BGD. AAVE <> BNB

INFRASTRUCTURE / TECHNICAL

EVALUATION

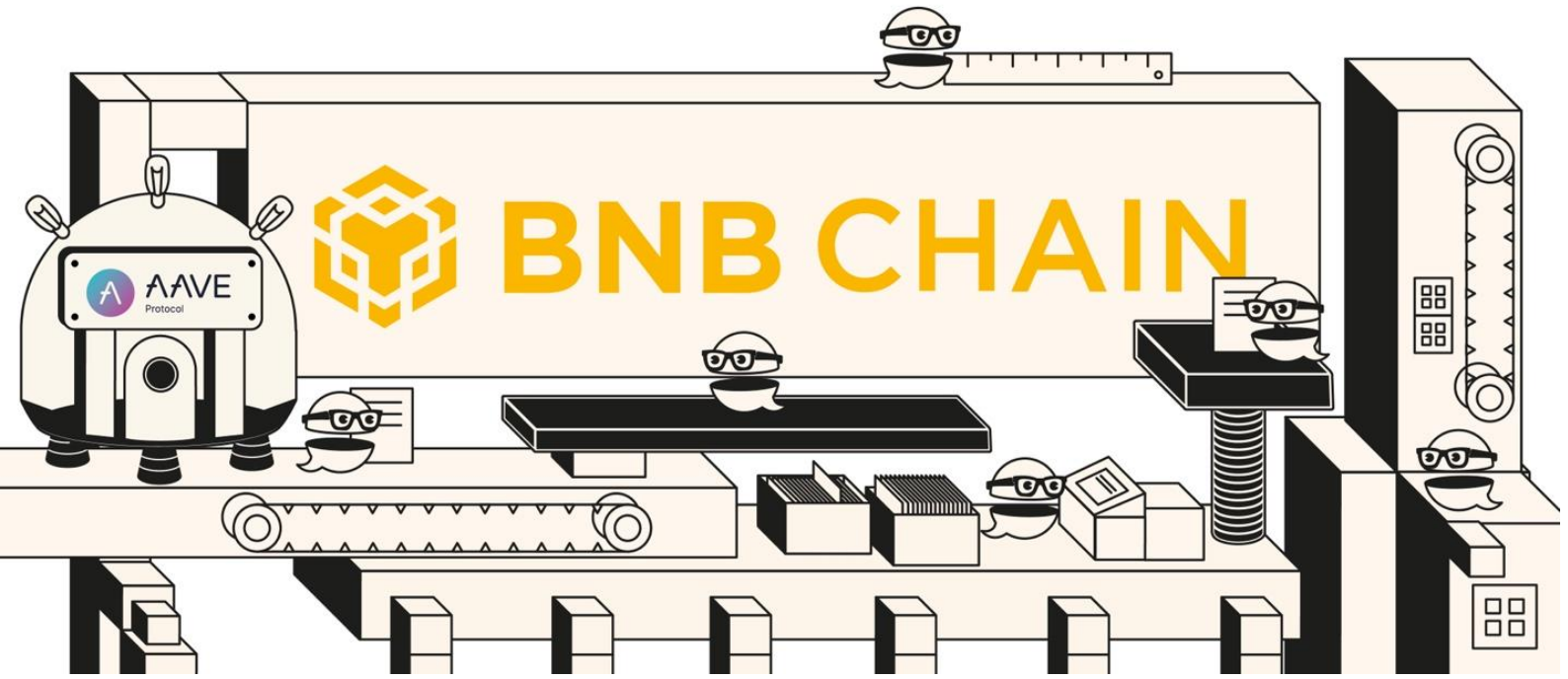


Table of Contents

Introduction

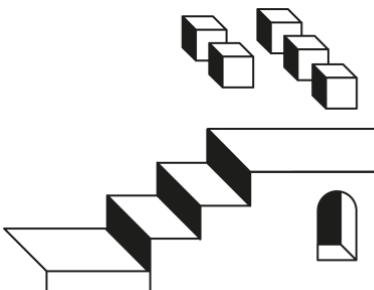
As we published before, we think the Aave community requires a technical/infrastructural analysis of new network candidates to host the liquidity protocol, from an entity like BGD looking for Aave's interest.

