[

Metis_banner

1920×845 127 KB

](https://europe1.discourse-cdn.com/business20/uploads/aave/original/2X/0/0b5fdd72e75735a58e7ae0b3352a9d6a85a8c6b7.jpeg)

As we published before, we think the Aave community requires a technical/infrastructural analysis of new network candidates to host the liquidity protocol, from an entity like BGD looking for Aave's interest.

Following the positive sentiment poll on Snapshot, this is an analysis of the Metis Andromeda network.

(A pdf version of this report can be found HERE)

DISCLOSURE.

This is an independent assessment of different technical components that we consider important for the Aave software to run optimally, not a categorical analysis stating the network is "good" or "bad", and no kind of "requirement" for Aave to be deployed on the candidate network. That decision is up to the Aave governance, no matter our opinion.

In addition, currently, we have absolutely no financial/investment/services-engagement/any kind of interest in the Metis ecosystem.

When doing the evaluation, we contacted the Metis team as an important source of information, which has always been exemplary and supportive, but everything in this report comes finally and exclusively from our independent criteria.

Report

1. Introduction to Metis

Metis (Andromeda) is a Layer 2 optimistic rollup, with EVM base compatibility and settling to Ethereum mainnet.

Initially forked from Optimism, Metis has evolved similarly in some core aspects, in parallel with taking a different direction in others, like management of the roll-up storage.

Same as with all other optimistic rollups, Metis is in an early stage, trying to improve its shape and infrastructure, together with addressing mechanics like its decentralization, cost-of-usage, or security.

2. Our methodology

This report is not trying to be a full analysis of the Metis network, but focusing on those aspects that would be important if the Aave community decides to deploy the Aave v3 liquidity protocol there.

In addition to being extensive enough, this report tries to be simple enough for medium participants on the Aave governance to understand. But given its technical nature, it is unavoidable to assume a certain familiarity with the basic concepts touched, like rollups, oracles, RPC nodes, or blockchain explorers, amongst others.

In order to simplify the interpretation of this report, we will evaluate each component important for Aave separately, and assign simplified "grades", defined as follow:

Optimal.

Fulfilling all minimal requirements, and with extra positive aspects.

Good.

Fulfilling the requirements, but improvements can be made.

Acceptable.

Fulfilling the requirements, but with "buts".

Needs improvement.

Mandatory requirements not fulfilled at all. Aave will not work properly

3. Evaluation

3.1. Oracle Infrastructure

The Aave protocol uses 3 types of oracles in an optimistic rollup like Metis. We consider that having Chainlink providing oracles, especially for the most important type (prices), is a must for any deployment, with alternatives only considered really ad-hoc, given the additional complexity added on evaluation/integration.

3.1.1. Price feeds

Used by the Aave protocol to price assets listed.

Metis HAS

Chainlink price feeds available for the major assets on the network

Additionally, there seem to be some other price feed oracles on Metis, but we don't think they should be considered for Aave.

3.1.2. L2 Sequencer Uptime feed

"flag" parameter indicating in real-time to the Aave protocol if a sequencer of a rollup (or any network involving some centralization on sequencing of transactions) is properly running.

Metis HAS

Chainlink L2 Sequencer Uptime, as presented HERE.

3.1.3. Proof-of-Reserve feeds

Component indicating to the Aave protocol if the reserves backing an asset are healthy. This system is not running yet, but the Aave community has approved starting to apply it for bridged assets, so directly related to a case like Metis.

Metis DOESN'T HAVE

Proof-of-Reserve feeds at the moment, but given the existing integrations with Chainlink, it should be a possibility in the future.

3.2. Blockchain explorer

For Aave, same as for any other blockchain project, block explorers like Etherscan are a fundamental component, specifically for the following:

1. Verifiable smart contracts code visualization.
2. Read/write interface with smart contracts.
3. Basic data analysis tool for misc aspects like token holders.

The official blockchain explorer of the Metis network can be found athttps://andromeda-explorer.metis.io/, and it is an instance of the open-source Blockscout.

Etherscan and white-labeled solutions of it are still several steps above other solutions like Blockscout. However, the basic functionalities required for Aave users/developers (read/write smart contracts, possible to verify smart contracts) are supported, so we think it is acceptable, even if adding some extra overhead on the tech integration.

