

Decentralized Finance (DeFi)

October 26, 2021

1 Decentralized Finance (DeFi)

Dr. Fabian Woebbeking | woebbeking@finance.uni-frankfurt.de

1.1 Literature and materials

- C. Harvey, A. Ramachandran and J. Santoro: DeFi and the Future of Finance, 2021. ([Online version HERE](#))
- Github repository: <https://github.com/cafawo/DeFi>
- HTML script: <https://cafawo.github.io/DeFi/defi.html>
- Jupyter script: <https://github.com/cafawo/DeFi/blob/master/defi.ipynb>



```
[1]: # Imports
import os
import requests
import pandas as pd
import matplotlib.pyplot as plt
```

2 Previously on ...

2.1 Blockchain

A blockchain is an immutable time-stamped series data record that can be distributed and managed among a cluster of computers, thereby providing:

- Data integrity (cryptography) and
- Decentralization (incentives aka mining).

We can use blockchain platforms to store information on digital assets, such as:

- Cryptocurrency: the **native asset** of a blockchain, e.g. Ether (ETH) on the Ethereum blockchain
- Tokens: **assets that build on top of a blockchain** platform, e.g. assets build on Ethereum such as DAI, Sushi or AAVE.
- Smart contracts: simple **if, when ... then statements** written into code on a blockchain.

2.2 Wallet

A wallet allows a user to interact with a blockchain:

- Identified by an address (e.g. to receive digital assets)
- Private key (e.g. to send digital assets or sign smart contracts)

3 Decentralized Finance

Decentralized finance aims at providing **financial services without a classical financial intermediary**. Such services include:

- Borrowing and lending
- **Exchange** (← **this lecture**)
- Derivatives
- Securitization (tokenization)

3.1 Source of trust

The biggest difference between traditional and decentralized finance is the source of trust:

- Traditional finance (centralized ledger)
 - Laws
 - Regulators
 - Institutions
- Decentralized finance (distributed ledger)
 - Publicly available information (blockchain)
 - Transparency / open source (auditability)

4 Decentralized Exchange (DEX)

How to build a decentralized market place for digital assets.

4.1 Current world (centralized exchange)

Paradoxically, crypto assets might live in a decentralized world, the majority of their trading (currently) does not.

Naturally, centralized exchanges use **centralized wallets** to store customer funds: * Controlled by the exchange, not the user * Target for hackers * Loss of keys or stolen keys * Often unregulated

In a decentralized system, users hold custody of their own funds!

4.2 DEX Protocol

Traditionally, laws, regulators and the exchanges themselves create rules, in order to facilitate:

- Price exploration
- Agreement to trade
- Trade settlement

A DEX protocol is a **set of audited (open source) smart contracts** that replaces the traditional set of rules.

Examples are: * Uniswap * EtherDelta * **0x** (← **this lecture**)

