A First Study of MEV on an Up-and-Coming Blockchain: Algorand

Burak Öz, 11.05.2023, TUM Blockchain Salon

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. Introduction

- *Maximal Extractable Value*
- *Algorand*

2. MEV & DeFi Ecosystem Analysis on Algorand

- ***Quantifying*** *Realized Extractable Value*
- ***Uncovering*** *Profitable Transactions*
- ***Evaluating*** *MEV Strategies*
- ***Privileged*** *Extractable Value*

Building the Most Profitable Block

Assume a miner has the following mempool …

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

Think of all the things that a miner can do when building his block; how could he maximize his revenue?

Copies Tx#3 and Tx#5 and earns the profits himself!
Backruns Tx#4 to liquidate a position!
More?

Maximal Extractable Value

The value miner earns by executing the discussed strategies 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 **execute the same strategies** by offering a sufficient payment to the proposer.[1]
- Currently, MEV is the **most prominent incentive** on permissionless, smart-contract-enabled blockchains, which grows with the expanding DeFi ecosystem.

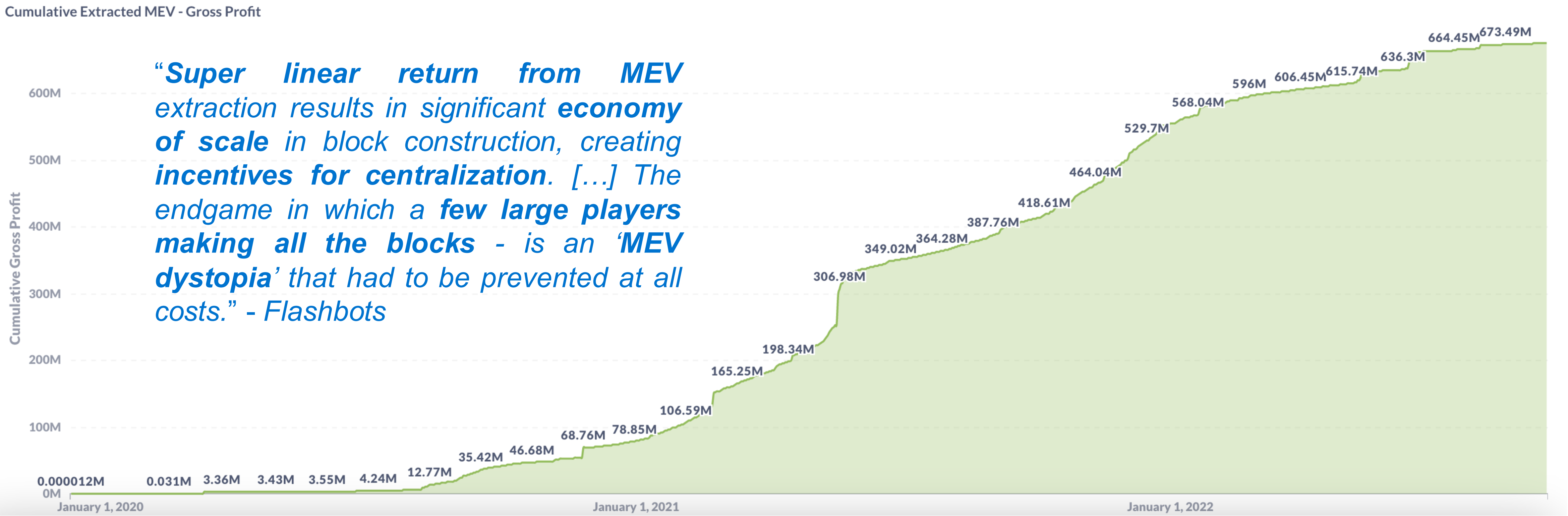
[1] Block proposers on Ethereum refrain from collecting MEV themselves as this could harm their reputation. Instead, they profit from the fees MEV searchers pay for prioritizing their transactions.
MEV meme taken from: https://collective.flashbots.net/t/your-favorite-mev-memes/68

