Decentralized Finance, Automated Market Makers, and Maximal Extractable Value!

Öz, B., Hoops, F., & Matthes, F. (2023). “Blockchain-based Systems Engineering”. Lecture Slides. TU Munich.

Chair of Software Engineering for Business Information Systems (sebis)
Department of Computer Science
School of Computation, Information and Technology (CIT)
Technical University of Munich (TUM)
wwwmatthes.in.tum.de

Outline

1. Decentralized Finance

2. Automated Market Makers

3. Maximal Extractable Value

The Birth of Decentralized Finance

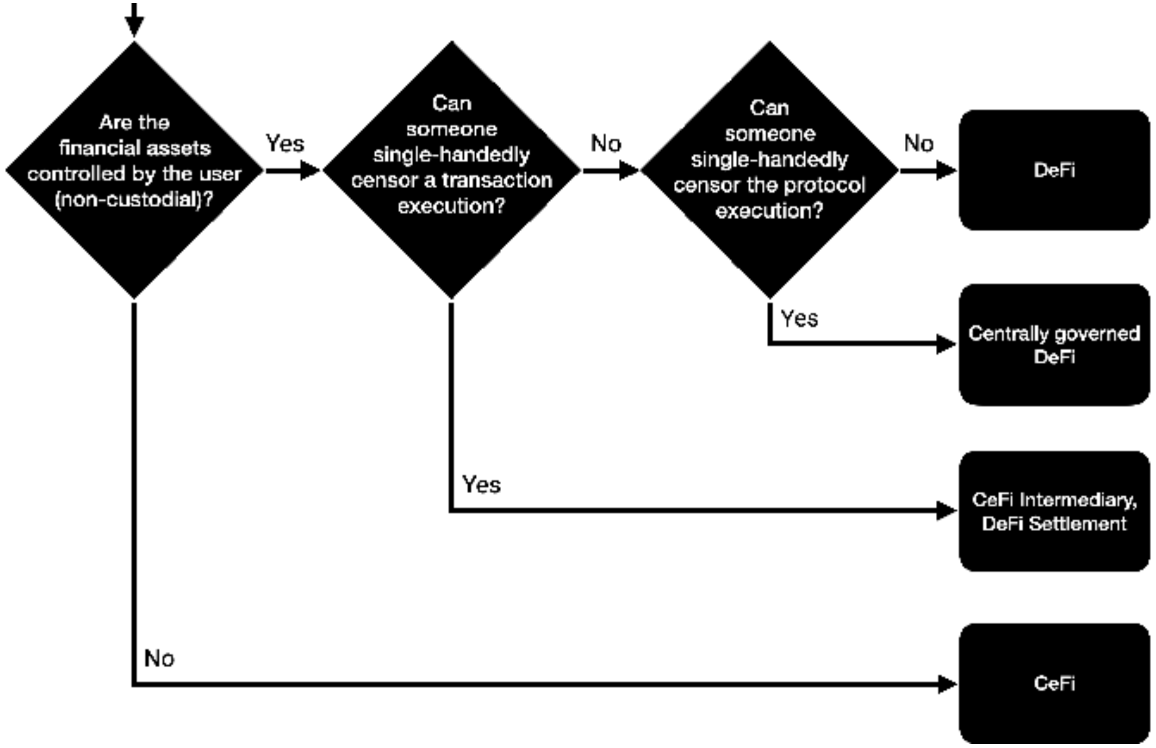
The emergence of Bitcoin enabled users to be in the custody of their money and do intermediary-free transfers. However, the capabilities of the Bitcoin Script limited the range of the financial interactions a user can do.

With the development of smart contract platforms, mainly Ethereum, the doors of financial services on blockchains opened widely as smart contracts enabled **programmable money** and financial assets like fungible and non-fungible tokens.

Decentralized Finance (DeFi) refers to the public, permissionless, interoperable finance ecosystem built on smart contract-enabled blockchains.

DeFi applications currently make up the **primary use case for blockchains** as they offer similar services to traditional/centralized finance (TradFi, CeFi) products but do it in a way where users;

- **maintain the custody** of their assets and
- have close to full **transparency** of every action.


Are the financial assets controlled by the user (non-custodial)?
Yes
Can someone single-handedly censor a transaction execution?
No
Can someone single-handedly censor the protocol execution?
No
DeFi
Yes
Centrally governed DeFi
Yes
CeFi Intermediary, DeFi Settlement
No
CeFi

Qin, Kaihua, Liyi Zhou, Yaroslav Afonin, Ludovico Lazzaretti and Arthur Gervais. “CeFi vs. DeFi - Comparing Centralized to Decentralized Finance.” ArXiv abs/2106.08157 (2021): n. pag.