Following the positive sentiment poll on Snapshot, this is an analysis of the BNB 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 BNB ecosystem.



Report

1. Introduction to BNB

BNB is a standalone blockchain, with EVM base compatibility. It's a smart-contract-enabled sidechain for the Binance Chain.

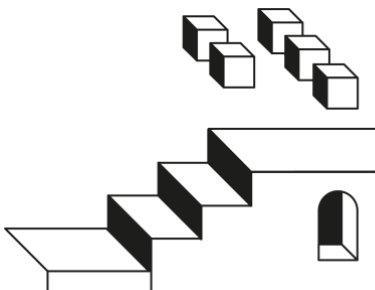
Initially forked from Geth has evolved similarly in some core aspects, but most notably changed the consensus algorithm to PoSA.

2. Our methodology

This report is not trying to be a full analysis of the BNB 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 medium participants on the Aave governance to understand. But 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 2 types of oracles in a standalone blockchain. 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.

BNB chain **HAS** Chainlink price feeds available for the major assets on the network

Additionally, there seem to be some other price feed oracles on the BNB chain, 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. This system is currently running on Avalanche, and the Aave community has approved starting to apply it for bridged assets, so directly related to a case like the BNB chain.

BNB chain **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:

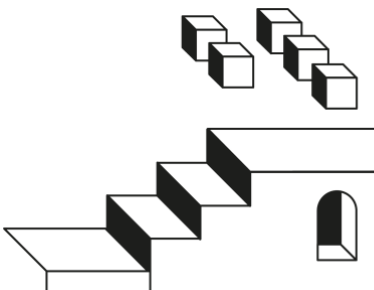
1. Verifiable smart contracts code visualization.
2. Read/write interface with smart contracts.
3. Basic data analysis tool for misc aspects like token holders.

The official blockchain explorer of the BNB network can be found at https://bscscan.com/, and it is an instance of Etherscan.

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 BNB chain in this case.

BNB chain **HAS** complete compatibility, dependent on the RPC there is also support for non-standard specific 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.

BNB chain 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, the BNB chain has 3 types of RPC endpoints:

1. “Official” public ones provided by the Binance infrastructure team on https://docs.bscscan.com/misc-tools-and-utilities/public-rpc-nodes like https://bsc-dataseed.binance.org/
2. Different public ones including POKT
3. Private ones by QuickNode and NODEREAL

Given the number of public providers and QuickNode support, we think the current options might be sufficient, especially as the BNB chain is an established blockchain already serving a huge amount of users.

The BNB team confirmed that INFURA support is coming soon.

The public RPC providers are rate limited at 5k requests per 5 minutes per ip, so should likely be suitable for a fallback.

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), EVM opcodes, native account abstraction/meta-transactions, chainId definition out of the norm, etc.

- The BNB chain has 4 custom pre-compiles 100-103 for handling BC(Binance beacon chain) and BSC(Binance smart chain / BNB chain) cross-chain which should not affect the protocol.
- The chainId behavior is appropriate, with the id 56 for the BNB chain not clashing with any other.
- BNB chain currently does not implement EIP 1559, 2929, 2930, and 2718 but efforts to align are ongoing.

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, the BNB chain is transparently supported by the majority of all the chain-agnostic wallets, like Metamask, Ledger, Coinbase Wallet, or Frame.

The most popular smart contract wallets (e.g. Safe) also support the BNB chain.

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, depending 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.

BNB chain **HAS** an instance of the Gnosis Safe contracts on-chain, using the official user interface and server infrastructure: https://app.safe.global/welcome?chain=bnb

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 the BNB chain with Foundry. Given its EVM compatibility, it should be perfectly doable with Hardhat too.

Tenderly has integrated the BNB chain (as BSC chain).

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, the BNB chain is supported on TheGraph.

BNB chain is also supported by Dune.

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.

It's important to highlight that the "official bridge" only allows permissioned bridging from BC <-> BNB, it does not support ETHEREUM <-> BNB. However, there are trusted bridges like layer zero which allow permissionless bridging from ETHEREUM to BNB chain.