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



*“**Super linear return from MEV** extraction results in significant **economy of scale** in block construction, creating **incentives for centralization**. […] 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*

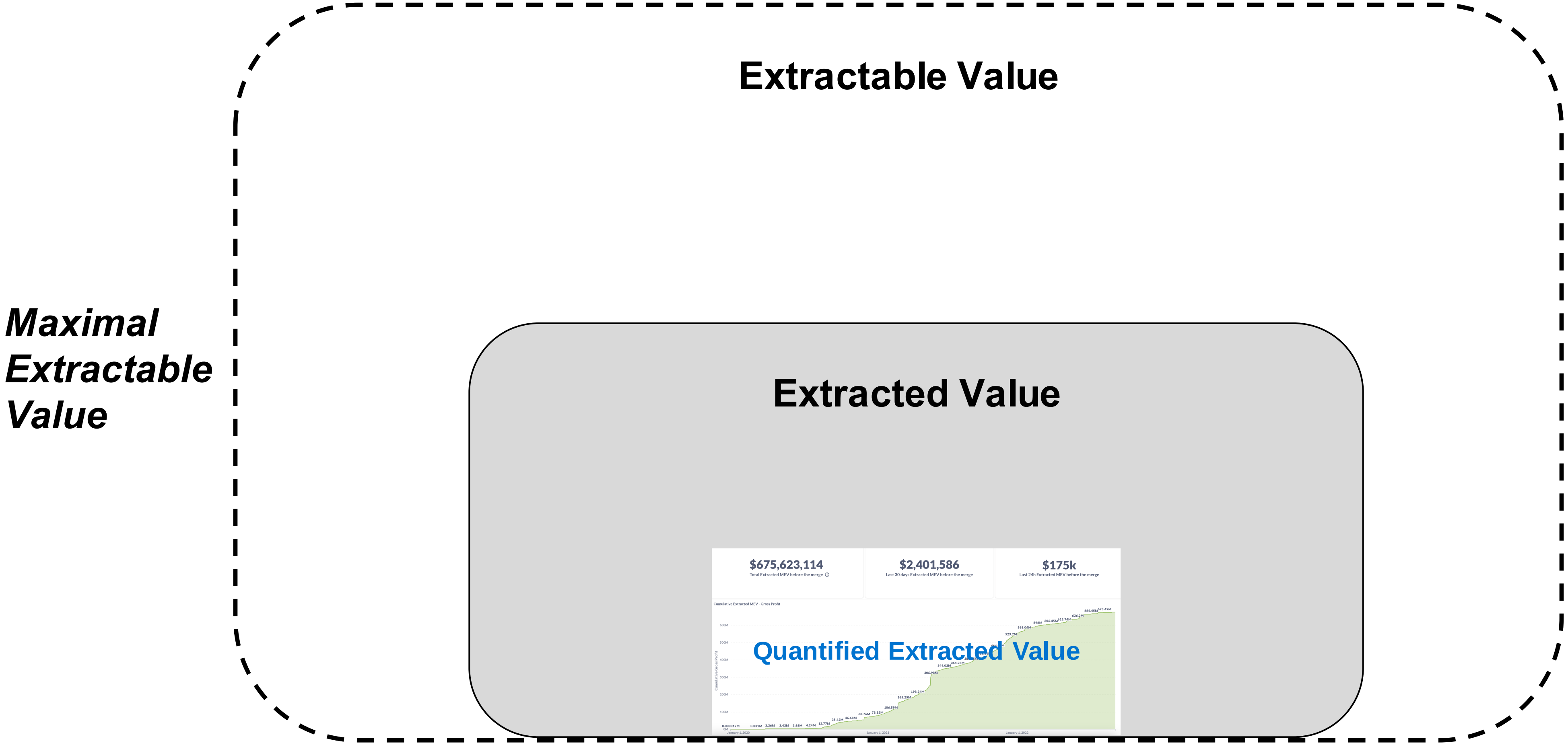
Pre-merge MEV data on [MEV-Explore]() by Flashbots

Maximal Extractable Value (cont.)

