

Lesson 11 - DeFi

Checking the status of the test networks

See [status](#)

Uint256 review

Library

This has a struct to hold the values and 2 operations on the values

The value is split into 2 parts high and low with

Low = least significant 128 bits, High. = most significant 128 bits

We need the implicit argument `range_check_ptr` for the functions.

Functions include

- `uint256_check`
- `uint256_add`
- `uint256_mul`
- `uint256_sqrt`
- `uint256_lt`
- `uint256_le`
- `uint256_unsigned_div_rem`

See the repo for others

Example of using Uint256 in Cairo

```
%builtins output range_check

from starkware.cairo.common.uint256 import (uint256_add, Uint256,
    uint256_mul)
from starkware.cairo.common.serialize import serialize_word

func main{output_ptr : felt*, range_check_ptr}(){
    alloc_locals;
    local num1 : Uint256 = Uint256(low=0,high=10);
    local num2 : Uint256= Uint256(low=0,high=3);
    let (local mul_low : Uint256, local mul_high : Uint256) =
uint256_mul(num1, num2);
    serialize_word(mul_high.low) ;

    return ();
}
```

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. ”

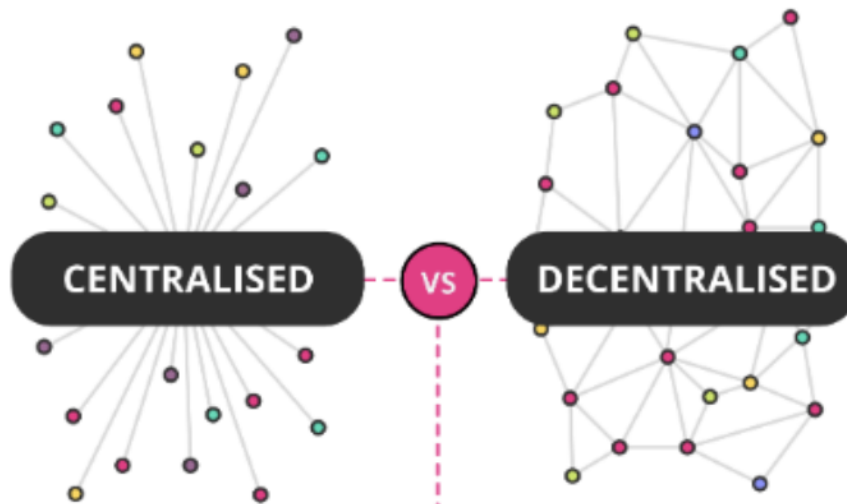
Areas

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

Decentralised Exchanges

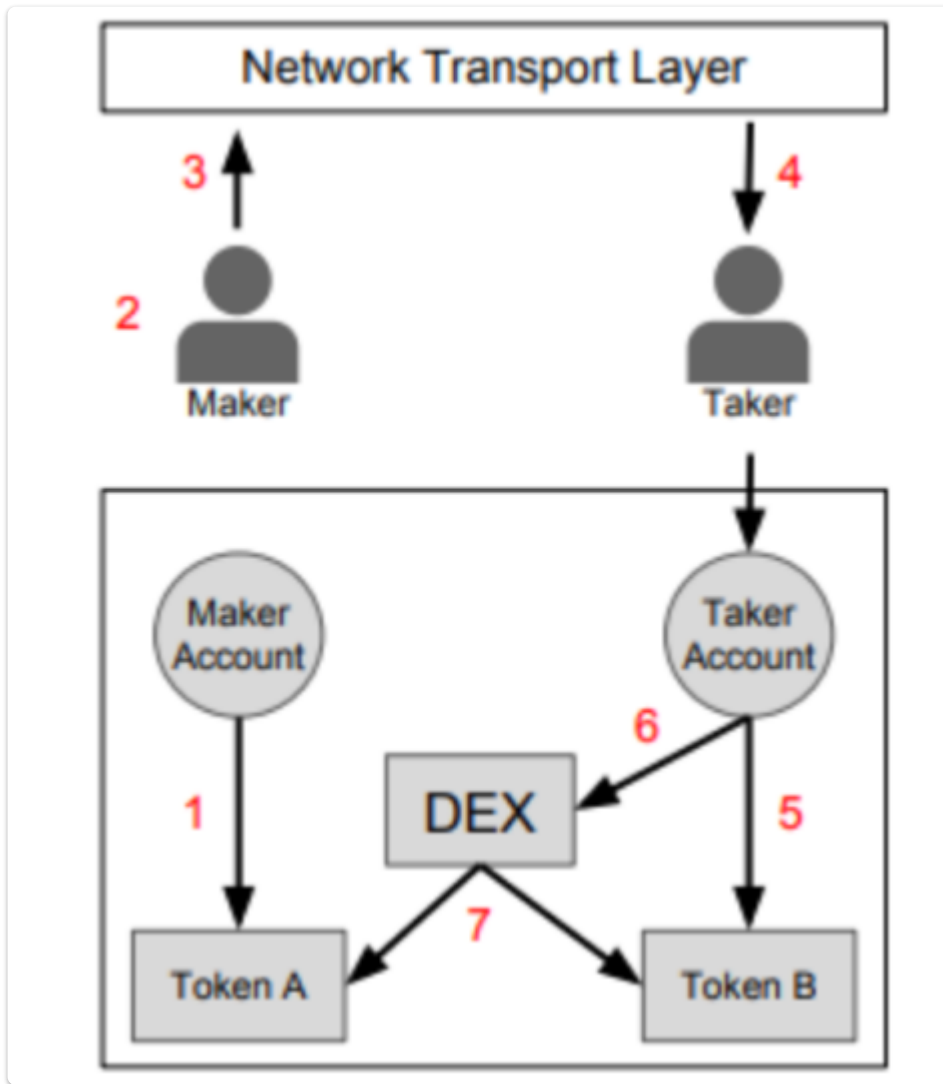
Decentralised Exchanges are a protocol to provide asset exchange without the platform holding the users assets

