KEY BUILDING BLOCKS OF DEFI

Decentralized finance – more commonly known as DeFi – has gained increasing traction over the last few months. With new services and platforms being launched every week, the environment has become increasingly complex despite its short history.

This article provides an overview of the key building blocks of DeFi and the regulatory implications under Japanese laws.

Key building blocks of DeFi

(1) decentralized exchanges
(2) automated market makers
(3) lending platforms
(4) aggregators
(5) vaults
(6) derivatives

DEX

Decentralized exchanges (**DEX**) provide users with a marketplace where they can buy and sell crypto assets. The basic concept of DEXes is similar to that of centralized exchanges. Stated differently, DEXes typically maintain order books and matching engines.

In some cases, both the order book and matching engine are on-chain, in other cases they are off-chain and only the settlement occurs on-chain.

Examples

Binance DEX
dydx
switcheo

From a regulatory perspective it is necessary to distinguish between the order book/order matching and the settlement.

Depending on the degree of decentralization, i.e. the degree a creator of a DEX can access the funds or control the smart contract via admin rights, activities may either be regulated or unregulated.

(Potentially) Regulated Activities

(1) order book/order matching >> crypto asset exchange service +/-
(2) safekeeping of deposited crypto assets in smart contract for settlement >> crypto asset exchange service in form of custody service +/-

	custodial[1]	non-custodial	regulated
off-chain order book		✓	yes
	✓		yes
on-chain order book controlled		✓	yes
	✓		yes
on-chain order book not controlled		✓	no
	✓		yes

AMM

AMMs do not have order books. Instead they use liquidity pools that consist of at least one pair of crypto assets. The price of each crypto asset is measured against the other asset in the pool.

Uniswap for example uses the following formula to determine the price of each crypto asset in the pool:

x * y = k

In this equation, x and y represent the number of each token in the pool. While x and y vary over time, k remains constant and allows the AMM to determine the price of each asset at any point of time.

If a user exchanges ETH for DAI in an ETH/DAI pool, for example, the price of DAI becomes more expensive relative to ETH. This opens arbitrage opportunities if the ETH price in the pool deviates from the actual market price. To make use of the arbitrage opportunity a trader must only supply DAI to the pool and withdraw ETH. As a result, the price of ETH will be rebalanced and aligned with the overall market price.

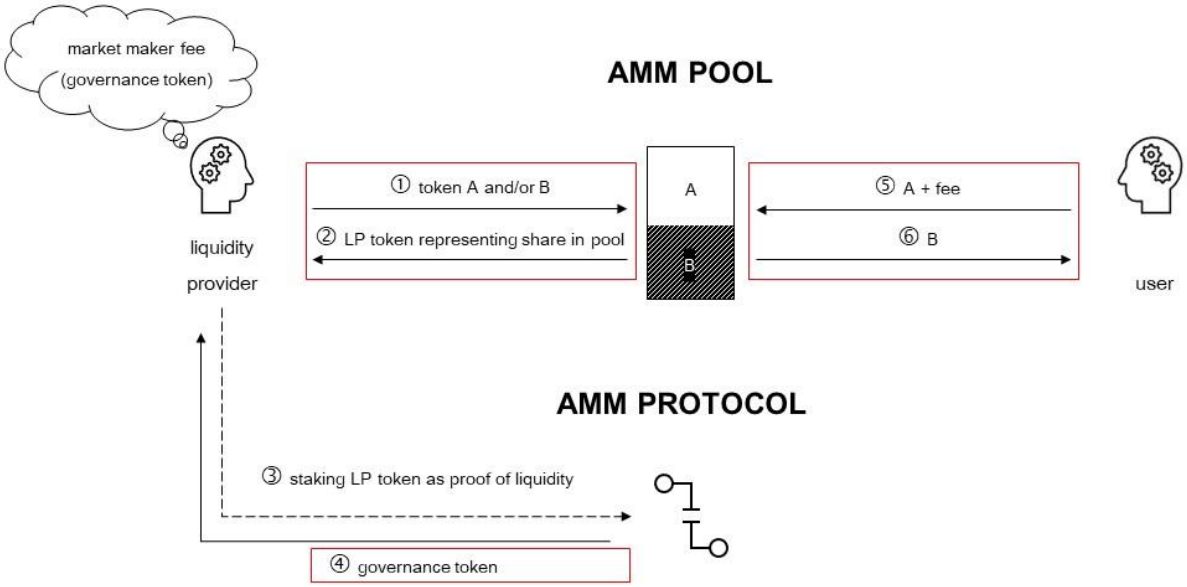
The liquidity in the pools is provided by liquidity providers (**LP**). In exchange for providing liquidity LPs participate in the fees charged for interacting with the pool and in some cases receive a governance token as additional incentive.