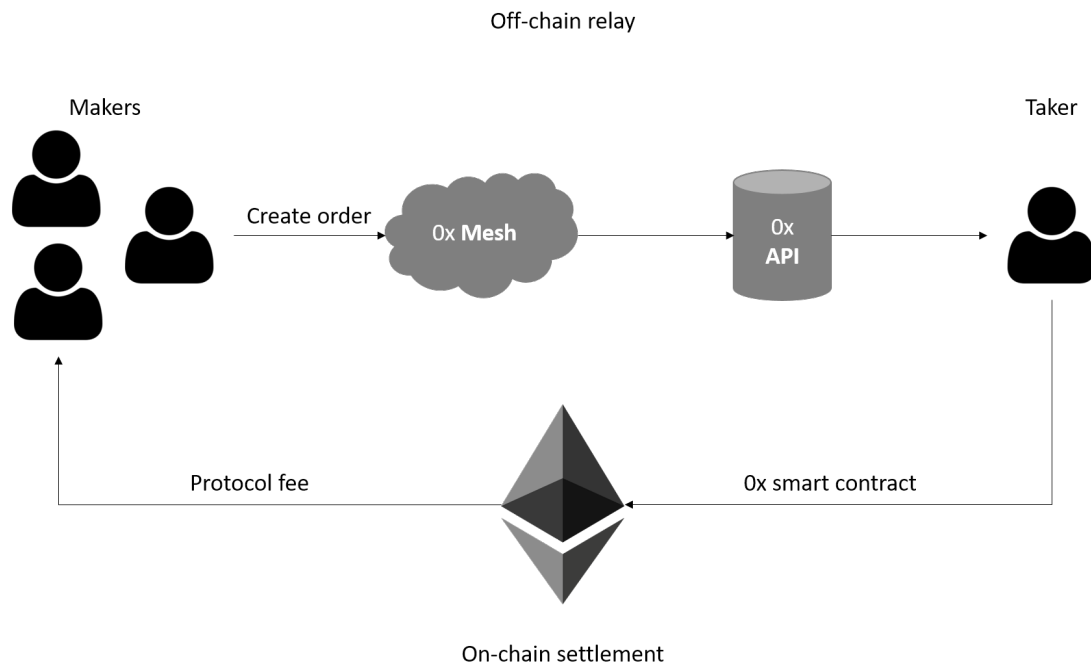
Please note that a protocol is not a user interface. This is, **we can build our own exchange UI based on an exchange protocol.**

4.3 Exchange mechanisms

1. **Order book** → typical exchange
2. **Request for quote** → over the counter (OTC)
3. Automated Market Making (AMM) → liquidity pools

4.4 A decentralized order book protocol (0x)

Ethereum can handle roughly 13 transactions per second that costs transaction fees (gas). In order to allow market makers to adjust (change or cancel) their orders for free and in higher frequency, price exploration is done off chain.



(The whitepaper is available [HERE](#))

4.5 Available assets

Here, assets are **tokens on the Ethereum blockchain** that follow a technical standard, such as ERC-20, ERC-721 or ERC-1155.

ERC-... are technical standards have been developed after the release of ETH* that allow tokens created on the Ethereum blockchain, such as ZRX, to interact with each other. (<https://ethereum.org/en/developers/docs/standards/tokens/erc-20/>)

* Ether, or **ETH**, is the native token of the Ethereum blockchain. Wrapped ETH, or **WETH**, refers to an ERC-20 compatible version of ether.

```
[35]: # Request tokens that are currently available
response = requests.get('https://api.0x.org/swap/v1/tokens')
response = response.json() if response.status_code == 200 else response.
↳status_code
available_tokens = pd.DataFrame(response['records'])
available_tokens
```

```
[35]:
```

	symbol	address	name \
0	ETH	0xeeeeeeeeeeeeeeeeeeeeeeeeeeeeeeeeeeeeee	Ether
1	WETH	0xc02aaa39b223fe8d0a0e5c4f27ead9083c756cc2	Wrapped Ether
2	ZRX	0xe41d2489571d322189246dafa5ebde1f4699f498	0x Protocol Token
3	DAI	0x6b175474e89094c44da98b954eedeac495271d0f	Dai Stablecoin
4	USDC	0xa0b86991c6218b36c1d19d4a2e9eb0ce3606eb48	USD Coin
..
98	REP	0x221657776846890989a759ba2973e427dff5c9bb	Augur
99	SETH	0x5e74c9036fb86bd7ecdc084a0673efc32ea31cb	sETH
100	STAKE	0x0ae055097c6d159879521c384f1d2123d1f195e6	xDAI Stake
101	TBTC	0x8daebade922df735c38c80c7ebd708af50815faa	tBTC
102	1INCH	0x111111111117dc0aa78b770fa6a738034120c302	1INCH

	decimals
0	18
1	18
2	18
3	18
4	6
..	...
98	18
99	18
100	18
101	18
102	18

[103 rows x 4 columns]