Pre-merge MEV data on MEV-Explore by Flashbots

MEV meme taken from: https://collective.flashbots.net/t/your-favorite-mev-memes/68

Maximal Extractable Value (cont.)



This visualization is not to scale!

The figure is inspired from [Alex Obadia](#) (Flashbots).

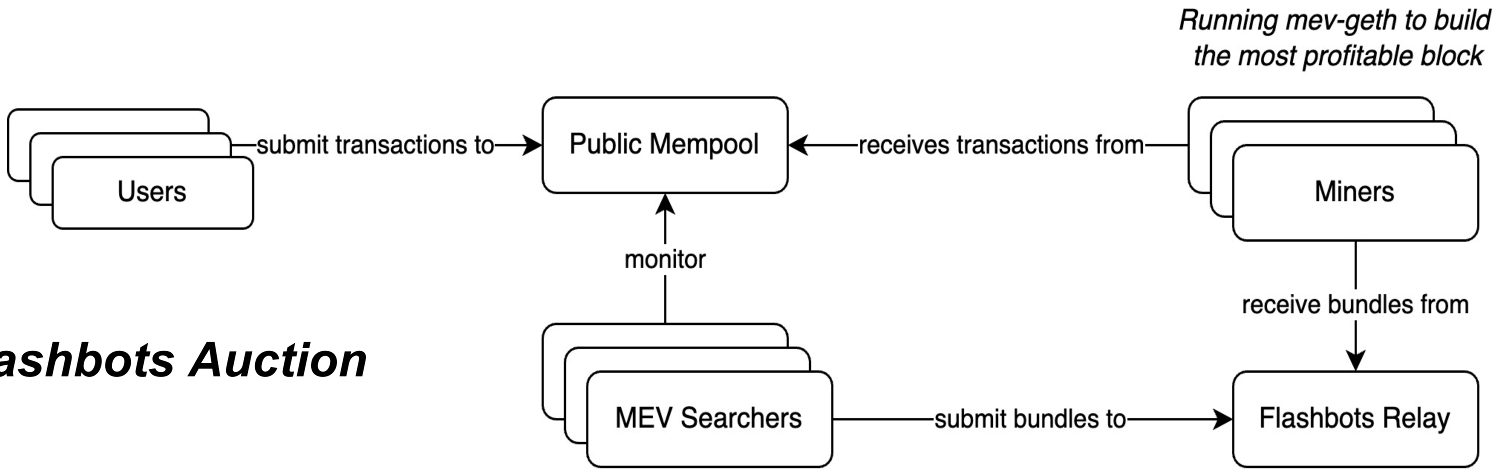
Does MEV Stop at Ethereum?

With the growing blockchain state (e.g., through DeFi), **MEV space becomes more complex** and potentially **more significant as an incentive**. Hence, the interest in studying MEV on Ethereum.

However, **MEV is not inherent to Ethereum**. It exists in any public, permissionless blockchain.

The properties of the underlying blockchain define the dynamics of how the MEV game is played.

- The native MEV extraction market on Ethereum was fee-based (**Higher Fee = Higher Priority**), taking place in **public**. Later on, we saw the development of off-chain, private markets like Flashbots Auction.



Flashbots Auction

Does MEV Stop at Ethereum? (cont.)

However, not all blockchains prioritize transactions based on fees; fixed-fee chains order the transactions based on the received order, i.e., **First-Come-First-Served** (FCFS).

Latency Wars!!

Algorand is "**currently**" an **FCFS blockchain with minimal, fixed fees**.

