slug: transparency-april title: Flashbots Transparency Report — April 2021 authors: [robert] tags: [transparency report] image: /img/transparency-january-1.jpeg hide_table_of_contents: false forum_link: https://collective.flashbots.net/t/flashbots-transparency-report-april-2021/865

April 2021 was a month of tremendous adoption, experimentation and learning from the community for Flashbots.

Overview

At the time of writing, mining pools accounting for more than 84% of the Ethereum network hash rate has adopted Flashbots, and the number of unique searchers who landed Flashbots bundles on chain has grown 1430% month on month to over 600 unique searchers in April. Maintaining software stability throughout the Ethereum Berlin Upgrade and improving core infrastructure has been a primary focus for Flashbots. In parallel, we finalized the spec for Flashbots Alpha v0.2, our 2nd major release of Flashbots, surveyed the community for technical feedback, and worked hard towards our release in May.

As an open research organization we stayed true to our commitment to learning from the community and iterating in public. Here are the highlights:

- Finalized Core v0.2 Proposal (target release: May 17)
- Launching Flashbots Transparency Dashboard v0
- Preliminary research on MEV on ETH2.0: through a presentation and a winning ETHGobal hackathon project

Flashbots Core Updates

Core v0.2 Proposal

In early April we published our initial proposal for Flashbots Core v0.2 to gather feedback and share our roadmap. We broke it down to two separate releases: v0.2 pre-release and v0.2 full release (target release date May 17). After hearing from a wide range of stakeholders, and discussing internally, we settled on the following set of features for v0.2:

v0.2 pre-release (released on April 12)

- Revamped auction pricing (pre-release): solve for bundle stuffing and maintain compatibility with gas price payments
- Discard bundles with reverting transactions (pre-release): avoid unintended transactions from landing on chain leading to less chain bloating

v0.2 full-release (target release date May 17)

- Bundle merging (full-release): More revenue for miners, higher chance of inclusion for searchers.
- Replace HTTP endpoints with WebSockets (full-release): Reduce latency, improved node security for miners.
- New geth config introducing strict profit switching (optional, full-release): Eliminates empty block race condition (i.e. mining 2 gwei transaction), but increases latency hence may impact profitability. We decided to remove two proposed features for this release:
- Proxy payment contract: this feature was originally designed to enable better logging and to enable future solutions that attempted to prevent time bandit attacks. It was removed after receiving feedback from the searcher community that the proxy payment contract would add additional costs without providing finality guarantees.
- Full block submission: this feature was removed from the v0.2 release in order to reduce the complexity of the current release.

Deprecating API keys

Flashbots Alpha originally launched with API keys for searchers during the testing phase, and implemented a permissionless authentication through the usage of signing keys in March. Flashbots deprecated API keys altogether in April.

Improved Documentation (docs.flashbots.net)

As we shipped new features in the last months our documentation occasionally fell behind (e.g. no guidance on how to use a testnet). However along with Core v0.2 we are updating our documentation and migrating it off of GitHub and on to a dedicated webpage. Expect to see documentation in the next week.

Flashbots Fair Market Principles (FFMP): Request for Comment

Flashbots Fair Market Principles aims to define a set of key principles and best practices upon which stakeholders of the Flashbots network can hold block producers (miners in ETH 1.0) accountable for their continued participation in the Flashbots Alpha. A set of principles and best practices are needed because of the technical limitations in Flashbots Alpha

that require some parts of the system to run on trust.

We are interested in feedback from the community on these principles and best practices. Please provide feedback and engage in discussion in the Flashbots forum.

MEV-Relay service degradation post-mortem

Over a period of approximately 3 days from April 16th to April 19th the MEV-Relay database was overwhelmed and unable to send bundles quickly to miners. The root cause was our database growing to the point of being overwhelmed when refreshing the stats view. We fixed this by temporarily disabling this view, you can read more details here.

Flashbots Data

Transparency Dashboard v0

As a part of our commitment to transparency Flashbots is releasing a dashboard that surfaces a collection of real time metrics on the Flashbots network and its stakeholders. The dashboard is a living product that will be updated monthly, and we highly suggest taking a look and providing us feedback on what kinds of things you found useful or interesting and what is missing. See the dashboard here.

Miner Adoption

Key metrics

Adoption of Flashbots has continued to steadily increase and at the time of writing 21 mining pools — and 5 of the top 5 — accounting for over 80% of Ethereum hashrate are receiving Flashbots bundles. 8 of the top 10 mining pool addresses are currently running MEV-Geth.

Source: Etherscan (5/12/2021)

The total profit that miners have made from Flashbots increased nearly 10X in April from ~1k ETH to ~10k ETH of profit. At the same time the average profit per block has stabilized at 0.18–0.2 ETH per block. It is expected that Flashbots' next release will increase both total profit and average profit per block.

Source: Flashbots. Miner profit is found by taking the increase in revenue from Flashbots bundles (e.g. coinbase payments) minus the opportunity cost of including Flashbots bundles (e.g. gas fees from displaced transactions).

