---

slug: frp-year-in-review title: FRP Year in Review authors: [sarah] tags: [research] image: /frp-yir-image.png hide_table_of_contents: false description: Flashbots Research Proposals (FRP) is a grants program that Flashbots uses to fund community research, work with collaborators, and ensure that researchers beyond our internal team have the resources they need to illuminate the dark forest. Read on for some highlighted FRPs, which have been completed in the last year. forum_link:

Flashbots Research Proposals (FRP) is a grants program that Flashbots uses to fund community research, work with collaborators, and ensure that researchers beyond our internal team have the resources they need to illuminate the dark forest. While FRPs have existed since early Flashbots, our pace of grants-making accelerated in the past year. This post outlines our goals and methodology for FRP and highlights some cool projects this program made possible. Through FRP, we want to ensure that MEV is not only one of the most intellectually engaging areas to do research, but also one where passionate researchers can always find funding and support for their work. In the past year, FRP has made large strides in that direction, allowing Flashbots to support a range of external researchers including seasoned academics, ecosystem contributors, and new entrants to independent MEV research.

We are excited about MEV research because:

- MEV research is inherently multidisciplinary, and those disciplines are often connected in novel ways.
- Competition in the MEV supply chain has produced an abundance of natural experiments in incentives and markets. Those experiments need to be communicated to the outside world for their full impact to be realized.
- MEV is at the heart of blockchain systems, and it is a core engine to inform future developments of the technology. Research can support future protocols in productively using MEV.
- By researching MEV, we support Ethereum in remaining transparent with informed and empowered participants collaborating in the pursuit of fair and efficient markets.

Flashbots has twice reshaped the Ethereum block building market through transformative products, starting with mev-geth and later mev-boost. Since the days of the MEV Pirate Ship, which predated the formal founding of Flashbots, there has been a culture of research in our community. This led Flashbots to have a dual engine design with both a Product and Research Organization internally. With this design, fulfilling our mandate as stewards of MEV has meant paving the way through both products and research. We engage with the research community in a variety of ways: by publishing our internal research, by giving context and collaborating with academic researchers, byhosting workshops that add an MEV-track to academic presentation venues, by aligning the community on important areas of inquiry with MEV Roasts (recent, archive), and by directly collaborating with external researchers through FRP projects.

Read on for some highlighted FRPs, which have been completed in the last year.

Recently Completed FRPs

FRP 10: Distributed Blockbuilding Networks via Secure Knapsack Auctions

FRP 10 proposes ways to construct distributed block builder networks using a secure knapsack solver. They do this with three methods: dynamic programming, using a greedy algorithm (recommended currently), and using multiparty computation (future-looking recommendation). First, the researchers attempt to build such a knapsack solver based on dynamic programming techniques. Then, they show how to build such a knapsack solver using a greedy algorithm and show benchmarks that provide evidence for pursuing the greedy algorithm approach. Finally, they discuss future research directions for MPC-based block building. FRP 10 produced a research report posted to the Flashbots Forum *Flashbots Fellow Mikerah, Responsible Flashbots Mate Jonathan Passerat-Palmbach*

FRP 18 : Cryptographic Primitives for Complete Privacy

FRP 18 surveyed the existing cryptographic solutions for a completely private mempool. Much of MEV extraction activity is possible due to the public nature of the Ethereum mempool. Searchers are able to identify value to extract by viewing the pool of unconfirmed transactions. By making the mempool private, many current MEV opportunities would no longer be

extractable, which could result in better execution of transactions with lower fees for users. However, even with a private mempool, MEV opportunities can still arise depending on factors like auction designs and intra user time dependence of orders. The researchers sought to determine which cryptographic privacy solutions are best suited to trustlessly solve the problem of creating a mempool where orders are private until they have been confirmed and their contents are no longer valuable for MEV extraction. They considered multi-party computation (MPC), verifiable delay functions (vdf), threshold encryption, zero knowledge (ZK), and witness encryption. They produced a table comparing properties of all the encrypted mempool solutions they compared. They found that threshold encryption is currently the most practical and that witness encryption is also promising. FRP 18 produced an academic paper and a blog post. *Flashbots Fellow James Stern, Responsible Flashbots Mate Jonathan Passerat-Palmbach*