4.6 The order object

A set of **trade conditions** provided by the market maker that can be **accepted by the taker**. Note that you don't buy or sell an order object but merely accept the conditions as they are.

```
[36]: WETH_address = '0xc02aaa39b223fe8d0a0e5c4f27ead9083c756cc2'
# Extract a random order from the
response = requests.get(f'https://api.0x.org/orderbook/v1/orders?
    ↳makerToken={WETH_address}&page=1&perPage=1')
response.json() if response.status_code == 200 else response.status_code

[36]: {'total': 74,
      'page': 1,
      'perPage': 1,
      'records': [{'order': {'signature': {'signatureType': 3,
      'r': '0x8b68caa394aeb80e18e868eef3d34c9af5e4701f4a98d5050b147ac584be3b39',
      's': '0x59cc1be1ce31bbd6e2cdb046b2a03d9594dfff68a4f9c69c6696c900ff377f03',
      'v': 28},
      'sender': '0x00000000000000000000000000000000000000000000000000000000',
      'maker': '0x4a45afd5a9691407b2b8e6ed8052a511ee7f01e9',
      'taker': '0x00000000000000000000000000000000000000000000000000000000',
      'takerTokenFeeAmount': '0',
      'makerAmount': '6262301345676014592',
      'takerAmount': '13874662000553355116544',
      'makerToken': '0xc02aaa39b223fe8d0a0e5c4f27ead9083c756cc2',
      'takerToken': '0xf629cbd94d3791c9250152bd8dfbdf380e2a3b9c',
      'salt': '1635180845765',
      'verifyingContract': '0xdef1c0ded9bec7f1a1670819833240f027b25eff',
      'feeRecipient': '0x00000000000000000000000000000000000000000000000000000000',
      'expiry': '1635180873',
      'chainId': 1,
      'pool':
      '0x0000000000000000000000000000000000000000000000000000000000000017'},
      'metaData': {'orderHash':
      '0x036919cbc9a0d2061ee470e5315fc5bcfc0ae3d115763560344ddc44c4decfd2',
      'remainingFillableTakerAmount': '13874662000553355116544',
      'createdAt': '2021-10-25T16:54:07.299Z'}}]}
```

Some relevant fields from the order object above:

```
'order': {
  # Who?
  'maker': '0xc0e554c1951c0193e020156f68dce15064769937', # Party that created the order
  'taker': '0x00000000000000000000000000000000000000000000000000000000', # Party that is allowed to fill the order
  # What?
  'makerToken': '0xaf4c09112788ed97ac9c6284abbd2443163cfc90', # ERC20 token the maker is selling
  'takerToken': '0x57ab1ec28d129707052df4df418d58a2d46d5f51', # ERC20 token the taker is buying
  # How much?
  'makerAmount': '3960000000000000000', # Amount of makerToken being sold by the maker
```

```

'takerAmount': '168299999999999980000', # Amount of takerToken being sold by the taker
'feeRecipient': '0x0f8c816a31daef932b9f8afc3fcaa62a557ba2f7', # Fees to incentivize off-c
'expiry': '1634218842',
'metaData': {
  'orderHash': '0x00391e442ecbd9b6a16ee4c75c1c843bec166ec93ac30ffa8fd0fc62d83ebd3a', # ID f
  'remainingFillableTakerAmount': '168299999999999980000',
  'createdAt': '2021-10-14T12:40:44.426Z'}

```

4.7 Order book

Let's say we want **exchange Ethereum against USD**.

We will borrow some terminology from foreign exchange markets, i.e. * Ethereum (WETH) will be our base asset and * USD (DAI) will be out quoted asset.

Thus, we will **quote the price of Ethereum in USD**.

