Project name

: Front-running protection via shielded mempool for OP Stack using threshold encryption (Stage 1: feasibility study)

Author name and contact info

(please provide a reliable point of contact for the project):

Shutter's Website & Shutter's Twitter

I understand that I will be required to provide additional KYC information to the Optimism Foundation to receive this grant

: Yes

I understand that I will be expected to following the public grant reporting requirements outlinedhere

: Yes

L2 recipient address

: 0xB476Ee7D610DAe7B23B671EBC7Bd6112E9772969

Which Voting Cycle are you applying for?

: 10

Which sub-committee should review your proposal? (Builders Grants, Growth Experiment Grants)

: Builders Grants

Project description

(please explain how your project works):

TL;DR:

The overarching goal of this grant is to propose to Optimism DAO to evaluate (and at a later stage implement) how to implement front-running and censorship protection via a shielded/encrypted mempool by threshold encrypting transactions until they're signed by the sequencer.

The problem we're aiming to solve:

Front-running and censorship are huge threats to the base layer neutrality of Ethereum and the L2 ecosystems. One specific problem this creates is that especially larger crypto investors, who are aware of front-running, are keeping billions of dollars side-lined from DeFi because they know that they'll get front-run.

Solution:

We propose to add a shielded mempool using threshold encryption to the OP Stack. One way to achieve this would be an implementation of the threshold encryption DKG as implemented by Shutter Network for Optimism, adding another module and more optionality for beneficiaries of the OP stack.

Benefits for builders on top of OP stack and their end users:

With a shielded mempool, we're expecting the following benefits, especially for DEXs and DEFI protocols and their end users of Optimism based rollups: a higher degree of base layer neutrality leading to a) better and fairer prices on DEXs and DeFi protocols on Optimism due to front-running protection and b) an additional censorship resistance layer.

For sequencers in the OP stack ecosystem, the added neutrality should result in better plausible deniability against anyone arguing that the sequencer role isn't neutral, i.e., end users or even regulators.

On Shutter Network:

Shutter Network is an open-source project that aims to prevent front-running on Ethereum L1/L2 by using a threshold cryptography-based distributed key generation (DKG) protocol.

Our primary instantiation of this protocol is what we call Rolling Shutter, which is a plug-in for L2s to protect their entire rollup from front-running/malicious MEV, as well as improve censorship characteristics. Rolling Shutter generally prevents the parts of MEV which are considered malicious (front-running, sandwich attacks) while leaving the distribution of the benign types of MEV (arbitrage, liquidations) to the chosen MEV distribution mechanism (most likely Optimism MEVA in this case). Rolling Shutter (as a plug-in) is essentially finished and ready for rollups to integrate.

Additional sequencer decentralization path:

Besides MEV, a secondary goal of the grant is to evaluate an additional sequencer decentralization path for Optimism.

The main goal of decentralization is censorship resistance. Because shutterizing increases censorship resistance, there might be an argument to be made that with Rolling Shutter, rollups won't have to decentralize the sequencer (as much), which could result in latency and overall system cost improvements.

Grant Structure

We would like to propose two stages of this grant, beginning with a short and cost-effective research/evaluation stage. After each stage, Optimism DAO and the proposer team can refine and choose whether and how to proceed with the actual implementation of Shutter.

We're not planning on selling OP tokens any time soon but rather see this grant as the first step towards mutual alignment between the OP and Shutter communities.

Rolling Shutter will always be optional to use, i.e., there always be the fallback of an unencrypted transaction path.

If implemented by a rollup using the OP stack, the Shutter keypers will act as the threshold encryption key generators, which ultimately enables the front-running protection. For this, they most likely would want to charge a small fee in ETH. The keypers will be governed by the (to be formed) Shutter DAO.

More info: Rolling Shutter: MEV protection built into Layer 2

Website

: https://shutter.network/

Twitter

: https://twitter.com/project_shutter

Discord/Discourse/Community:

Telegram: Join Group Chat

Other relevant links

(including any demos): Shutter Network · GitHub , https://blog.shutter.network

Additional team member info

(please link):

jannikluhn · GitHub

schmir-at-bb (Ralf Schmitt) · GitHub

pepae (Luis) · GitHub

ulope (Ulrich Petri) · GitHub

cducrest · GitHub

ezdac (Max Langenfeld) · GitHub

Smokyish (Tatu) · GitHub

jakubalsoori · GitHub

Please link to any previous projects the team has meaningfully contributed to

: https://beamerbridge.com/ , https://trustlines.network/ , https://raiden.network/ , https://dump.today/

Relevant usage metrics

(TVL, transactions, volume, unique addresses, etc. Optimism metrics preferred; please link to public sources such as Dune Analytics, etc.): Prevented # of front-running/sandwich attacks

Competitors, peers, or similar projects

(please link): https://twitter.com/koeppelmann/status/1559146241325514754

Creating a Highly Scalable and MEV-Resistant DeFi Ecosystem Using Arbitrum and Fair Sequencing Services, Optimism -

MEV Wiki

Is/will this project be open sourced?:

Yes

Optimism native?

: No

Date of deployment/expected deployment on Optimism

: 8/1/2023

What is the problem statement this proposal hopes to solve for the Optimism ecosystem?:

Maximally Extractable Value or MEV is the revenue the block producer (e.g., validator, miner, sequencer) can extract via front running, injecting, reordering, or censoring transactions. Malicious MEV and front-running are recognized to be among the final unsolved fundamental issues in the blockchain space. Almost all of us active Ethereum users have been victimized at least once by a malicious MEV extraction like front-running or sandwich attacks without even being aware of that. Front-running results not only in loss of funds but can also cause damage to the network by delaying transaction times and raising gas fees.

