M +0.51%	0.33% –	$167.30M +0.46%	4.70% –
Tether	USDT	$760.25M -6.23%	3.29% +0.45	$595.39M +0.76%	4.57% +0.32
Uniswap	UNI	$211.26M -0.80%	0.32% +0.03	$16.45M +5.61%	5.54% +0.20
Compound Governance Token	COMP	$169.55M +1.30%	0.89% -0.02	$29.58M +0.02%	6.99% -0.06
ChainLink Token	LINK	$159.42M -0.01%	0.48% –	$18.96M +0.01%	5.48% –
Wrapped BTC (Legacy)	WBTC	$112.17M –	0.00% –	$34k +0.01%	2.32% –
0x	ZRX	$106.99M +1.21%	0.87% -0.02	$16.46M +0.08%	7.77% -0.06

Yearn

Yearn Finance is a suite of products in Decentralized Finance (DeFi) that is designed to generate yield on smart contract platforms like Ethereum. The protocol is maintained by various independent developers and is governed by YFI holders.

Core Products

Vaults

Capital pools that automatically generate yield based on opportunities present in the market. Vaults benefit users by socializing gas costs, automating the yield generation and rebalancing process, and automatically shifting capital as opportunities arise. End users also do not need to have a proficient knowledge of the underlying protocols involved or DeFi, thus the Vaults represent a passive-investing strategy.

Earn

The first Yearn product was a lending aggregator. Funds are shifted between dYdX, AAVE, and Compound automatically as interest rates change between these protocols. Users can deposit to these lending aggregator smart contracts via the Earn page. This product completely optimizes the interest accrual process for end-users to ensure they are obtaining the highest interest rates at all times among the platforms specified above.
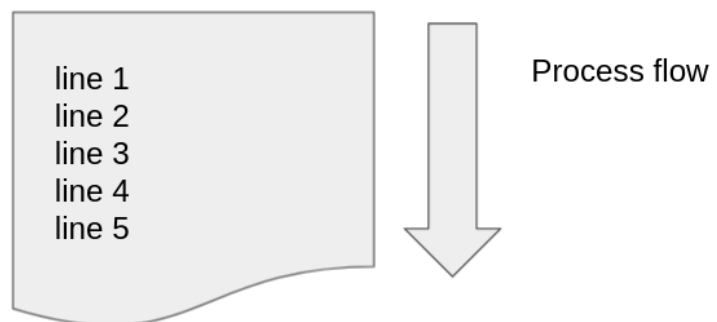
Aave and flash loans

An innovative financial product

Does a risk free loan with no collateral required, of virtually any value , with an extremely low fee (0.09 %) seem to good to be true ?

Imagine that line 2 in this contract increases the account balance by 5
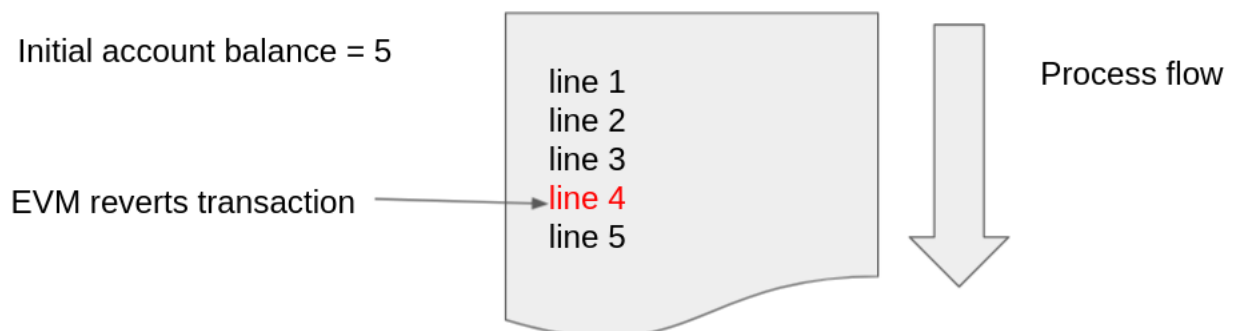
Processing a transaction

