TL;DR

BGD has started the integration of Chainlink's Proof-of-Reserve into Aave, initially targeting the protection over "bridged assets" in non-Ethereum networks on which Chainlink can provide Proof-of-Reserve feeds.

Context

The approach of the Aave community towards deployments of the protocol on other networks apart from Ethereum has always been really proactive, starting with Polygon and Avalanche during the Aave v2 phase; following with Optimism, Arbitrum, Fantom, and Harmony during the Aave v3 phase.

From a high-level perspective, this comes as usual with a risk/reward equilibrium associated. Every new network has a quite different user base and count, for who Aave becomes available. At the same time, expansion to a new chain also translates into new risks of different natures, both economical and technical.

A sub-set of those risks is currently associated with the nature of some of the assets listed on non-Ethereum networks: bridged assets.

Bridged assets are representations of a base asset in chain A (usually Ethereum), in chain B (e.g. Avalanche), where they get listed on Aave. For example, WETH.e, listed on Aave v3/v2 Avalanche, is a representation of the WETH locked in a "bridge" smart contract on Ethereum.

Even if in certain cases there is the assumption that bridged assets are fully equivalent to the base asset locked in another network, technically this is not true, as they are completely different smart contracts, with different security and market profile.

It is possible to argue that the nature of these bridged assets, together with the assumptions made to make the pool functional in the networks, is one of the main sources of technical risk for those Aave deployments.

Lately, the Aave community has already seen this kind of risk becoming a meaningful event in the case of Aave v3 Harmony, with the Harmony bridge getting exploited, and the Aave v3 Harmony pool consequently getting affected, as described on this thread

The community also just had important governance votes on the possibility of the Safety Module covering different Aave v2 deployments:

- Aave Arc https://snapshot.org/#/aave.eth/proposal/bafkreieeyh6pbqwhgryo6v67oxlmnfhaptrgkc3u7y6bvz2y3jdkxgrrh4

- Aave v2 Polygon
  https://snapshot.org/#/aave.eth/proposal/0x7da4985b2d5b1cbe6bbc0992d5c86030cedef2013487e4b53b4244c315c90155

- Aave v2 Avalanche
  https://snapshot.org/#/aave.eth/proposal/bafkreiba2pdfwoesezgpedf37bjfgadxmaigavoulek5wayqb7f2tz6byy

For obvious reasons, minimizing any kind of technical risk should be a high priority of the community if the decision is to apply the mechanism of the Safety Module on deployments on which bridged assets are one of the main risk components.

Since the Harmony incident, from BGD we have been trying to move forward what we think is an important priority for the community, even if still a technology rolling up: Chainlink Proof-of-Reserve.

What is Proof-of-Reserve?

Proof-of-Reserve is a system by Chainlink that, as described HERE, allows for reliable monitoring of reserve assets, and usage of that data feed directly on-chain.

Until now, Proof-of-Reserve has been oriented for assets like fiat-backed stablecoins, but also to an initial set of "wrapped" assets like WBTC, whose reserves are funds stored in a different blockchain/network (Bitcoin in the case of WBTC).

BGD has been in discussions with Chainlink for some time about the design and possibility of expanding Proof-of-Reserve to other bridged assets, and we think now the system is developed enough to start its integration on some of the deployments of the Aave protocol, raising the bar of assurance for bridged assets.

Aave <> Chainlink Proof-of-Reserve integration

From our perspective, this integration has high priority enough to start the process as soon as possible, and with a progressive approach.

We will be sharing more details during the following weeks, but the first target will be the activation of a Proof-of-Reserve mechanism for all the networks on which the technology of Chainlink is available, affecting bridged assets.

This will be done via a system assuming perfect backing of all the bridged assets on a specific Aave deployment, in terms of

Proof-of-Reserve: if any anomaly is detected on the Proof-of-Reserve of 1 single asset, the system will try to apply the highest possible protections on the pool. We will be revealing the specifics of the implementation in the following 1-2 weeks.

In parallel, we are working in more sophisticated mechanism for usage of Proof-of-Reserve, but we think this basic mechanism can give important protection versus the complexity it introduces, and the cost impact for the Aave users.