

BGD. AAVE <> BASE

INFRASTRUCTURE / TECHNICAL EVALUATION

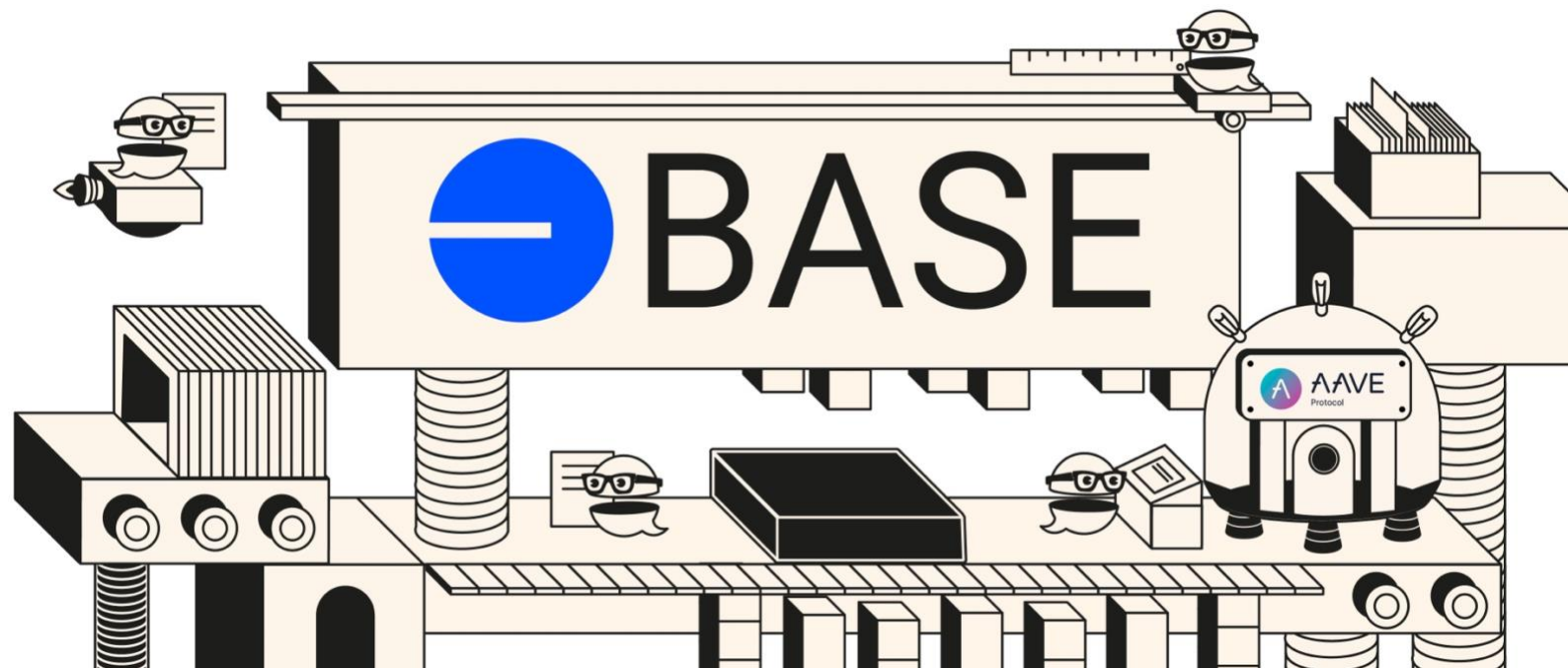
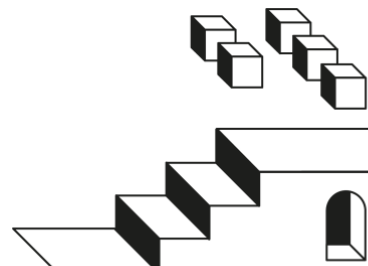


Table of Contents

Introduction	3
Disclosure	3
Report.....	4
1. Introduction to Base	4
2. Our methodology.....	4
3. Evaluation.....	6
3.1. Oracle Infrastructure	6
3.2. Blockchain explorer	7
3.3. Compatibility with Ethereum RPC standard	8
3.4 Compatibility with Ethereum account format (addresses)	8
3.5. RPC public endpoints and providers	9
3.6. Custom behavior (lack of) of the execution layer	10
3.7. Support of wallet providers	11
3.8. On-chain multi-signature infrastructure.....	12
3.9. Transactions simulation infrastructure (fork).....	13
3.10. Chain data/indexing solutions	14
3.11. Bridging infrastructure: assets, messages	14
3.12. Commitment in security incidents.....	15
3.13. Network security/technical model	16
Summary	18



Introduction

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.