Algorand

Consensus

- Adopts a **Byzantine-Fault Tolerant** (BFT) consensus protocol combined with **Pure-Proof-of-Stake** (PPoS).
  - **No fixed set of consensus participants** or a **certain amount to be staked**.
  - **Voting power** in consensus is **proportional to the stake**.
  - Uses Verifiable Random Functions (**VRF**) to determine consensus participants (**efficient**, **unpredictable**)

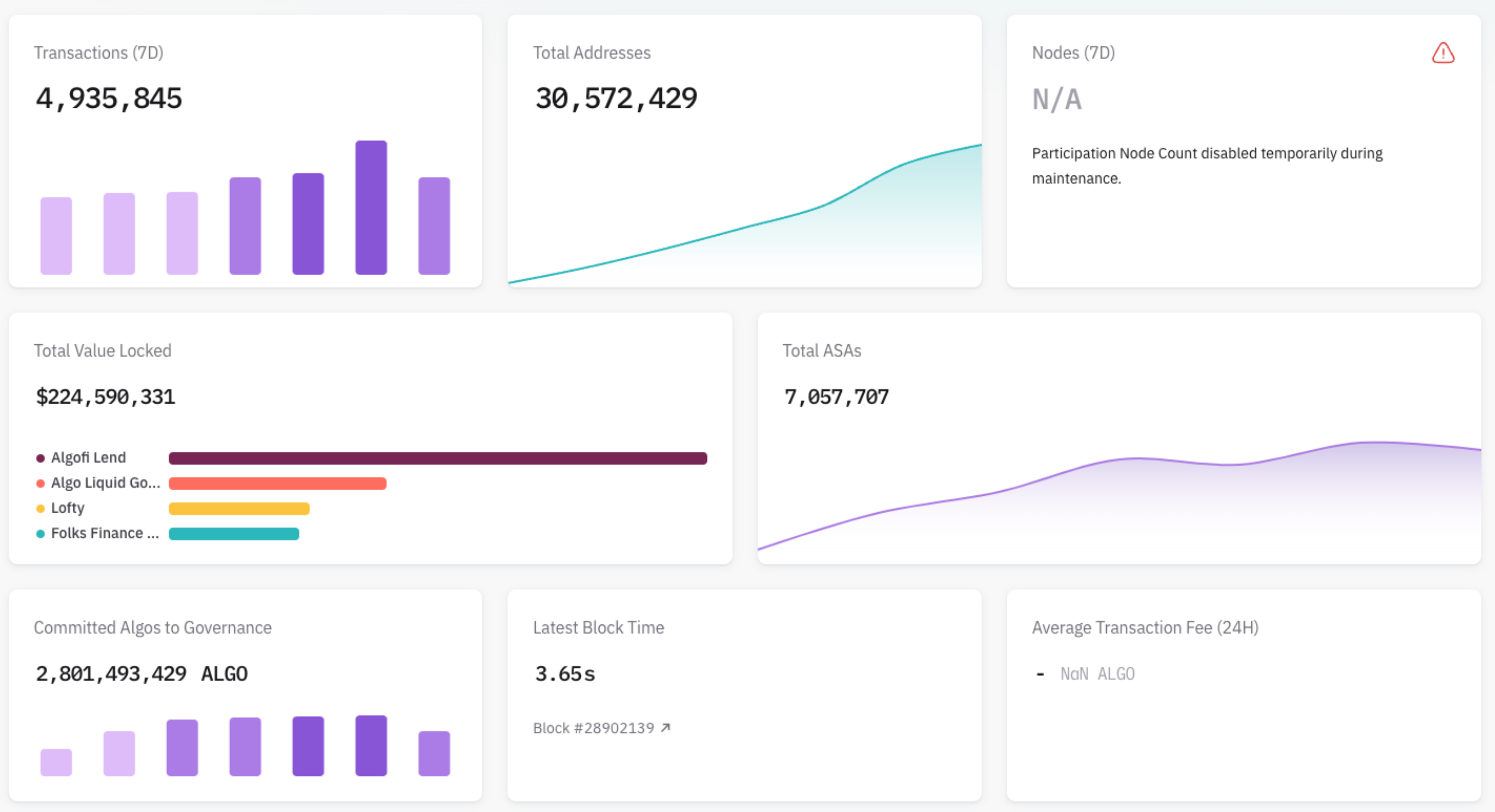
Economics & Incentives

- **Demand for block space is below the available space.** Paying the min. fee (0.001 ALGO) suffices.
- **Consensus participants are not rewarded**.
  - No block rewards.
  - Transaction fees are collected in a pool controlled by the Algorand Foundation.

