mev [re]search-athon (sign up)

Date: Saturday, March 4, 2023

Venue: pirateship hackerhouse at ethdenver

Livestream: https://meet.google.com/fot-iiof-jkm

Food: Breakfast + light lunch will be provided

Brought to you by Flashbots. Special thanks to Rook, Blocknative, Gauntlet, DBA, Fenbushi.

wtf is a [re]search-athon

> Every now and then, when I look around, I find myself, along with many of you lingering on this page, trapped in the parable of the blind men and an elephant
>
> While MEV is a critical metric for network security in any distributed system secured by economic incentives it is also a multidiciplinary design space that lies in the intersection of economics, security and cryptography. While anyone may bring *something* to the table regardless of domain of expertise, cross-domain collaboration often incurs higher communications overhead due to vastly different frames of references. Moreover, boundaries of organizations add friction to open collaboration in exploratory research or emergent design problems. We often see withholding of information due to differences in strategic interests, unnecessary redundancies or gaps across organizations, or failure to align on a common understanding due to a lack of shared context. We end up circling around local optima, involuntarily fall into turf wars from unnecessary collisions.
>
> Everyone in the MEV space has their own journey. To me, Flashbots is a live experiment in open collaborative R&D. It started out as an inter-disciplinary research collective - the MEV Pi-rate Ship. "A perpetual salon" as James Preswich fondly recalls in MEV: the first five years. A lot of the validation and iteration of the early Flashbots designs happened in MEV roasts, which stem from "Treasure Map Roast" on our irl Pi-rate Ship hackerhouse, as a means to force function the crystalization of shower thoughts research with artificial deadlines. We roast and troll in good jest, to get us over our own insecurities, and we matchmade specialized (surplus) human capital for execution of strategies.

The MEV Research-athon is yet another social experiment for collaborative research. We invite [re]searchers, protocol designers, data scientists from different organizations that are tackling a common problem space, to hack on some shared challenges.

Researchers can form "Special Purpose Vessels" - flash organizations of 3-5 researchers that team up based on interest in a particular challenge, to tackle specific research problems in an irl workshop.

To overcome the Babel Tower in collaboration, much of the day will be spent on calibration of knowledge via curated talks. Each of the talk should make references to prior speaker's framework, language and mental models to maintain consistency.

By the end of the workshop, each of the teams should present their research question and methodologies similar to a research proposal for FRP, or design specifications, prototypes, etc..

Ideally, the research-athon may inspire participants to continue after the irl workshop, and turn the ideas and prototypes into POCs, blogposts, papers or future presentation.

For this particular mev [re]searchathon, the teams may be invited to present at our joint virtual event with ETHGlobal - Scaling Ethereum: **MEV.wtf 2023** (more details to come).

auctions.design

09:30 - 11:00 Coffee Meets Bagel: [re]searchathon SPV matchmaking

- Review or re-read papers for today's session, and come up with questions for each speaker.
- Refine the 3 research questions around order flow auction design.
- Divide up into Special Purpose Vessels (3-5 people each).

Note: We may be roasting Tarun's ETHDenver mainstage talk - Why are cross-chain auctions so hard? over coffee, sandwiches and memosa on the pirateship hackercouch.

11:00 - 11:30 Censorship-Resistance in On-Chain Auctions (Paper | Slides) | Max Resnick (Rook)

Abstract: Smart contracts offer a way to credibly commit to a mechanism, as long as it can be expressed as an easily computable mapping from inputs, in the form of transactions on-chain, to outputs: allocations and payments. But proposers decide which transactions to include, allowing them to manipulate these mechanisms and extract temporary monopoly rents known as MEV. Motivated by both general interest in running auctions on-chain, and current proposals to conduct MEV auctions on-chain, we study how these manipulations effect the equilibria of auctions.

Formally, we consider an independent private value auction where bidders simultaneously submit private bids, and public tips, that are paid to the proposer upon inclusion. A single additional bidder may bribe the proposer to omit competing bids.