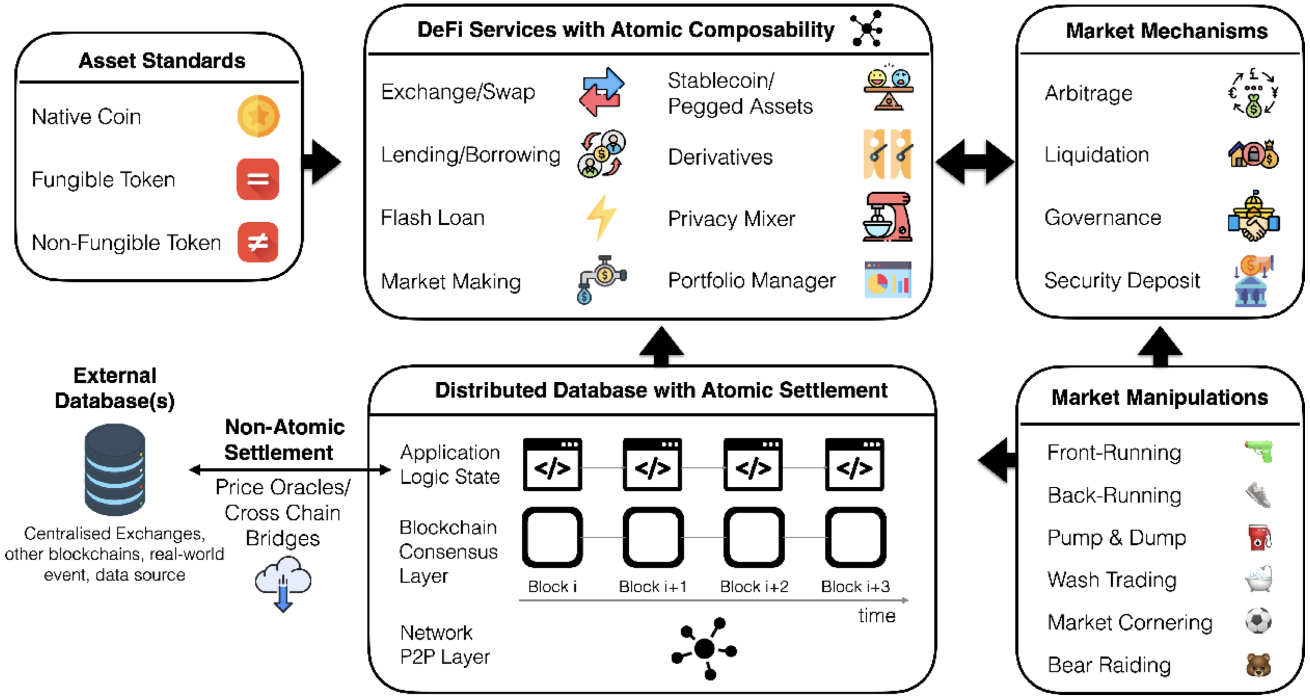
High-level Overview of DeFi

DeFi protocols use blockchain-based assets to enable various financial instruments and services.

- Exchanges
- Lending/Borrowing protocols
- Derivative Trading platforms
- Staking platforms

These protocols implement their business logic using the **state structure** of the underlying blockchain. With every confirmed transaction, the protocols sequentially execute certain operations which **transition the DeFi state into a new one in an atomic way**.[1]

DeFi protocols also do **non-atomic interactions** with protocols living outside the blockchain using oracles and cross-chain bridges[2].



Asset Standards

Native Coin

Fungible Token

Non-Fungible Token

DeFi Services with Atomic Composability

Exchange/Swap

Stablecoin/ Pegged Assets

Lending/Borrowing

Derivatives

Flash Loan

Privacy Mixer

Market Making

Portfolio Manager

Market Mechanisms

Arbitrage

Liquidation

Governance

Security Deposit

External Database(s)

Centralised Exchanges, other blockchains, real-world event, data source

Non-Atomic Settlement

Price Oracles/ Cross Chain Bridges

Distributed Database with Atomic Settlement

Application Logic State

Blockchain Consensus Layer

Network P2P Layer

Market Manipulations

Front-Running

Back-Running

Pump & Dump

Wash Trading

Market Cornering

Bear Raiding

Qin, Kaihua, Liyi Zhou, Yaroslav Afonin, Ludovico Lazzaretti and Arthur Gervais. “CeFi vs. DeFi - Comparing Centralized to Decentralized Finance.” ArXiv abs/2106.08157 (2021): n. pag.

[1] Atomicity refers to a transaction being fully executed (with all the interactions it does) or none at all based on certain conditions.

[2] Cross-chain bridges are infrastructures that enable asset transfer between two blockchains through token locking/burning and unlocking/minting on smart contracts.

