[

Linea_banner

1920×845 117 KB

](https://europe1.discourse-cdn.com/flex013/uploads/aave/original/2X/1/1fef5aa6542468424ace9883b5a09495c62218d4.jpeg)

Following our framework of Aave's infrastructure evaluation and the positive signaling by the community ontemp check stage, we present the analysis of the Linea network, regarding its suitability to deploy an instance of the Aave v3 (v3.2) protocol.

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 Linea ecosystem.

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

Report

1. Introduction to Linea

Linea is a Layer 2 ZK rollup, using validity proofs to have low-cost transactions, but inheriting the security of Layer 1, Ethereum.

Other high-level characteristics of linea are:

- EVM equivalence and bytecode compatibility, which means that applications are deployed as it is from Ethereum to the Linea network without any custom modification.
- Unlike most ZK rollups, transaction data is posted instead of state diffs in the form of blobs.
- The validity proofs system is based on SNARK proofs.

Linea was released (mainnet) onJune 13th, 2023.

2. Our methodology

This report is not trying to be a full analysis of the Linea network, instead focusing on the aspects important to the Aave community should it decide to deploy the Aave v3 (v3.2) liquidity protocol there.

In addition to being extensive, this report tries to be simple enough for all participants in Aave governance to understand. But given its technical nature, it is unavoidable to assume a certain familiarity with some relevant concepts, such as rollups, oracles, RPC nodes, or blockchain explorers, amongst others.

To simplify the interpretation of this report, we will evaluate each key component for Aave separately, and assign simplified "grades", defined as follows:

[

gold

1042×1042 94.2 KB

](https://europe1.discourse-cdn.com/flex013/uploads/aave/original/2X/9/953c2dd4b2ee708c1e7fde98a80a395c26f0de05.png)

Optimal

. Fulfilling all minimal requirements, and with extra positive aspects.

[

silver

1042×1042 70.2 KB

](https://europe1.discourse-cdn.com/flex013/uploads/aave/original/2X/2/2f4f226bffa222ec14ed36888aa9049cdd357bfa.png)

Good

. Fulfilling the requirements, but improvements can be made.

[

bronze-high

1042×1042 73.3 KB

](https://europe1.discourse-cdn.com/flex013/uploads/aave/original/2X/1/1f54830400754f5d78ca9d0eeea5e3130d6dbe4f.png)

Acceptable

. Fulfilling the requirements, but with “buts”.

[

bronze-low

1042×1042 29.9 KB

](https://europe1.discourse-cdn.com/flex013/uploads/aave/original/2X/c/cb5db063988736a6b6a2f112c4ad0f75d7496d00.png)

Needs improvement

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

3. Evaluation

[

silver

1042×1042 70.2 KB

](https://europe1.discourse-cdn.com/flex013/uploads/aave/original/2X/2/2f4f226bffa222ec14ed36888aa9049cdd357bfa.png)

3.1. Oracle Infrastructure

The Aave protocol uses different types of oracles in a standalone blockchain. We consider that having Chainlink providing oracles, especially for prices, is a must for any deployment, with alternatives only considered on an ad-hoc, given the additional complexity added on evaluation/integration.

3.1.1. Price feeds

Used by the Aave protocol to price listed assets

Linea HAS

Chainlink price feeds as of now.

There are other oracle providers in Linea, but we would only recommend launching with Chainlink oracles.

3.1.2. L2 Sequencer Uptime feed

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

Linea DOESN’T HAVE

an oracle for fetching L2 Sequencer Uptime, but we have confirmed with the Linea team the feed is being worked on.

3.1.3. Proof-of-Reserve feeds

Component indicating to the Aave protocol if the reserves backing an asset are healthy, for example in bridged tokens.

Linea DOES NOT HAVE

proof-of-reserve feeds.

[

gold

1042×1042 94.2 KB

](https://europe1.discourse-cdn.com/flex013/uploads/aave/original/2X/9/953c2dd4b2ee708c1e7fde98a80a395c26f0de05.png)

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.

Linea has multiple block explorers, including but not limited to:

- https://lineascan.build/ powered by Etherscan technology.
- A blockscout instance https://explorer.linea.build/.
- Phalcon Explorer.

[

gold

1042×1042 94.2 KB

](https://europe1.discourse-cdn.com/flex013/uploads/aave/original/2X/9/953c2dd4b2ee708c1e7fde98a80a395c26f0de05.png)

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 a node, of Linea in this case.

