Analytical and Empirical Evaluation of the Feasibility of MEV Extraction Techniques on the Algorand Blockchain

Parshant Singh, May 08, 2023, Kick-off Presentation Guided Research

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

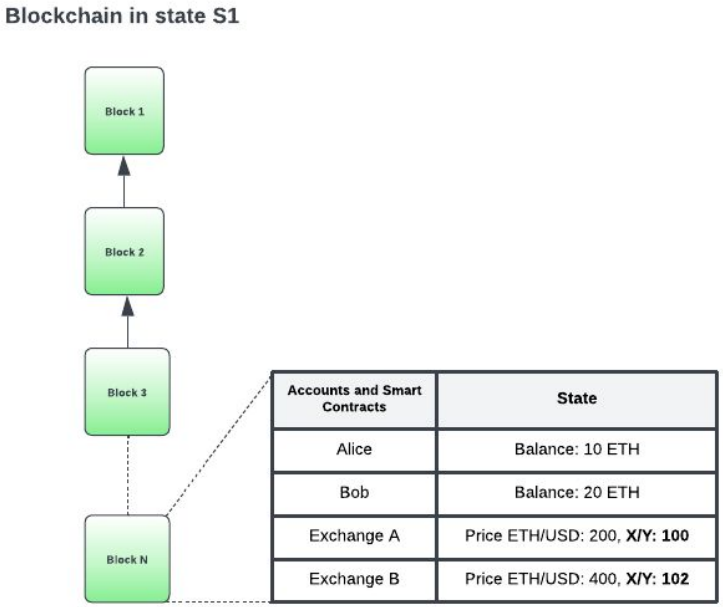
1. Motivation and Background Information
2. Research Objectives
3. Timeline

Scenario 1

State Level Profitable Transaction Discovery
(Arbitrage)

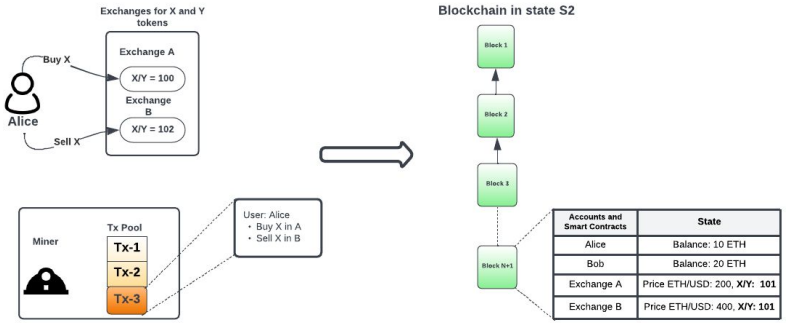
For more information visit https://github.com/cusma/algorand-school

Motivation and Background Information



- A public, permissionless smart contract blockchain is a replicated state machine where state refers to account balances and smart contract storage.
- Decentralised Exchanges are applications which allow users to exchange tokens
- Supply and demand determine the price.
- No automatic mechanism to balance the prices across exchanges.

Motivation and Background Information

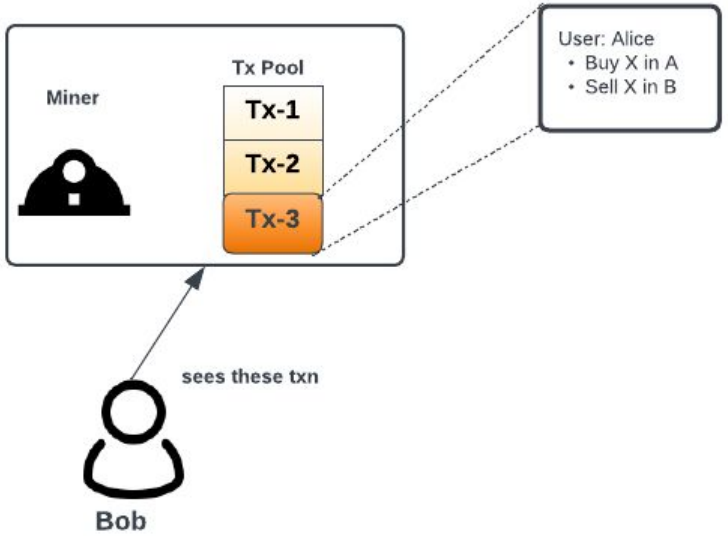


- Alice monitors the state and spots the price difference.
- Issues a transaction to buy X on the cheap exchange and sells on the expensive one to make profits.
- Miner picks up the transaction, bundles it in a block.
- Alice makes a profit on the opportunity she spotted by monitoring the blockchain state.

Scenario 2

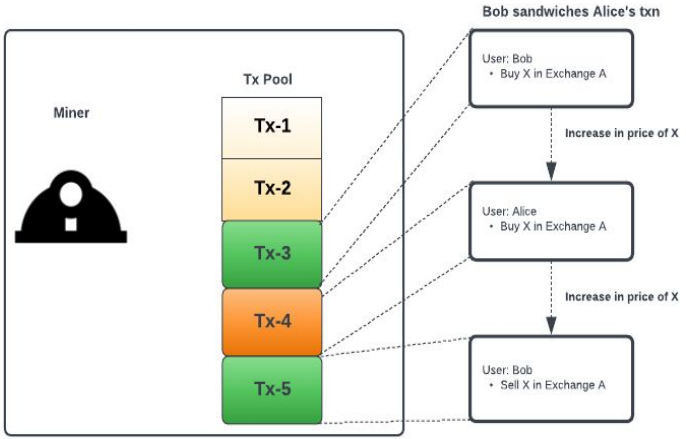
Network Level Profitable Transaction Discovery
(Frontrunning, Backrunning, Sandwich Attack)

Motivation and Background Information



- Blockchains have sequential, deterministic execution and the transaction is public and visible to everyone in permissionless blockchains.
- If Bob sees a transaction in the pool that involves buying token X on exchange A, he can calculate the impact of this transaction on the prices and take position accordingly.
- As Bob can monitor the pool, he can attempt to do such operation when he sees a trade.
- However, he needs to ensure his transaction is executed before the trade he spotted.