No direct economic incentive for block proposers!

We say "**currently**" as the market can become **fee-based in congestion times**.

Algorand’s Network Metrics and Properties



Currency	**ALGO**
Block time	**< 3.9s**
Finality	**Immediate**
Block size	**5 MiB**
Max. Throughput	**6,000 transactions**
Transaction Fee	**0.001 ALGO[1]**
Circulating Supply	***7.2B***
Total Supply	***10B***

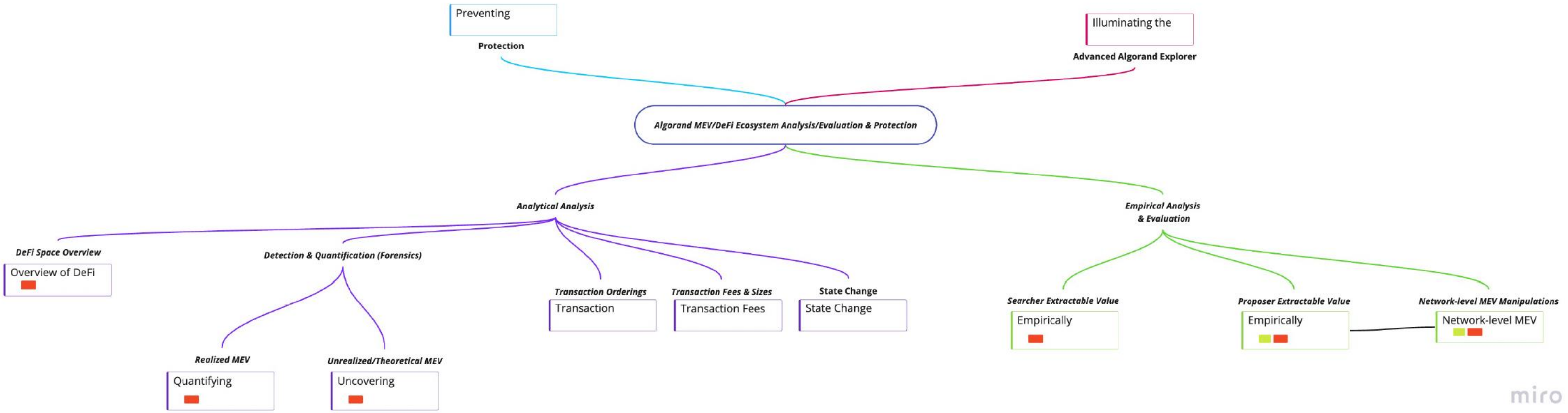
[1] 0.001ALGO ≈ $0.00017

ASA = Algorand Standard Assets (fungible + non-fungible)

Dashboard screenshot taken from: https://metrics.algorand.org/#/

Studying MEV on Algorand

- We are interested in understanding **the impact of the dynamics of a blockchain on MEV**.
- With its **novel consensus approach** and **distinct incentive and transaction fee mechanism**, Algorand makes a good case study.



Outline

1. Introduction
- *Maximal Extractable Value*
- *Algorand*

2. MEV & DeFi Ecosystem Analysis on Algorand
- ***Quantifying*** *Realized Extractable Value*
- ***Uncovering*** *Profitable Transactions*
- ***Evaluating*** *MEV Strategies*
- ***Privileged*** *Extractable Value*

Quantifying Realized Extractable Value

To understand the extend of how MEV already affects Algorand; we first want to **measure the realized value**.

DEX-DEX Arbitrages

CEX-DEX Arbitrages

Sandwiches

Liquidations

Lower bound on extracted value

Quantifying Realized Extractable Value

Arbitrages

Arbitrage refers to **the simultaneous purchase and sale** of an asset on different exchanges, **profiting from the price difference**.