Vitalik "centralised exchanges go burn in hell as much as possible"



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 maker's signed order to the DEX contract. 7. The DEX contract authenticates maker's 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.
-



EtherDelta

DECEMBER 2017 ETHER DELTA IS ATTACKED

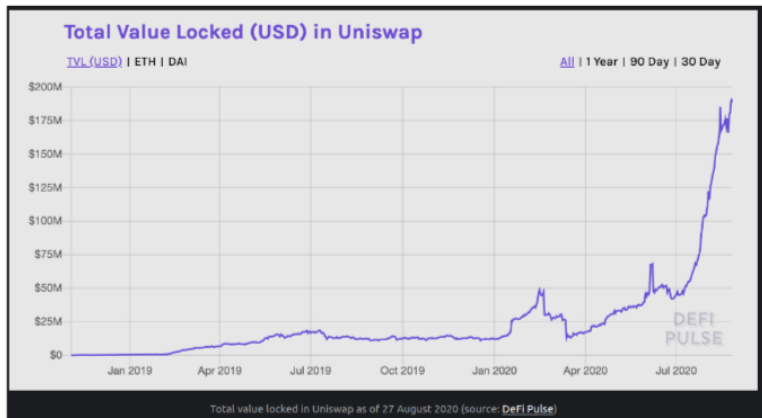
The DNS for Ether Delta is redirected to a fake site
Many people send tokens to this site thinking it is genuine
308 ETH stolen

Uniswap

The first ideas came from Vitalik, Nick Johnson and Martin Koppelman 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



- 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).



Add Liquidity

[Clear All](#)