It is important to highlight that we have noticed some problems with data visualization on the explorer, but they should be easily fixable.

3.3. Compatibility with Ethereum RPC standard

Basic compatibility with the Ethereum nodes RPC de-facto standard (eth_, web3_

) is quite an important requirement for Aave or any other protocol, given that it helps to have tools built for Ethereum (or other similar networks) working out-of-the-box just by plugging them to node, of Metis in this case.

Metis HAS

complete compatibility, only lacking certain non-standard specific endpoints (e.g. trace_*).

3.4 Compatibility with Ethereum account format (addresses)

One of the strengths of non-Ethereum networks (e.g. Polygon, Avalanche C-Chain, etc) is its compatibility with Ethereum private/public keys of accounts. This allows existing account holders on those networks to use the others without creating an ad-hoc wallet for it.

Metis is fully compatible with the Ethereum account format.

3.5. RPC public endpoints and providers

Basic and reliable public RPC infrastructure is a must for Aave, as it is the way to connect to the network, both for data reading and transaction submission.

From what we are aware, Metis has 2 types of RPC endpoints:

1. An “official” one provided by the Metis infrastructure team onhttps://andromeda.metis.io/?owner=1088
2. Integration with POKT, with the endpoint onhttps://metis-rpc.gateway.pokt.network

The lack of other providers like Alchemy, Infura, or QuickNode could be problematic, especially because Aave expanding to a network has generally implied growth in usage in orders of magnitude. If finally approved by the community, we will insist with the Metis team that both the infrastructure should be prepared for high-load and that it is quite important to have more providers.

3.6. Custom behavior (lack of) of the execution layer

Whenever a network has custom/extended behavior with respect to Ethereum, it is important to be aware of it and evaluate if it has any impact on the Aave protocol.

Examples of this potential behavior are the presence of new pre-compiles (compared with Ethereum or similar rollups like Optimism), EVM opcodes, native account abstraction/meta-transactions, chainId definition out of the norm, etc.

Independently, even if not doing a full evaluation of the mvm

(Metis Virtual Machine) implementation (it is a relatively daunting task), we have checked the following, given that historically have been critical aspects:

- The chainId

behavior is appropriate, with the id 1088

for Metis Andromeda not clashing with any other.

- The mvm

opcodes on its codebase are the same as the opcodes are same as onOptimism.

- The mvm

pre-compiles on its codebase are the same as the pre-compiles onOptimism.

Additionally, we have a confirmation from the Metis team that there is no custom basic behavior affecting the model of execution on the virtual machine.

3.7. Support of wallet providers

Wallet products like Metamask, Ledger, Coinbase Wallet, and others, are fundamental pieces of the infrastructure for users to access the Aave protocol. So it is a strong requirement for a network to be supported by a subset of them.

Given its EVM compatibility in the context of this document, Metis is transparently supported by the majority of all the chain-agnostic wallets, like Metamask, Ledger, Coinbase Wallet, or Frame.

It is possible that other types of wallets (e.g. based on smart contracts) don’t support Metis, but it is something expected in a young network and doesn’t have any negative consequence from the infrastructure perspective.

3.8. On-chain multi-signature infrastructure

The permissions on the Aave ecosystem are directly held by on-chain governance smart contracts or scheduled to be like that once cross-chain governance infrastructure can be applied across all the networks.

However, different protection/emergency mechanisms, like the capability of canceling cross-chain governance proposals, or pausing an Aave asset/pool, depend on the Aave Guardian, who is capable of acting faster than the governance process.

Consequently, having on-chain multi-signature contracts is a requisite to have Aave on a different network, with a high preference for industry-standard tools like Gnosis Safe.

Metis HAS

an instance of the Gnosis Safe contracts on-chain, but the user interface and server infrastructure are not the official Safe, but a fork on metissafe.tech

We have contacted the team of the Metis community maintainingmetissafe.tech, confirming with them that:

- The code of the fork is open source on github.com/metissafe.
- They have full commitment to keeping the fork in line with Safe main upstream.
- Even in an emergency scenario with no infrastructure up, it is possible to spin up a dockerized instance of metissafe, following the instructions on the repository.

