Project Name:

Kevlar

Author name and contact info

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

Shresth Agrawal (shresthagrawal.31@gmail.com)

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

Yes

L2 recipient address:

TBD

Which Voting Cycle are you applying for?

: TBD

Grant category:

Tooling

Project description

(please explain how your project works):

Most people interact with Ethereum, EVM-based chains, or rollups like Optimism using RPC-based wallets, such as MetaMask. These wallets entrust centralized infrastructure providers, like Infura, Alchemy, or Optimism Foundation, to run the consensus client logic on their behalf and respond to their RPC queries correctly. This centralization leads to risks for users since a malicious RPC provider can mislead the wallet with fake payments and balances. Furthermore, it is increasingly being recognized that centralization also poses undesired liability for central providers. Thus, both users and providers are better off decentralizing. But so far technical roadblocks remained. We recently released the first usable light client construction for PoS Ethereum, Kevlar. Kevlar is an easy-to-use tool that first syncs with the chain using an efficient light client construction and starts a local RPC proxy server that you can add to your RPC-based wallet, like MetaMask, turning it completely trustless without affecting user experience. Kevlar uses an Optimistic Light client construction which can sync 10x faster and with 180x lower bandwidth requirements than the traditional light client construction. This construction was proposed in our recent academic paper “Proofs of Proof-of-Stake with Sublinear Complexity”.

Currently, there doesn’t exist any light client construction for rollups themselves. We believe that we can combine our work from the academic papers we wrote, “Proofs of Proof-of-Stake with Sublinear Complexity” and “Light Clients for Lazy Blockchains”, to come up with a superlight client for rollups. Through this grant, we will fund the research accompanied by a proof of concept implementation for the first superlight client for Optimism.

Kevlar, our first proof-of-concept of a superlight client, currently works for PoS Ethereum. With this grant, we will extend Kevlar to work with Optimism.

Project links:

Website: https://kevlar.sh/

Discord/Discourse/Community: Kevlar

Paper:

1. Proofs of Proof-of-Stake with Sublinear Complexity (PDF: https://arxiv.org/pdf/2209.08673.pdf, Code/Benchmarks: GitHub - lightclients/poc-superlight-client: POC construction of superlight client for Ethereum Proof of Stake using interactive bisection games)
2. Light Clients for Lazy Blockchains (PDF: [2203.15968] Light Clients for Lazy Blockchains)

GitHub:

1. Kevlar (GitHub - lightclients/kevlar: Light client-based RPC Proxy for PoS Ethereum)

Relevant Tweet Threads

twitter.com

**Shresth Agrawal**

@shresth3103

Today, we are announcing "Kevlar" (github.com/shresthagrawal…), a tool that makes Metamask, or any RPC-based wallet, completely trustless! Kevlar first runs a light client to quickly sync with the beacon chain and then starts a local RPC proxy that you can add to your wallet

1:41 AM - 14 Oct 2022 740

150

twitter.com

**Shresth Agrawal**

@shresth3103

After releasing Kevlar, we received several questions regarding the inner workings of the RPC proxy. Kevlar is made up of two main components: the sync client, and the RPC proxy. The RPC Proxy is implemented as a separate library, “Patronum” (github.com/shresthagrawal…)

7:45 PM - 15 Oct 2022 26

4

twitter.com

**Dionysis Zindros**

@dionyziz

Today, I am happy to announce our latest work, "Proofs of Proof-of-Stake with Sublinear Complexity", in collaboration with @shresth3103 @jneu_net @ErtemTas which we just uploaded to arXiv:arxiv.org/pdf/2209.08673… This is the first superlight client for proof-of-stake. 1/

3:40 AM - 20 Sep 2022 320

74

Additional team member info

(please link):

- Dionysis Zindros (Stanford)

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

Dionysis

has a long list of influential peer-reviewed academic publications in the blockchain field (SeeDionysis’ Scholar). Examples of such papers include “Proof-of-stake sidechains”, and “Non-Interactive Proofs of Proof-of-Work”. Dionysis is one of the four co-founders of OpenBazaar.