Initial account balance = 5

line 1
line 2
line 3
line 4
line 5

Process flow

Final account balance = 10

Transactions are atomic

Initial account balance = 5

line 1
line 2
line 3
line 4
line 5

EVM reverts transaction

Process flow

Final account balance = 5
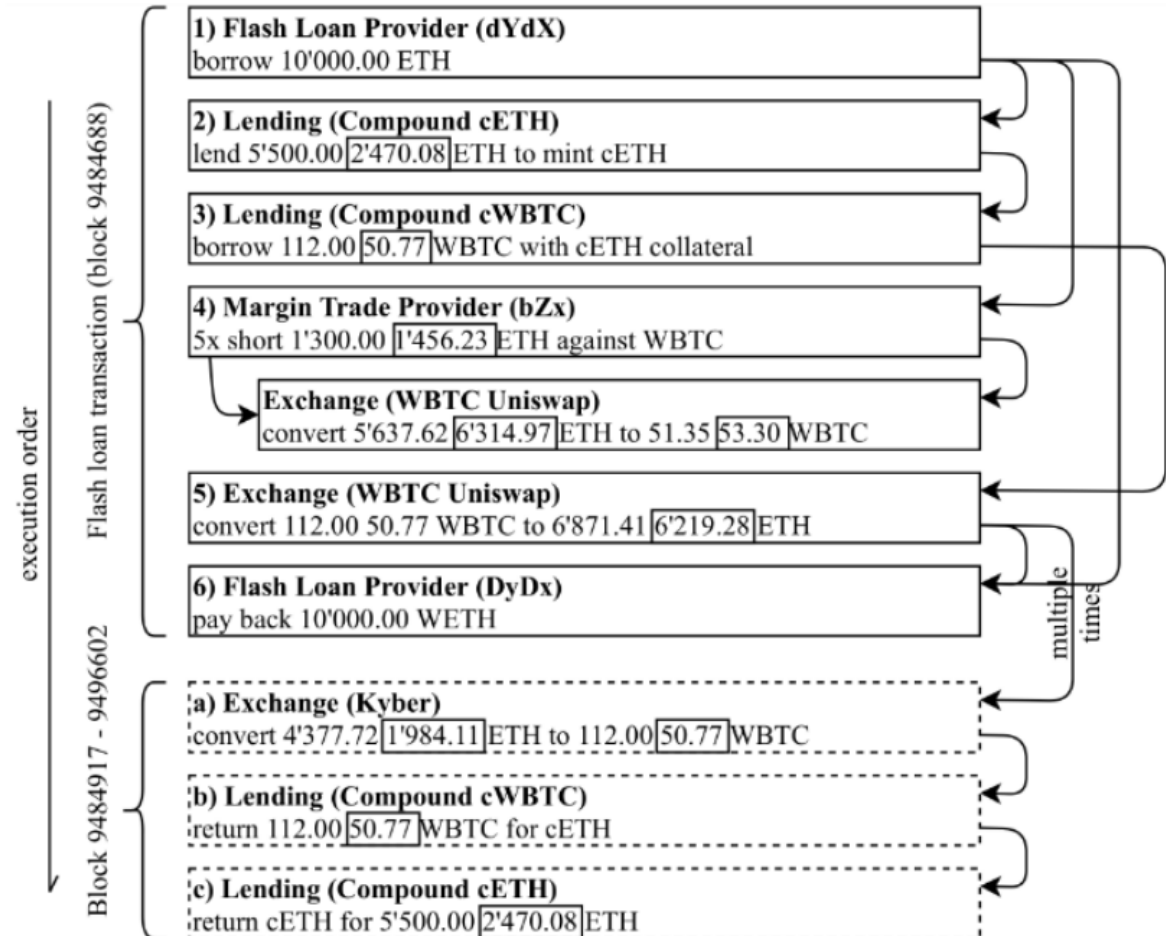
Attacking DeFi with flash loans

Attacking the DeFi Ecosystem with Flash Loans for Fun and Profit

Kaihua Qin, Liyi Zhou, Benjamin Livshits, and Arthur Gervais

Imperial College London, United Kingdom
{kaihua.qin,liyi.zhou,b.livshits,a.gervais}@imperial.ac.uk

Abstract. Credit allows a lender to loan out surplus capital to a borrower. In the traditional economy, credit bears the risk that the borrower may default on its debt, the lender hence requires upfront collateral from the borrower, plus interest fee payments. Due to the atomicity of blockchain transactions, lenders can offer *flash loans*, i.e., loans that are only valid within one transaction and must be repaid by the end of that transaction. This concept has lead to a number of interesting attack possibilities, some of which were exploited in February 2020.