Censorship is the other issue we're tackling with this: even with the fallback of being able to post transactions on L1, due to the delay of doing so, the current iterations of rollups aren't real-time censorship resistant.

How does your proposal offer a value proposition solving the above problem?

:

Rolling Shutter is an innovative MEV protection project that uses an implementation of the DKG protocol directly in L2/rollups to protect all dapps deployed on the rollup and users' transactions. The result is that all dapps and DeFi protocols deployed on the given rollup are protected from malicious MEV by default and - crucially - remain fully composable within that rollup. As an added benefit, having the block producer sign encrypted orders will also increase censorship resistance, reducing the downsides of more centralized rollup operator setups even further.

This shouldn't affect the benign types of MEV, such as arbitrage, liquidations, or back-running. For this, Rolling Shutter plugs neatly into auction-based systems such as Optimism's MEVAs.

More generally speaking, we love the modularity prospects that the OP stack offers. We think that this vision has the potential to grow the size of the L2 market and especially the amount of diversity of different rollup implementations. In that context, we're excited about Shutter potentially adding to that stack and increasing diversity and the market size for L2.

Why will this solution be a source of growth for the Optimism ecosystem?

:

We think this proposal has the potential to contribute to builders wanting to build on top of the OP stack along three axes:

1. Mainstream is fed up with crypto because they feel left out. They perceive the crypto ecosystem to be intransparent and unfair. The fact that unsophisticated users are getting front-run consistently doesn't help at all. The number of profits extracted due to front-running is most probably already over $1bn on Ethereum alone.
2. More sophisticated and larger users know that they are getting front-run, so a larger number of them don't even interact with DeFi at all.
3. In this regard, we believe front-running resistance to be one of the key enablers for true mainstream adoption.
4. We think the added censorship resistance in the form of additional plausible deniability arguments for the sequencer (from a regulatory perspective) could be a strong selling point and could help present Optimism as a truly robust, censorship-resistant infrastructure.
5. More generally, adding to Optimism having a more complete MEV strategy should establish Optimism as an even stronger player in the MEV space.

Has your project previously applied for an OP grant?

: No

Number of OP tokens requested

: 30000

Did the project apply for or receive OP tokens through the Foundation Partner Fund?

: No

If OP tokens were requested from the Foundation Partner Fund, what was the amount?

: -

How much will your project match in co-incentives?

(not required but recommended, when applicable): -

How will the OP tokens be distributed?

(please include % allocated to different initiatives such as user rewards/marketing/liquidity mining. Please also include a justification as to why each of these initiatives align with the problem statement this proposal is solving.):

Proposal for token distribution:

We would like to propose two stages of this grant, beginning with a short and cost-effective research/evaluation stage. After each stage, Optimism DAO and the proposer team can refine and choose whether and how to proceed with the actual implementation of Shutter.

Stage 1 - Feasibility Study (this proposal)

Deliverables:

1. Creation of requirements for front-running mitigation in Optimism rollup.(Critical)

2. Basic economic analysis and IT viability of Shutter <> Optimism rollup. An example of this would be to estimate the trade-off between a fee for the front-running protection vs. the avoidance of loss due to front-running for a typical user. (Critical)

3. Creation of architecture diagram of Shutter + Optimism rollup.(Critical)

4. Creation of blog post including deliverables above + showcase of Shutter with mock rollup sequencer.(Critical)

5. Preparing a decision-making document with the trade-offs of implementing Shutter, which provides options for MEV mitigation in the later stages.(Critical)

Stage 2 - Mainnet release & implementation (potential follow-up proposal)

Over what period of time will the tokens be distributed for each initiative?

Shorter timelines are preferable to longer timelines. Shorter timelines (on the order of weeks) allow teams to quickly demonstrate achievement of milestones, better facilitating additional grants via subsequent proposals:

For the feasibility study stage, the estimated time to complete the phase is 6 FTE weeks across two months.

We’re open to any kind of vesting or milestone schedule in order to ensure more long-term alignment.

Please clearly define the milestones you expect to achieve in order to receive milestone based installments. Please consider how each milestone relates to incentivizing sustainable usage and liquidity on Optimism. Progress towards each milestone must be trackable:

Within this stage 1, we originally didn’t intend to introduce milestones, however we’re open to do so if that’s desired.

Why will incentivized users and liquidity on Optimism remain after incentives dry up?

:

Benefits to Optimism users are via less loss due to front-running and better censorship resistance. Those benefits aren’t connected to short term liquidity incentives but will make Optimism a better marketplace overall long term.

Please provide any additional information that will facilitate accountability

(smart contracts addresses relevant to the proposal, relevant organizational wallet addresses, etc.): Shutter for MEV protection:

Shutter Network · GitHub

Rolling Shutter: MEV protection built into Layer 2

Shutterized Beacon Chain - Execution Layer Research - Ethereum Research

Shutter Governance (live implemented as shielded voting in Snapshot):

https://twitter.com/SnapshotLabs/status/1580674555710181378

Shutter brings shielded voting to Snapshot

Talks:

MEV day in Amsterdam: Protection built into L2 using threshold encryption by Jannik Luhn at MEV-Day - YouTube

Devcon 6: https://archive.devcon.org/archive/watch/6/shielded-voting-using-threshold-encryption/?tab=YouTube

Dappcon: #DappCon22 : Day 2 - How dApps Can Be Protected From Front-Running, Luis Bezzenberger - YouTube

Twitter space with Snapshot and Gnosis Safe: https://twitter.com/safe/status/1600856115650199556

Interview with blockchain socialist: MEV: existential threat to blockchains or solvable problem? - The Blockchain Socialist

Confirm you have read and agree to the Eligibility Restrictions

(here): I have read the Eligibility Restrictions and agree to abide by their conditions