Note that USD cannot be settled on the Ethereum blockchain, hence, we will use a stable coin called DAI that is pegged to the USD (i.e. **1 DAI = 1 USD**).

```

[7]: base_address = '0xc02aaa39b223fe8d0a0e5c4f27ead9083c756cc2' # WETH
    qoted_address = '0x6b175474e89094c44da98b954eedeac495271d0f' # DAI

    response = requests.get(f'https://api.0x.org/orderbook/v1?
    ↪baseToken={base_address}&quoteToken={qoted_address}&perPage=1000')
    order_book = response.json() if response.status_code == 200 else response.
    ↪status_code
    order_book

```

```

[7]: {'bids': {'total': 6,
  'page': 1,
  'perPage': 1000,
  'records': [{'order': {'signature': {'signatureType': 3,
    'r': '0x8d175580952eba3af374aa38fb6ad10a4060bac617e4a2f847e511808c23aa56',
    's': '0x0baf13f642d984ac25a645da97fac80798fb2fdcf80ad5103a7843efb182b3ff',
    'v': 28},
    'sender': '0x00000000000000000000000000000000000000000000000000000000',
    'maker': '0x6c2d992b7739dfb363a473cc4f28998b7f1f6de2',
    'taker': '0x00000000000000000000000000000000000000000000000000000000',
    'takerTokenFeeAmount': '0',
    'makerAmount': '128437601237776373645312',
    'takerAmount': '31183476371052789760',
    'makerToken': '0x6b175474e89094c44da98b954eedeac495271d0f',
    'takerToken': '0xc02aaa39b223fe8d0a0e5c4f27ead9083c756cc2',
    'salt': '1635152576941',
    'verifyingContract': '0xdef1c0ded9bec7f1a1670819833240f027b25eff',
    'feeRecipient': '0x00000000000000000000000000000000000000000000000000000000',
    'expiry': '1635152618',

```



```

    'chainId': 1,
    'pool':
'0x0000000000000000000000000000000000000000000000000000000000000000'},
    'metaData': {'orderHash':
'0x15681e5d86e7a29e0f794588ea9154a71696eb0ba72faabf7298ec62f254bf3e',
    'remainingFillableTakerAmount': '0',
    'createdAt': '2021-09-28T19:18:59.600Z'}}},
{'order': {'signature': {'signatureType': 3,
    'r': '0xf78071c2a9dc43f223941df22bafa0e8b3c6785c88c44034cfc87e08a8668c99',
    's': '0x3ce3f575639b2b6fb468d1c8defcd59f8d0864f5b1d9e3fbe87f6573b2f78730',
    'v': 27},
    'sender': '0x0000000000000000000000000000000000000000',
    'maker': '0x6c2d992b7739dfb363a473cc4f28998b7f1f6de2',
    'taker': '0x0000000000000000000000000000000000000000',
    'takerTokenFeeAmount': '0',
    'makerAmount': '1000000000000000000',
    'takerAmount': '41395998404874717888512',
    'makerToken': '0xc02aaa39b223fe8d0a0e5c4f27ead9083c756cc2',
    'takerToken': '0x6b175474e89094c44da98b954eedeac495271d0f',
    'salt': '1635152600563',
    'verifyingContract': '0xdef1c0ded9bec7f1a1670819833240f027b25eff',
    'feeRecipient': '0x0000000000000000000000000000000000000000',
    'expiry': '1635152642',
    'chainId': 1,
    'pool':
'0x0000000000000000000000000000000000000000000000000000000000000017'},
    'metaData': {'orderHash':
'0x9dce7b80741c6cbd514ab94e01746ed54069e71048c83b4800cc2e1168b5ef50',
    'remainingFillableTakerAmount': '41395998404874717888512',
    'createdAt': '2021-10-25T09:03:21.538Z'}}},
{'order': {'signature': {'signatureType': 3,
    'r': '0x8f7581708396f7890f9c0188f21e450bd085a1b6fdc04ee3e682d52ce7564286',
    's': '0x2c666d1655b41e19a4a8f1bafd7d4f9c1cd7015b75bf1ce0459e8d424fc19418',
    'v': 27},
    'sender': '0x0000000000000000000000000000000000000000',
    'maker': '0x6c2d992b7739dfb363a473cc4f28998b7f1f6de2',
    'taker': '0x0000000000000000000000000000000000000000',
    'takerTokenFeeAmount': '0',
    'makerAmount': '1000000000000000000',
    'takerAmount': '41399424127704212963328',
    'makerToken': '0xc02aaa39b223fe8d0a0e5c4f27ead9083c756cc2',
    'takerToken': '0x6b175474e89094c44da98b954eedeac495271d0f',
    'salt': '1635152593023',
    'verifyingContract': '0xdef1c0ded9bec7f1a1670819833240f027b25eff',
    'feeRecipient': '0x0000000000000000000000000000000000000000',
    'expiry': '1635152635',
    'chainId': 1,