Linea HAS

major JSON-RPC compatibility, only with some missing support for eth_newFilter

and eth_newBlockFilter

RPC calls that should not affect the Aave v3 protocol.

[

gold

1042×1042 94.2 KB

](https://europe1.discourse-cdn.com/flex013/uploads/aave/original/2X/9/953c2dd4b2ee708c1e7fde98a80a395c26f0de05.png)

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.

A significant strength of non-Ethereum networks is that they support the same account derivation system as Ethereum, so EVM wallets are natively compatible.

Linea is fully compatible with the Ethereum public-private key account format.

[

gold

1042×1042 94.2 KB

](https://europe1.discourse-cdn.com/flex013/uploads/aave/original/2X/9/953c2dd4b2ee708c1e7fde98a80a395c26f0de05.png)

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.

Currently, besides the public RPC (https://rpc.linea.build), Linea has support from numerous RPC node providers, including but not limited to:

- Alchemy
- Quicknode
- Blast
- DRPC

[

silver

1042×1042 70.2 KB

](https://europe1.discourse-cdn.com/flex013/uploads/aave/original/2X/2/2f4f226bffa222ec14ed36888aa9049cdd357bfa.png)

3.6. Custom behaviour (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, chainId definition out of the norm, etc.

Independently, even if not doing a full evaluation of the Linea-zkEVM implementation, we have checked the following, given that historically have been critical aspects:

Linea has numerous differences to Ethereum and its various sidechains. Some more relevant ones are listed below:

- The chainId

behavior is appropriate, with the id 59144

for Linea not clashing with any other.

- Linea has equivalence (address and logic) with the ecRecover and identity Ethereum pre-compiles, which covers the needs of Aave.
- Linea currently uses the London version of the Ethereum Virtual Machine (EVM). Latest EVM versions like Paris, Shanghai, and Cancun are currently not available

. Although this is not the most optimal, it is acceptable when deploying contracts related to Aave.

- As Shanghai and Cancun EVM versions are not introduced, the following opcodes are not available on linea BLOBHASH

, BLOBBASEFEE

, MCOPY

, PUSH0

, TLOAD

, TSTORE

. DIFFICULTY

/ PREVRANDAO

opcode behaves differently from L1 and instead of returning the RANDAO value from the previous block, it returns a fixed value of 2

.

- Some precompiles such as point evaluation and secp256r1 are

not available on Linea. The MODEXP

precompile on Linea currently only supports arguments (base, exponent, modulus) that do not exceed 512-byte integers. The recipient of a transaction on Linea (the address in to

) cannot be in the range 0x01

-0x09

. All these differences should be acceptable.

- As of the latest v3.6 release, the network has a fixed block time of 2 seconds with block limit of 30m and transaction gas limit of 24m.

[

gold

1042×1042 94.2 KB

](https://europe1.discourse-cdn.com/flex013/uploads/aave/original/2X/9/953c2dd4b2ee708c1e7fde98a80a395c26f0de05.png)

3.7. Support of wallet providers

Wallet products like Rabby, 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 it is major EVM compatibility, Linea is supported by the majority of chain-agnostic EVM wallets.

[

gold

1042×1042 94.2 KB

](https://europe1.discourse-cdn.com/flex013/uploads/aave/original/2X/9/953c2dd4b2ee708c1e7fde98a80a395c26f0de05.png)

3.8. On-chain multi-signature infrastructure

The permissions on the Aave ecosystem are directly held by on-chain governance smart contracts.

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, which 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.

Linea DOES

HAS

an official instance of the Gnosis Safe contracts on-chain, supported natively inside the official interface.

[

gold

1042×1042 94.2 KB

](https://europe1.discourse-cdn.com/flex013/uploads/aave/original/2X/9/953c2dd4b2ee708c1e7fde98a80a395c26f0de05.png)

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.

In terms of tooling that can be used for simulation supporting Linea:

- Tenderly has support for Linea.
- The Phalcon simulator doesn't support Linea.
- Hardhat supports Linea.
- Since Linea is bytecode compatible, tools such as foundry are natively supported.

[

gold

1042×1042 94.2 KB

](https://europe1.discourse-cdn.com/flex013/uploads/aave/original/2X/9/953c2dd4b2ee708c1e7fde98a80a395c26f0de05.png)

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.

