FINTECH BROCHURE

OA LEGAL

SWISS INNOVATIVE LAW FIRM

DECENTRALIZED FINANCE (DeFi)

TABLE OF CONTENTS

DECENTRALIZED FINANCE

DeFi uses programmable self-executing smart contracts enabling the creation of new financial instruments and digital assets.

Decentralized finance essentially involves a brand-new financial system being built on top of the public blockchain networks such as Ethereum, Bitcoin or EOS. DeFi has emerged as one of the most active sectors in the blockchain space, with a range of use cases for developers, individuals, and institutions. The creation of Decentralized Applications (hereafter:' "dApps") on public blockchains gives the opportunity to create new financial instruments.

July 2020 was a remarkable moment in time for the DeFi ecosystem. The total value of crypto locked upon smart contracts, dApps and protocols built on Ethereum went from 2 billion dollars to 5 billion dollars in nearly four weeks. The increasing popularity of Yield farming was one of the factors causing this growth.

Decentralized finance has many advantages over the traditional financial infrastructure. Some significant advantages are listed in the circle.

DEFI TOOLS

TOKENIZED INVESTMENTS

e.g. Codefi, Polymath

DECENTRALIZED BORROWING & LENDING PLATFORMS

e.g. Compound, Aave

DECENTRALIZED MARKETPLACES

1. Marketplace for derivates
   (e.g. Synthetix, dYdX)
2. Decentralized exchanges ("DEXEs"):
   - Automated Market Makers
   (e.g. Uniswap, Bancor)
   - Open order book exchanges
   (e.g. Radar Relay)

DECENTRALIZED IDENTITY (COMPLY WITH KYC REGULATIONS)

e.g. 3Box, Bloom

DECENTRALIZED INSURANCE SERVICES

e.g. Nexus Mutual, Opyn

DECENTRALIZED PAYMENT CHANNELS / AGGREGATORS

e.g. Raiden, Lightening / e.g. 1inch, Paraswap

The importance of liquidity for the growth and development of Decentralized Finance

Liquidity, the availability of liquid assets to a market or company, is one of the most important aspect of any type of financial market. Liquidity largely affects how the price of an asset will move. When there is not enough liquidity, there is a problem of high price volatility and inefficient conversions between assets.

Liquidity pools were created to avoid this lack of liquidity. Liquidity pools are considered as an important achievement in the decentralized institution building. Decentralized liquidity is the pillar of Decentralized Finance. That is why it is worth to start with the functioning of liquidity pools before getting deeper into decentralized tools such as decentralized exchanges and decentralized borrowing and lending platforms making use of these liquidity pools.

LIQUIDITY POOLS

What are liquidity pools?

Liquidity pools are algorithmic-based smart contracts that perform autonomous, peer-to-contract token trades.

The purpose of the liquidity pools is to enhance liquidity by creating a large pool of liquidity, which makes trading possible according to a constant product formula. This constant product formula ensures the constant value ratio of each reserve even as the ratio of the assets would change.

Liquidity pools encourage liquidity holders to provide their liquidity to a liquidity pool. The liquidity provider is rewarded by receiving a percentage of the trading fee.

Liquidity pools has significant advantages which are listed in the circle.

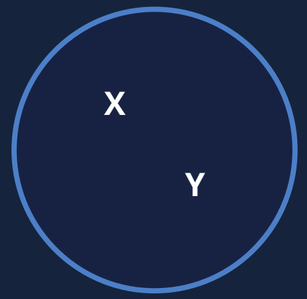
- Remove the dependence of tokens on trade volume;
- Make use of automated smart contracts who are creating more competitive involvement in market –making;
- Offer a complete and automatic transparency on the use of funds;
- Ensure that liquidity is constant at every price level;
- Contain automated pricing which enables passive market making (no central party can block the process).

- Give anyone the opportunity to become a liquidity provider and earn;
- Have an automated distribution of fees to the liquidity providers.

How does liquidity work?

Liquidity pools show the high potential of decentralized cryptocurrency markets.

Let us take the example of a single liquidity pool that holds two tokens X and Y: each pool creates a new market for that particular pair of tokens.



When a new pool is created, the first liquidity provider sets the initial price of the assets X and Y in the pool. Every following liquidity provider will use the same exchange rate. Liquidity pools rely on arbitrage opportunities and not on external price settings. When the initial price of the tokens in the pool is no longer the same as the current global market price, arbitrage traders will see an arbitrage opportunity by buying an asset from a lower price market and selling the asset in a higher price market.