Searcher Adoption

Key Metrics

The number of unique active searchers using Flashbots multiplied several times in April. Measuring searchers is difficult as one searcher may use multiple accounts and contracts. As such we use three metrics to measure unique searchers: unique EOAs, unique contracts interacted with, and unique signing keys seen in the relay. Furthermore, we only count searchers who have had their bundles included on-chain.

Source: Flashbots.

Although Flashbots bundles typically have 0 gas price transactions, bundles do have an "effective" gas price that can be found by taking the bundle's coinbase transfer payments divided by the gas that the bundle consumes. MEV-Geth compares the bundle's gas price to the gas price of transactions at the tail end of the block, which we refer to as the "tail gas price." As you can see in the above graph the bundle gas price closely tracked tail gas price until roughly the start of March, when there was an uptick in searcher adoption on Flashbots. At that point the median bundle gas price was substantially higher than the tail gas price and the difference between the two continued to grow until it stabilized in April.

Source: Flashbots

Battle of the Bots

In early April sandwich bots turned on each other as several attackers deployed malicious tokens designed to drain the funds of sandwich bots. To work these malicious tokens needed to evade sandwich bots simulations and take advantage of how Flashbots operates. Ultimately one attacker made hundreds of ETH from draining sandwich bots. Read this thread for a

fascinating look at how sandwich bots work and the extremely adversarial environment in which they operate.

The Bandits of Ethereum's Uncles

By now almost everyone knows the meme that "Ethereum's mempool is a dark forest." Before last month few knew that the dark forest also extends to Ethereum uncles. Two enterprising bots have been monitoring uncles for vulnerable transactions that they could exploit, and several Flashbots searchers have had value extracted from falling into this trap. Again, read this thread for another fascinating look into bots and the everchanging landscape in which they operate.

Miraculous Deployment and Mining For Fossils

A new searcher deployed a contract without having any ETH because they were able to extract value in the next transaction and pay for their contract deployment with that extracted value. What's more this searcher finds and executes on arbitrage opportunities on EtherDelta, a DEX that was started in 2016, which makes it a veritable fossil in the fast moving DeFi space.

Flashbots Research

MEV After The Merge (https://youtu.be/Hjd9WowOa3g)

Flashbots and Nethermind presented at the ETHGlobal Scaling ETH conference on MEV After The Merge. They covered what MEV is, how MEV could exist after The Merge, how MEV would impact validator rewards, and how an MEV solution like Flashbots may be implemented in ETH2.

ETHGlobal MEV on ETH2 Hackathon Submission with Lido and Nethermind

Team members from Flashbots, Nethermind, and Lido worked together on an implementation of how a Flashbots-like MEV solution could be implemented in ETH2. The implementation is a combined ETH1+ETH2 client running on the Rayonism testnet that used tips from Ethereum users to prioritize transactions in ETH1 blocks, have the ETH1 block validated on the beacon chain, and share the tip among the various parties involved (ETH1 client, validator pool, and the validator).

Scaling ETH Roast

This month's Roast revolved around the scaling of Ethereum, and the shape MEV will take in the rapidly coming future. Justin Drake was the Roast Master on this occasion, and he did an awesome job asking all the tough questions, and guiding us through MEV in Ethereum 2 and L2s, with presentations by Phil Daian, Alex Obadia, Eli Ben-Sasson from Starkware, Karl Floersch from Optimism, Georgios Konstantopoulos from Paradigm, and panels with Vitalik, Phil, Georgios, Barry Whitehat, Stani Kulechov, and David Goldberg. The Roast recording can be found here: https://youtu.be/krlAqKsdLkw.

Research Collaborations

We issued a new Flashbots research grant to Hashcloak for work on cryptography-based solutions for auction privacy. Flashbots Alpha does not guarantee privacy for searchers, and while we are working on an SGX approach to the problem, we are looking into alternatives that do not require trusted hardware. A working document for Hashcloak's work on Order-Revealing Encryption for providing mempool privacy can be found here. This effort is part of our larger approach to the problem of defining and implementing a good auction mechanism for MEV extraction. This problem has many facets, including defining what "good" means considering the different actors involved. We welcome new contributors, you can find more about our research lines and our grants process in our github research repository.

Flashbots Community

Tornado Cash

Tornado Cash built a privacy preserving relay that uses Flashbots to allow users to withdraw their ETH without depending on a third party to pay transaction fees. Check it out here.

Bundle Explorer

A community member built a simple explorer to examine blocks with Flashbots bundles included in them and display some information about those bundles. You can see it here.

Pendle uses Flashbots for fairer launches

Many new projects finds that their token sales are sniped by bots that monitor pending transactions and buy immediately after new tokens have been listed. Pendle used Flashbots to avoid public mempools and add liquidity to their pool several times without bots being able to snipe it. As a result more users were able to buy in at much better prices overall, and the Pendle team was satisfied with their outcome.

About Flashbots

Flashbots is a research and development organization formed to mitigate the negative externalities and existential risks posed by miner-extractable value (MEV) to smart-contract blockchains, starting with ethereum.

We are not your typical startup, we are fully remote and our principles are based on that of a pirate hacker collective. We are actively recruiting talented, self-directed individuals to join our crew. You can find out more about us and our open positions on our Github.