Basic Details

Project name:

dm3 protocol

Author name and forum name (please provide a reliable point of contact for the project):

Eduardo (TG @Vegayp)

L2 recipient address:

0x11Ee133A1408FE2d7c62296D7eB33F234b774503

Which Voting Cycle are you applying for?:

Cycle 11

I confirm that I have read the landing pages for theBuilders 13 and Growth Experiments 15 Sub-Committees and that I have determined my proposal is best suited to be reviewed by the Builders Sub-Committee:

Yes.

Project Details

What are you going to build?

:

The dm3 protocol is a lightweight messaging protocol based on web3 technology, with a focus on secure end-2-end encryption, decentralization, scalability, and interoperability. The core of the protocol is a registry (dm3-registry) for the relevant communication information such as public keys for encryption and signatures and delivery information. Messages are delivered via a decentralized network of delivery service nodes that serve as a message cache or gateway to another messaging protocol or service.

The dm3 registry is based on ENS, i.e. the dm3 profile is added as a text record to the ENS name.

Storing data on Ethereum Mainnet is expensive hence it is appealing to use other storage solutions that offer more compelling rates. To facilitate this ERC-3668: CCIP Read: Secure offchain data retrieval introduces CCIP, a standard that can be used to securely retrieve off-chain data. While the solution is focussed on ENS, the methodology can be adapted to any other data from Optimism.

Optimism-Resolver is an CCIP Resolver that retrieves data from optimism and validates the integrity of this data in a trustles manner using merkle proofs.

The dm3 protocol can be utilized to make existing protocols and services interoperable, i.e. users of one ecosystem can easily send messages to users of another ecosystem. Messaging components based on dm3 (dm3 embedded) can be used by any dApp to integrate messaging functionality (e.g. for in-app messaging or support messaging).

With the available Optimism Resolver, applications can now implement the registry for their users in Optimism for an effective and cost-efficient way. The dm3 reference implementation uses Optimism-based profiles for dm3 users (ENS subdomains) that do not have their own ENS name.

Why is what you are going to build going to succeed?:

1. We are building a Public Good, we don’t have any competitor, because as a Public good our intention is to implement our protocol to benefit the Optimism, the web3 messaging, and web3 ecosystem.
2. We are building alongside the ENS community: a cohort of value driven developers, community members and enthusiasts.
3. Managing ENS records is very expensive in mainnet, our solution brings a mass adoption case to ENS and optimism. The provided Optimism Resolver works trustlessly and can be used for any ENS application. The mechanism can be applied to any other information which must be verifiable on mainnet.
4. We provide a standardized protocol for message exchange to web3 that enables interoperability for messaging in the Ethereum Ecosystem (inkl. L2s), other EVM-based chains, Non-EVM chains, as well as centralized services (like web2 messengers).
5. The dm3 protocol enables interoperability without the need to change existing protocols and services significantly, without compromising security and privacy. This makes it easy to make protocols and services dm3 compatible. Existing dApps can use dm3 embedded components to integrate secure messaging with only 2 lines of code.

Is your project likely to bring new builders to the Optimism ecosystem? If so, please describe how:

Yes, by providing these components be labelled as a public good and open source:

1. OptimisimProofVerifier [L1]: Contract on Ethereum Mainnet that can validate whether a sequence of data is stored on a certain optimism contract.
2. OptimismResolver [L1]: Contract on Ethereum Mainnet that implements theENSIP-10: Wildcard Resolution - ENS Documentation Flow
3. PublicL2Resolver [OP]: A fork of the ens Public Resolver Contract on Layer2
4. Proof-Provider Backend [Centralized]: Calculates the actual Proofs to each data read from optimism. The current implementation utilizes a centralized service for the proof generation. Nevertheless, provided proofs are trustless as the validity of the data is proven by merkle proofs. To eliminate the possible single point of failure of this service, a fully decentralised solution is in development.