There are 2 types of bridging affecting Aave: assets and generic messaging. In the case of the BNB chain, the state of these 2 types is as follows:

- **Assets**. Regarding the security of the BEP20 smart contracts for bridged assets (and the BNB token itself), if/when the community decides to deploy on the BNB chain and with which assets, a more thoughtful assessment of the code should be done, following the previous listing cases. From our side, we have checked assets like AAVE, USDC, and USDT, and all of them share or same or really similar codebase: a simple BEP20 version, with burn/mint capabilities by an entity defined as "bridge".
  It is important to note though, that AAVE and USDC are behind an upgradability proxy administered by an EOA (tagged as *Binance deployer address*). We informed the BNB chain team, which confirmed us their security department will look for improvements.
- **Generic messaging**. This is especially important for Aave, in order to activate cross-chain governance. As stated before, there's no native bridge but there are multiple other bridge solutions with generic messaging support.

There are additional bridges like LayerZero, Celer, AnySwap, Wormhole, Hyperlane, and more.

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 BNB chain are no exception.

We have checked and found the following:

- There is **no** ongoing program on Immunify at this moment for the BNB chain itself
- There is an ongoing bug bounty program for the BNB chain on bugcrowd
- On the prevention side, there's a community initiative https://www.avengerdao.org/ with tooling to prevent hacks.
- If an incident would happen the BNB team confirmed to us 24/7 availability.
- A private channel of communication will be kept between the BNB team and the assigned technical team of the Aave community (e.g. BGD), for any necessary update concerning the network and consequently, Aave on BNB.

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, the BNB chain is technically an independent blockchain but acts as a side-chain of the Binance beacon chain.

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

3.13.1. Transactions flow

Being a geth fork with no changes to transaction flow, it's exactly the same as on Ethereum.

3.13.2. Storage mechanism: Greenfield

Greenfield is a decentralized storage mechanism more similar to s3.

From our external perspective, Greenfield seems to be in quite an early stage and while being an interesting development it isn't very relevant for the Aave ecosystem.

3.13.3. Upgradeability and control model

BNB chain network upgrades via hard forks are coordinated by the validators via POSa. In addition, there's a governance infrastructure to adjust certain protocol parameters, without requiring a hard fork.

3.13.4. Security audits

The Binance Team assured us that all code changes are audited. The last round of audits was performed by Verichains, TrailOfBits, and Certik.

The audits are currently closed source and therefore cannot be independently validated.

3.13.4. Decentralization

BSC is currently having **50** validators out of which **29** are active (selected every 24h). For more information on the current validators list: BNB Chain | Binance Staking and for the current selection mechanism: BEPs/BEP131.md at master · bnb-chain/BEPs · GitHub

A good overview of all the infrastructural smart contracts of the BNB chain can be found HERE.

4. Summary


ORACLE INFRASTRUCTURE
ON-CHAIN MULTI-SIGNATURE INFRASTRUCTURE
BLOCKCHAIN EXPLORER
TRANSACTIONS SIMULATION INFRASTRUCTURE (FORK)
COMPATIBILITY WITH ETHEREUM RPC STANDARD.
CHAIN DATA/INDEXING SOLUTIONS
COMPATIBILITY WITH ETHEREUM ACCOUNT FORMAT (ADDRESSES)
BRIDGING INFRASTRUCTURE: ASSETS, MESSAGES
RPC PUBLIC ENDPOINTS AND PROVIDERS
COMMITMENT IN SECURITY-INCIDENTS
CUSTOM BEHAVIOR (LACK OF) OF THE EXECUTION LAYER
NETWORK SECURITY/ TECHNICAL MODEL
SUPPORT OF WALLET PROVIDERS

From our analysis, we conclude that the BNB chain, is an acceptable network candidate in regard to technical requirements, with no current hard blocker for the Aave v3 protocol to work properly.

Centralization and bridged assets are the weaker aspects of the infrastructure, while everything else has good results in our evaluation.

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.

We think the aspects the community should evaluate more carefully before making a decision are those related to the network's security. With only 53 validators and a high barrier of entry for new validators, BNB is placed on the lower end of the decentralization spectrum. With no native permissionless bridge for Binance-pegged-assets, there is also a high degree of centralization.

It is up to the community to decide if the risks derived from this centralization are worth it, combined with any other considerations of no technical nature.