UNI ETH



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%



Min Price



103.94



UNI per ETH

Max Price



192.82



UNI per ETH

Full Range

Insufficient UNI balance

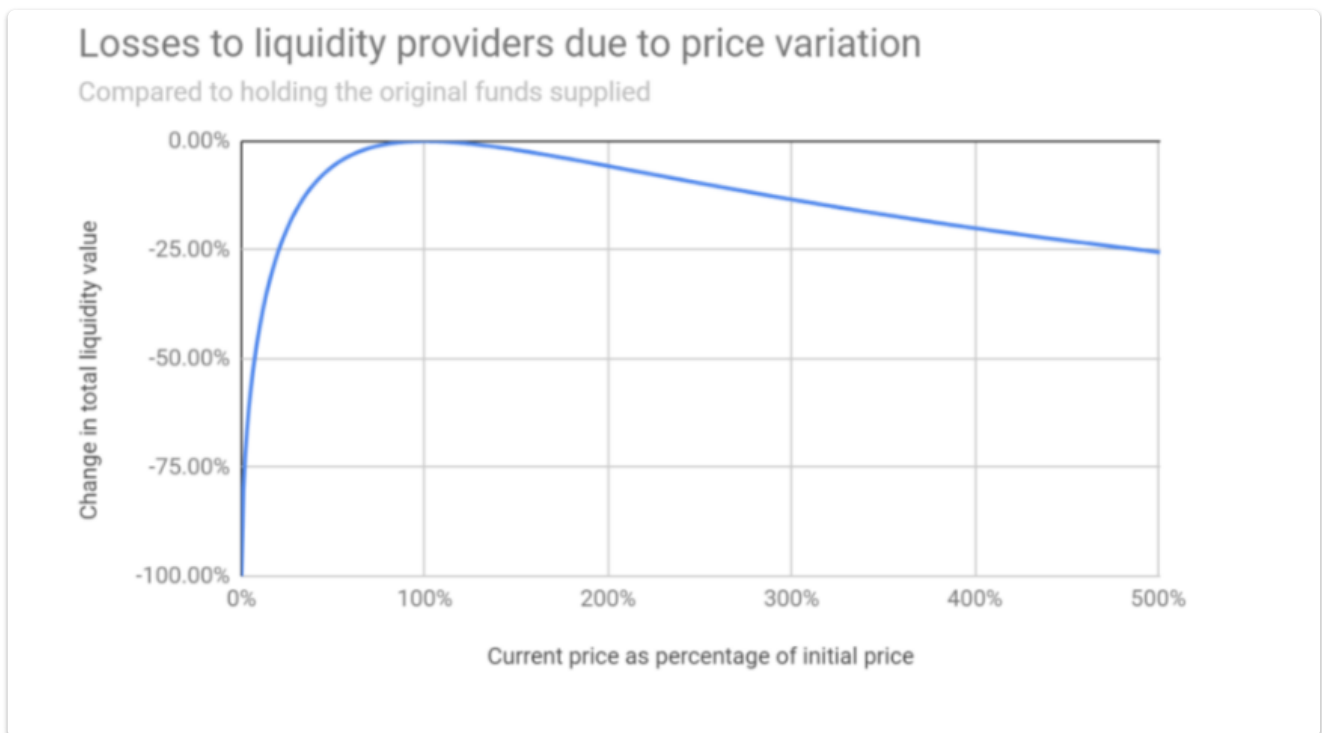
LP Tokens

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

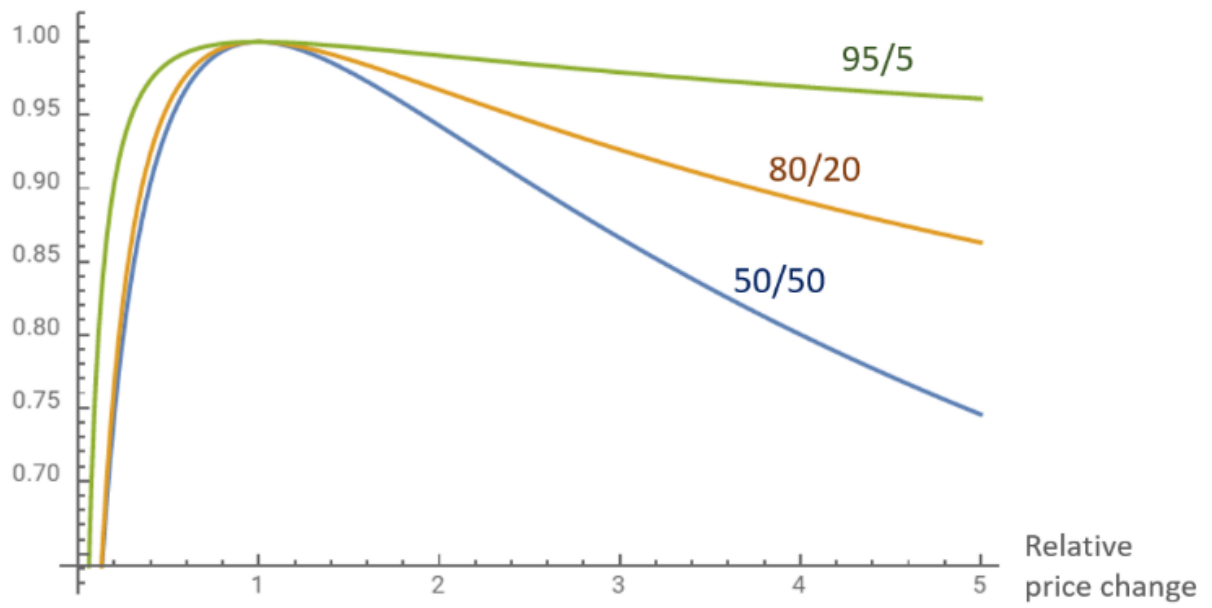
RISKS WHEN USING AN AMM

- Slippage
Large trades can move the price
- Impermanent loss
As a result of volatility



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.