This will allow developers, apps, and non-messaging projects to use the resolver for any ENS based applications, adapt the methodology to any other data verification problem, and to utilize the dm3 protocol to include messaging features.

The dm3 protocol aims to enable interoperability between messaging applications. Different ecosystems, protocols, and services can use the common ENS-based registry (dm3 registry) to publish communication parameters. Depending on the application, there is a need to create and manage dm3 profiles (and thus ENS names or subnames). With the possibility to do this on Optimism effectively and cheaply, Optimism is promoted as a platform for this information.

Is your project likely to improve the quality of developers in the Optimism ecosystem? If so, please describe how:

Yes, by allowing developers to build not only focusing on one chain, or one app, but with the interoperable factor embedded in their code.

Also, adding secure messaging functionalities to apps valorizes those apps by adding user friendly UX, even more, if this is interoperable with other messaging apps from the very beginning.

As shown in the milestones, we provide with the OptimismResolver a library which can be used by any other ENS bases application to build Layer-2 storage for ENS content. Also, we will integrate this in our reference implementation of dm3 allowing users to manage their profiles on Optimism. As this is a reference implementation, other projects implementing the dm3 protocol are invited to copy this approach

Is your project likely to improve the commitment of developers in the Optimism ecosystem? If so, please describe how:

We will provide a constant stream of updates to the protocol, as well as audits, and a community built code, so we are certain that many apps and protocols will remain on the optimism ecosystem to not only implement new updates to the original code that we provided, but also with the approach of building in consensus for the benefit of the ecosystem and therefore, their own protocols.

Provide us with links to any of the following for the project:

- Website: https://dm3.network/
- Specification: https://dm3.readthedocs.io
- Twitter: https://twitter.com/dm3protocol
- Discord/Discourse/Community: Common Ground
- Github: GitHub - corpus-io/Optimism-Resolver, https://github.com/corpus-io/dm3 GitHub - corpus-io/dm3-spec: White paper, protocol spec, ...

Do you have any metrics on the project currently? (TVL, transactions, volume, unique addresses, etc. Optimism metrics preferred; please link to public sources such as Dune Analytics, etc.):

The dm3 twitter account (@dm3protocol

) has 682 followers.

The dm3 protocol has already been presented at several conferences (e.g. at Devcon 6 in Bogota dm3 - Decentralized Secure and Open Messaging Protocol - YouTube), is intensively discussed in the ENS community (Standardization web3 messaging - Standards - ENS DAO Governance Forum, Dm3 - decentralized messaging for web3 - Integrations - ENS DAO Governance Forum) and received a small ENS public goods grant (ENS Small Grants). Dm3 was also discussed in several twitter spaces for example ENS Town Hall | Q4 2022 - YouTube

The dm3 protocol coordinated with different web3 messaging providers, the first implementations into other protocols will be

started in March.

The optimism resolver has just been finished, respectively some further developments are still in progress. Since the security audits have not yet been performed, these components are not yet in practical use. The deployment is also very closely coordinated with ENS developers.

Who are your competitors?:

There are several web2 and web3 messaging protocols, services, and apps. Actually, almost all of those applications are separated into siloed ecosystems with no interoperability. The dm3 protocol is the first protocol approach with special focus on interoperability, based on web3 technology. As the goal of dm3 is interoperability, other protocols, services, and apps are not considered as competitors but as cooperation partners to accomplish a interoperable messaging landscape.

For the Optimism Resolver other signer based implementations are known. Our implementation based on trustless proofs can be adapted and used for the ENS use-case or others.

What differentiates you from your competitors?:

Our implementation of the Optimism Resolver is open source and a public goods approach. Based on Merkle proofs for all involved storage slots, it works completely trustless.

The dm3 protocol is focused on the minimal needed architecture to establish secure (encrypted) and private communication. Also, scalability and decentralization are essential features of the protocol.

What makes the dm3 protocol particularly distinctive compared to other messaging protocols is that it does not aim to replace other solutions, but rather to combine a variety of different solutions that are especially adapted to their user requirements without compromising security and confidentiality.