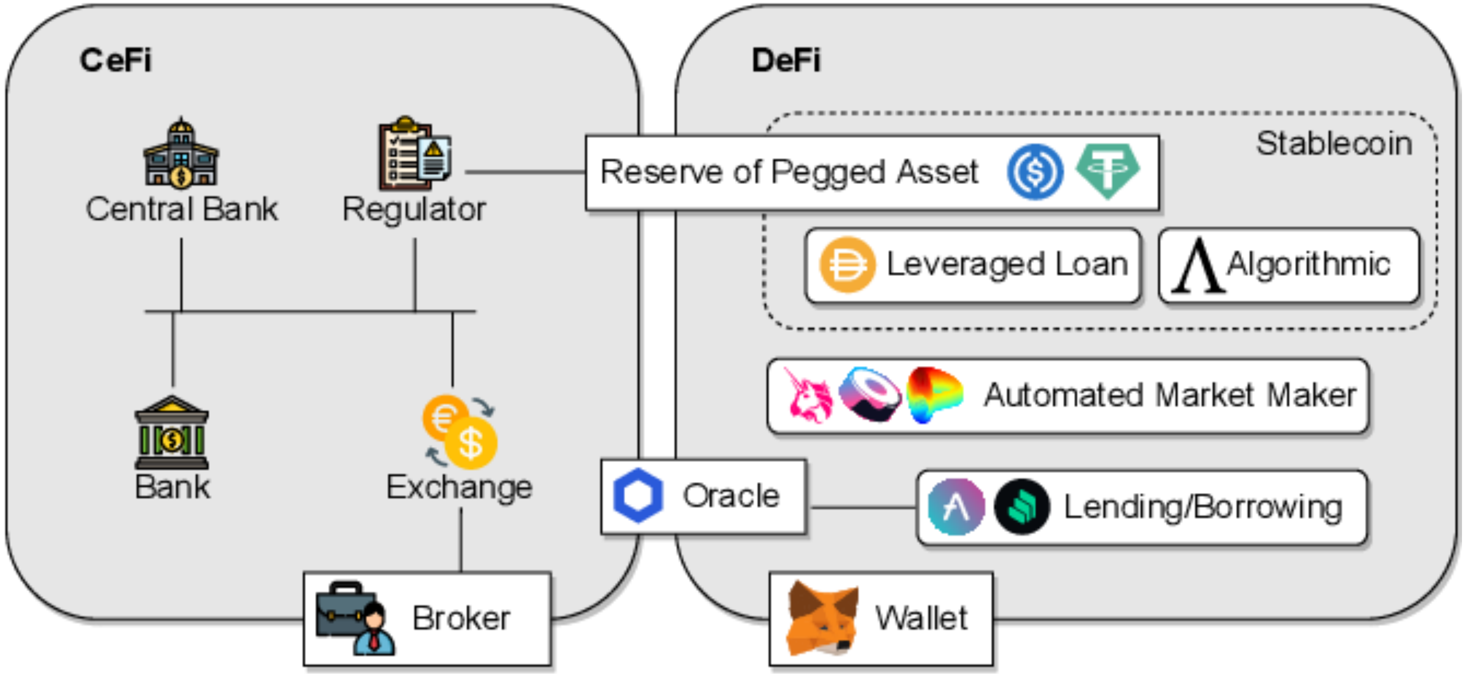
DeFi vs CeFi

Property	DeFi	CeFi
Custody	▪ Users retain complete control of the assets and determine how they are spent. ▪ Users are responsible for key management to utilize the assets.	▪ Companies store the assets for the users. ▪ Users have to trust the companies.
Transparency	As the underlying blockchain which hosts the smart contracts is public and transparent, all interactions and data are publicly visible and verifiable.	▪ Operational logic is black box; execution steps cannot be traced. ▪ Historical data is not publicly available unless the protocol explicitly publishes it. Even then, users have to trust the correctness of the data.
Privacy	Pseudonymous	KYC/AML
Availability	Open 7/24	Business hours, Monday to Friday
Fees	Blockchain transaction fees and protocol-specific fees	Protocol-specific fees

DeFi vs CeFi (cont.)

Although CeFi and DeFi have fundamental differences, they can co-exist and enable features for each other.

- Reserve-based stablecoins like USDC or USDT
- Oracles fetching data (e.g., price info) from CeFi exchanges



Qin, Kaihua, Liyi Zhou, Yaroslav Afonin, Ludovico Lazzaretti and Arthur Gervais. “CeFi vs. DeFi - Comparing Centralized to Decentralized Finance.” ArXiv abs/2106.08157 (2021): n. pag.

Outline

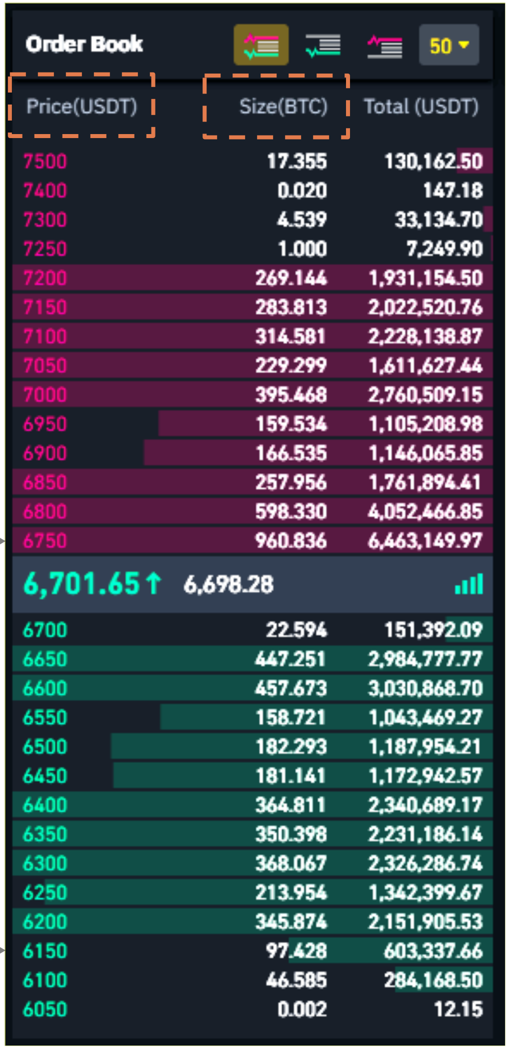
1. Decentralized Finance
2. Automated Market Makers
3. Maximal Extractable Value

Exchanges

An *exchange* is a marketplace where users can trade assets. In traditional finance, the **order book** is the de facto exchange design where market makers provide liquidity by placing limit orders on both sides of the market (**bid** and **ask**).

- Market orders are filled either by the lowest ask price or the highest bid price.
- Works efficiently when there is **enough liquidity** of assets traded, enabling a **low bid-ask spread**[1] and **fast order filling**.
- **Liquid markets** have order books with **sufficient depth**[2], making individual orders **less likely to affect the price**.
- Depth of an order book shows the **robustness** of the market!

deep


Order Book

50

Price(USDT)	Size(BTC)	Total (USDT)
7500	17.355	130,162.50
7400	0.020	147.18
7300	4.539	33,134.70
7250	1.000	7,249.90
7200	269.144	1,931,154.50
7150	283.813	2,022,520.76
7100	314.581	2,228,138.87
7050	229.299	1,611,627.44
7000	395.468	2,760,509.15
6950	159.534	1,105,208.98
6900	166.535	1,146,065.85
6850	257.956	1,761,894.41
6800	598.330	4,052,466.85
6750	960.836	6,463,149.97
6,701.65↑	6,698.28	
6700	22.594	151,392.09
6650	447.251	2,984,777.77
6600	457.673	3,030,868.70
6550	158.721	1,043,469.27
6500	182.293	1,187,954.21
6450	181.141	1,172,942.57
6400	364.811	2,340,689.17
6350	350.398	2,231,186.14
6300	368.067	2,326,286.74
6250	213.954	1,342,399.67
6200	345.874	2,151,905.53
6150	97.428	603,337.66
6100	46.585	284,168.50
6050	0.002	12.15

shallow

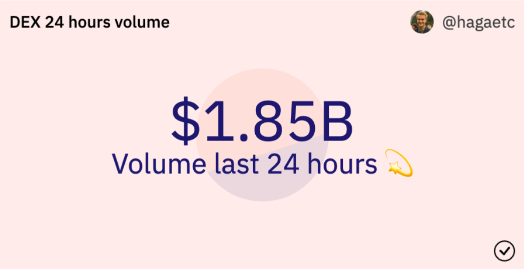
Order book image taken from: https://academy.binance.com/en/glossary/order-book

[1] Spread: The price difference between the lowest ask and the highest bid

[2] Depth: Quantity of assets traded at each price level (price * size)

Decentralized Exchanges

Like centralized exchanges in traditional finance, DeFi supports **decentralized exchanges** (DEX). Currently, DEXs are some of the most popular applications on Ethereum with nearly $1.85B cumulative daily trading volume.