Anyone can become liquidity provider for a pool by depositing liquidity in the pool in return for special pool tokens called LP tokens representing the ownership stakes in the liquidity pools. Liquidity providers receive a commission in the form of a pro-rata share of the trading fee paid when a trade is facilitated. The more people trade in a pool, the more liquidity providers earn on the fees and so the value of their shares grow. **In this way, liquidity is always constant**.

Each token trade that a liquidity pool facilitates results in a price adjustment according to a deterministic pricing algorithm called Automated Market Makers. The bigger the pool is in comparison to a trade, the lesser the price impact occurs, so large pools can accommodate bigger trades without moving the price too much. The more people trade in a pool, the more liquidity providers earn on the fees and so the value of their shares grow.

DECENTRALIZED EXCHANGES

Decentralized Exchanges are smart contracts allowing users to trade digital assets without the need for a central authority to hold their funds.

Decentralized exchanges can be order book peer-to-peer exchanges (e.g. Radar Relay) similar to the traditional order book exchanges or can be decentralized exchanges based on the previous mentioned liquidity pools. These liquidity pools are used to secure the availability of constant liquidity when trading crypto assets.

Automated Market Makers, a decentralized exchange based on liquidity pools will be discussed in the following paragraph.

Automated Market Makers

Uniswap
Bancor

Automated Market Makers issues & solutions

Impermanent loss
Multi-token exposure
Opportunity cost

Automated Market Makers

Automated Market Makers enable the creation and running of openly accessible on-chain liquidity for different tokens.

Automated Market Makers (hereafter: “AMM”) based Decentralized Exchanges (hereafter: “DEXEs”) have proven to be one of the most impactful Decentralized Finance innovations. Instead of using a traditional buy/sell order book, both sides of trades are pre-funded by on-chain liquidity pools. Market making is done automatically.

In the following paragraph we highlight two examples of Automated Market based Decentralized Exchanges, named Uniswap and Bancor.

Uniswap

Uniswap version 1 is an on-chain system of smart contracts on the Ethereum blockchain, using cryptocurrency, ETH, as the medium of trade. Uniswap is a Constant Product Market Maker (hereafter: “CPMM”). The liquidity pools store a pooled reserves of two assets. Liquidity is provided for both assets, maintaining the invariant that the product of the reserves cannot decrease.

The liquidity providers get a part of the trading fee in proportion to their share in the pool. In this way, providing liquidity is incentivized.

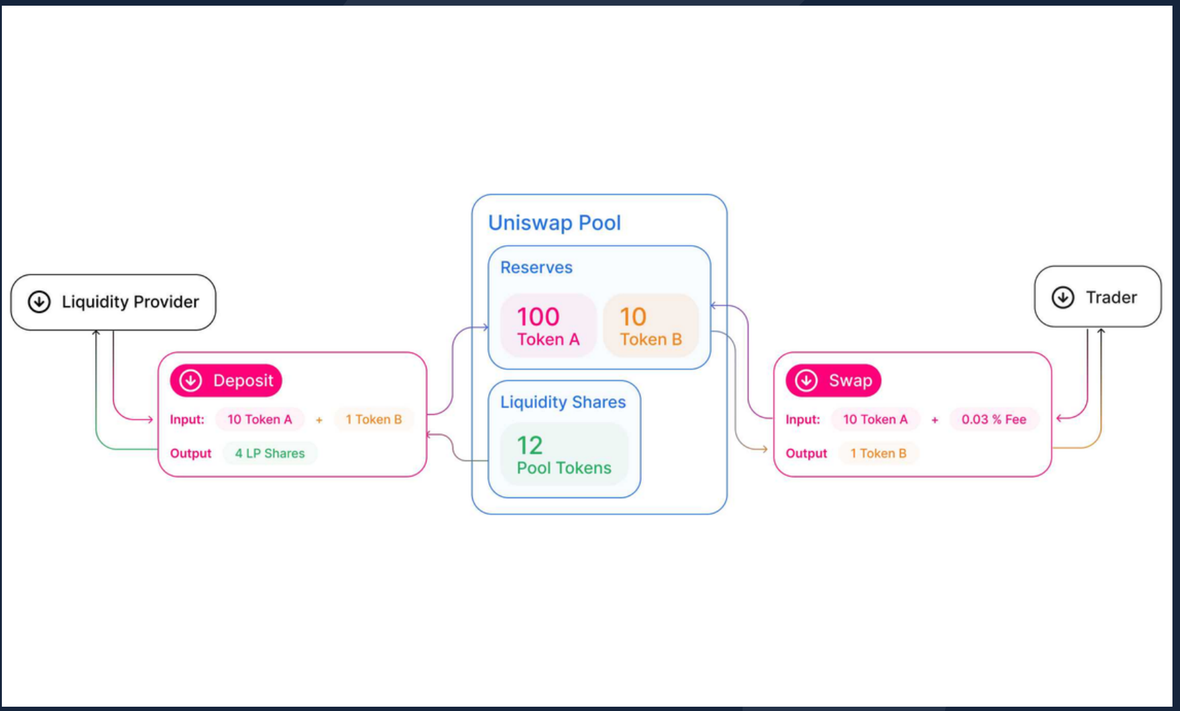
Uniswap launched recently his version 2 which is a new implementation of its formula, with several new highly-desirable features such as arbitrary pairs between ERC20s, a hardened price oracle and flash swaps.