We can use **heuristics** to spot arbitrages on historical transaction data:

For a transaction T with n swaps $s_1, \ldots, s_n$;

$\boldsymbol{H_1}$: Transaction includes multiple swaps ($n > 1$)

$\boldsymbol{H_2}$: The swapped tokens form a cycle where the input token of swap s_i is the output of s_{i-1}. This implies that the first swap's input token must match the last swap's output ($s_1.input.token == s_n.output.token$).

$\boldsymbol{H_3}$: The input amount of s_i must be less or equal to the output of s_{i-1}. This implies that the input amount of the first swap must be less or equal to the output of the last swap ($s_1.input.amount <= s_n.output.amount$).

Hence, the swap generates profit.

Transaction Action:

- Swap 139.095043641361099086 Ether For 5.7648024 WBTC On Sushiswap
- Swap 5.76480241 WBTC For 2,269,314.669822 USDT On 0x Protocol
- Swap 2,269,314.669822 USDT For 1,352.124212080924112964 Ether On Uniswap V2

Uncovering Profitable Transactions

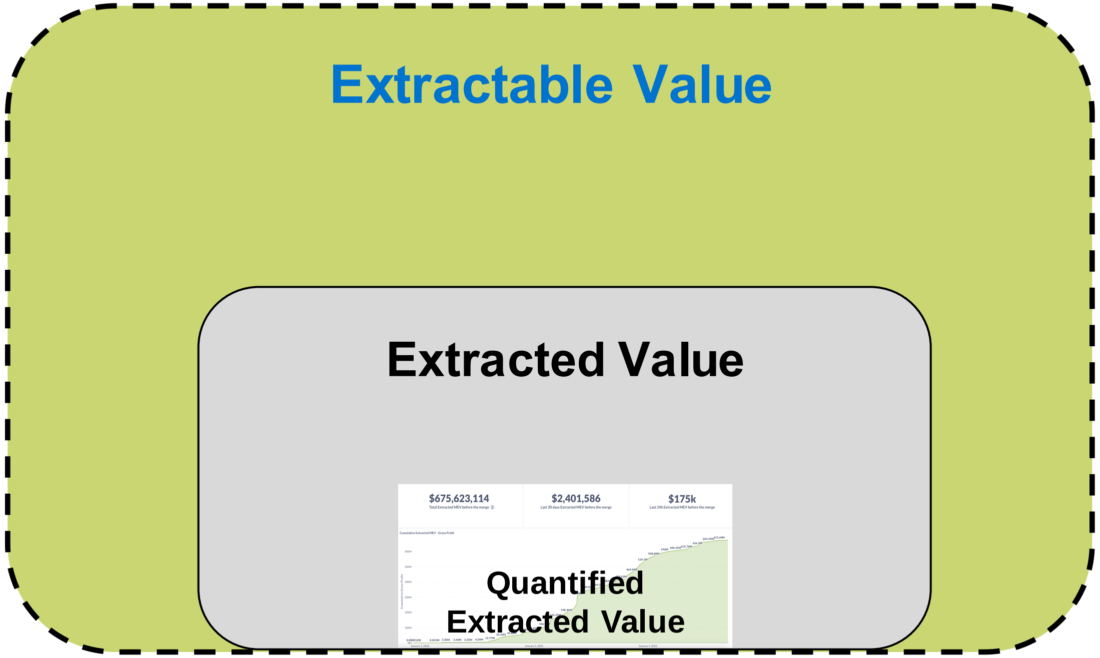
Although quantified extracted value hints us the magnitude of MEV, it does not paint the whole picture.

Extractable Value

Given a state and a snapshot of the mempool, **find profit-generating transactions** (i.e., the value that could have been extracted)**.**

Research Objectives

- Finding a close-to-optimal algorithm to **detect opportunities** (starting with arbitrages) concerning block time.
  - Cycle-detection algorithms like Bellman-Ford may not suffice[1]
  - Solving a convex optimization problem[2]
- Regenerating previous states and running the algorithm to **estimate the extractable value**.
- Comparing extracted value with the extractable value.