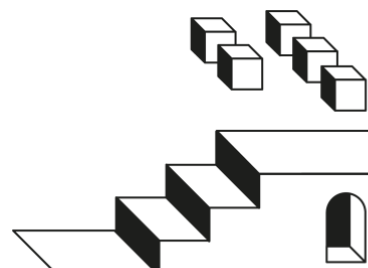
Following the positive sentiment poll on Snapshot, this is an analysis of the Base network.

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 Base/Coinbase ecosystem.

When doing the evaluation, we contacted the Coinbase 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 Base

Base is a Layer 2 optimistic rollup, with EVM base compatibility and settling to Ethereum mainnet.

Additionally, Base is built on the Optimism OP-Stack, with the Base team joining as core contributors to it, together with the Optimism team. Therefore, Base mainnet is really similar to Optimism mainnet, infrastructure-wise.

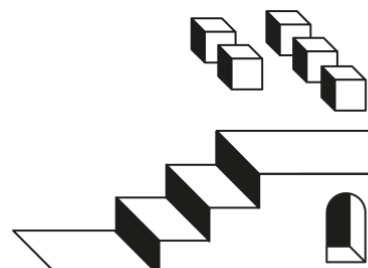
Same as with all other optimistic rollups, Base is in an early stage, trying to improve its shape and infrastructure, together with addressing mechanics like its decentralization, cost-of-usage, or security. Mainnet has been live since 13th July 2023 (developers-only), with plans for fully opening it beginning of August.

2. Our methodology

This report is not trying to be a full analysis of the Base 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 all participants in the Aave governance to understand. However, 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.



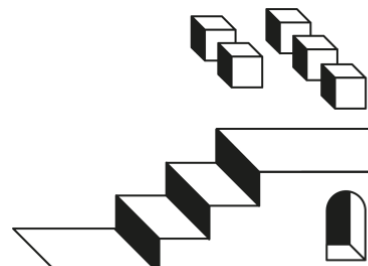
Good. Fulfilling the requirements, but improvements can be made.



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 Optimism. 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.

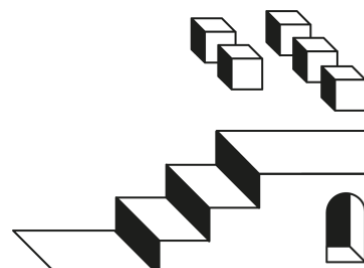
Base **HAS** Chainlink price feeds available for the major assets on the network. Currently on testnet, but we have confirmed with the Chainlink team they will be available on mainnet at launch.

Additionally, there seem to be some other price feed oracles on Base, 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.

Base **WILL HAVE** Chainlink L2 Sequencer Uptime, confirmed to us by the Chainlink team.



3.1.2. Proof-of-Reserve feeds

Component indicating to the Aave protocol if the reserves backing an asset are healthy.

Base **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.



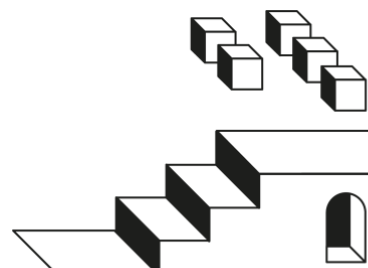
3.2. Blockchain explorer

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 Base network can be found at <https://basescan.org/>, and it is a white-labeled instance of [Etherscan](#).

Alternatively, there is also a [Blockscout](#) deployment.





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 Base in this case.

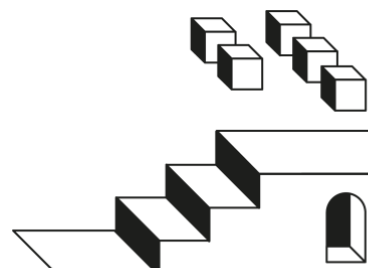
Base **HAS** complete compatibility, with the main node being op-geth, an adaptation of go-ethereum. Depending on the node provider there can also be support for non-standard endpoints (e.g. `trace_*`) in the future.



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.

Base is fully compatible with the Ethereum account format.