Bancor

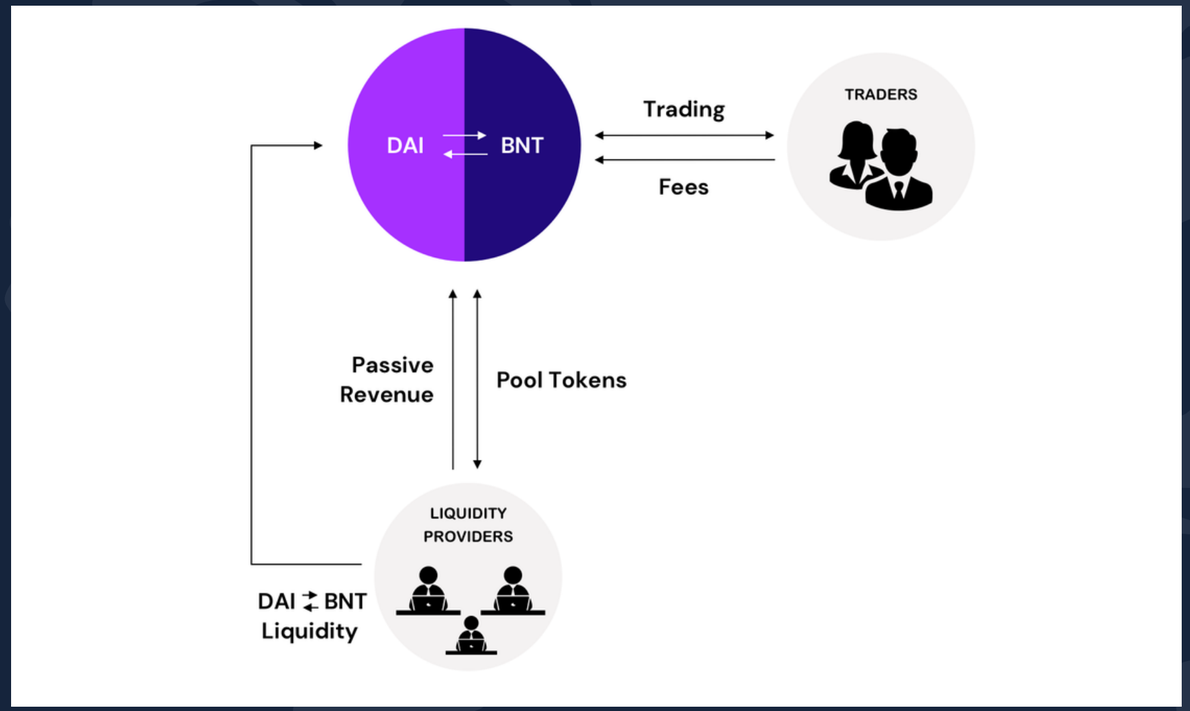
Bancor version 1 is a decentralized protocol for automated liquidity provision for all type of blockchain-based asset, such as Ethereum and EOS. The Bancor Protocol enables automatic price determination and an autonomous liquidity mechanism for tokens on smart contract blockchains. Bancor makes use of his own native currency token called Bancor Network Token.

Bancor launched recently his version 2, which is a new implementation with several new highly-desirable features such as a new design Dynamic Automated market Maker (with Chainlink price Oracles), single token exposure, support for lending protocols and efficient bonding curve reducing slippage.