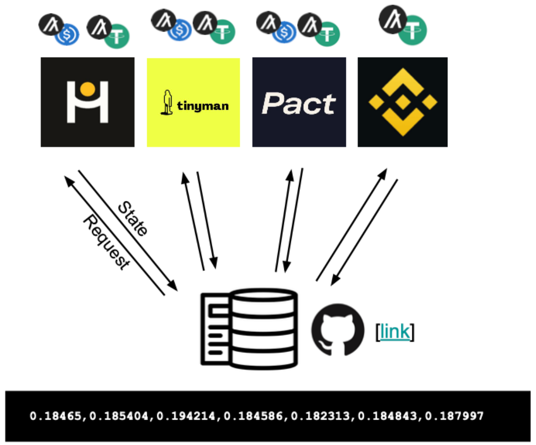


[1] https://arxiv.org/abs/2103.02228
[2] https://noxx.substack.com/p/dex-arbitrage-mathematical-optimisations

Uncovering Profitable Transactions

State-level CEX-DEX Arbitrages

1. Track prices across exchanges and store it for future analysis
   - Currently, only tracking ALGO/USDC & ALGO/USDT
   - Store a tuple for every block
     - {*Binance Price, AMM_1 Price, AMM_2 Price, …, Block Number*}
   - https://github.com/jonasgebele/algo_mev



Analysis of Maximal Extractable Value on the Algorand Blockchain, Jonas Gebele, https://wwwmatthes.in.tum.de/pages/cw84zvafgcxu/Guided-Research-Jonas-Gebele

Uncovering Profitable Transactions

State-level CEX-DEX Arbitrages

2. Spot the price discrepancies between exchanges and calculate the profitability.

Given CEX and DEX (only constant product AMMs) prices, let's find the **profitable price range** (min CEX, DEX deviation w.r.t. fee).

Asset 1: X, Asset 2: Y, DEX: $X * Y = k$

Let D denote the DEX price (Y/X), and S denote the spot market price.

If $S > D$, an arbitrageur can swap Y for X in the DEX and sell the received X in the spot market to make profits.

$$D < S(1-f)^2$$

Using this inequality, given S and fee f, **one can calculate the max D price for the arbitrage to be profitable**.

If $D > S$, an arbitrageur can swap Y for X in the spot market, and sell the received X at the DEX to make profits.

$$D > \frac{S}{(1-f)^2}$$

Using this inequality, given S and fee f, **one can calculate the min D price for the arbitrage to be profitable**.

Min. Deviation Formula: https://www.mathcha.io/editor/BgEV1hBDtnqu481q4hxoz4BYunw6QWqIQ7eOz

Uncovering Profitable Transactions

State-level CEX-DEX Arbitrages

Theoretical MEV on Tinyman v1.1 on the Algorand/USDC market

Analysis of Maximal Extractable Value on the Algorand Blockchain, Jonas Gebele, https://wwwmatthes.in.tum.de/pages/cw84zvafgcxu/Guided-Research-Jonas-Gebele

Evaluating MEV Strategies

The **MEV market of a blockchain is directly impacted by its transaction ordering dynamics**. On Ethereum, one can **prioritize** a transaction through **fee adjustments or off-chain bribes**. This option is out on Algorand as fees do not flow to the block proposers. Therefore, proposers are assumed to follow the **default Algorand implementation** that orders transactions based on their arrival (**FCFS**).

No network-level Frontrunning → ***Cannot spot a transaction in the mempool and attempt to frontrun it***
Probabilistic Backrunning → ***Latency games to be the first to backrun***
State-level Frontrunning → ***Latency games to get positioned top of the block***

Moreover, it is **non-trivial for proposers to plan a strategy beforehand** due to the **cryptographic sortition algorithm** and **relatively fast block time**. Mimics PoW-like probabilistic proposer election.

Research Objectives

- What techniques does Algorand block proposers employ when ordering transactions in the blocks they build?
- How can position-dependent MEV strategies be executed on the Algorand blockchain?
- Is it feasible to generate profits by analyzing the last blockchain state and developing a strategy based on it?
- Which protocols and tokens are more suitable for searchers?