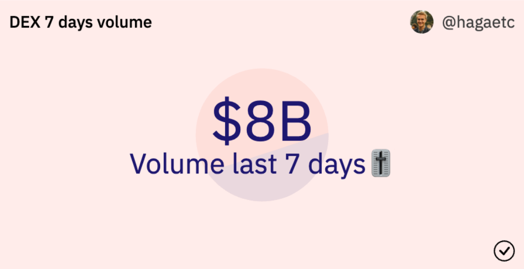


DEX 24 hours volume

@hagaetc

$1.85B

Volume last 24 hours 💫



DEX 7 days volume

@hagaetc

$8B

Volume last 7 days 🗿

The first DEX implementations on Ethereum also **followed the familiar order book design**. However, soon it was realized that such DEXs suffer from **slow execution** of the underlying blockchain and **high transaction fees due to complex on-chain operations** like order matching.

EtherDelta was one of the first DEXs operating on Ethereum. It followed the order book model. In 2018, U.S. Securities and Exchange Commission charged its founder for operating an unregistered national securities exchange, and the platform shut down.

EtherDelta

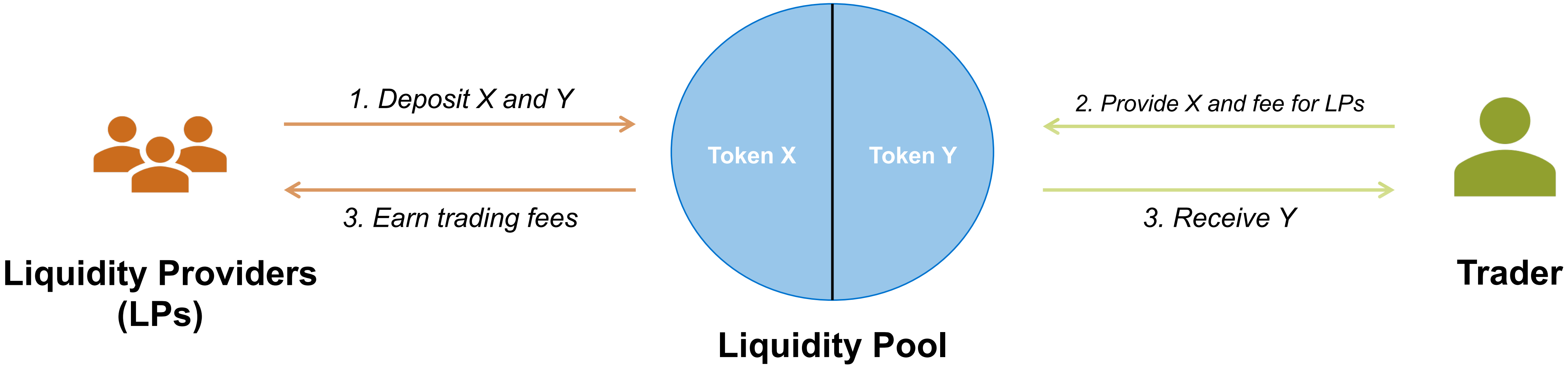
See more metrics about DEXs here: https://dune.com/hagaetc/dex-metrics

11 DeFi, AMMs, and MEV! - Öz, B., Hoops, F., & Matthes, F. (2023). "Blockchain-based Systems Engineering". Lecture Slides. TU Munich.

Automated Market Makers

The **Automated Market Maker** (AMM) design emerged to enable efficient trading in DeFi through intermediary-free, algorithmic market-making using smart contracts.

- AMMs **replace order books with liquidity pools** where liquidity providers (LPs) deposit assets to both sides of the pools, and the smart contracts automatically handle **market-making** and **price discovery**.
- LPs earn rewards based on their share in the pool and the trading volume, as every trade pays a fee (≈ 0.3%).



This slide is inspired from the DeFi MOOC by UC Berkeley.

11 DeFi, AMMs, and MEV! - Öz, B., Hoops, F., & Matthes, F. (2023). “Blockchain-based Systems Engineering”. Lecture Slides. TU Munich.

Automated Market Makers (cont.)

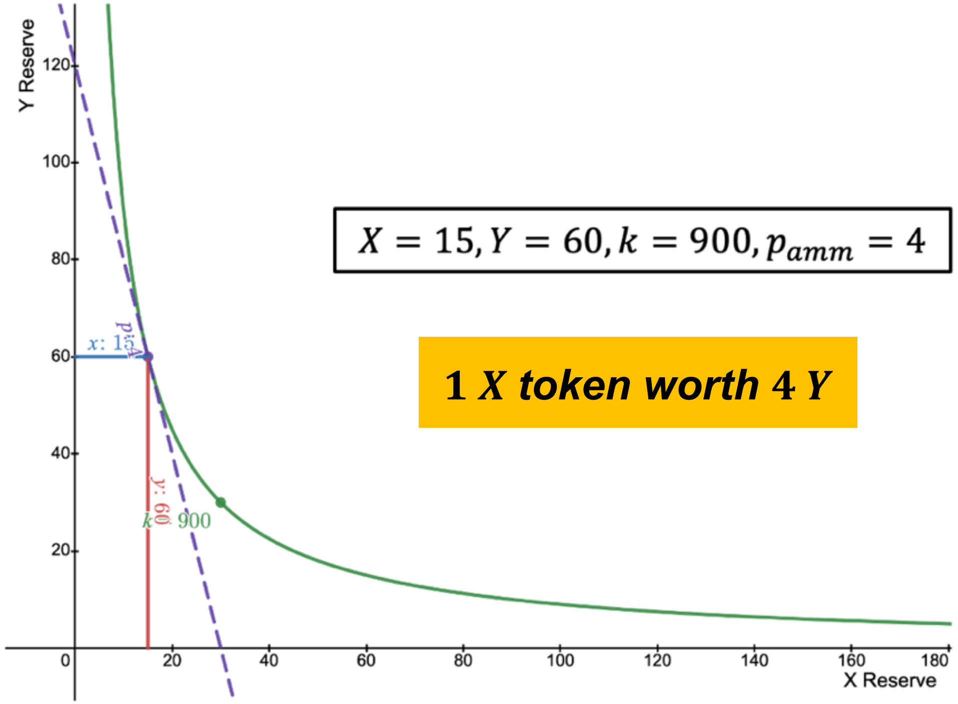
The smart contract of an AMM is programmed to follow a **market-making function** to **determine the input/output amount** given a trade request.

