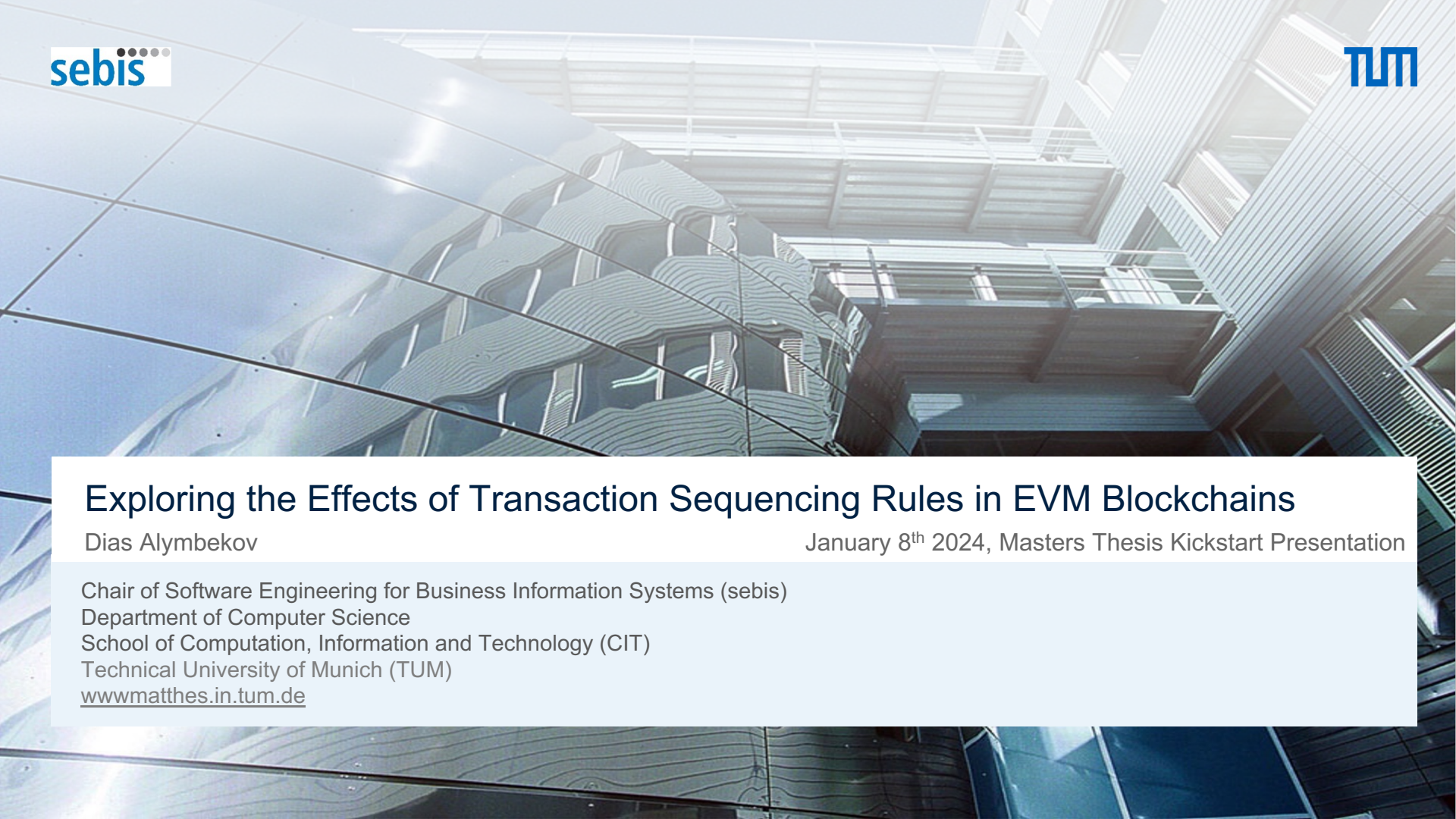


Exploring the Effects of Transaction Sequencing Rules in EVM Blockchains

Dias Alymbekov

January 8th 2024, Masters Thesis Kickstart Presentation

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

- Motivation
- Problem Statement
- Research question
- Considerations
- Methodology
- Timeline

Motivation

Centralized exchanges

- Trades are executed and settled by intermediaries
- Lower autonomy of personal funds
- Transactions are executed sequentially based on arrival time

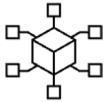
- “As of 2022, the locked capital in DeFi protocols exceeds $40 billion U.S. dollars.”