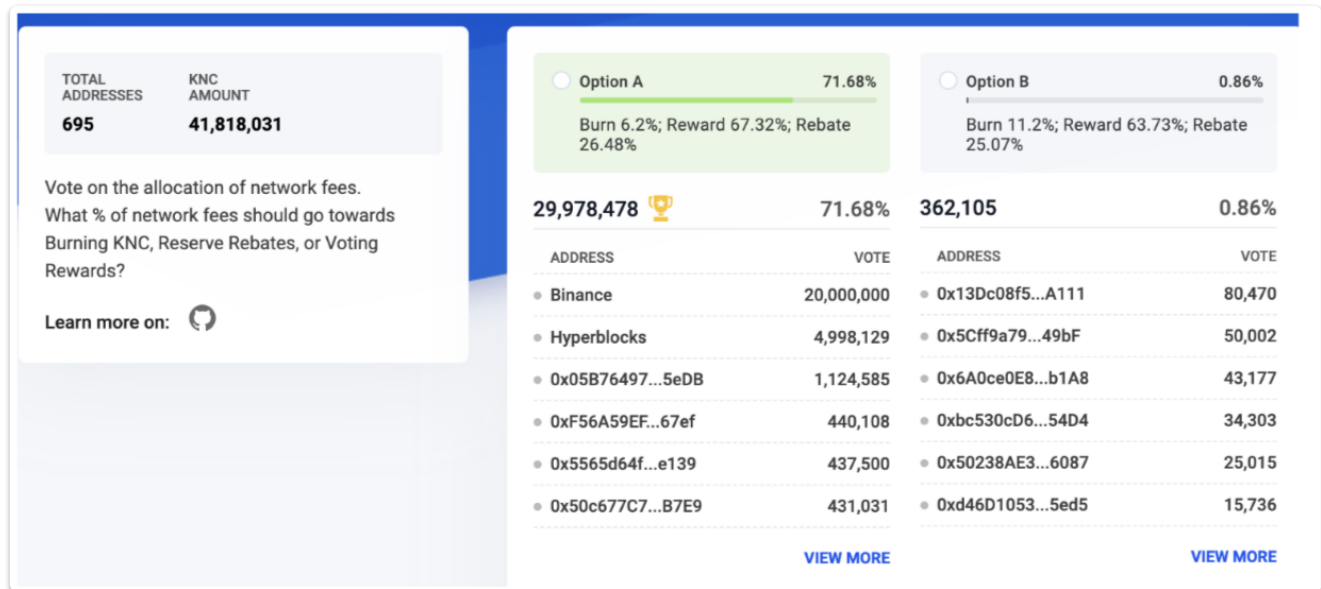
Impermanent Loss



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



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 APY ▾	
				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.	—

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

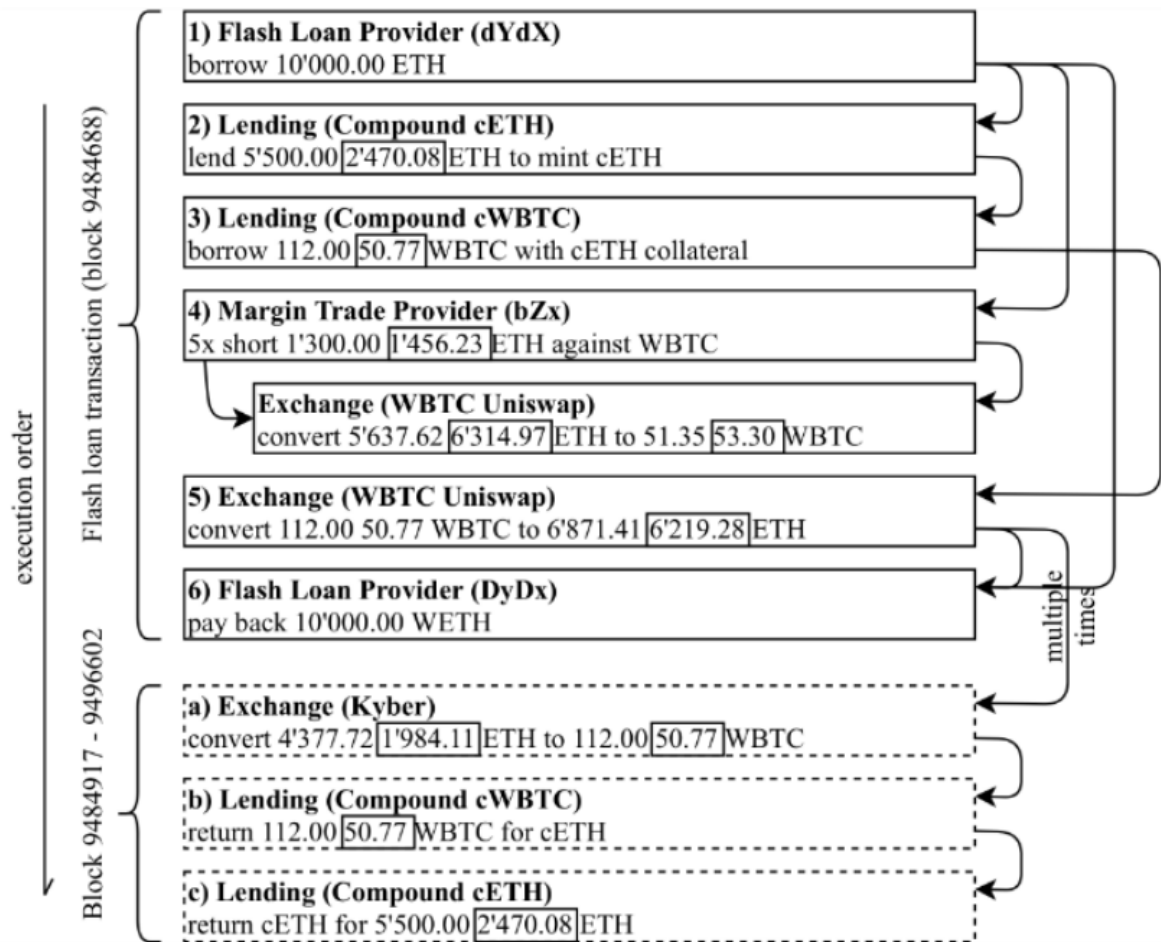
line 1
line 2
line 3
line 4
line 5

Process flow

EVM reverts transaction

Final account balance = 5

Attacking DeFi with flash loans



DeFi on Starknet

See the ecosystem page for an [overview](#) of projects

Uniswap

See [announcement](#) from Nethermind

See Unistark [repo](#)

We will look at this in more detail when we look at warp.

