

[

Sonic_banner

1920×845 108 KB

](https://europe1.discourse-cdn.com/flex013/uploads/aave/original/2X/9/92806722ade6bbdc1ee3d696ecd447b1e20353a3.jpeg)

Following [our framework of Aave's infrastructure evaluation](#) and the positive signaling by the community on the [forum](#), we present the analysis of the Sonic blockchain

regarding its suitability to deploy an instance of the Aave v3 (v3.2 and upcoming v3.3) 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, we currently have absolutely no financial, investment, services-engagement, or other interest in the Sonic ecosystem.

Report

1. Introduction to Sonic

Sonic is an EVM-compatible L1 blockchain with a big focus on performance: providing infrastructure that allegedly supports over 10,000 TPS and short finality, while not sacrificing Ethereum compatibility.

Other high-level characteristics of Sonic are:

- Sonic uses a combination of Asynchronous Byzantine Fault Tolerance (ABFT) and Directed Acyclic Graphs (DAG) as a consensus mechanism.
- The execution layer is what we could denominate as a performance-augmented version of the EVM and DB associated.
- It includes a native asset bridge (Sonic Gateway) with a fail-safe mechanism to Ethereum.

2. Our methodology

This report does not attempt to analyze the Sonic blockchain fully; instead, it focuses 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.

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

Sonic HAS

[Chainlink price feeds](#) as of now.

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

3.1.2. Proof-of-Reserve feeds

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

Sonic 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.

[

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, block explorers like Etherscan are a fundamental component, specifically for the following:

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

The official Sonic network explorer, which is an instance of Etherscan, can be found at <https://sonicscan.org/>.

Alternative explorers can be found at <https://explorer.soniclabs.com/>, and <https://146.routescan.io/>

[

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 Sonic in this case.

Sonic network fully

compatible with the Ethereum standard. Alchemy provides detailed documentation of its JSON-RPC API, which can be found [here](#).

[

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.

Sonic IS

fully compatible with the Ethereum 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.

Sonic HAS

an official RPC endpoint at [**https://rpc.soniclabs.com**](https://rpc.soniclabs.com).

Third-party RPCs are also available by [Ankr](#), [Alchemy](#), [dRPC](#) and [thirdweb](#).

[

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, native account abstraction/meta-transactions, chainId definition out of the norm, extra compilation/execution layers, etc.

Sonic has augmented the EVM with the so-called SVM (Sonic Virtual Machine), which mainly increases speed/performance, while keeping compatibility. We checked that:

- The chainId

behavior is appropriate, with the id 146

for Sonic not clashing with any other.

- Sonic supports the Cancun/Deneb EVM version except for Blob transactions with non-empty blobs.
- Sonic node implementation has forked from go-Ethereum on its [Triodia \(v1.14.4\)](#) release. From there, it has been modified to add support for the Tosca VM, as can be seen [here](#).
- Tosca (SVM) introduces dynamic translation, where multiple code instructions can be executed simultaneously by a single instance. This results in more efficient execution and reduced processing time.
- Tosca includes an extensive conformance framework comparing execution paths and execution results between Geth and SVM, including random paths and random inputs. This is covered (amongst other testing) on the [LaScala suite](#).
- Sonic also introduces Carmen, a different storage system supporting Tosca's high-speed execution. It changes the current key-value storage system used in the EVM for a new file-based stateDB, which eliminates the need to map the current state in key-value pairs, amongst other database performance improvements, increasing speed and decreasing storage usage.

Even if by design the execution layer of Sonic has important internal differences with the “plain” EVM, we have seen important effort to keep compatibility and conformance with the Ethereum spec.

[

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, Sonic 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 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.

Sonic 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:

- Tenderly has support for Sonic.
- Phalcon simulator doesn't support Sonic.
- Foundry and Hardhat are supported Sonic.

[

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.

Sonic [is supported on multiple data-indexing solutions](#), including both [Dune](#) and [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, proper bridging infrastructure to/from is a must for any candidate network.

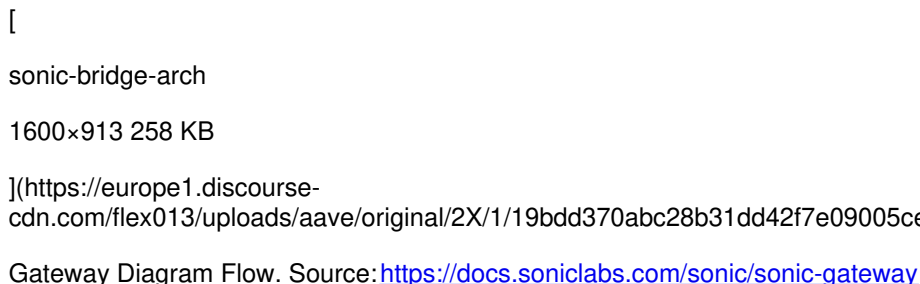
3.11.1 Assets Bridging

Sonic's native system (Sonic Gateway) provides ERC20 functionality while including a fail-safe mechanism that safeguards user assets.