FRP 21: MEV in Fixed Gas Price Blockchains

While a lot of focus has been given to the MEV market on blockchains with dynamic gas prices, few have considered MEV on blockchains with fixed gas prices. FRP 21 sought to understand MEV on blockchains that have a fixed gas price. The researchers looked at Terra Classic as an example blockchain. In analyzing successful arbitrages completed around a major de-pegging event of the native token, the researchers found that many successful arbitragers did not require large amounts of startup capital or sophisticated strategies involving more than four hops. However, MEV searchers who were running more complex strategies including multiple virtual machines and wider geographic coverage were more profitable and won more arbitrage opportunities. Their findings suggest that in fixed gas blockchains, successful MEV searching is about winning on latency. FRP 21 led to a research paper posted on Arxiv and a blog post. *Flashbots Fellow Facundo Carrillo, Responsible Flashbots Mate Elaine Hu*

FRP 22: Quantifying the Impact of Frontrunning and Randomness on UX

FRP 22 sought to quantify the impact of frontrunning and randomness on user experience. As the body of literature studying MEV and transaction execution in blockchains has grown, a variety of formal models have been formulated in order to convey results in specific settings. This diversity in models can make it difficult to compare related results and require repeated work in inventing models for new settings. FRP 22 proposed a general queuing theoretic model for adversarial transaction ordering in order to address this problem. While queuing theory traditionally does not consider complex incentives and previous work on transaction scheduling in blockchain focuses on first-in-first-out or fee-based ordering, the model proposed in FRP-22 is constructed with MEV in mind. The paper demonstrates how the model can be used to understand environments like constant function automated market maker (CFMM) trading as well as the impact of phenomena like sandwiching and resultant execution price. The model is intended to serve as a larger framework to facilitate standardized formal analysis of different settings such as different chain rules, decentralized application interactions, presence of reverse auctions or order flow characteristics. FRP 22 led to a research paper posted on Arxiv and a blog post. *Flashbots Fellow Andrew Macpherson, Responsible Flashbots Mate Quintus Kilbourn*

FRP 23: Welfare, AMMs and MEV

FRP 23 studied a simple model of the welfare of constant function market maker (CFMM) users. The researchers established the ideal case where all trades can happen simultaneously at the walrasian equilibrium prices and allocations. This metric became the benchmark to study how much of that utility can be recovered in the sequential case by a given CFMM. Their study found that when one agent has the role of proposing the block with scarce block space, they can obtain higher expected utility than otherwise identical agents. This also gives a lower bound on the maximal extractable value exposed. FRP 23 was written up as a research paper posted to Arxiv. *Flashbots Fellows Bruno Mazorra and Nikete, Responsible Flashbots Mate Xyn Sun*

FRP 26: Credible Commitments via Open Games

FRP 26 aimed to identify new types of MEV and explore how MEV estimation varies depending on the beliefs of the players involved in a game in which credible commitments can be made. They used 20squares compositional game theory software, which allows for fast prototyping of game-theoretic models, simulations, and analysis. They modeled some thought experiments around the prisoner's dilemma with credible commitments and then generalized these experiments to a more tangible case involving frontrunning and swaps in an automated market maker (AMM). FRP 26 produced an interactive model, which you can explore here. *Flashbots Fellow 20squares, Responsible Flashbots Mate Xyn Sun*

FRP 27: Auction Simulations under PBS

FRP 27 looked at the current auction mechanism in the Proposer-Builder Separation paradigm using compositional game theory (also used in FRP 26 and described above). They produced a model that allows users to simulate and check equilibrium strategies for different kinds of auctions in a modular and extendable way. This model allows user to check their expected outcome given a bidding strategy with some assumed auction design and given that every player plays according to a fixed strategy. FRP 27 produced an interactive model you can explore here. *Flashbots Fellow 20squares, Responsible Flashbots Mate Jolene Dunne*

FRP 28: Contingent Fees in Order Flow Auctions

FRP 28 looked at contingent fees in order flow auction design to determine if contingent or up-front fees produce better outcomes. Contingent fees are fees that are only paid if the order is included in a block. Up-front fees are paid as the auction terminates, regardless of whether the order is successfully executed. Contingent fees are appealing in that they lower risk and capital requirements for participating bidders, as well as being the status quo in Ethereum block auctions. However, order flow auctions constitute a different paradigm, calling for rigorous analysis. The researchers modeled an order flow auction with contingent fees, with up-front payments, and with both. The results suggest that auction designers should minimize contingent fees. When more payments are contingent on execution, revenue and execution probability decreases while effective spreads in equilibrium increase. Although one may seek to remedy these issues in contingent fee markets with a reputation system, the researchers point out there are substantial implementation challenges to this approach. FRP 28 led to a blog post and a paper posted to Arxiv. *Flashbots Fellow Max Resnick, Responsible Flashbots Mate Quintus Kilbourn*

Ongoing FRPs

Aside from the recently completed FRPs, we currently have seven FRPs in some stage of startup or ongoing research, which range in specialty across cryptography, sociology, technical communications, and formal modeling.