- The most popular market-making function is the **constant product**.

Constant Product AMM

In a two-token, constant product market, say a market for X and Y, the **product of the assets' reserves** (x, y) is **constant** k, and their relative ratio determines the price p_{amm}.

$$x * y = k\ (const)$$
$$p_{amm} = y/x$$



$X = 15, Y = 60, k = 900, p_{amm} = 4$

1 X token worth 4 Y

The curve of a constant product AMM which has 15 X and 60 Y tokens.

The figure is created using the Uniswap math (with LVR) Desmos graph.
This slide is inspired from: Öz, B.: Die Kosten der Automated Market Makers. *BSDEX*. 2023.

Automated Market Makers (cont.)

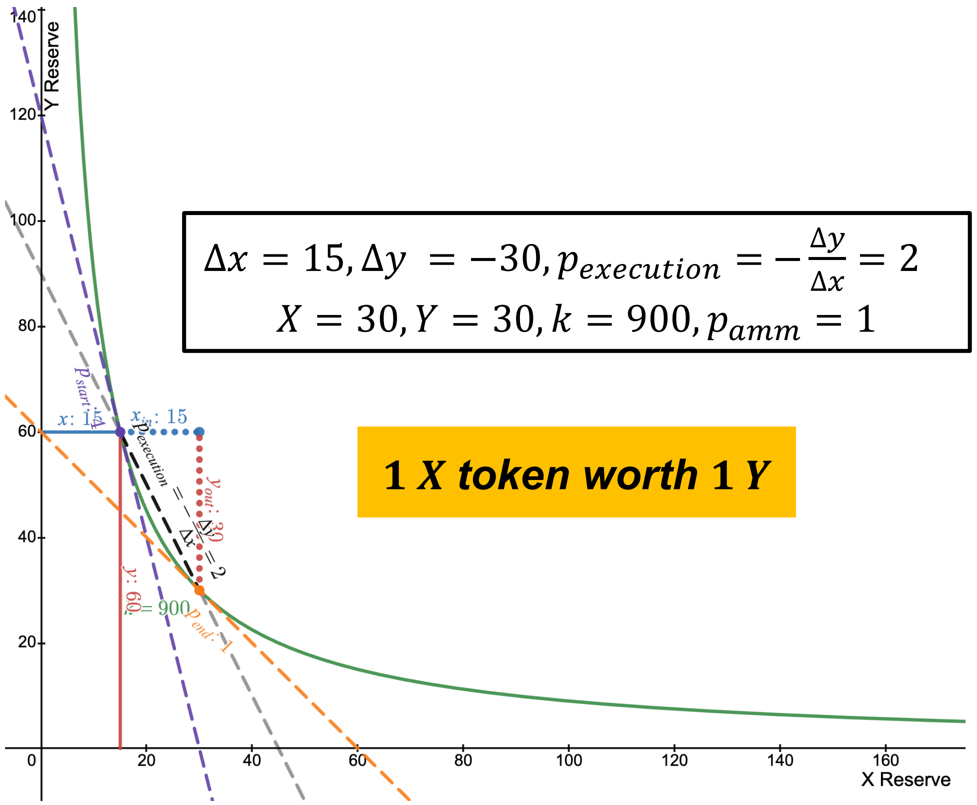
Each new trade on an AMM **changes pool reserves** $(\Delta x, \Delta y)$ **while keeping** k **constant**.

$$(x + \Delta x) * (y + \Delta y) = k$$

Example Trade

Assume the same AMM from the previous slide; let's calculate the output amount (Δy) for a trade of $15\ X$. *(For simplicity, we ignore the DEX fees)*

1. $X = 15,\ Y = 60,\ x * y = k = 15 * 60 = 900$ — *Initial state*
2. $\Delta x = 15$ — *Trader inputs 15 X*
3. $(x + \Delta x) * (y + \Delta y) = k$ — *Trade must keep k constant*
4. $\Delta y = \dfrac{k}{(x + \Delta x)} - y = \dfrac{900}{30} - 60 = -30$ — *AMM returns 30 Y*
5. $p_{execution} = -\dfrac{\Delta y}{\Delta x} = 2$ — *Trader receives 2 Y for 1 X*
6. $X = 30, Y = 30, k = 900, p_{amm} = 1$ — *Final state*



$$\Delta x = 15, \Delta y = -30, p_{execution} = -\frac{\Delta y}{\Delta x} = 2$$
$$X = 30, Y = 30, k = 900, p_{amm} = 1$$

1 *X* token worth 1 *Y*

The updated price of the AMM after a trade of $15\ X$ for $30\ Y$.

Depending on the size of the trade, the AMM price p_{amm} also changes!

- For an infinitely small trade, p_{amm} would remain constant and match the execution price $p_{execution}$.
- With the increasing trade size, the difference between p_{amm} and $p_{execution}$ also grows, resulting in **expected slippage**.[1]

[1] There is also an *unexpected slippage* which refers to the difference between the price when the order was placed and when it was confirmed.

The figure is created using the Uniswap math (with LVR) Desmos graph.
This slide is inspired from: Öz, B.: Die Kosten der Automated Market Makers. *BSDEX*. 2023.