Will your project be composable with other projects on Optimism? If so, please explain:

Yes, by design the dm3 protocol aims to be composable with:

1. Optimism ecosystem protocols and apps that aims for messaging interoperability
2. Mainnet and optimisms apps that make use of ENS.
3. Adaption of the Optimism Resolver approach for other use-cases where data verifiability is needed
4. Usage of embedded messaging components

Team

Who are your founders?:

The dm3 protocol was developed as one of the products of the web3 product studihttps://corpus.ventures/. Corpus was founded by Christoph Jentzsch, Dr. Johannes Pfeffer, Steffen Kux, and Jork Leonhardt. The dm3 project (currently in the spin-off phase with the aim of managing Public Good as a non-profit association. The foundation of a DAO is planned.) is managed by Steffen Kux and Heiko Burkhardt as technical lead.

What makes your founders well-positioned to accomplish your goals with this project (1-2 sentences on each)?:

We (corpus.ventures) build web3 products. Our roots go back to the birth of Ethereum, hardened by the experience of TheDAO, slock.it, aleth.io, atpar.io and many more projects. Strongly driven by Ethereum's values such as openness, interoperability, censorship resistance and decentralisation.

We are a German GmbH based in Bahnhofstr. 32, 09648 Mittweida, Germany. Corpus as a product studio is developing dm3 with the intention to spin it off into a non-profit organisation with the core values mentioned above to create a robust protocol.

Tell us about the rest of your team (if there are more teammates):

Steffen Kux (CEO) previously in slock.it

Heiko Burkhardt (CTO)

Eduardo Vega-Patiño (Community Lead) previously in: TEC Commons, ENS, Akasha Barcelona.

Mayra Castillo (Community manager)

Alex Plutta (Software Engineer)

Is this your first Web3 project?:

No

If not, what else have you built? (Share links, Github repository, or any other useful information.):

1. https://gashawk.io/
2. https://tokenize.it

I understand that Builders grants are subject to a 1 year lock-up, as explained further inthis post 2: [Yes/No]:

Yes

Is your project funded? If so, provide an estimate of how many months of funding runway your project has:

The project is currently sponsored by corpus.ventures. We have invested an approximate of 400k since the first line of code back in February of 2022.

We currently have funds to run for at least 3 months, and we are actively seeking public goods funding to help increase our team and the sustainability of the protocol in the long term.

Grant Request

What is the size of the grant request? (50k OP max):

50k

How do you justify the size of the grant?:

The funds will be used for the following:

1. Finalize and prepare Optimism Resolver contracts for an (external) audit.

Estimation: 17k€

(finalize development, tests, documentation, internal security audit), the costs for the external audit are NOT included! It is estimated to appr. 35k€-70k€!

)

1. Support audit and post-audit follow-up.

Estimation: 10k€

(work with auditors, implementation suggestions, solve all problems)

1. Investigate and explore approaches to decentralize proof creation.

Estimation: 28k€

(evaluation of appropriate approaches, implementation PoC, testing, internal security audit, opt. external software audit), the costs for the external audit are NOT included! It is estimated to appr. 15k€!

1. Implement and finalize L2-Management of dm3 profiles (on Optimism)

Estimation: 18k€

(integration of OptimismResolver into dm3-user management, implement UX for reference implementation, implement dm3 library (and API) to use optimism integration also for other registries, …)

1. Develop generalized ENS resolver for ENS

Estimation: 13k€

(add proof generation for general ENS information, implement/extend backend components and decentralized (building on 3)

1. Incentivize the implementation of the dm3 protocol into the Optimism Ecosystem.

Estimation: 18k€

(supporting integration, further implementation of dm3 embedded components, creation of examples and reference material, …)

Roadmap

Describe in discrete steps your plan for accomplishing your project:

1. Launch of the optimism resolver.
2. Implementation of the optimism resolver on ENS
3. Preparation of the smart contracts for the audit
4. Support audit
5. Launch of the interoperability initiative.
6. Integration with other messaging protocols (plan 3).
7. Launch of educational season about Public Goods and interoperability.
8. Support of integration of messaging functionality into optimism based applications.