```



```

    'metaData': {'orderHash':
'0x82968253357ef2a68866be3a1e6bc11671feee722fb49548b797447c4324d714',
    'remainingFillableTakerAmount': '41426579938955717771264',
    'createdAt': '2021-10-25T09:02:57.141Z'}}},
    {'order': {'signature': {'signatureType': 3,
    'r': '0x2c5a84e769250da38628c431299ae6d9657472863547a6b0d22857a208cc6975',
    's': '0x12d53bc3d0157bcf747b29828a0799b570a46726894849ea68b1a00b76b19b55',
    'v': 28},
    'sender': '0x0000000000000000000000000000000000000000000000000000000000000000',
    'maker': '0x6c2d992b7739dfb363a473cc4f28998b7f1f6de2',
    'taker': '0x0000000000000000000000000000000000000000000000000000000000000000',
    'takerTokenFeeAmount': '0',
    'makerAmount': '3500000000000000000000',
    'takerAmount': '145000959461348371070976',
    'makerToken': '0xc02aaa39b223fe8d0a0e5c4f27ead9083c756cc2',
    'takerToken': '0x6b175474e89094c44da98b954eedeac495271d0f',
    'salt': '1635152576887',
    'verifyingContract': '0xdef1c0ded9bec7f1a1670819833240f027b25eff',
    'feeRecipient': '0x0000000000000000000000000000000000000000000000000000000000000000',
    'expiry': '1635152618',
    'chainId': 1,
    'pool':
'0x000000000000000000000000000000000000000000000000000000000000000017'}},
    'metaData': {'orderHash':
'0xbcd44bc609d81f9f49696e89e7aedb70424e932db35d06a4bca7a2adb303067',
    'remainingFillableTakerAmount': '145000959461348371070976',
    'createdAt': '2021-10-25T09:02:59.080Z'}}}}}}

```

Let us analyze the order book in a human friendly format from a **price taker perspective**.

Bid, i.e. the price at which the **taker sells WETH** for USD

```

'makerAmount': '17323698973795344711680', # Amount of DAI being bought by the taker
'takerAmount': '4585635752723798528',      # Amount of WETH being sold by the taker

```

Ask, i.e. the price at which the **taker buys WETH** for USD

```

'makerAmount': '10000000000000000000',      # Amount of WETH being bought by the taker
'takerAmount': '38006811467435057610752',    # Amount of DAI being sold by the taker

```

We could quote prices (and volumes) in WETH or DAI, here we use DAI, hence,

\$

$$Price = \frac{\text{Amount in quoted currency (e.g. DAI)}}{\text{Amount in base currency (e.g. WETH)}} \quad (1)$$

\$

```

[16]: quotes = []

for q in order_book['bids']['records']:

```

```

if q['metaData']['remainingFillableTakerAmount'] != '0':
    # Quote: DAI received per WETH
    price = int(q['order']['makerAmount']) / int(q['order']['takerAmount'])
    # Volume in DAI (DAI is stored as bigint with 18 decimals)
    volume = int(q['order']['makerAmount']) / 10**18
    orderHash = q['metaData']['orderHash']
    quotes.append(('Bid', price, volume, f'>>> One WETH pays ${price:.2f}$ DAI', orderHash))
for q in order_book['asks']['records']:
    if q['metaData']['remainingFillableTakerAmount'] != '0':
        # Quote: DAI paid per WETH
        price = int(q['order']['takerAmount']) / int(q['order']['makerAmount'])
        # Volume in DAI (DAI is stored as bigint with 18 decimals)
        volume = int(q['order']['takerAmount']) / 10**18
        orderHash = q['metaData']['orderHash']
        quotes.append(('Ask', price, volume, f'>>> One WETH costs ${price:.2f}$ DAI', orderHash))

quotes = pd.DataFrame(quotes, columns=['Side', 'Price in DAI', 'Volume in DAI', 'Price taker perspective', 'Order ID'])
quotes.sort_values(by='Price in DAI', inplace=True)
quotes