Shresth

has been working as a blockchain and smart contract developer for the past five years. He has contributed to various projects such as ParaSwap, dOrg, Gelato, Libp2p, HOPR, etc.

Relevant usage metrics

(TVL, transactions, volume, unique addresses, etc. Optimism metrics preferred; please link to public sources such as Dune Analytics, etc.):

It is hard to present any metrics for the research itself but here are some metrics regarding Kevlar:

- Currently, over 500 users have already downloaded Kevlar. This can be seen in the weekly downloads of the npmjs page @lightclients/kevlar - npm
- 187 stars on the relevant GitHub
- Currently Kevlar is in the process of getting integrated into MetaMask Kevlar by kumavis · Pull Request #16384 · MetaMask/metamask-extension · GitHub)

The above metrics are for the PoS Ethereum Kevlar. We will work on the Optimism version of Kevlar when this grant is disbursed.

Competitors, peers, or similar projects

(please link):

There are currently no light clients for rollup chains.

Is/will this project be open-sourced?

Yes

Optimism native?:

Partially, Optimism will be the first rollup chain to have a light (and superlight) client construction.

Date of deployment/expected deployment on Optimism:

TBD

Ecosystem Value Proposition:

Optimism Foundation currently runs the main public RPC server used by most users. The other alternative suggested in the documentation is 3rd party provider Alchemy (Networks, Public RPC Endpoints, & APIs | Optimism Docs). This creates a huge centralization risk for the Optimism network. For example, it enables a compromised server to conduct double spending against the users.

The proposal aims to build the foundations required to add support for light and even superlight clients for Optimism. If we are successful then our proposed construction can be immediately productionized which will allow Optimism users to run efficient light clients on their system locally and become trustless.

Optimism will be the first rollup chain to support light clients. The community will enthusiastically receive this, as it reaffirms Optimism's commitment towards decentralization and user safety. Illustrating that Optimism supports and values decentralization will further drive up its adoption by users who are currently reluctant to adopt it, leading to the long-term growth of the ecosystem.

Number of OP tokens requested:

150,000 OP

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?:

NA

How much will your project match in co-incentives?

(not required but recommended, when applicable):

NA

Proposal for token distribution:

We plan to use 100,000 OP to compensate the scientists and engineers working on the research and the development of the Proof of concept Optimism superlight client over a period of 4 months. Kevlar is a completely open-sourced, community-owned project and the only way to support it is through grants. Therefore we will use rest 50,000 OP to retroactively fund the existing work and future research and development of Kevlar.

Here are some concrete tasks:

- Theoretical construction

. We will write out, in the form of a paper, the superlight client construction for Optimism rollup, following our previous scientific work on PoS superlight clients and lazy light clients.

- Build a PoC for Optimism light client

. We will create a prototype implementation of the first Optimism light client, making use of our theory from the previous bullet point.

- Benchmark the construction

. We will run simulations to measure and compare the performance of our new construction as compared to Optimism full nodes that require synchronizing with the whole chain. The motivation for these benchmarks is to determine whether it is feasible to embed the trustless light client within a browser-based or mobile wallet such as MetaMask, making it completely trustless.

- Documentation

. Document the API endpoints and the process required to participate in the prover network. Provide documentation for developers who want to extend their Optimism full nodes to add support for serving light and superlight clients.

- Infrastructure

. Deploy 4 sample provers that can participate in the prover network to enable light and superlight clients for Optimism for a period of the next six months.

This grant doesn’t claim to create a production-ready implementation for the Optimism lightclient. The aim of the grant is to propose the theoretical construction, build a proof of concept, benchmark the feasibility, and lay out the groundwork required for light client support in Optimism. A subsequent grant proposal could be made after the successful execution of this grant to further productionize the light client support.

Please provide any additional information that will facilitate accountability:

(smart contracts addresses relevant to the proposal, relevant organizational wallet addresses, etc.) NA