

# TL;DR

Define a clear and transparent set of evaluation points for networks seeking to get Aave v3 deployed, for the community and technical contributors to have a reference on what is required from a technical standpoint.

## Rationale

For already a couple of years, the general direction of Aave has been to deploy and connect instances of the liquidity protocol in not only Ethereum, but also on different networks, with Aave v2/v3 being on Polygon, Avalanche, Optimism, Arbitrum, Fantom and Harmony.

This strategy is rewarding to the ecosystem, with new profiles of users having Aave at reach, but also introduces different types of risk.

From a technical perspective, we believe something the community is still lacking is a transparent and precise framework of requirements that the ecosystem of a network candidate for deployment of Aave should have as a reference.

A framework like this enables technical entities or community members like ourselves (BGD) to do independent assessments of a network, which in turn will allow the not-so-technical audience to do more informed votes to decide if a new deployment should happen or not.

Additionally, we think it is fundamental that these kind of analysis happen publicly, showing that every network is from a technical perspective neutrally evaluated.

## Candidate network's requirements

The following is a list of what we consider important aspects to check when evaluating if a network is mature enough for the Aave liquidity protocol to be deployed:

- Oracle infrastructure.

The Aave liquidity protocol requires a really reliable price oracles infrastructure connected. This means in practice having a fully distributed set of entities submitting prices by reaching some kind of consensus.

In practice, Aave has a quite long-lasting relationship with the Chainlink protocol, which has the most battle-proven infrastructure in the blockchain field, so having Chainlink oracles is a quite important requirement and a big plus. Alternatives could be considered, but initially, preferring Chainlink.

It is a plus if other oracles helping with protocol safety (e.g. Proof-of-Reserve, Sequencer availability flag for rollups, ...) are available too.

- Quality block explorers.

Even if easily undervalued and overlooked, a good block/transaction/smart contracts explorer is quite vital for users (especially those technical) of a network. It is both a source of transparency (e.g. verified smart contracts) and a last-resort user interface to both read data and make transactions.

In practice, we think Etherscan (or white-label solution) explorer is a quite strong plus for any candidate, and alternatives should be carefully evaluated.

- Compatibility with Ethereum RPC endpoints.

Compatibility with all eth\_\*

, web3\_\*

, net\_\*

is required, with support for trace\_\*

(e.g. Erigon) being a plus.

- Disclosure of any non-EVM/Ethereum extra/different feature of the network.

Deviations from Ethereum should be properly disclosed, both those that work differently compared with Ethereum and new ones enabling extra mechanisms. This obviously includes if the network is not EVM-compatible.

- Quality RPC endpoints/providers.

It is mandatory to have RPC endpoints or layers on top of them (e.g. POCKET network, Alchemy, Infura, etc) with really

good reliability and availability. A reasonable public RPC, reliable and with not too low rate limits is required. In addition, having dedicated nodes with access control based on allowListed Aave's smart contracts addresses is a plus.

- No "weird" chainId

behavior.

The chain id of the network should be a different one than other EVM-compatible chains. All out-of-the-box mechanisms on this should be carefully evaluated, and considered initially as a big minus, as it will affect the protocol's functionality (e.g. meta-transactions features) and security model.

- Support by major wallet providers.

Kind of a consequence of the RPC/chainId

points, but it is mandatory that at least web/desktop-first wallets like Metamask, Frame, Ledger, and Trezor support the network.

- Address formatting.

Proper disclosure if the address format of the candidate network is not exactly the same as Ethereum, for example, if there is any transformation mechanism.

- On-chain multi-signature infrastructure.

This slightly depends on bridging infrastructure, but generally, it is quite important for the network to be available on platforms like Safe, given the temporary multi-signature requirements of the Aave protocol before applying cross-chain infrastructure; or even for emergency actions.

- Liquidity on assets' to be listed.