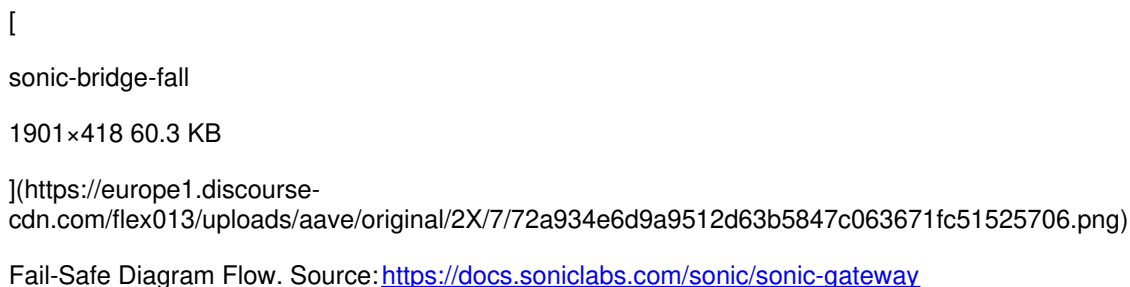
Bridging assets are processed in "heartbeat" intervals with the following timing:

- Ethereum → Sonic: 10 minutes.
- Sonic → Ethereum: 1 hour.

During these intervals the queued transactions are batched and processed together, reducing costs. If users want to have their assets bridged instantly, they can pay an extra fee for the additional "heartbeat," which also batches the pending requests and bridges them.



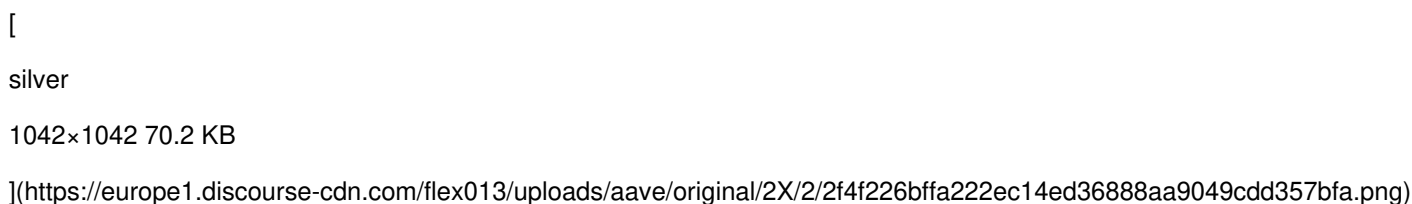
In the event of the Gateway or the Sonic is down for 14 consecutive days, users can withdraw their bridged assets directly on Ethereum. This period is immutable and cannot be modified.



3.11.2 General Message Bridging

The Sonic Gateway bridge does not support cross-chain message passing.

However, since [multiple third-party bridges](#) support Sonic, a.DI can be seamlessly integrated using these adapters, particularly Chainlink CCIP, the [LayerZero](#) and [Hyperlane](#).



3.12. Network security/technical model

At the core of any candidate network analysis are its morphology (which type of network it is) and security model.

Regarding its morphology/type, as previously mentioned, the Sonic network is an independent L1 blockchain and does not rely on Ethereum.

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

3.12.1. Upgradeability and control model (decentralization)

- Sonic is a new blockchain with roots in the Fantom Foundation. It is still in a migration process, so it uses the Fantom on-chain governance. This on-chain voting system allows FTM stakers to participate in decision-making proposals for the blockchain. The proposals are submitted by stakers paying a 100 FTM fee; during a certain period, the stakers can vote. At least 55% of the stakers must vote, and the proposal needs to achieve at least 55% of the quorum to be

accepted. Validators already voted for migrating Fantom block rewards to Sonic, which can be found [here](#).