Note: We support integration of messaging functionality by providing the packages (npm), well documented examples and reference implementations. Also, we provice direct development support while integrating dm3 embedded components or developing dm3 compatibility functions. Incentivation by monetary payments will not be done.

Please provide any additional information that will facilitate accountability: (smart contracts addresses relevant to the proposal, relevant organizational wallet addresses, etc.)

The current version of the L2 contracts (see Optimism-Resolver/contracts/l2 at main · corpus-io/Optimism-Resolver · GitHub) are deployed at 0xb20Eb9648b4a818AA621053f1AA1103C03f2dF57 (see also Contract Address 0xb20eb9648b4a818aa621053f1aa1103c03f2df57 | Optimism).

The L1 contracts (see https://github.com/corpus-io/Optimism-Resolver/tree/main/contracts/l1) are not yet deployed on mainnet (as audit is not yet finished).

Does your plan depend on the receipt of OP tokens?:

No. But it would help us on the objective to become a non-profit organisation building a Public Good. This 50k not only will help us positioning on the optimism ecosystem, but also economically will boost outreach and developing teams.

What is your plan for the use of the OP token after the 1 year lock-up?:

The token will be used to support further development of the dm3 protocol and L2 (Optimism) integration of dm3 profiles, support interoperability activities (integration of dm3 embedded components, implementation of dm3 compatibility) and community integration.

Please provide benchmark milestones for this project. These milestones should guide the Optimism community on the progress of your project during the 1-year lock-up period.

1. Optimism Resolver

1.1 Finalization of the Optimism Resolver (OPR)

The library will be available at Github. The OPR consists of resolver smart contract on L1 (CCIP for reading off-chain/L2 data with proof and verification), the L2 resolver smart contract (to store the information in L2) and the proof provider service (backend to generate the trustless proof).

1.1.1 Release of version 1.0 in Github until July 31, 2023. 1.1.2 Audit of the smart contracts until September 30, 2023.

1.2 Integration with ENS on L2 (Optimism)

Integration of the OPR as a fully supported storage method for ENS subdomains. It will be used as dm3 storage for dm3-usernames and for other ENS applications (fully compatible and usable in the ENS app).

1.2.1 PoC of dm3-usernames on OP until June 30, 2023 1.2.2 Release of ENS integration for general use until September 30, 2023 (after audit and deployment of the smart contracts).

1. dm3 Protocol

2.1 Finalize specification and implementation of interoperability to other messaging protocols and/or services

The dm3 protocol specification defines the interoperability layer. Based on the specification, the reference implementation of the base protocol and all protocol extensions are provided. As part of the interoperability initiative, other protocols/services are extended to become dm3 compatible by providing the essential interfaces (adding their registry to ENS, containing the dm3 profiles) and providing delivery service nodes as gateway to their network. For the delivery service nodes, configuration tools are provided

2.1.1 Release of the specification (base protocol DM3MTP) - finished 2.1.2 Release of the specification of protocol extensions: Storage spec (until April 15, 2023), Message access (until April 30, 2023), Key derivation (until May, 30 2023), Layer 2 Registry (until June 15, 2023), Privacy Onion routing (until August, 31, 2023), Group Messages (until October, 31, 2023). 2.1.3 Release of the reference implementation for each specification (1 month after spec release). 2.1.4 Release of delivery service configurator (command line, web app) until May 31, 2023 2.1.5 Release of delivery service docker images until July 31, 2023.

Integration into 3 protocols/service finished (cooperation!) until June 30, 2023

2.1.6. Integration into 6 protocols/service finished (cooperation!) until December 31, 2023

2.1.7. Start standardization process (OASIS) until January 31, 2024

2.2 Finalize embedded components to integrate in dApps (in particular in Optimism based applications)

Embedded components as easy to use components to integrate into dApps are provided as GitHub repo and npm packages. An extension to integrate dm3 embedded as a support channel with accompanying tools is developed.