Automated Market Makers (cont.)

Unlike trades on an AMM, liquidity addition or withdrawal (L_x,L_y) **keeps the AMM price p_{amm} constant while updating k.**

- To keep p_{amm} unchanged, an LP must **supply an equal value of assets** to both liquidity pools.

$$\boxed{p_{amm} = \frac{y}{x} = \frac{y + L_y}{x + L_x}}$$

Example Liquidity Addition

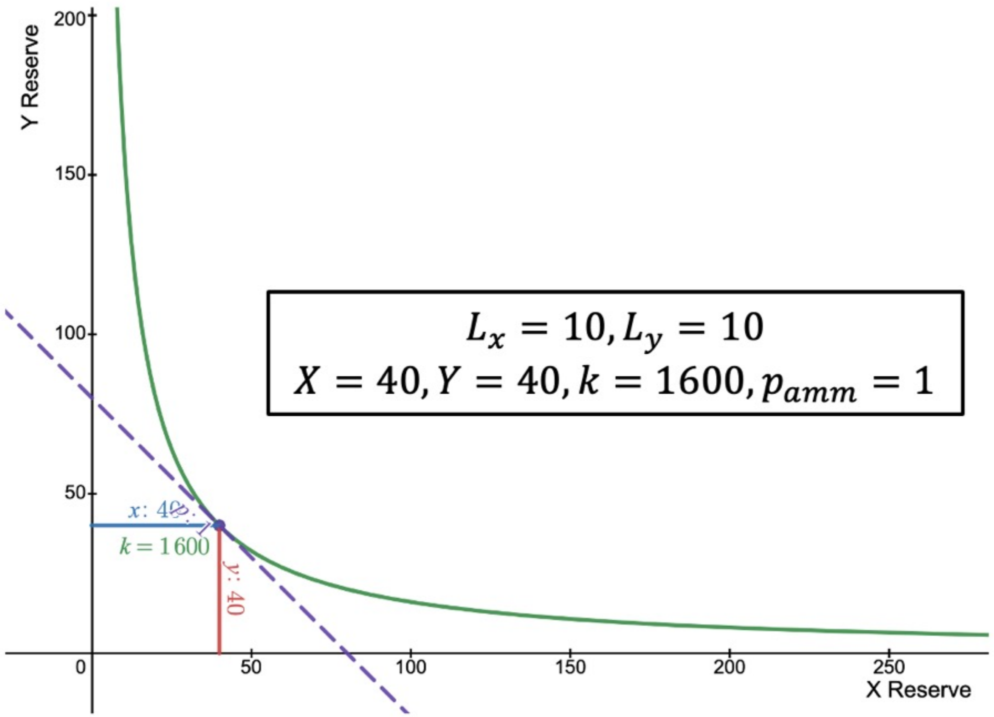
Assume the same AMM from the previous slide; let's calculate the new AMM state after an LP deposits $10\ X$ and $10\ Y$ tokens.

1. $X = 30, Y = 30, k = 900, p_{amm} = 1$ *Initial state*

2. $p_{amm} = \frac{y}{x} = \frac{y + L_y}{x + L_x}$ *LP must keep p_{amm} constant*

3. $p_{amm} = 1 \Rightarrow L_x = L_y = 10$
   $p_{amm} = \frac{30 + 10}{30 + 10} = 1$ *p_{amm} remains constant*

4. $X = 40, Y = 40, k = 1600, p_{amm} = 1$ *Final state*



$L_x = 10, L_y = 10$
$X = 40, Y = 40, k = 1600, p_{amm} = 1$

The updated curve of the AMM after a liquidity provision of $10\ X$ and $10\ Y$.

Remember that LPs earn rewards from each trade based on their share in the pool.

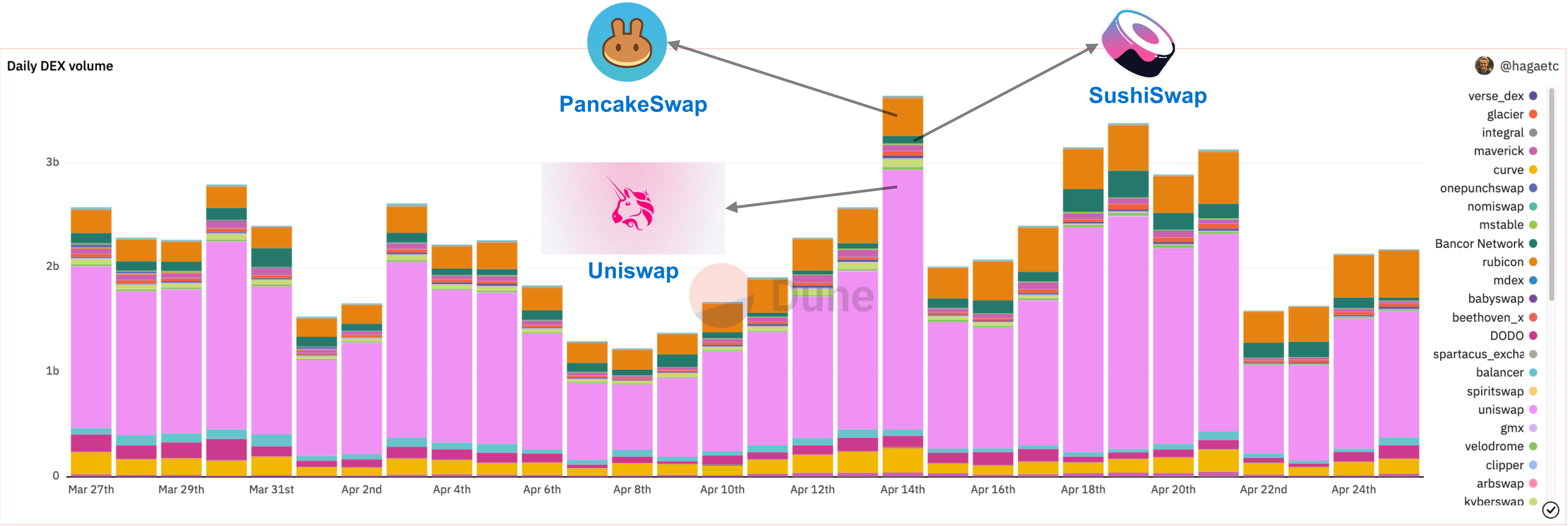
The figure is created using the Uniswap math (with LVR) Desmos graph.
This slide is inspired from: Öz, B.: Die Kosten der Automated Market Makers. *BSDEX*. 2023.