We show that even if bids are completely sealed, tips reveal bids in equilibrium, which suggests that encrypting bids may not prevent manipulation. Further, we show that collusion at the transaction inclusion step is extremely profitable for the colluding bidder: as the number of bidders increases, the probability that the winner is not colluding and the economic efficiency of the auction both decrease faster than 1/n. Running the auction over multiple blocks, each with a different proposer, alleviates the problem only if the number of blocks is larger than the number of bidders. We argue that blockchains with more than one concurrent proposer can credibly execute auctions on chain, as long as tips can be conditioned on the number of proposers that include the transaction.

11:30 - 12:00 **Numerical analysis of non-atomic trade execution protocol (Slides)** | AC (Cron Finance)

Abstract: This talk will give researchers, protocol designers and smart contract developers a complete understanding of methods necessary to analyze and verify functional logic for continuous non-atomic execution DeFi protocols. It will also give curious users and blockchain-aware audiences a glimpse of the magic that goes into bringing these useful new primitives on chain.

A big part of building an AMM with theoretically large unbounded loops (virtual orders) is the potential to push the system beyond the gas and compute bounds of the EVM. In addition, the complexity of non-atomic trade execution demands various mechanisms to address MEV, PFoF, DDoS, gas griefing, etc., which must all fit in a single smart contract.

We demonstrate how these breakthrough features can be miniaturized to fit within the storage requirements of a single contract, and demonstrate new numerical analytic methods to validate the system in the presence of optimizations which allow for unchecked arithmetic and the potential for overflow or underflow.

We will also share our apparatus used to benchmark, test, simulate, and analyze the numerical accuracy of our code, a hyper-optimized TWAMM based on the concept introduced by Dave White, Dan Robinson, and Hayden Adams. This work is the product of over a year of continuous development, and we believe the tools, learnings and discoveries we've made along the way will be invaluable to future builds in the space.

12:00 - 12:30 **From auctions.google.com to auctions.best (Paper)** | Tarun Chitra (Gauntlet)

Abstract: Akbarpour and Li (2020) formalized credibility as an auction desideratum where the auctioneer cannot benefit by implementing undetectable deviations from the promised auction and showed that, in the plain model, the ascending price auction with reserves is the only credible, strategyproof, revenue-optimal auction. Ferreira and Weinberg (2020) proposed the Deferred Revelation Auction (DRA) as a communication efficient auction that avoids the uniqueness results from Akbarpour and Li (2020) assuming the existence of cryptographic commitments and as long as bidder valuations are MHR. They also showed DRA is not credible in settings where bidder valuations are α-strongly regular unless $\alpha>1$. In this paper, we ask if blockchains allow us to design a larger class of credible auctions. We answer this question positively, by showing that DRA is credible even for α-strongly regular distributions for all $\alpha>0$ if implemented over a secure and censorship-resistant blockchain. We argue ledgers provide two properties that limit deviations from a self-interested auctioneer. First, the existence of smart contracts allows one to extend the concept of credibility to settings where the auctioneer does not have a reputation -- one of the main limitations for the definition of credibility from Akbarpour and Li (2020). Second, blockchains allow us to implement mechanisms over a public broadcast channel, removing the adaptive undetectable deviations driving the negative results of Ferreira and Weinberg (2020).

orderflow.auction

12:30 - 13:00 **An anatomy of order flow (slides)** | Tom Schmidt - Dragonfly Capital Partners

13:00 - 13:15 **Probabilistic Approach to MEV-aware DEX Design (Slides)** | Amir Bandeali - 0x

13:15 - 13:30 **MEV Implications on DEX Order Flow (Slides)** | Danning Sui - 0x

13:30 - 14:00 **Order Flow Auction Treasure Map (Slides)** | Quintus Kilbourn - Flashbots

14:00 - 15:30 **[Roast] OFA Beauty Contest** | Roast Master: Dan Robinson - Paradigm

- Rook | Max Resnick (Rook)

- MEV-Wallet (slides | James Preswich
- Wallet-Boost | Dan Marzec (Blocknative)
- MEV-Share (Slides) | Robert Miller (Flashbots)

15:30 - 17:00 **Breakout sessions into SPVs**

17:00 - 18:00 **[Roasted] SPV Presentations** | Roast Master: Phil Daian (Virtual)

backrunning.party (invitation)

19:00 - midnight Wynkoop Brewing Company - 1634 18th St, Denver, CO 80202, USA