- FRP 24 aims to quantify MEV on optimistic rollups.
- FRP 25 analyses fairness granularity- the timing of receipt of transactions- in first come first serve transaction sequencing protocols.
- FRP 29 looks at the current MEV landscape of Ethereum layer-2 protocols and considers the possible impact of the introduction of decentralized sequencers.
- FRP 30 is an empirical study of MEV sharing schemes, systems that offer MEV profit payments back to users.
- FRP 31 looks at the MEV benefits of encrypted mempools for users.
- FRP 32 studies the socioeconomic effects of cryptocurrency redistribution in a rural area.
- FRP 33 works to develop an attestation stack for protocols that run in a trusted execution environment (TEE).

Once each project produces results, they will be posted tothe Flashbots forum.

Notes on the FRP Program

The FRP Program allows Flashbots to fund community MEV research, collaborate externally, and force-multiply our small team. We work with a range of researchers via FRP, including university faculty members, industry researchers, and students.

FRP is administered using this Github repository. You can see what we have funded by looking through the active, closed, and stagnant folders. FRP-1 was submitted in early 2021, and we recently accepted our 33rd FRP! While some FRPs are unpaid (when most appropriate for the collaborators and nature of the project), we typically offer a standard $15K for each project with $10K at acceptance and $5K at completion. We have an FRP section of the Flashbots Forum where you can ask questions related to existing FRPs.

FRP received a generous gift from Moloch DAO, which provided grant funding for FRP 10, FRP 18, FRP 19, FRP 20, and FRP 22 (and from which we have remaining funds to distribute).

FRPs are expected to be about six weeks of full time work for the submitter, who is called a Flashbots Fellow once their

proposal is accepted. The work can also be completed part-time over a longer period. Each accepted proposal has a Flashbots mate who oversees the project, usually someone from within Flashbots Research. This mate is tasked with checking in as-needed with the submitter and reviewing and guiding the project. Sometimes the internal collaborator gets more involved with the project and will jointly author the project output, like papers and blog posts. Other times the fellow works independently with occasional support from their internal contact.

We accept FRPs for a few reasons: * Interest: a community member submits a technically-sound proposal that interests our team and someone is available to be the internal collaborator * Existing collaboration: a member of the Flashbots Research team has invited a potential collaborator to submit a proposal for work where they already hope to contribute * Recruitment: the submitter is considering joining Flashbots full time, and an extended collaboration on an FRP on a topic relevant to their potential work helps us mutually decide if this is best

We reject FRPs for a few reasons: * Priorities: the research direction does not fit with our current priorities * Team interest and time: no Flashbots Mate volunteers to serve as the internal contact for the project due to lack of bandwidth or interest-alignment * Technical fit: the proposal does not indicate the submitter could work independently to produce high quality research. This could be due to requirements for support we are not able to meet, a less technically sound proposal, or requirements for context that we are not able to provide (like confidential data)

In the three years of the FRP program, we have accepted 25 proposals by Flashbots Fellows (plus 7 internal proposals made by mates in the early days of Flashbots Research, which we used to shape internal research directions). Of the 25 accepted external proposals, 15 are completed and 7 are currently ongoing projects. We are proud to support the MEV research community through the FRP program and excited to continue! Over time, we plan to grow the FRP program, with goals like funding PhD student researchers and supporting projects too ambitious to fit within a six-week scope of work. Reflecting on a few years of FRP, the program has helped the small team from Flashbots to engage with many researchers we admire and to support work we are glad is available- this program has been an undeniable success for Flashbots Research!

The legacy of the decision to add a community grants program in the early days of Flashbots has resulted in a more intellectually diverse MEV research ecosystem. This lives on with our current group of seven active Flashbots Fellows, the most we have ever had simultaneously. Thanks to all our current and former Flashbots Fellows!

You can follow along with FRP on the Flashbots forum and submit proposals via Github.

Thanks to Alejo Salles, Quintus Kilbourn, Andrew Miller, Robert Annessi, and Fred Hjalmarsson for their helpful comments on this post.