Aave

See the aave-starknet project [repo](#)

Phase 1 [announcement](#) of the completion of the Aave / Starknet [bridge](#)

The system allows the following:

- Liquidity providers can “bridge” their Aave v2 Ethereum aTokens via the Aave <> StarkNet bridge to/from StarkNet.
While being on StarkNet, the representation of the aTokens there keeps accruing the yield of Aave on Ethereum, but also allows the liquidity provider to for example “sell” them to Starknet users for a premium, or even use them in one of the Starknet DeFi applications that are continuously appearing.
 - StarkNet users (mainly those holding assets on the network) are able to “buy” the StarkNet aToken representations, not being submitted to transaction costs of Ethereum. And by holding them in their wallet, they accrue yield.
 - If any AAVE rewards program would be active on Aave v2 Ethereum, the system allows holders of aTokens on StarkNet to accrue those AAVE rewards over time, and claim AAVE on Ethereum, whenever they decide to.
-

See [blog](#)

ZKX is building a protocol that allows trading asset derivatives on StarkNet.

They are introducing an "Adaptive Balancing Rate" which is intended to give a rate that adapts quickly in volatile markets.

- Swap Liquidity Mining

This incentivises participation and introduces some gamification into the product in order to increase the overall volumes.

- T-Swaps

These are options that allow profits when the market is volatile or moving lower.

- Decentralised Limit Order Book (DLOB)

"In one sentence, the decentralised limit order book enables the trader to work in a fast-paced environment. What's more important for us, we run on the principle of decentralised and permissionless. And our order book is completely decentralised and not controlled by anyone"

- Liquid Governance

As a reward for your participation in the protocol you are given governance shares that allow you to vote on how the protocol is governed.

Briq

"Briq is NFT matter"

"We want to make NFTs more composable, interoperable, and on-chain. We want NFTs to swoosh seamlessly from one game to another, to be the backbone of the metaverse. We want briq to be a composability system to give NFT matter and easily compose them."

briqThemesResourcesConnectCreate

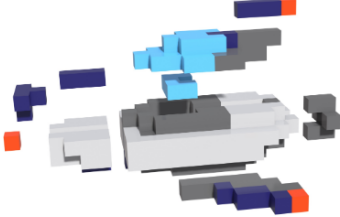
Collect


briqs are construction blocks stored on the blockchain. You can use them to build anything you want.

Technically, they're ERC-1155 tokens stored on Starknet, an Ethereum layer two solution allowing cheap transaction costs.

Your briqs are yours, forever.

[Check out our briq boxes →](#)





Build

Assemble your briqs to create NFTs. These NFT are called sets.


Transfer, sell, lend, break your NFTs any way you want.

Disassemble your set to get your briqs back and build something new.

[Start building →](#)

"You can mint briqs, build a set with your briqs, transfer your set to someone, disassemble a set to get the briqs back and build something new.

Anything built out of briqs is an NFTs. You can think of briq as NFT building blocks."



The StarkNet Yield Aggregator

Grow your Ethereum assets cheaply on the most sophisticated Layer 2

[Deposit](#)
[Learn more](#)
[Join 1000+ others on Discord](#)

Apply to become a contributor New

Build new vaults using Cairo, the StarkNet native smart contract programming language

[Join us →](#)

Projected APY
4.2%

Your position
0 USDC of Vault TVL 108.346426 USDC

[Learn about Risks](#) [Trade ETH to get USDC on JediSwap](#)

Available balance: 0 USDC
Max deposit: 34028236692093846346374607431768.211 USDC

Max withdraw: 0 USDC

Deposit Amount

Withdrawal Amount

[Deposit](#)
[Withdraw](#)

Nexus Staking
Stakers LORDS to receive trading fees

Projected APY
1158.8861261266477654 LORDS of Vault TVL 55723.236573895813170137 LORDS

[Learn about Risks](#) [Trade ETH to get LORDS on JediSwap](#)


Available balance: 99000 LORDS
Max deposit: 340282366920938463463.375 LORDS

Max withdraw: 1158.8861261266477654 LORDS

Deposit Amount

Withdrawal Amount

[Deposit](#)
[Withdraw](#)



[Swap](#)
[Liquidity](#)
[Stake](#)
[Vote](#)
[Rewards](#)