2.2.1. Release of version 1 on GitHub until April 30, 2023 2.2.2. Release of npm packages until May 31, 2023 2.2.3. Specification of embedded support framework until December 31, 2023 2.2.4. Release of embedded support framework until February 28, 2024 2.2.5. Integration into 3 dApps supported (technically support only) until July 31, 2023 2.2.6. Integration into 6 dApps supported (technically support only) until December 31, 2023

Please define critical milestones for this project. Critical milestones are meant to show good-faith efforts to accomplish the project. Non-completion of these milestones could lead to revocation of remaining grant rewards.

1. Optimism Resolver

1.1 Finalization of the Optimism Resolver (OPR)

1.1.1 Deployment of the resolver smart contracts on L1 until Otober 15, 2023 1.1.2. Deployment of the resolver smart contracts on L2 until Otober 15, 2023

1. dm3 Protocol

2.1. Finalize specification and implementation of interoperability to other messaging protocols and/or services

2.1.1. Release of the full dm3 specification at https://specification.dm3.network until October 31, 2023. 2.1.2 Release of integration guide for further integrations until October 31, 2023 2.1.3. Release of dm3 reference implementation with L2 storage until November 30, 2023

2.2 Finalize embedded components to integrate in dApps (in particular in Optimism based applications)

2.2.1 Release of repository and npm packages until May 31, 2023

Optimism Relationship

Does your project solve a problem for the Optimism ecosystem?:

1. Currently there is no mainstream reason for a mainnet user to use optimism.
2. Currently there is no utility of ENS in Optimism.
3. Trustless validation of Optimism data on Layer1
4. Adding secure messaging to apps
5. Adding messaging interoperability to web3 (and also web2) protocols and services

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

If an ENS user uses the Optimism Resolver as his default Resolver they can store data such as text records on optimism and benefit from the more appealing transaction costs of the OP ecosystem.

The data stored on optimism can be simply retrieved by a CCIP compliant client like ethers.js by a single line of code.

The dm3 protocol acts as lean base protocol for web3 messaging, allowing other protocols and services to add information to the dm3 registry and using delivery services as gateways to the dm3 messaging ecosystem. Embedded messaging components can be used to add messaging functionalities into any dApp with only 2 lines of code.

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

There are currently around 50k ENS monthly users, with the amounts of registrations of ENS names surpassing 2 millions, with the launch of the name wrapper and the possibilities of the subdomains update, it becomes very clear that all those users could be using optimism to set their records for their ENS names, saving thousands of dollars in gas not only bringing users in a constant stream (the records tend to change along the year) but also in funds, by the use of bridges, exchanges and other apps needed for someone new in the optimism ecosystem. Now if we consider the messaging ecosystem, the exponential growth increases even more. Other messaging solutions or protocols can use dm3 alongside the ENS registry and can now decide to use optimism for their infrastructure.

How committed are you (and your team) to building on Optimism?:

Extremely committed. We believe we have a solution that benefits a wide range of relevant protocols like ENS and brings attention and usage of the Optimism infrastructure. This commitment isn't only about our protocol but also on two ends:

1. Education and visibility about interoperability.
2. Implementation of our protocol as a public good in other apps and layers.

Is your project Optimism Native?:

Yes, on the resolver end, it is exactly tailored for the Optimism ecosystem using the Op Stack. On the messaging side of the protocol: it is completely agnostic but it opens a path for Optimism to be used as a registry point.

Confirmations

I understand that I will be required to provide additional KYC information to the Optimism Foundation to receive this grant: [Yes/No]:

Yes

I understand that I will be expected to following the public grant reporting requirements outlined here: [Yes/No]:

Yes

Thank for reading until this point! We are excited to be able to submit this grant.