Privileged Extractable Value

Privileged extractable value (i.e., Monarch MEV[1]) refers to the **value** a network **coordinator can extract**.

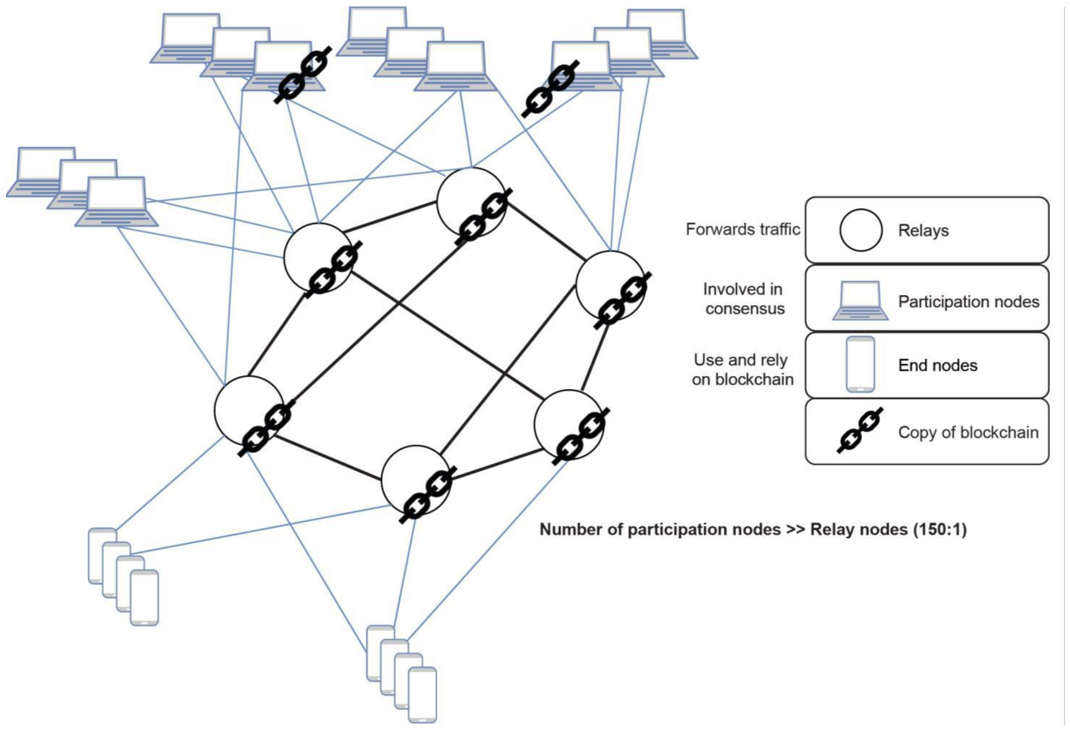
- On Algorand, **Monarchs** are **block proposers** running participation nodes alongside **relay nodes** controlling the network traffic.
- **As block proposers or relays have no direct economic incentive** to contribute to the network**, we investigate whether MEV incentivizes them**.

Proposer Extractable Value

- Block proposers have the power to determine which transactions are included in their block, and in which order (can execute any MEV strategy - ~~FCFS~~).

Vertical Integration with Relays

- Although proposers decide which transactions go into their block, relay nodes are responsible for the propagation on the network.
- **What are the manipulations a relay node can do?**
  - censor/delay transactions
  - delay consensus?
- **Is there an incentive for an MEV searcher or a proposer to collude with a relay node?**



Algorand Network Model

[1] https://archive.devcon.org/resources/6/this-is-mev.pdf

The Algorand network figure is taken from the slides of TUM Chair of Network Architectures and Services.

MEV on Algorand

M.Sc.

Burak Öz

burak.oez@tum.de

Technische Universität München
Faculty of Informatics
Chair of Software Engineering for Business Information Systems

Boltzmannstraße 3
85748 Garching bei München

Tel +49.89.289. 17132
Fax +49.89.289.17136

matthes@in.tum.de
wwwmatthes.in.tum.de