Following our framework of Aave's infrastructure evaluation and the positive outcome of thetemperature check, we present the analysis of GnosisChain regarding its suitability to deploy an instance of the Aave 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 GnosisChain ecosystem.

When doing the evaluation, we contacted the Gnosis 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 GnosisChain

GnosisChain positions itself as a side chain of Ethereum. Technically, it is an EVM-based layer one network, with PoS (Proof-of-Stake) consensus.

The main difference - besides slightly lagging behind mainnet EIPs - is the dual token model used for consensus (GNO) and gas (xDAI).

2. Our methodology

This report is not trying to be a full analysis of the GnosisChain network but focuses 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 sidechains, 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 follows:

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 2 types of oracles in the case of a network like GnosisChain: prices and PoR (Proof-of-Reserve). 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.

GnosisChain HAS

Chainlink prifce feeds available for the major assets on the network

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

3.1.2. Proof-of-Reserve feeds

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

GnosisChain 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 GnosisChain network can be found athttps://gnosisscan.io/, 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 GnosisChain in this case.

GnosisChain HAS

complete compatibility with go-ethereum. Depending on the node provider there can also be support for non-standard 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.

GnosisChain 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, GnosisChain has 3 types of RPC endpoints:

1. An "official" high-availability public RPC provided by the core devs.
2. Public ones provided by different projects (including one hosted by Gnosis' Core Team).
3. Private ones like QuickNode, Pokt.

You can find a full list of available options here:RPC Providers | Gnosis Chain or on Chainlist.

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.

Given the alignment with the Go-Ethereum node implementation (geth) we checked that:

- The chainId

behavior is appropriate, with the id 100

for GnosisChain not clashing with any other.

- There are no extra opcodes compared with Ethereum.

- There are no extra pre-compiles compared with Ethereum.

Additionally, we have a confirmation from the GnosisChain 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, GnosisChain is transparently supported by the majority of all the chain-agnostic wallets, like Metamask, Ledger, Coinbase Wallet, or Frame.

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.

GnosisChain HAS

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

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

Tenderly supports GnosisChain.

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, GnosisChain is supported onTheGraph, Dune, GoldSky, and others.

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 GnosisChain, 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 is possible to bridge assets via https://omni.gnosischain.com/bridge. Assets bridged are minted as ERC-677.

Regarding the security of the ERC-677 smart contracts for bridged assets, there was an exploit affectingAgave, an Aave v2 fork. While this vector was mitigated in a hard fork of the network, Aave v3 also has improved reentrancy guards to protect against this class of attack vectors.

- Generic messaging.

GnosisChain supports bi-directional generic message passing. This is especially important for Aave, in order to activate cross-chain governance.

In addition to the default bridging mechanism of GnosisChain, there are additional third-party bridges present there like LayerZero or Hyperlane, amongst others.

3.12. Commitment to 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 GnosisChain are no exception.

Apart from the extensive security procedures “native” to GnosisChain or inherited from geth, the GnosisChain 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 GnosisChain.

Finally, we are aware of the commitment of Gnosis to good security practices, 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, GnosisChain is technically a layer one, very similar to Ethereum itself.

Regarding its security model, the approach with GnosisChain is almost the same as Ethereum mainnet with the core difference that the validator requirements are reduced from 32ETH to 1GNO (so it’s a lot cheaper to run a validator).

3.13.1. Centralization points

- The bridge is controlled by a 4-of-8 multisig.
- The bridge governance is controlled by an 8-of-16 multisig.

There is a decentralization roadmap for the bridge, following a similar concept likea.DI, which can be found HERE.

3.13.2. Upgradability strategy and sync with Ethereum

In terms of upgrades and the procedures surrounding them, GnosisChain needs to perform hard forks similar to Ethereum Mainnet.

The GnosisChain team has confirmed that the strategy to sync with Ethereum upgrades is ad-hoc, but they are fully committed to keeping as much sync as possible with Ethereum.

A list of recent hard forks can be found HERE

3.13.3. Security procedures

GnosisChain has an active bounty on Immunefi:

- Up to $2’000’000 on the bridge contracts.
- Up to $50’000$ for the interfaces.

3.13.4. Security audits

A list of the audits of GnosisChain, mainly focused on its bridging infrastructure, can be foundHERE.

An overview of all the infrastructural smart contracts of GnosisChain can be found on theofficial docs.

- wxDAI
- GNO
- Beacon Chain

- Arbitrary message bridge
- xDAI bridge

4. Summary

From our analysis, we conclude that GnosisChain, 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 Ethereum, and a really good maturity, with years running.

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 Polygon or Avalanche.

Similar to other side chains, there is an important degree of centralization on the bridge, 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.

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