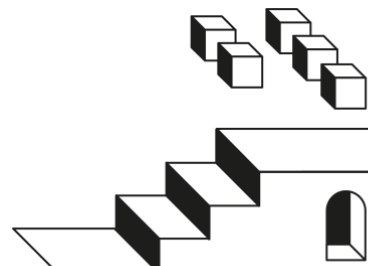
3.5. RPC public endpoints and providers

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, Base has 2 types of RPC endpoints:

1. An “official” one is provided by the Base infrastructure team on <https://developer-access-mainnet.base.org/> but submitted to rates limits.
2. Private ones like QuickNode, Blast, and Blockdaemon

The lack of more public providers at this point is acceptable, but could be problematic.





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.

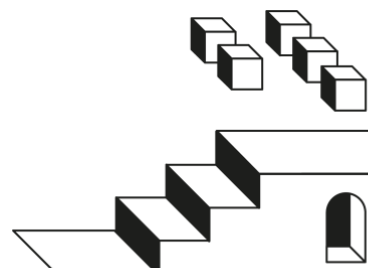
Examples of this potential behavior are the presence of new pre-compiles (compared with Ethereum or similar rollups like Optimism), EVM opcodes, native account abstraction/meta-transactions, chainId definition out of the norm, etc.

Base is fully aligned with the Optimism execution layer implementation (Bedrock version), being part of the OP-Stack. This is really important from Aave's perspective, given the protocol is already flawlessly running on Optimism mainnet.

Even if not doing a full evaluation of the Optimistic 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 `8453` for Base not clashing with any other.
- There are no extra opcodes compared with Optimism.
- There are no extra pre-compiles compared with Optimism.

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



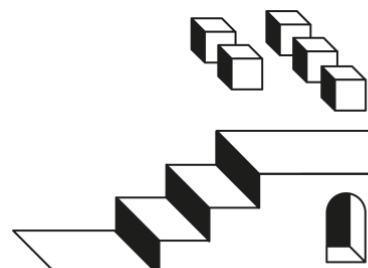


3.7. Support of wallet providers

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, Base 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 Base, but it is something expected in a young network and doesn't have any negative consequence from the infrastructure perspective.





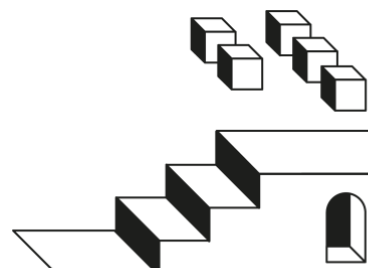
3.8. On-chain multi-signature infrastructure

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.

Base **HAS** an official instance of the Gnosis Safe contracts on-chain, supported natively inside the official [interface](#).





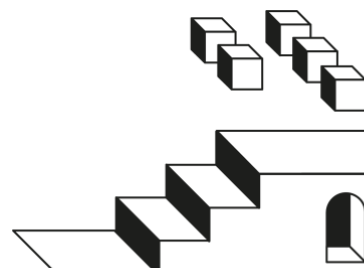
3.9. Transactions simulation infrastructure (fork)

ately, 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 Base with Foundry. Given its EVM compatibility, it should be perfectly doable with Hardhat too.

Tenderly has confirmed support for Base beginning of August 2023.





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, Base is supported on [TheGraph](#), [Dune](#), [Covalent](#), and [GoldSky](#).

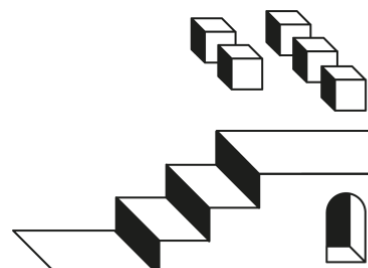


3.11. Bridging infrastructure: assets, messages

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 Base, the state of these 2 types is as follows:

- **Assets.** sub-use case of the generic messaging infrastructure focused on assets like ERC20 or ERC721. For end users, it will be possible to bridge assets via bridge.base.org. Details about it are not available at the moment, given it is not available on the mainnet developers' phase, but it is safe to assume it will share similar characteristics as Optimism mainnet.



Regarding the security of the ERC20 smart contracts for bridged assets, if/when the community decides to deploy on Base 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 the ERC20 implementation and procedures, which mirror Optimism's.

- **Generic messaging.** Base 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 Base, there are additional third-party bridges present there like Axelar, Celer, LayerZero or Wormhole.