0x2e4c...1018
Alpha Görli

USDC

0.00

0.00

USD

0.00

0.00

Slippage:0.3%

Deadline:in 1 hour

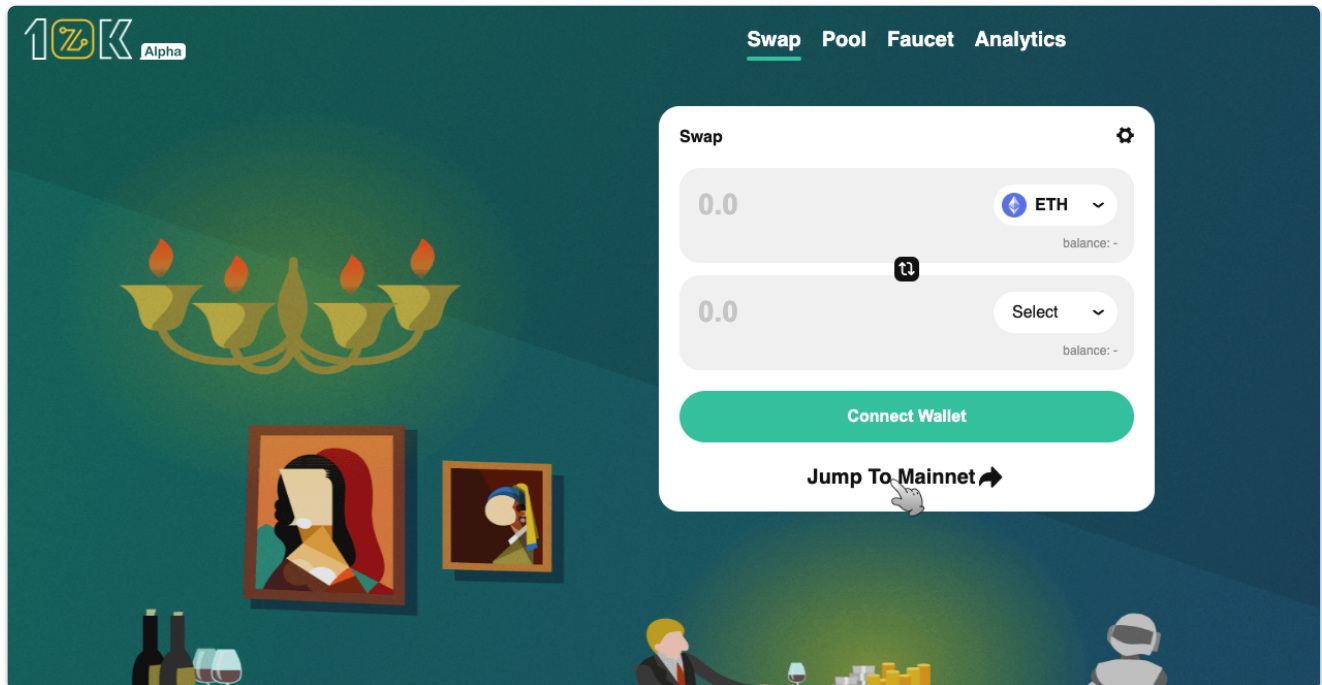
Swap

10kSwap

10K Swap is an automatic market maker

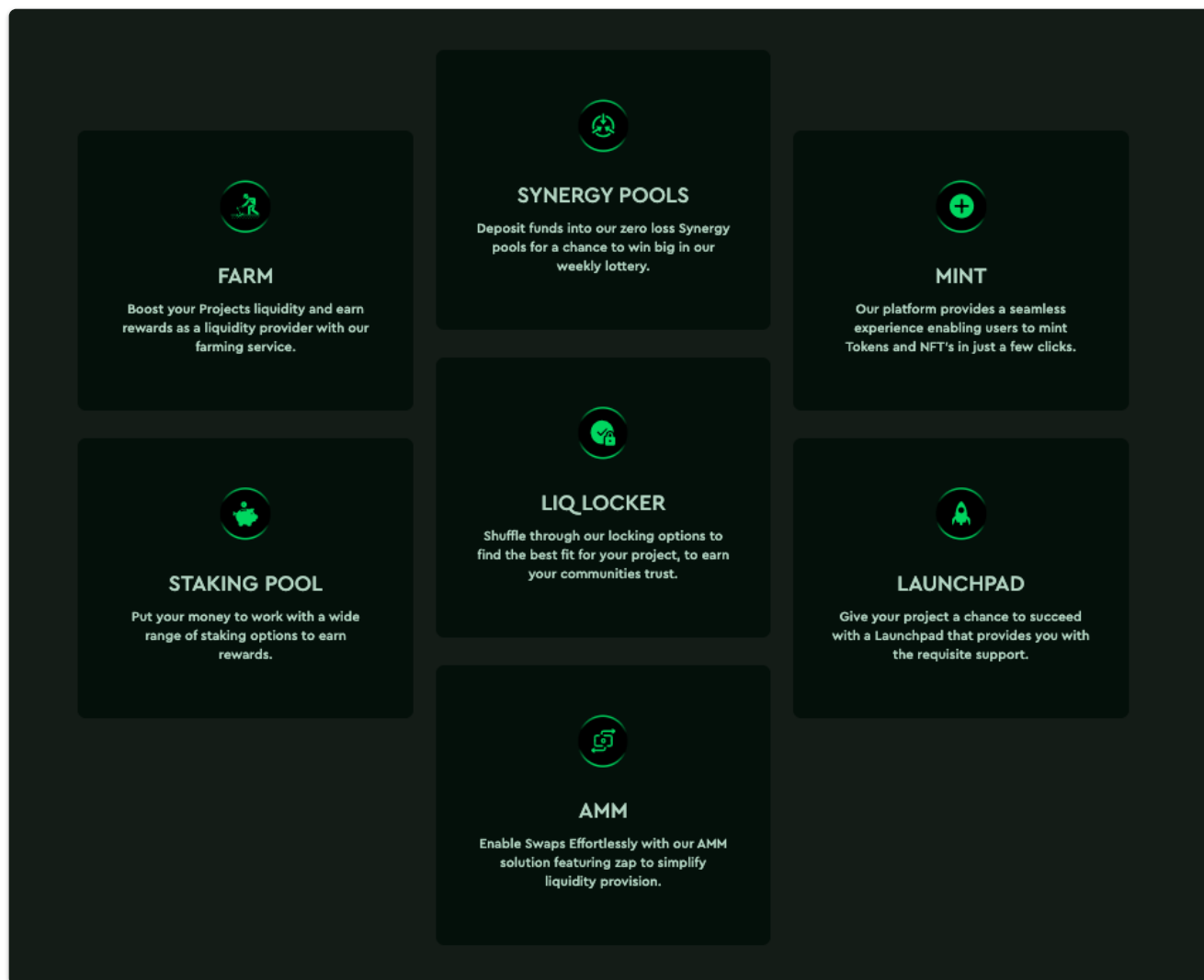
See [app on goerli](#)