Decentralized exchanges

1

Transactions are executed using smart contracts without intermediaries

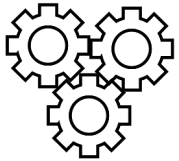
No intermediaries



2

The nature of permissionless blockchains guarantees access to trading infrastructure

Permissionless blockchains



4

Require sequencing rules

Transactions are executed sequentially in batches. Transactions in each batch are sequenced by block builders

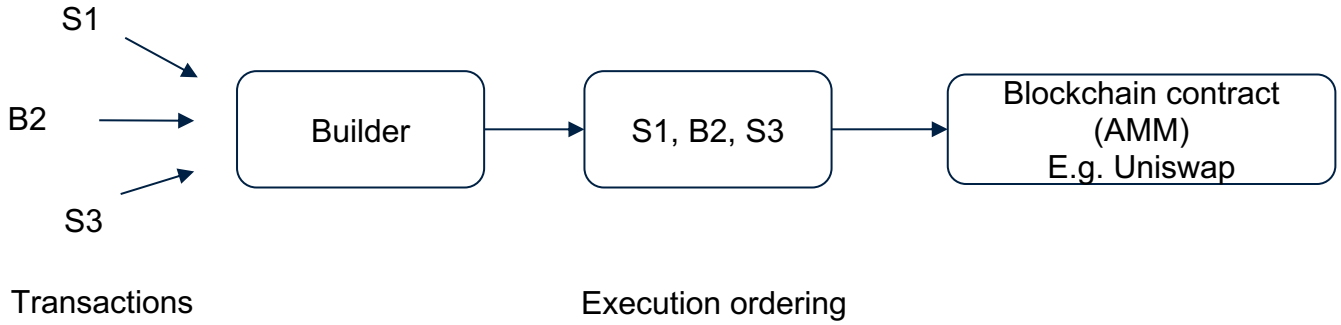
3

Greater autonomy and flexibility

Users can have autonomy and flexibility to use funds in different exchanges

Problem statement

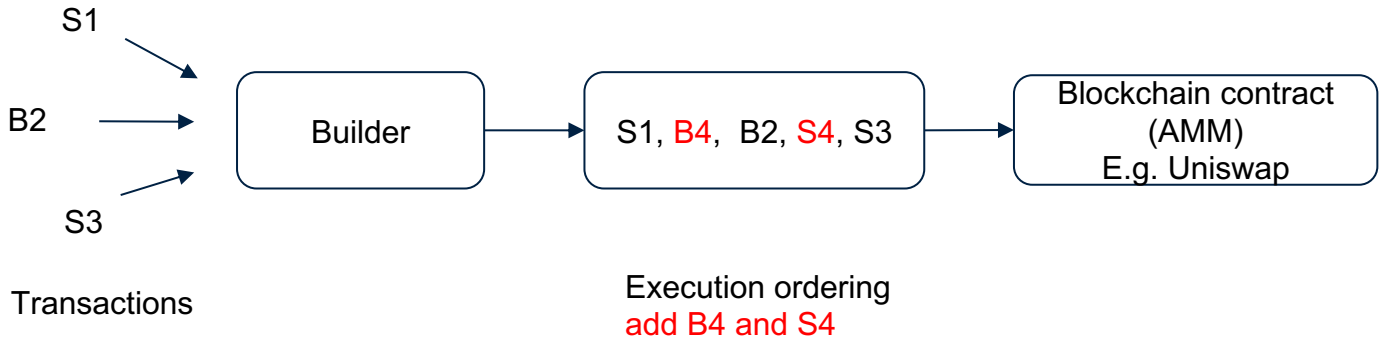
Problem statement: Sequencing of transactions in a block[1] (1/4)



- Block builders package trades into blocks
- Block builders need to sequence the transactions
- Transactions in each block are executed sequentially (not in parallel)