Examples

Uniswap
Curve

[1] Creator of smart contract controlling a user's funds has far-reaching admin rights and may be able to transfer deposited funds (after amendment) of smart contract.

Balancer



(Potentially) Regulated Activities

(1) exchange of crypto asset with LP token ①② >> crypto asset exchange service -/
(2) exchange of crypto assets ⑤⑥ >> crypto asset exchange service -/
(3) safekeeping of deposited crypto assets in smart contract controlling the AMM pool >> crypto asset exchange service in form of custody service +/-
(4) issuance of LP token ② >> issuance of security +/-
(5) issuance of incentives ④ >> crypto asset exchange service similar to ICO -/

LENDING

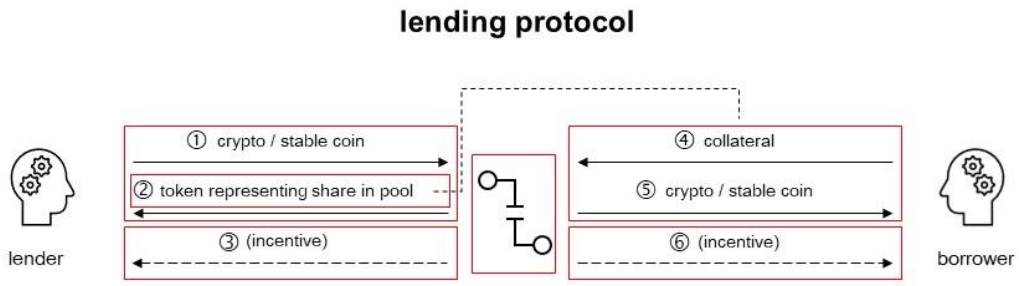
To borrow funds via one of the existing lending platforms, users must deposit crypto assets to the protocol. When supplying funds to the lending protocol, lenders receive a token representing their share in the lending pool. This token may be used as collateral when borrowing funds from the protocol.

Depending on the protocol, an additional token, typically in form of a governance token, may be issued to both the lender and borrower as an incentive to use the platform.

Borrowers pay interests to the protocol which either forwards them directly to the lender or releases them once the lender decides to unlock his funds from the protocol.

Examples

Compound
Aave



(Potentially) Regulated Activities

(1) exchange of crypto asset with token representing share in pool ①② >> crypto asset exchange service +/-
(2) exchange of token representing share in pool with crypto asset ④⑤ >> crypto asset exchange service +/-
(3) safekeeping of deposited crypto assets in smart contract controlling the lending pool >> crypto asset exchange service in form of custody service +/-
(4) issuance of token representing share in pool ② >> issuance of security /-
(5) issuance of governance tokens as incentive ③⑥ >> crypto asset exchange service /-

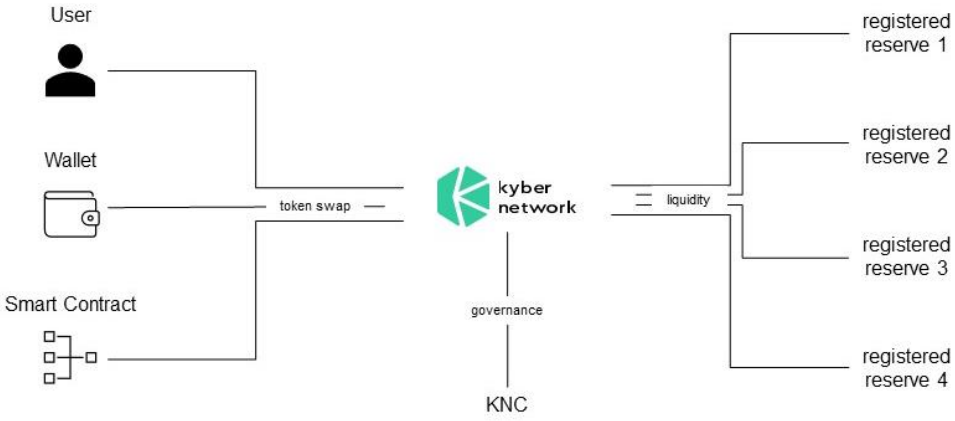
AGGREGATORS

Aggregators connect users, wallets, and smart contracts with liquidity. By doing so, they allow them to swap tokens for the best price available across multiple platforms.