- Like others L1s, the blockchain client upgrades is coordinated via the node validators.
- Currently [36 validators](#) are running the Sonic network, and they have being migrating block rewards from Fantom → Sonic to incentivize the validators migration. More detail can be found [here](#). New validators can start securing the blockchain by staking at least 500,000 S tokens and registering in the Staking and Consensus smart contract; more information on how to register as a validator can be found [here](#).
- The bridge is a non-upgradeable contract managed by a [3-of-4 super admin](#) multisig known as the Sonic Council, which has a 5-day delay period for any actions. Other important smart contracts (e.g., WETH and USDC.e) are upgradeable by another [3-of-4 Safe wallet](#) with no Timelock delaying upgrades. A full list of relevant smart contract addresses can be found in the Sonic documentation [here](#).

3.12.2. Security audits

Sonic's security audits were done by OZ, Quantstamp, and Certora. They can be found [HERE](#).

3.12.3 Security programs (e.g. bug bounty)

Sonic has announced a partnership with Immunefi for a [\\$2M bug bounty program](#).

3.12.4. Transaction lifecycle

The transaction lifecycle takes approximately 1-2 seconds. This involves the following steps:

1. A user submits a transaction, and a validator node receives the transaction.
2. The validator node batches the incoming transaction into a new event block. Each event block is a vertex in the validator's DAG.
3. The event block is asynchronously communicated to other node validators. They share their own event blocks and those they have received from others. The ABFT system allows validators to incorporate these blocks into their local DAGs.
4. Once most validators receive and agree on an event block, it becomes a root event block and is incorporated into the main chain, which contains the final consensus among all event blocks.

3.12.5 Sonic Gateway Permissions

A full list of the bridge contract can be found in the documentation [here](#).

Contract

Role/Permissions

Admin (mainnet)

Admin (Sonic)

Upgradable

[UpdateManager

](<https://etherscan.io/address/0xB0bECf0fBfE431D42bA0FbD8dFBFbB0DCFd62Da4>)

Central point for updating the bridge's parameters

[Safe 3-of-4](#)

[Safe 3-of-4](#)

Yes

[StateOracle

](<https://etherscan.io/address/0xB7e8CC3F5FeA12443136f0cc13D81F109B2dEd7f>)

Update the chain state

UpdateManager

UpdateManager

No

[TokenDeposit

](https://etherscan.io/address/0xa1E2481a9CD0Cb0447EeB1cbc26F1b3fff3bec20)

Receive users' deposits. Update the ProofVerifier address

[Safe 3-of-4](#)

only deployed on mainnet

Yes

[Bridge

](https://sonicscan.org/address/0x9Ef7629F9B930168b76283AdD7120777b3c895b3)

Claim users' deposits from L1. Update the ProofVerifier address and Token deposit address

only deployed on Sonic

[Safe 3-of-4](#)

Yes

[ValidatorsRegistry

](https://etherscan.io/address/0x72965045A6691E5A74299D1e878f303264D4D910)

update the proof validators

UpdateManager

UpdateManager

No

[TokenPairs

](https://etherscan.io/address/0xf2b1510c2709072C88C5b14db90Ec3b6297193e4)

set ERC20 tokens that can be bridged

[Safe 3-of-4](#)

[Safe 3-of-4](#)

Yes

[ProofVerifier

](https://etherscan.io/address/0x921B147a90Ef738BBb7c2c89D88ea9d8Af3e9306)

validate witness proof about a storage slot value on the other chain

-

-

No

[ExitAdministrator

](https://etherscan.io/address/0x7390251Bf35AA7eA7C196fc4750bd5d6c5918329)

Withdraw tokens if the bridge/chain is down for 14 days

-

only deployed on mainnet

No

3.13. Miscellaneous

Other high-level information regarding the network that is relevant to mention.

- The FeeM (fee monetization) is an interesting strategy for rewarding Dapp developers. Up to 90% of the fees generated by Dapp transactions are sent to them. The FeeM system operates as an oracle collecting the call traces and pairing them with the individual registered projects off-chain. More information can be found [here](#).
- As usual, a private channel of communication will be kept between the Sonic labs and the assigned technical team of the Aave community (e.g. BGD), for any necessary update concerning the network and consequently, Aave on Sonic.

4. Summary

From our analysis, we conclude that Sonic, even if in a pretty early stage, is an acceptable network candidate in regard to technical requirements, with no current hard blocker for the Aave v3 (v3.2, upcoming v3.3) protocol to work properly.

[

Sonic_grades

1920×1729 251 KB

](https://europe1.discourse-cdn.com/flex013/uploads/aave/original/2X/a/af8a95587c6b5d05b13915d19654af5d5ff23293.jpeg)

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.