[1] Matheus V. X. Ferreira, David C. Parkes, Credible Decentralized Exchange Design via Verifiable

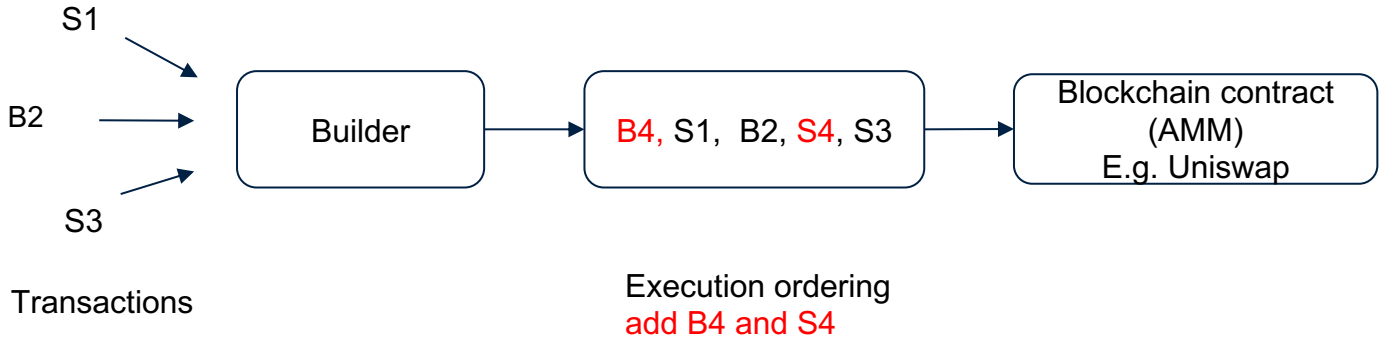
Problem statement: Sequencing of transactions in a block [1] (2/4)



- Block builders have power to insert or reorder any transaction in a block
- Rational block builders would manipulate order to maximize profit

[1] Matheus V. X. Ferreira, David C. Parkes, Credible Decentralized Exchange Design via Verifiable

Problem statement: Sequencing of transactions in a block [1] (3/4)



- Block builders have power to insert or reorder any transaction in a block
- Rational block builders would manipulate order to maximize profit

[1] Matheus V. X. Ferreira, David C. Parkes, Credible Decentralized Exchange Design via Verifiable

Problem statement: MEV extraction can be defined as a Knapsack problem

The 0-1 knapsack problem is formally defined as follows:

- $tx_1, ..., tx_n$ - a set of concurrent transactions
- $m_1, ..., m_n$ - gas price
- $g_1, ..., g_n$ - units of gas
- $m_i g_i$ - sequencer fee for inclusion of tx_i
- x_i - flag to indicate if tx_i was included
- L - maximum gas that can be included in a block

$$\max \quad \sum_{i=1}^{n} x_i m_i g_i$$

$$\text{s.t.} \quad \sum_{i=1}^{n} x_i g_i \leq L,$$

$$x_i \in \{0, 1\}.$$

Figure 1: Knapsack optimization problem for inclusion of transaction in a block

Objective function: maximize miner fee earned while staying under block's gas limit

Problem statement: Ordering techniques have different effects on miners and traders

Miner's profit 

- Rational miners will always manipulate ordering to maximize profit
- Mechanisms such as priority gas ordering or flashbots auctions are designed to maximize miners' profits

Trade fairness 

- It is impossible to find a sequencing rule that would prevent miners from obtaining risk-free profit.
- There are sequencing rules that provide provable guarantees.
- Relays with private pools, batch auctions can mitigate effects of MEV

Considerations: Is it possible to enforce and measure trade fairness?

Considerations: Enforcing fairness is not straightforward (1/2)

Challenge to control multiple blocks	• Multiblock deviations cannot be prevented by a single block level strategies
Different starting points of block builders	• Different mempool views • Different access to liquidity
Fairness is subjective	• There are different ways to measure fairness • Protocols can introduce priority queues to give priority to searchers that bring more value

Academic research distinguishes several techniques to measure fair sequencing for users

How to formalize measurement of trade fairness?