Other aggregators constantly look for the best yield and distribute the supplied funds accordingly.

Examples

1inch
Kyber



(Potentially) Regulated Activities

(1) intermediary services for the exchange of crypto assets >> crypto asset exchange service +/-
(2) search of and execution at best price >> investment advice -/

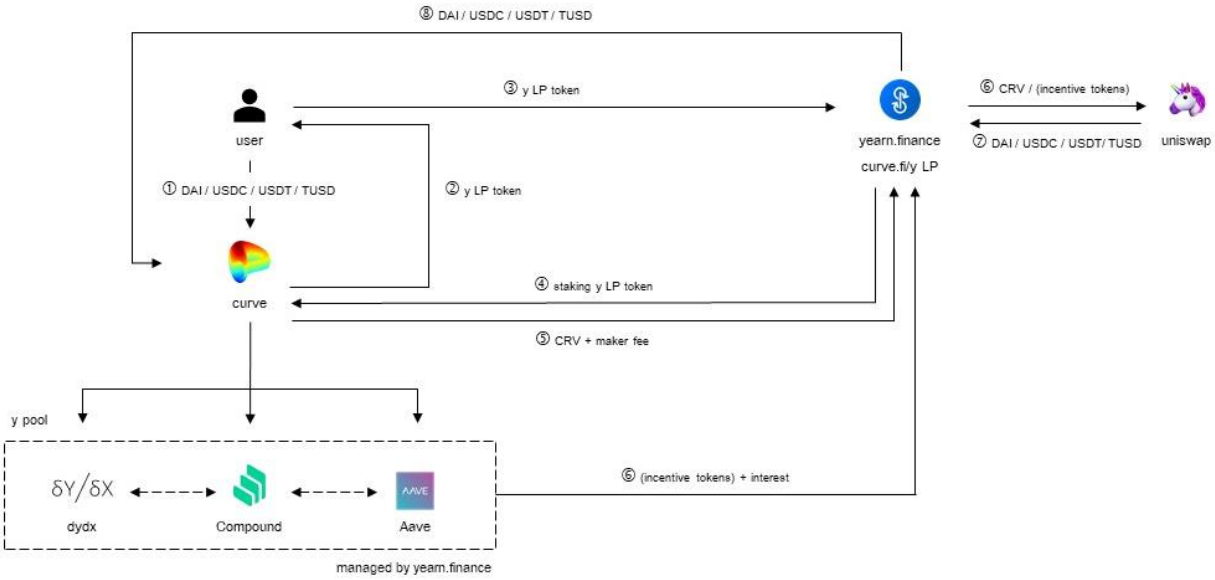
VAULTS

Vaults automatically optimize the returns on the funds supplied to them. To do so, they plug into multiple AMMs and lending protocols and move the funds wherever they generate the highest returns.

Where AMMs and lending protocols issue tokens as incentive, vaults automatically sell and reinvest them into the vault. One of the most prominent examples is yearn.finance.

Examples

yearn



(Potentially) Regulated Activities

(1) deposit of y LP token to vault ③ >> crypto asset exchange service in form of custody service /-
(2) allocation of crypto assets to pools with highest yield >> investment advice /-

DERIVATIVES

Derivatives platforms allow users to speculate and hedge their positions. For efficiency and cost reasons exchanges such as dydx use a hybrid off-chain/on-chain solution. The order book and order matching is performed off-chain while the margins paid by users of the platform are maintained by the protocol on-chain.

The infrastructure most derivatives exchanges operate on, is similar to that of DEXes.

Examples

dydx

(Potentially) Regulated Activities

(3) order book/order matching >> financial instrument business operator license +/-
(4) deposit of margin to smart contract managing deposited funds >> crypto asset exchange service +/-

CONTACT

So Saito
Partner
s.saito@innovationlaw.jp

Joerg Schmidt
Foreign Associate
j.schmidt@innovationlaw.jp

DISCLAIMER