3.9. Transactions simulation infrastructure (fork)

Lately, a really important development experience component is the ability to execute test transactions (simulations) on forked production networks.

A good part of the tooling around Aave depends on simulations by using different libraries/frameworks like Hardhat, Foundry, or Tenderly. This way, it is possible to rapidly prototype new developments, get extra assurances on governance proposals and protocol upgrades, change risk parameters, etc.

As it is our main smart contracts development framework, we have tested that it is possible to do fork simulations on Metis with Foundry. Given its EVM compatibility, it should be perfectly doable with Hardhat too.

Currently, Tenderly is not integrating Metis Andromeda, but the Metis team is working on a potential integration.

3.10. Chain data/indexing solutions

For different projects and entities integrating Aave, and even if not a blocker for deployment, it is important that solutions like TheGraph or Dune are operating on the candidate network, to avoid building from scratch data pipelines.

Given its EVM general compatibility, Metis is supported on TheGraph, but the documentation and the details of a hosted service are relatively scarce on https://docs.metis.io/dev/graph

Metis is not supported by Dune.

3.11. Bridging infrastructure: assets, messages

Given the central role of Ethereum in the DeFi and Aave ecosystems, proper bridging infrastructure to/from is a must for any candidate network.

There are 2 types of bridging affecting Aave: assets and generic messaging. In the case of Metis, the state of these 2 types is as follows:

- Assets.

sub-use case the generic messaging infrastructure supported by Metis. For end users, it is possible to bridge assets via https://bridge.metis.io/home, with the same delays as in the case of Optimism: 1-2 minutes from Ethereum to Metis; ~7 days from Metis to Ethereum.

In terms of user experience, there is a small airdrop for gas expenses when bridging assets to Andromeda.

Regarding the security of the ERC20 smart contracts for bridged assets (and METIS token itself), if/when the community decides to deploy on Metis and with which assets, a more thoughtful assessment of the code should be done, following previous listing cases.

From our side, we have checked assets like AAVE, USDC, USDT and METIS, and all of them share or same or really similar codebase: a simple ERC20 based on the OZ version, with burn/mint capabilities by an entity defined as “bridge”.

- Generic messaging.

Metis supports bi-directional generic message passing, with the same mechanism as Optimism. This is especially important for Aave, in order to activate cross-chain governance.

In addition to the default bridging mechanism of Metis, there are additional ones like Celer, Multichain, or LayerZero.

3.12. Commitment in security-incidents

Having proper mechanisms and procedures to prevent and react to security incidents is something quite fundamental for any platform and application, and networks like Metis are no exception.

We have directly checked with the team and confirmed the following:

- On the prevention side, Metis has an Immunefi bug bounty campaign running.
- Currently, the Metis bridge is aligned with the codebase of Optimism, which gives cumulative security in terms of multiple teams and security professionals.
- If any incident would happen, Metis has confirmed to us that will immediately react and execute at least the following measures:
- Act as fast as possible to protect against damage.
- Contact the technical side of Aave.
- Engage independent security experts to assess the security problem and the reaction to it.
- Properly community the Aave community about the incident, and the next steps.
- Act as fast as possible to protect against damage.
- Contact the technical side of Aave.
- Engage independent security experts to assess the security problem and the reaction to it.
- Properly community the Aave community about the incident, and the next steps.
- A private channel of communication will be kept between the Metis team and the assigned technical team of the Aave community (e.g. BGD), for any necessary update concerning the network and consequently, Aave on Metis.

3.13. Network security/technical model

At the core of any candidate network analysis are its morphology (which type of network it is) and security model (which parties are involved in the control over the network; decentralization degree).

Regarding its morphology/type, Metis is technically an optimist rollup. As mentioned before, initially Metis was a fork of Optimism, and even if it evolved since its inception, it is a pretty important consideration, given that Aave is already present in Optimism.

Regarding its security model, there are multiple aspects to analyze.

3.13.1. Transactions flow

A detailed explanation can be found HERE, but in summary:

1. When a user wants to execute a transaction, he submits it to the so-called set of Block Producers

, broadcasting each other the transactions through a peer-to-peer network (Peer Network

), and notifying the user with a transaction receipt when it gets processed. At the current stage, we could consider this as a single entity, as Block Producers are centralized, and controlled by the Metis team

.