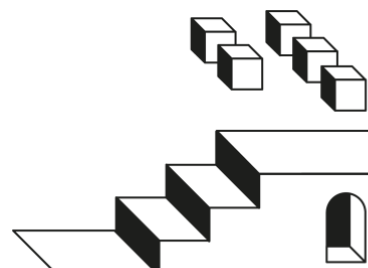


3.12. Commitment in security incidents

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

Apart from the extensive security procedures “native” to Base or inherited from the OP-Stack, the Base team will keep a private channel of communication with the assigned technical team of the Aave community (e.g. BGD), for any incident of update concerning the network and consequently, Aave on Base.

Finally, we are aware of the commitment of Coinbase to good security practises, which further solidifies this part of the evaluation.





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, Base is technically an optimist rollup, and especially important, as an instance of the OP-stack, closely similar to Optimism mainnet.

Regarding its security model, the approach with Base is almost the same as Optimism mainnet: a so-called Stage 0 optimistic rollup, with centralized components that will be decentralized over time.

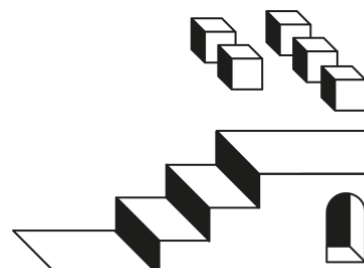
3.13.1. Centralization points

- Base has a single and centralized sequencer, receiving transactions, processing them, and doing the roll-up to be settled on Ethereum mainnet.
- The Base infrastructure of smart contracts is generally upgradeable, and controlled via multi-sig, including components like bridging and its assets. This is common practice on the initial stage of optimistic rollups, similar to Optimism mainnet.

There is a clear decentralization roadmap of Base, which can be found [HERE](#).

3.13.2. Upgradability strategy and sync with OP-Stack

In terms of upgrades and the procedures surrounding them, we have confirmed with the Base team that:



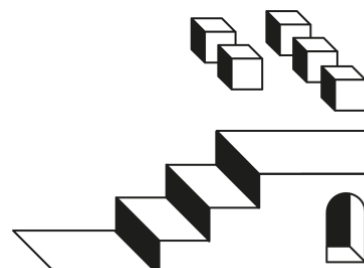
- There is a series of procedures to keep in sync Base with the OP-Stack infrastructure, both in terms of off-chain components (e.g. sequencer) and smart contracts. All introduced changes on the OP-Stack are to be reviewed and quality-tested by the Base team.
- Once the OP-Stack superchain strategy develops more, all upgrades of superchains (including Base) will be managed commonly, in a higher layer.
- Base is the second official core development team of the OP-Stack, so there is full alignment with the first, the Optimism team.

3.13.3. Security procedures

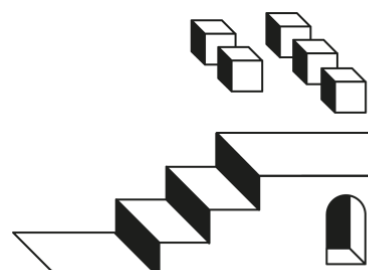
We have directly checked with the team and confirmed the following:

- Being part of the OP-Stack, Base inherits the security assurances of Optimism, being:
 - All layers were audited by multiple parties: OpenZeppelin, SigmaPrime, Trail of Bits, Sherlock, Code4rena, and Coinbase Security team.
 - Ongoing [bug bounty programs](#).
- The collaborative approach between 2 different teams like Base's and Optimism's on the OP-stack gives extra security assurance.
- Base is actively engaging security firms in the space to provide their services to end users and protocols on their network.
- The Base team has commented to us that the Coinbase bug bounty program could be applicable in certain parts of the infrastructure <https://hackerone.com/coinbase>

An overview of all the infrastructural smart contracts of Base can be found [HERE](#).



Summary



From our analysis, we conclude that Base, even if in a really early stage (not fully released on mainnet), is an acceptable network candidate in regard to technical requirements, with no current hard blocker for the Aave v3 protocol to work properly. Our main consideration for this conclusion is the inherited infrastructure from the OP-Stack, and the presence of Aave on both Optimism mainnet and Metis Andromeda, a fork of it.

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.

In terms of aspects for the community to focus on, we think those related to liquidity and risk are probably more significant than technical ones in this case, given the early stage of the network.

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