Uniswap



Bancor



Automated Market Makers issues & solutions

First generation Automated Market Makers such as Bancor and Uniswap were confronted in their first version with several issues. Bancor and Uniswap both released a new version in which they try to solve these specific problems.

Impermanent loss

Version 1 of the AMMs were programmed to keep up a fixed balance of assets in a liquidity pool. The weight of the assets retained their balance while the prices of the underlying assets fluctuate. AMMs do not automatically adjust their exchange. This is causing liquidity providers to suffer from a financial deficit.

Multi-token exposure

First generation AMMs commonly require liquidity providers to provide an equal amount of the represented assets in the pool. As a result, liquidity providers are unable to keep their long exposure to a single asset, and instead have to split their exposure by holding an additional ERC20 reserve asset.

Opportunity cost

Liquidity providers have opportunity costs for the assets locked down. When the liquidity provider did not earn any (or enough) interest on the provided liquidity, the liquidity provider could have used the assets on for example a borrowing and lending platform to earn (a higher) interest on them.

UNISWAP version 2

Arbitrary pairs

Uniswap version 2 allows any ERC20 token to be pooled with any other ERC20 token (ERC20/ERC20). This gives liquidity providers the flexibility to maintain a more diverse combination of ERC20 token positions and create more potential pool combinations for trades to pull liquidity from.

This reduces friction for token communities and allows both teams and holders to build and benefit from deeper, permissionless liquidity. It is no longer necessary to pool only a pair of tokens between ERC20 and ETH.

Flash Swaps

The Uniswap version 2 flash swaps allow users to lend unlimited money from a liquidity pool without upfront cost before paying for them later in the transaction. Flash loans allow Uniswap users to make fewer transactions, thereby reducing fees.

BANCOR version 2

Chainlink oracles

Creation of a new Automated Market Maker design named Dynamic Automated Market Makers (hereafter: “DAMMs"). They hold the relative value of their reserves constant using prices from Chainlink oracles instead of relying on arbitrage traders. All liquidity providers in the pool should be able to withdraw the same amount as they staked plus a share of the fees.

Single token staking

Users have the option in Bancor version 2 to provide only liquidity to a single ERC20 token. Users do not longer have the obligation to hold a separate reserve token. The single token exposure makes it possible to hold a long-term position while earning trading fees on those single tokens.

Decreased opportunity costs

Bancor version 2 gives the ability to create Automated Market Makers integrated with existing lending protocols. This will increase profitability liquidity providers as they can generate lending interest on top of trading fee. The lending interest decreases opportunity costs.

DECENTRALIZED LENDING / BORROWING

Decentralized Lending/borrowing protocols are smart contracts handling the lending or borrowing process without the need for an intermediary.

The interest rates in these protocols are variable because they are determined by the supply and demand for an asset on the platform. There are lower risks for lenders because of the secured loans with more collateral than borrowed value.

The following paragraph illustrates an example of a decentralized lending/borrowing protocol:

Compound is an algorithmic autonomous interest rate protocol.

The first version of Compound was launched as an experiment to earn interest or enable borrowing.

Compound version 2 guarantees frictionless borrowing of Ethereum tokens, allowing any supported asset as a guarantee to obtain a loan. Users have a flexible choice in the assets they wish to borrow.

What makes Compound popular is that all those that contribute an asset receive immediately interest. This flexible lending mechanism is a key element of Compound. Compound incentives liquidity by relying on the interest rate model. When there is a high demand for a certain asset, the amount of tokens available to withdraw or borrow will decrease. At the same time, supplying tokens will be incentivized, interest rate will rise and the borrowing will be dis-incentivized.

STAKING

Staking involves holding funds in a cryptocurrency wallet to support the security and operations of a blockchain networks to receive rewards. Staking allowed Ethereum 2.0 to upgrade from a Proof of Work to Proof of Stake consensus algorithm.

Proof of Stake allows for the verification of the authenticity of transactions without the need of a centralized third party. Proof of stake chains produce and validate new blocks through the process of staking. Staking involves validators who vote on the next block and their weight of the vote depends upon the size of its stake. This means that validator's economic stake plays a big role.

Participations lock up their coins so they can be randomly selected by the protocol at specific intervals to create a block. Participations that stake larger amounts of coins have a higher chance of being chosen as the next block validator. How much one can earn by running a validator will depend on various factors such as the total amount of validators, penalties, hosting costs and reliability.

Core to the success of a Proof of Stake network is the willingness of participants to stake their coins on the network in order to adequately secure the blockchain.