Monetary value

Potential functions of liquidity pools

Price of anarchy

Considerations: How is trade fairness enforced?

Considerations: Fairness can be enforced using different levers (2/2)

Consensus-level mechanisms	• Fairness can be enforced on protocol level (ex: FIFO using pseudo-timestamps)
Application-level ordering	• Applications can use auctions to sell the right execute first transaction in a block
Cryptographic rules	• Protocols can increase fairness by obfuscating input (ex: SGX, threshold decryption, zk-proofs)

Transaction execution fairness can be enforced on different layers of the blockchain stack

Initial area of interest	Fairness-aware consensus-level sequencing algorithms	Sequencer-level sequencing algorithms	On-chain application-level fair sequencing algorithms	Off-chain application-level fair sequencing algorithms
Description	- Transaction order-fairness is treated as a third consensus property. Fairness is enforced as a part of the consensus algorithm	- Transaction order-fairness is enforced by a block builder (sequencer).	- Applications can introduce application-level algorithms to ensure fair execution of transactions or introduce application specific rules.	- Optimal ordering can be found by algorithms executed off-chain
Examples of used techniques	- Relying on timestamps - Input-aware techniques - Utilizing cryptographic techniques to introduce privacy	- Relying on timestamps - Input-aware techniques - Utilizing cryptographic techniques to introduce privacy	- Auctions - Priority queues	- Heuristics that can solve NP-complete problems
Notes on fairness guarantees	- Enforcement of order-fairness on consensus layer ensures enforcement of fairness guarantees by the base-layer protocol	- Fairness cannot be guaranteed by the protocol but there is a set of verifiable rules that can provide fairness guarantees.	- Fairness is maintained bythe application-level rules	Fairness can be maximized using optimal heuristics (this can lead to more optimal results)
Complexity considerations	- Need to consider communication complexity - Runtime complexity is bounded	- Runtime complexity is bounded by polynomial algorithms	- Runtime complexity depends on the definition of fairness	- Can apply approximation algorithms to solve NP-complete target functions
Examples	Aequitas, Wendy, Pompe, Quick-Fairness, Themis	Priority gas ordering, Flashbots, random, FIFO, Dictatorship, metadata mechanism	On-chain auctions, Prioritization of frequent users	Cowswap's batch auctions

Bibliography

[1] Matheus V. X. Ferreira, David C. Parkes, Credible Decentralized Exchange Design via Verifiable Sequencing Rules. https://arxiv.org/pdf/2209.15569.pdf Accessed: 2023-10-23. 2023.

[2] Alex Nezlobin, A few thoughts on the optimal extraction of stat arb MEV. https://twitter.com/0x94305/status/1618744497864851459 Accessed: 2023-10-23. 2023.

[3] Quintus Kilbourn, A Transaction Ordering Rules Taxonomy. https://collective.flashbots.net/t/a-transaction-ordering-rules-taxonomy/1082/1 Accessed: 2023-10-23. 2023.

[4] Bruno Mazorra, Michael Reynolds, Vanesa Daza, Price of MEV: Towards a Game Theoretical Approach to MEV. https://arxiv.org/pdf/2208.13464.pdf Accessed: 2023-10-23. 2023.

[5] Shashank Motepalli, Luciano Freitas, Benjamin Livshits SoK: Decentralized Sequencers for Rollups. https://arxiv.org/pdf/2310.03616.pdf Accessed: 2023-10-23. 2023.

[6] Akaki Mamageishvili, an Christoph Schlegel, Shared Sequencing and Latency Competition as a Noisy Contest. https://arxiv.org/abs/2310.02390 Accessed: 2023-10-23. 2023.

[7] Defi pulse - the decentralized finance leaderboard. https://www.defipulse.com/ Accessed: 2023-10-23. 2023.

[8] Flashbots. https://docs.flashbots.net/ Accessed: 2023-10-23. 202

Dias Alymbekov
dias.alymbekov@tum.de

Technical University of Munich (TUM)
TUM School of CIT
Department of Computer Science (CS)
Chair of Software Engineering for
Business Information Systems (sebis)

Boltzmannstraße 3
85748 Garching bei München

+49.89.289.17132
matthes@in.tum.de
wwwmatthes.in.tum.de