Automated Market Makers (cont.)

AMMs are considered more suitable for fully on-chain implementation and adoption than order books.

- Instant liquidity (no need to wait for a matching order)
- No maintenance is required by LPs to keep the prices up-to-date
- Simple implementation (x*y=k)

Today, AMMs such as **Uniswap** take the dominant market share (nearly 60%) of the DEX trading space.



See more metrics about DEXs here: https://dune.com/hagaetc/dex-metrics

Outline

1. Decentralized Finance

2. Automated Market Makers

3. Maximal Extractable Value

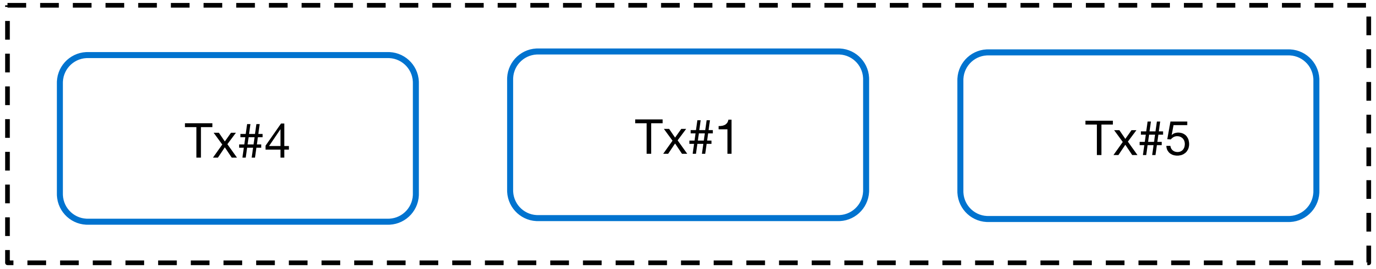
Building the Most Profitable Block

Assume that Florian is the next block proposer and has the following **mempool**.
Which transactions should he include in his block to maximize his profits? (block size = 3 Txs)

ID	Content	Gasprice
1	Alice transfers Bob 500 USDC	0.3 Gwei
2	Charlie transfers the ownership of a Bored Ape NFT to Bob	0.15 Gwei
3	Dennis swaps 2 ETH for 3000 USDC on Uniswap and swaps the 3000 USDC for 3.5 ETH on Sushiswap (makes 1.5 ETH profit)	0.1 Gwei
4	Alice deploys a new ERC20 contract	0.55 Gwei
5	Charlie calls a vulnerable contract to drain the funds in it (makes 10 ETH profit)	0.2 Gwei

As Florian is a **rational player**, we would expect him to pick the transactions which have the **highest gasprice**.

Florian's Block



Tx#4

Tx#1

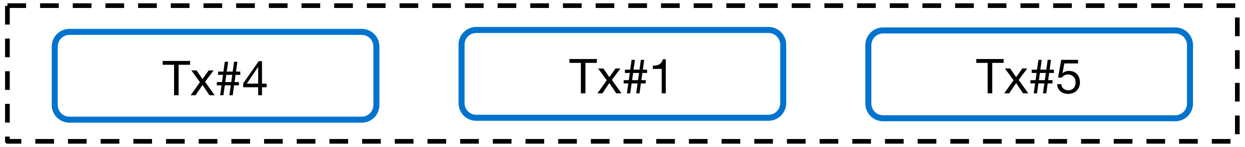
Tx#5

Can he do better?

Building the Most Profitable Block (cont.)

Think of **all the things that Florian can do when building his block**; does the following block actually **maximize his profits**?

Florian’s Block


Tx#4 Tx#1 Tx#5

ID	Content	Gasprice
1	Alice transfers Bob 500 USDC	0.3 Gwei
2	Charlie transfers the ownership of a Bored Ape NFT to Bob	0.15 Gwei
3	Dennis swaps 2 ETH for 3000 USDC on Uniswap and swaps the 3000 USDC for 3.5 ETH on Sushiswap (**makes 1.5 ETH profit**)	0.1 Gwei
4	Alice deploys a new ERC20 contract	0.55 Gwei
5	Charlie calls a vulnerable contract to drain the funds in it (**makes 10 ETH profit**)	0.2 Gwei

What stops Florian from copying Tx#3 and Tx#5 and earning the profits himself?

Florian’s Profit Maximizing Block (+11.5 ETH)

Florian Tx#3 Florian Tx#5 Tx#4

Maximal Extractable Value

The 11.5 ETH that Florian earns by inserting his own transactions and ignoring the original Tx#3 and Tx#5 is known as **Maximal Extractable Value** (**MEV**).