There is not really any threshold of liquidity for the network to have in order to host the Aave protocol, given the possibility of setting caps and different risk-averse modes on the configuration. Still, we believe that a good aggregated size counting all the assets to be listed should be quite mandatory for deployment, as the deployment/evaluation effort already consumes resources from the Aave community.

- Reliable and feature complete bridging infrastructure.

Aave has been evolving on cross-chain control of other networks from Ethereum during the last year. Currently, not having a generic messaging bridge or at least 2-3 different bridge messaging providers should automatically disqualify any network candidate, as it would force Aave to go against the trend of removing Aave Guardian's intervention.

Additionally, there should be a good security assessment of the smart contracts of the assets to be listed (e.g. understanding there is no room for reentrancy on the ERC20 of bridged assets).

- Full disclosure of network security and points of centralization

. Every single point

of control (consensus, multi-signature contracts, etc) of the network needs to be fully disclosed to the Aave community and carefully evaluated. Given the variety of mechanism and innovation out there, it is difficult to fully define a minimum threshold for the different components of the network, but aspects like having a single EOA controlling critical infrastructure immediately disqualifies the candidate. Especially important to understand the security model of the bridging infrastructure.

It is also included on this point mechanism like fraud-proofs on optimistic rollups.

- Commitment in a catastrophe scenario on the network.

Things can go wrong, even if the network candidate looks optimal. Before any deployment, and even if most probably it is not mandatory to have a detailed plan of action, there should be some soft commitment from the community behind the network candidate to handle ad-hoc the relation and coverage of Aave in a catastrophe scenario. Aave links its reputation to each one of the new networks, so there should be a clear counterpart to it.

- Simulation/fork infrastructure.

Both tooling and security procedures on the tech side of the Aave community depend importantly (and as time passes, more) on being able to do testing on mainnet data via fork, to be as close as possible to the production environment.

This is usually a direct consequence of having quality RPC endpoints/providers, but additionally, support of the network by a tool like Tenderly is pretty important.

- Support of data indexing solutions.

TheGraph, Dune, Trueblocks, ... Not mandatory, but it is a good plus, giving the big developers' community around Aave depending on those services.

- Post-deployment contact channel with entities around Aave.

Expert parties (mainly tech) of the candidate network should be available on a dedicated channel (e.g. Telegram, Discord) with entities surrounding Aave, like BGD or others.

## How this framework should be used?

Even if not so frequent, it is realistic to have in the order of 3-4 network candidates a year to have Aave deployed. Part of BGD's commitment is to help the community with the evaluation of those, defend Aave's interests, and try to be as transparent as possible.

We propose the following steps before a deployment can happen:

1. Forum post by the candidate's network, presenting the fundamentals of their ecosystem.

The description should describe non-technical aspects of the network, as it is done currently. Optionally, technical aspects of this framework can be included, as they will facilitate further analysis.

1. Sentiment poll on Snapshot.

To show general support or not on the deployment, before any serious resources of the Aave community get allocated to a deeper evaluation. This step could be done with the framework approved [HERE](#) involving a 150k YES minimum quorum.

1. Technical evaluation.

BGD or whatever technical provider will evaluate fully independently the suitability of the network, following the framework in this document. This will consist of going through all publicly available documentation, together with contacting tech teams associated with the candidate to get as much information as possible.

Once done, the review will be presented on the Aave governance forum. It is important to understand that there is no concept of passing/not-passing a review; it will be just an extra resource for the community to, later on, emit an informed vote

.

1. Snapshot vote to approve deployment.

The final vote for the Aave community (after discussing and evaluating pros/cons) to approve or not have the Aave liquidity protocol on the candidate network. If passing, a technical provider like BGD will be approved by Aave to support the candidate with the smart contracts deployments".

From our side, we have already started applying this framework on networks that have already community support like for example [Metis](#). We encourage teams looking for Aave v3 deployments to reach to us (if we didn't yet), for if any clarification is needed.