Linea is supported on multiple data-indexing solutions, including both limited to Dune or TheGraph.

[

gold

1042×1042 94.2 KB

](https://europe1.discourse-cdn.com/flex013/uploads/aave/original/2X/9/953c2dd4b2ee708c1e7fde98a80a395c26f0de05.png)

3.11. Bridging infrastructure: assets, messages

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

The Linea network has proper bridge infrastructure for both transferring assets and generic messaging With respect to the functionality of Governance V3 and a.DI, their native bridge supports cross-chain messaging, and there are also other third-party bridge providers available.

For bridging assets, as with other chain/rollup bridges, the Canonical Token Bridge will deploy a standard upgradeable ERC20 contract, inheriting its logic from OZ ERC20PermitUpgradeable contract.

[

gold

1042×1042 94.2 KB

](https://europe1.discourse-cdn.com/flex013/uploads/aave/original/2X/9/953c2dd4b2ee708c1e7fde98a80a395c26f0de05.png)

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 rollups like Linea are no exception.

From our research and communications with the Linea team:

- There is an ongoing program on Immunefi for Linea with a maximum payout of $100k.
- A private channel of communication will be kept open between the Linea team and the assigned technical team of the Aave community (e.g. BGD), for any necessary update concerning the network and consequently, the deployment of Aave on Linea.

[

silver

1042×1042 70.2 KB

](https://europe1.discourse-cdn.com/flex013/uploads/aave/original/2X/2/2f4f226bffa222ec14ed36888aa9049cdd357bfa.png)

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).

The Linea network is a rollup based on validity proofs, inheriting the security of the Ethereum base layer. However, at the moment, there are the following considerations:

3.13.1. Sequencer and Proposer Downtime

Like all rollups, Linea network uses a sequencer, which is responsible for processing transactions on the L2 blockchain itself.

There is no mechanism to have transactions be included if the sequencer is down or censoring. Only the whitelisted proposers can publish state roots on L1, so in the event of failure, the withdrawals are frozen.

3.13.2. Upgradeability and control model (decentralization)

Currently, the Linea network has meaningful centralized control, with a4-of-8 multi-sig having super-admin control on a sophisticated system allowing updates on core contracts, bridges, permissioned actors, and can publish blocks by effectively overriding the proof system. Another important thing to note is that there is no timelock for code updates.

You can find a breakdown of permissionsHERE.

Given the early stage of the technology, this control is understandable and relatively similar to other L2 networks.

3.13.3. Security audits

Linea network has been submitted to multiple audits and security procedures, on all layers (L1, L2, cryptography).

All of them can be found HERE.

3.13.4. Transaction lifecycle

The Linea documentation contains an extensive explanation of the transaction lifecycleHERE, but to summarise:

1. Transactions are submitted to the mempool, validated and ordered by the Linea sequencer, then executed and added to a block. This results in soft finality within about 2 seconds.
2. Transaction data is sent to the state manager, conflated into batches, and used to generate ZK proofs (zk-SNARKs) through a two-stage process involving inner and outer proofs.
3. The batch containing the transaction, along with its proof and blob data, is submitted to Ethereum mainnet. After verification and a waiting period, the transaction reaches hard finality, typically within 8-32 hours.

3.13.5. Data availability

As previously commented, on Linea all the transaction data is submitted to Ethereum, so data availability boils down to Ethereum, which can be considered the highest standard at the moment. At the moment there is no available node software that can reconstruct the state from the L1 data.

All the technical documentation about Linea can be foundHERE. Additionally, the system's smart contracts addresses can

be found HERE.

4. Summary

[

Linea_grades

1920×2009 274 KB

](https://europe1.discourse-cdn.com/flex013/uploads/aave/original/2X/1/1bb6ec0052aa71e0e8d68d3ab39bc548edbc7fc9.jpeg)

From our analysis, we conclude that Linea, even if in a relatively early stage of decentralization, is an acceptable network candidate regarding technical requirements, with quite strong infrastructure and tooling. We don’t see any blocker for the Aave v3 (v3.2) 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.

Same as with other rollups, there is an important degree of centralization, but this is expected given the early stage of this technology. However, the validity-proofs rollup nature of Linea is a pretty strong aspect to consider.