```

```

[16]:
   Side  Price in DAI  Volume in DAI  Price taker perspective \
5  Bid    4115.805991  127407.008650  >>> One WETH pays $4115.81$ DAI
4  Bid    4116.099876  126634.064209  >>> One WETH pays $4116.10$ DAI
3  Bid    4116.794676  127793.480870  >>> One WETH pays $4116.79$ DAI
2  Bid    4118.128451  126634.064209  >>> One WETH pays $4118.13$ DAI
1  Bid    4118.201386  128824.073458  >>> One WETH pays $4118.20$ DAI
0  Bid    4118.771099  128437.601238  >>> One WETH pays $4118.77$ DAI
6  Ask    4139.599840   41395.998405  >>> One WETH costs $4139.60$ DAI
7  Ask    4139.942413   41399.424128  >>> One WETH costs $4139.94$ DAI
8  Ask    4140.188676   41401.886760  >>> One WETH costs $4140.19$ DAI
9  Ask    4140.587659  144920.568053  >>> One WETH costs $4140.59$ DAI
10 Ask    4142.181740  144976.360906  >>> One WETH costs $4142.18$ DAI
11 Ask    4142.657994   41426.579939  >>> One WETH costs $4142.66$ DAI
12 Ask    4142.884556  145000.959461  >>> One WETH costs $4142.88$ DAI

```

```

                                Order ID
5  0x4fbb605f6e760fc8a02cd9d95651fd717a9a47157463...
4  0xa51678c1492c07bcee639896120168b19d205b2cf060...
3  0x89c37b3cf804db8fa4bc9450625128eea02c231bc75f...
2  0x38f31015b44dad59a55b4c72d1cef843c5bef7ae7e4...
1  0x19b51466022dac2df638095300d258ca3ae0d9fba96c...
0  0xf00a4ce77f47947b047cb28c28d2a291f36d345b25ac...
6  0x9dce7b80741c6cbd514ab94e01746ed54069e71048c8...
7  0x381d3bcf18c55afcef85a465b9c3c8438698f7b9d2e8...

```

```
8 0x5cf7d80667078615af327f9400c016c2fe61a8858257...
9 0x40c563833e325d1fa1dc6f12e78c88022a8f86a03998...
10 0x8e7b22a45c896fef9c77b46953eb383aba87de6f6e30...
11 0x82968253357ef2a68866be3a1e6bc11671feee722fb4...
12 0xbcde44bc609d81f9f49696e89e7aedb70424e932db35...
```

4.8 Submitting an order

4.8.1 Market order

Submit orders for the lowest available purchase or highest possible sale price.

4.8.2 Limit order

Submit orders with a condition on the (average) execution price.

```
[ ]: def market_order(base_address:str, quoted_address:str):
      pass

def limit_order(base_address:str, quoted_address:str, limit:float):
      pass
```

4.9 Settlement

Submitting a signed order object (0x smart contract) to the Ethereum blockchain

5 Coming up ...

5.1 Automated Market Making (AMM)

- AMM system where the taker trades against a liquidity pool.
- Uniswap example

5.2 Efficiency and arbitrage

- Discussion of protocols and their problems
- Price exploration and trading between protocols

```
[39]: # This is just generating the HTML and PDF version of the script.

# jupyter nbconvert vdt.ipynb --to slides --post serve --SlidesExporter.
→reveal_scroll=True
local_dir = %pwd
os.system(f'jupyter nbconvert defi.ipynb --to html')
# Generate PDF
os.system(f'jupyter nbconvert {local_dir}/defi.ipynb --to pdf')
```

[39]: 0

Thank you for your attention.