1. Another set of entities denominated Sequencers

receives all the different transactions produced by the Block Producer/s

from different users, ordering them and generating/updating 2 Merkle trees: 1 containing all the ordered transactions of the network, another containing all the state updates. All the data is forwarded to a system called Memo, factually the storage backup layer of the rollup. At the current stage, the Sequencer is centralized and controlled by the Metis Team

.

1. The Sequencer

submits the new roots of the transactions and state Merkle trees to Ethereum, the moment on which we can consider the “batch” as finalized (this is not really accurate in optimistic rollups, but for simplification purposes).

In parallel to this, another set of entities - denominated Verifiers

, fetch from Memo all the information of the transactions and re-executes them, verifying that they are correct. In addition, it monitors what the Sequencer

has submitted to Ethereum, to check that it is fully consistent (no fraud).

If any fraud is detected by a Verifier

, they can submit a transaction on Ethereum to activate the Insecure Transaction State

, a mode by which the network halts until there is a resolution (if there was actually a fraud or not). It is important to highlight that the Verifier needs to pay fees to start this process, to avoid spam. This is a pretty critical point, given that factually Aave, same as any other application, will not be running.

Currently, any entity can run the verifier softwareHERE, but to report on-chain on Ethereum about potential fraud, the entity needs to be whitelisted by the Metis governance.

3.13.2. Storage mechanism: Memo

Storage on Andromeda relies on the usage ofMemo, a decentralized storage system.

A detailed analysis of this technology is out of the scope of this report, but the system is a combination of pure distributed storage (e.g. IPFS), together with layers of data consistency and availability on top, based on the usage of a MEMO token.

From our understanding, Metis has a User role on Memo, so “reader/writer” of data there.

From our external perspective, Memo seems quite early-stage technology, not as mature as similar ones like IPFS (and its data availability layer Filecoin), Arweave or others.

3.13.3. Upgradeability and control model

As previously mentioned, multiple components of the Metis network are controlled by the so-called Metis Governance.

At the moment, that governance is exercised via a Gnosis Safe 4-of-6 multi-sig. The Metis team has communicated to us that all those keys are properly segregated amongst different people/entities and managed via hardware devices.

Regarding smart contracts upgradeability, currently, all of them have a mechanism by which the Metis Governance can do upgrades, or change different parameters, like those related to the bridging infrastructure.

In summary, given the stage of the project, there is important centralized control, but comparable in more or less degree with similar optimistic rollups like Optimism.

3.13.4. Security audits

The Metis network has undergone3 audits: 2 for a set of smart contracts regarding the METIS token on Ethereum and some staking functionalities, and another for the node implementation forked initially from the modified version of Geth used by Optimism.

Even if those components seem to be validated, we think it could be a good idea to have some extra audit of the whole system as it is right now, as, for example, we don’t see any review covering the transaction flow end-to-end, or the storage strategy via Memo

.

A good overview of all the infrastructural smart contracts of Metis Andromeda can be foundHERE.

4. Summary

[

Metis-summary-final

1920×1950 227 KB

](https://europe1.discourse-cdn.com/business20/uploads/aave/original/2X/d/dc1646e9a68974a29b03ae4212444861b2ceee14.jpeg)

From our analysis, we conclude that Metis, even with aspects to improve, is an acceptable network candidate in regard to technical requirements, with no current hard blocker for the Aave v3 protocol to work properly.

An expansion of Aave there will imply allocating some development resources for both the initial setup, together with some overhead of maintenance and monitoring over time, similar to other networks like Optimism or Arbitrum.

We think the aspects the community should evaluate more carefully before taking a decision are those related to the network’s security.

Similar to other optimistic rollups, there is an important degree of centralization, but this is expected given the early stage of this technology. It is up to the community to decide if the risks derived from this centralization are worth it.

For the following steps, we think it is appropriate to have some reporting from the risk side of the community@ChaosLabs and @Pauljlei from Gauntlet), followed by the creation of a final Snapshot vote for the community to approve a deployment and activation of Aave v3 on Metis Andromeda.