This paper is the first to explore the implication of transaction atomicity and flash loans for the nascent decentralized finance (DeFi) ecosystem. We show quantitatively how transaction atomicity increases the arbitrage revenue. We moreover analyze two existing attacks with ROIs beyond 500k%. We formulate finding the attack parameters as an *optimization problem* over the state of the underlying Ethereum blockchain and the state of the DeFi ecosystem. We show how malicious adversaries can efficiently maximize an attack profit and hence damage the DeFi ecosystem further. Specifically, we present how two previously executed attacks can be "boosted" to result in a profit of 829.5k USD and 1.1M USD, respectively, which is a boost of 2.37× and 1.73×, respectively.

Flash Loans on Uniswap

Uniswap V2 flash swaps allow you to withdraw as much as you want of any ERC20 token on Uniswap at no upfront cost and do anything you want with them (execute arbitrary code), provided that by the end of the transaction execution, you either:

- pay for all ERC20 tokens withdrawn
- pay for a percentage of ERC20 tokens and return the rest
- return all ERC20 tokens withdrawn
  Liquidity provider fees are enforced by subtracting 0.3% from all input amounts, even if the input ERC20 tokens are being returned as part of a flash swap.

Summer of DeFi

From (https://twitter.com/econoar/status/1526417888029970432)
It's August 2020
Your friend pings you on Discord about a new defi contract from a well known deployer
You quickly load up diffchecker and paste in the code to compare it to the last food farm.
No diffs, it all checks out
APY is 45000%.
You ape in your net worth
Life is good

Approximate Milestones

Pre 2020

First DEXs
Uniswap

Early 2020

Synthetix
Aave - Flash loans
Ampleforth
Compound
Yearn.finance

Summer 2020

YAM
Food coins
Sushi swap

Autumn 2020

Area cools
NFTs increasingly popular

Food Coins

Some products

- YAM
- Sushi
- Hotdog
- Burger
- Kimchi
- Spaghetti

- Pizza

Products promoted with
Social Networking / Memes / Emojis / Gamification

Yam

YAM = AMPL + YFI

Yam the emoji that drew $400M in less than a day
"$90M USD was deposited in the protocol within the first 90 mins
Less than 24hrs later, more than $400M has been deposited in Yam's smart contracts,
and YAM has climbed to ~$95."

From Coindesk The Rise of Crypto's 'Weird DeFi' Moment

Decentralized finance (DeFi) started out by imitating the regular financial world, but the
way its pieces can be mixed and matched has become so easy that new entrants are
starting to get strange.

Yearn Finance (YFI), YAM, Spaghetti, Based, whatever today's variant is – the "Weird DeFi"
cohort keeps growing.
Yearn.Finance seems to have been a key shift in the market. It's effectively a robo-adviser
for yield in a smart contract, but something about it got creative juices flowing.

Weird DeFi started earlier than this. But the broader crypto world first noticed it with YAM,
which seems to be a serious effort to unite people first and BUIDL later.

Weird DeFi has also advanced the model of fair token distributions, where all participants
have equal access to distributions from launch. But that's not without tradeoffs.

YAM seemed to begin the era of "liquidity first, purpose later." (In actuality: liquidity first,
get copied, explode and then resolve to carry on. Purpose comes eventually.)

YAM - the first food coin

Taking inspiration from Yearn, Ampleforth and Compound

Aug 11 - YAM launches
- In the launch announcement, the founders noted that no formal audits had been conducted on the protocol and that this was a "10-day project from start to launch", resulting in criticism from people immune to hype.
- In less than 24 hours after launch, YAM Finance is already managing around $580 million in crypto assets.

Aug 12 / 13 - A bug is discovered, which made the governance unworkable.
- Within 6 hours the price of YAM falls from $160 to $4

brock Y
@brockjelmore

i'm sorry everyone. i've failed. thank you for the insane
support today. i'm sick with grief

9:01 AM · Aug 13, 2020 · Twitter for iPhone

Fair Launch

(From fairlauch.capital)
What is a Fair Launch?

➡️ A decentralized crypto network that is earned, owned and governed by the community from the outset.
➡️ Everyone can participate on equal footing.
➡️ There is no early access, pre-mine or allocation of tokens.