See [github](#)



Stark DeFi

A DeFi Solutions Hub



Astraly

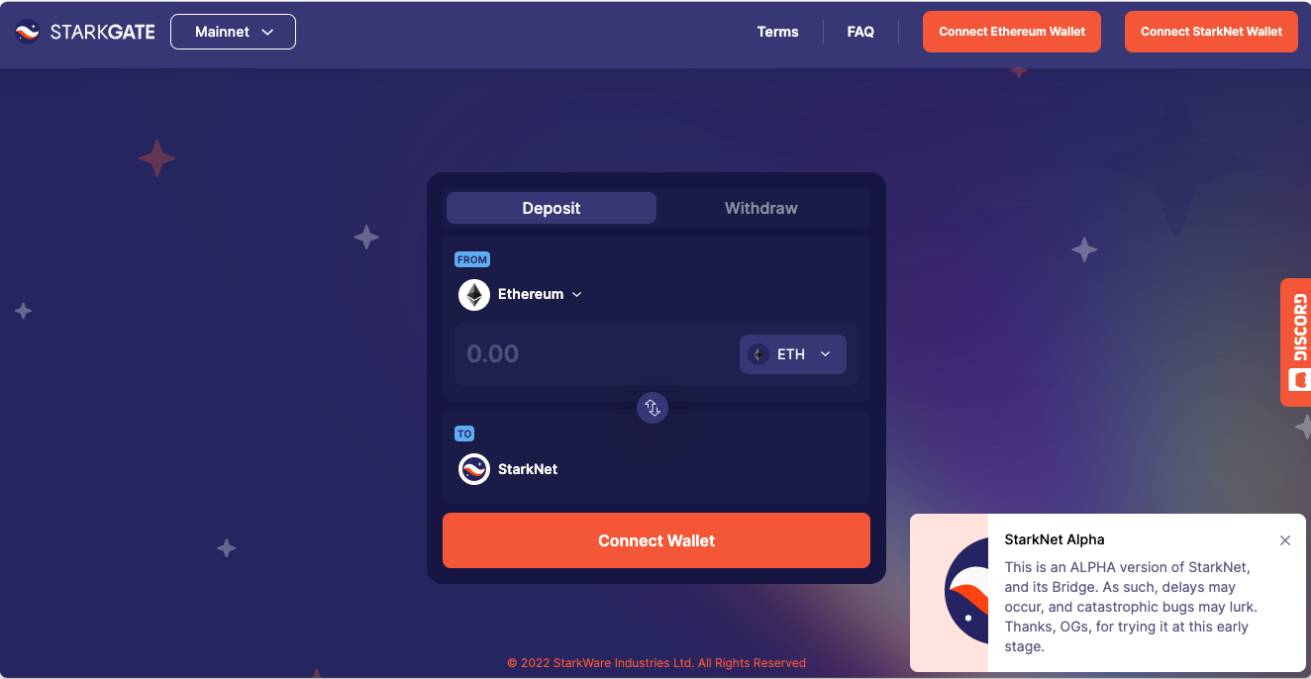
Astraly is a fundraising and community building platform. Buy ASTR tokens, stake them and receive lottery tickets to invest in the listed projects.