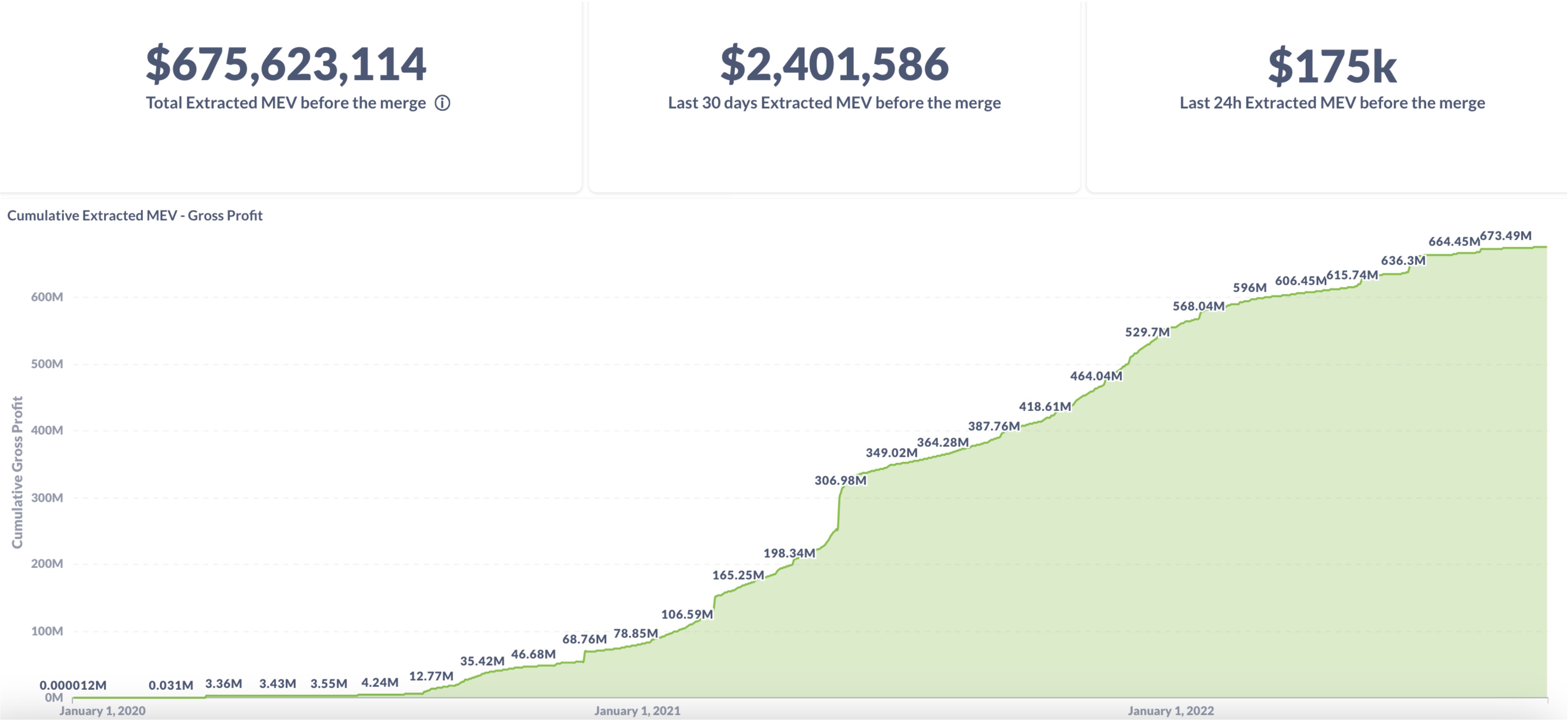
- MEV refers to the **maximum value** a **privileged actor**, like a block proposer, can **extract** from the protocol by **inserting**, **reordering**, or **censoring transactions**.
- However, **MEV is not specific to block proposers**; anyone monitoring the mempool could have also attempted to **copy the profitable transactions** and **prioritize** them by offering a higher gasprice.[1]
- Currently, MEV is the **most prominent incentive** on permissionless, smart-contract-enabled blockchains, which grows with the expanding DeFi ecosystem.

> *"Super linear return from MEV extraction results in significant* ***economy of scale*** *in block construction, creating* ***incentives for centralization****. Block producers who integrate with trading firms can get an inherent advantage in building the best blocks. The endgame in which a few large players making all the blocks - is an '****MEV dystopia****' that had to be prevented at all costs."*
>
> *Flashbots*[2]

[1] Block proposers on Ethereum refrain from collecting MEV themselves as this could harm their reputation. Instead, they profit from the fees MEV searchers pay for prioritizing their transactions.

[2] Flashbots is a research and development organization formed to mitigate the negative externalities posed by MEV.

Maximal Extractable Value (cont.)



$675,623,114
Total Extracted MEV before the merge ⓘ

$2,401,586
Last 30 days Extracted MEV before the merge

$175k
Last 24h Extracted MEV before the merge

Cumulative Extracted MEV - Gross Profit

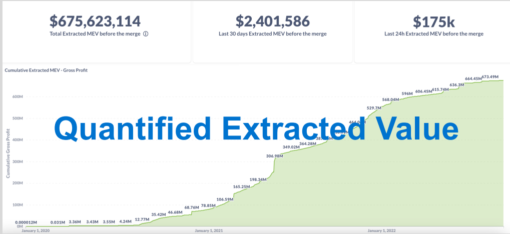
Pre-merge MEV data on MEV-Explore by Flashbots

Maximal Extractable Value (cont.)

Maximal Extractable Value

Extractable Value

Extracted Value



$675,623,114
Total Extracted MEV before the merge

$2,401,586
Last 30 days Extracted MEV before the merge

$175k
Last 24h Extracted MEV before the merge

Quantified Extracted Value

This visualization is not to scale!

The figure is inspired from Alex Obadia (Flashbots).

11 DeFi, AMMs, and MEV! - Öz, B., Hoops, F., & Matthes, F. (2023). "Blockchain-based Systems Engineering". Lecture Slides. TU Munich.

Outlook

- Since 2019[1], MEV has significantly affected the permissionless blockchains on various layers;

Incentive Mechanisms | **Economics** | **Consensus Security** | **…**

- The MEV problem is studied by many research groups, including the Ethereum Foundation.
- **At sebis, we are working on the following questions**:
  - *How does MEV affect consensus mechanisms and the application ecosystem?*
  - *How prominent of an incentive is MEV? (Detection & Quantification)*
  - *What solutions exist to mitigate the negative externalities of MEV?*
  - *Does MEV exist in other blockchains with similar properties to Ethereum?*
  - and many more …
- If you are interested in working on MEV, contact Burak Öz.

[1] MEV emerged with the development of the DeFi ecosystem on Ethereum. You can find more resources here.