YIELD FARMING

Yield farming is a way of trying to maximize a rate of return (fix or variable interest) on capital by providing liquidity to different Decentralized Finance protocols.

While staking allows users to make passive income with their cryptocurrencies, yield farming goes one-step further by allowing users to maximize these returns. Yield farming is when you lend out a token on an open source money market protocol for a return beyond the token price appreciation.

Yield

Amount of interest or rewards 'grown' on top of the underlying crypto assets when to put use in Decentralized Finance platforms. Many Decentralized Finance protocols reward liquidity providers because they are trying to gather as much liquidity as possible to launch their Decentralized Finance application.

Yield farmers

Yield farmers are trying to maximize their yield. Usually, they try to obtain the highest yield by switching between multiple different Yield farming strategies such as staking tokens, lending, borrowing or supplying capital to liquidity pools.

Yield farming can generate a return of almost 10% of the annualized percentage yield (hereafter: “APY”). Three important key elements to these high returns are “liquidity mining”, “leverage” and “risks”.

Liquidity mining

Liquidity mining creates an extra incentive for yield farmers.

The yield farmer gets a new token as well as the usual return that is already generated by using a certain protocol in exchange for the farmer’s liquidity. In certain protocols, the rewards are higher than the initial capital. This gives the incentive to lose the initial capital and get more rewards in the distributed tokens.

e.g. a decentralized lending platform starts the liquidity mining of a certain type of tokens by giving it higher rewards to the users who were borrowing assets with the highest APY. This incentivize farmers to start borrowing these assets because the value of minted tokens was compensating them for the high borrow rates they had to pay.

Leverage

Leverage means using borrowed money to increase the potential return of an investment.

Yield farmers can deposit their coins as collateral to one of the lending protocols and borrow other coins. They can then use the borrowed coins as further collateral and borrow even more coins. By repeating the whole procedure, farmers can leverage their initial capital a few times over.

Risks

Taking risks is inherent to yield farming.

- Risks inherent to the use of smart contracts;
- Risks inherent to the use of Decentralized Finance;
- Risks related to taking overcollateralized loans during the leverage;
- Risk that yield farming strategy / mix of strategies can become obsolete very quickly.

What’s next?

We believe that the future looks bright for Decentralized Finance. Using the Decentralized Finance technology gives endless opportunities. New ground- breaking Decentralized Finance applications are increasing in popularity, are becoming more and more cost-efficient and will soon be adopted on a large global scale. While Switzerland is currently working on a regulatory framework for Distributed Ledger Technology (Distributed Ledger Technology Brochure), decentralized finance stays mostly unregulated. Decentralized Finance will not disrupt traditional financial markets but will be a serious alternative candidate and both systems will be complementary.

OA Legal assist clients in every step of DLT project. If your project entails staking and yield farming, we assist you in obtaining the relevant non-action letter from the Swiss Financial Market Supervisory Authority (FINMA).

For more information on how OA Legal can assist you, please contact one of our Fintech specialists.

Alexandre de boccard

adeboccard@oalegal.ch

Fabien Gillioz

fgillioz@oalegal.ch

Deborah Lechtman

dlechtman@oalegal.ch

OUR OFFICE

1, place de Longemalle
1204 GENEVA
Phone: +41 22 786 88 66
eFax: communications@oalegal.ch
email: info@oalegal.ch

Disclaimer

This Decentralized Finance Brochure (hereafter: “Brochure”) is published for informational purposes only and should not be construed as legal advice on any specific facts or circumstances. You should not act upon the information in this Brochure without seeking prior advice from a qualified lawyer licensed in your country or jurisdiction. OA Legal does not guarantee the timeliness, accuracy, or completeness of the information, opinions and analysis contained herein. All information, analysis and opinions may be amended at any time without any prior notification. No part of this Brochure is legally binding or enforceable and is made without express or implied warranties or representations of any kind. OA Legal will not accept any liability whatsoever for any loss or damage resulting from the use of, or reliance on, the Brochure. The information contained in this Brochure may not be used or reproduced - even in parts – in any other context.

Abbreviations

AMM	Automated Market Makers
APY	Annual Percentage Yield
CeFi	Centralized Finance
CPMM	Constant Product Market Maker
dApps	Decentralized Applications
DeFi	Decentralized Finance
DAMMs	Decentralized Automated Market Makers
DEXEs	Decentralized Exchanges
EIPs	Ethereum Improvement Proposals
PoS	Proof of Stake