[app on goerli](#)
[github](#)

Flashloans on Starknet


See [Repo](#)

Starkgate



Layerswap

Layerswap allows connection between exchanges and Starknet


 **Layerswap**


Exchange → Network

Network → Exchange

From

To


 **Binance** ▼

 **StarkNet** ▼

To StarkNet address

0x123...ab56c

Amount


0.0045 - 0.015  **ETH** ▼

You will receive

- ▼

Enter StarkNet address


Orbiter


 **Orbiter**


L2 BridgeL2 Data


Connect a Wallet

SenderMaker


Token  ETH


From
 Ethereum at least 0.005 [Max](#)



To
 StarkNet 0 ?

CONNECT A WALLET

 Gas Fee Saved | Save \$0.11 ~ \$0.71 ?

 Time Spend 180s | Save 10min ?

MakerDAO Starknet DAI Bridge

[App on goerli](#)

[Github](#)

StarkEx

See [Docs](#)

StarkEx allows self-custodial trading and payment transactions for applications such as DeFi and gaming.

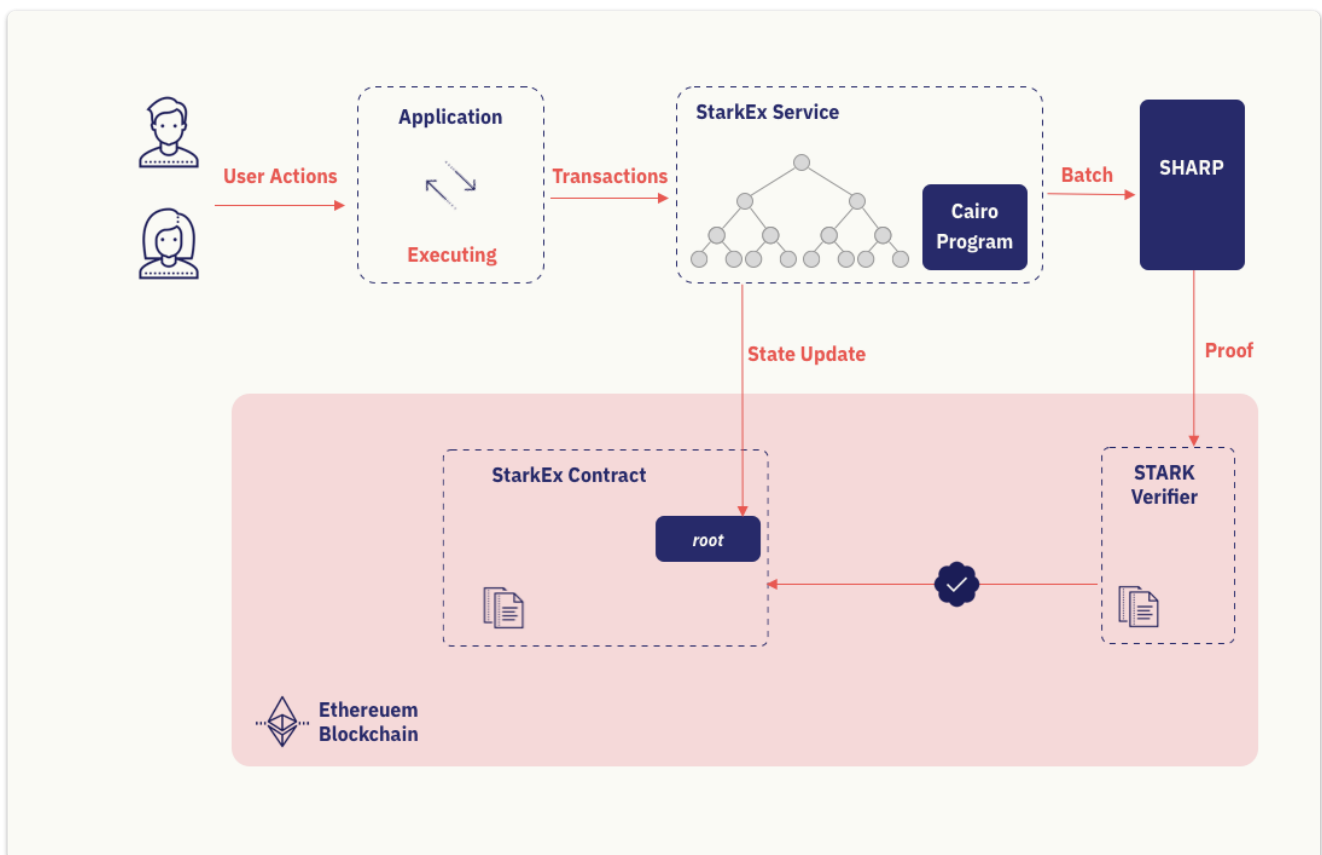
It has 270B cumulative trading and 65M transactions settled, with 1.25B total value locked.

StarkEx currently supports ETH, synthetic assets, and the following tokens:

- ERC-20
- ERC-721
- ERC-1155

StarkEx can also support tokens on other EVM-compatible blockchains.

StarkEx is a mature platform that has been deployed on Ethereum Mainnet since June 2020. Before its Mainnet deployment, over 50M StarkEx transactions were settled on both public and private Ethereum testnets.



StarkEx is trading focussed whereas Starknet allows generic computation