Motivation and Background Information



Sandwich attack

What we discussed in previous slides, i.e, including, excluding, or changing the order of transactions during the block production process is known as Maximum Extractable Value in blockchains.

- MEV has been studied extensively since 2020 in Ethereum [1].
- However, MEV is not inherently Ethereum based.
- Any blockchain with these properties - public transaction pool, smart contract based can be impacted by this.
- Algorand is one such blockchain satisfying the above conditions.

1. Flash Boys 2.0: https://arxiv.org/pdf/1904.05234.pdf

NO TRANSACTION-ORDERING BY FEE
(transaction fees go to Algorand Foundation)

- Unlike in Ethereum, Algorand doesn't incentivise miners to prioritize transaction based on transaction fees.

Algorand PPoS Consensus

- **Scalable** 6000 TPS, billions of users
- **Fast** < 3.9 s per block
- **Secure** 0 downtime for over 23M blocks
- **Low fees** 0.001 ALGO per txn
- **No Soft Forks** prob. < 10^{-18}
- **Instant Transaction Finality**

Outline

1. Motivation and Background Information
2. Research Objectives
3. Timeline

Motivation and Background Information

Goal of this Guided Research is to empirically evaluate the feasibility of MEV extraction strategies on the Algorand Blockchain

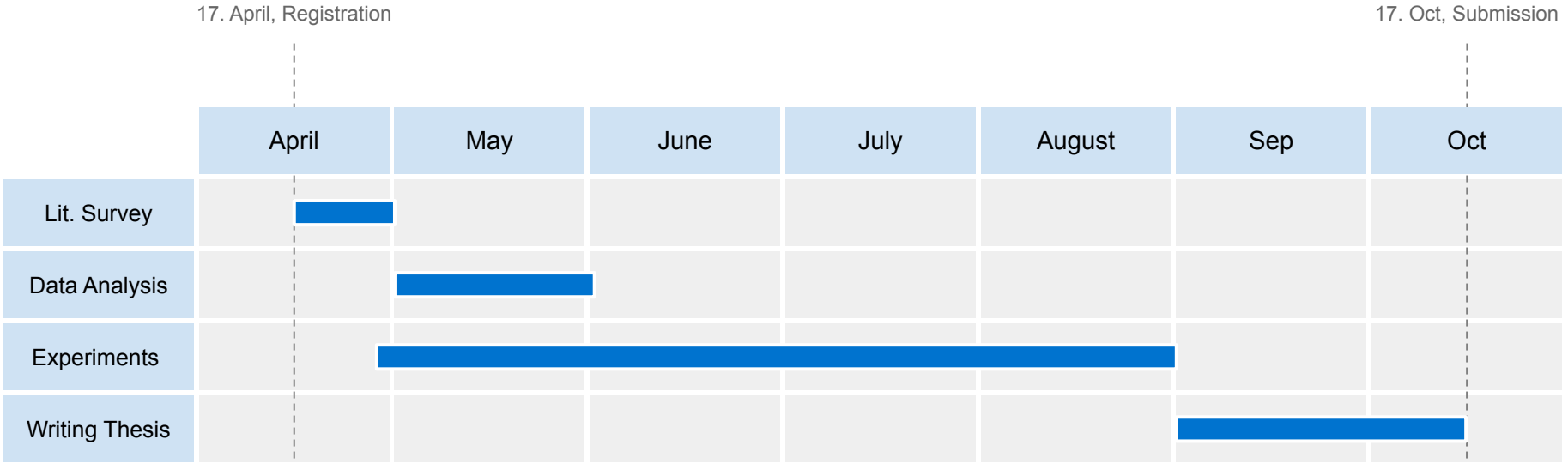
01	**Is it feasible to generate profits by analyzing the last blockchain state and developing a strategy based on it ?**	• Monitor the state, run an algorithm to check if any opportunity exists and execute it on mainnet and testnet. • Employ algorithms discussed in [1] and [2] that have been shown to be effective for executing trades.
02	**Is it possible to execute position-dependent MEV strategies on the Algorand Blockchain ?**	• Monitor the transaction pool through our Algorand Node and execute strategy
03	**What are the techniques that Algorand block proposers employ when ordering transactions in the blocks they build ?**	• Since we need to prioritize our transactions, we need to understand what strategies block proposers employ (if any) while generating blocks.

[1] L. Zhou, K. Qin, C. F. Torres, D. V. Le, and A. Gervais, "High-frequency trading on decentralized on-chain exchanges," in 2021 IEEE Symposium on Security and Privacy (SP). IEEE, 2021, pp. 428–445.
[2] L. Zhou, K. Qin, A. Cully, B. Livshits, and A. Gervais, "On the just-in-time discovery of profit-generating transactions in defi protocols," in 2021 IEEE Symposium on Security and Privacy (SP). IEEE, 2021, pp. 919–936.

Outline

1. Motivation and Background Information
2. Research Objectives
3. Timeline

Timeline


17. April, Registration
17. Oct, Submission
April
May
June
July
August
Sep
Oct
Lit. Survey
Data Analysis
Experiments
Writing Thesis

Parshant Singh
parshant.singh@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.

wwwmatthes.in.tum.de