TL;DR

After doing a deep technical analysis of the Aave v2 Ethereum upgrade to v3, we have noticed important tradeoffs that have to be made going along this upgrade path.

We would like to open a community discussion regarding the upgrade plan for a new deployment of Aave v3 on Ethereum, keeping Aave v2 Ethereum running, without upgrading.

Context

Approximately six months ago, on March 2022, Aave v3 was deployed following a multi-chain strategy: Polygon, Avalanche, Arbitrum, Optimism, Fantom, and Harmony. On some of those networks, the presence of Aave was new (Arbitrum, Optimism, Fantom, Harmony); while on others (Polygon, Avalanche), there were already existing deployments of Aave v2.

This launch process was community-coordinated:

1. The Aave genesis team presented the development of Aave v3 to the community.

2. The community signaled a clear approval on the forum, given the innovation and technical superiority of v3 vs v2. Licensing of the protocol was discussed and voted on.

3. The communities of the different networks candidates for v3 presented their proposals for Aave to approve deployments there. E.g. Aave v3 on Avalanche HERE, Aave v3 on Polygon HERE, and so on.

4. Deployment was performed on the networks decided by the community.

On the proposals of deployments on networks where Aave v2 already existed (Polygon, Avalanche), a topic that appeared was if the route should be to upgrade the smart contracts of v2 to v3 (given that it was theoretically possible to do it by modifying the v3 implementation) or to simply do a "clean" new deployment of Aave v3, and let v2 and v3 live together on those networks.

After some discussion and arguments in favor of a new deployment like THIS, that was the decision for Polygon and Avalanche. And so Aave v3 Polygon and Aave v2 Avalanche were born.

But something that was implicitly derived from different threads of discussions was that Aave v2 Ethereum, being the biggest pool of all on v2, should go through an upgrade of its smart contracts, and consequently, don't deploy a new Aave v3 Ethereum pool, but waiting for the upgrade to be implemented. Aspects that were taken into consideration were especially the Ethereum network congestion (high cost to migrate), additional costs of managing the migration, and also that, superficially, it seemed the technical upgrade process would be pretty seamless.

The goals of an Aave v2 to v3 Ethereum upgrade

During the last months, one of the tasks to tackle by BGD on Aave has been the implementation/adaptation of the Aave v3 codebase to be able to upgrade Aave v2 Ethereum with it. We knew it was possible, even if challenging (especially in the testing phase), given the high stakes of such a "hot" upgrade of a production system, with an order of billions within.

We set ourselves certain goals to achieve with this upgrade:

- On-chain integrators (other smart contracts) of v2 should not be affected

. This means that all addresses of the protocol (Pool, Addresses Provider, aTokens, debt tokens, etc) would remain the same. In addition, all interfaces would remain completely backward compatible, with only additions for the new v3 features.

- Off-chain integrators should not be affected.

This means that, apart from the previous points of addresses and interfaces, also all events will remain compatible; again, only with new events added "on top" of the new features.

- Introduce as less tech overhead as possible, but knowing there would be.

Currently giving technical maintenance to the Aave liquidity protocol means supporting 4 different shapes of systems in production, across 10 separate deployments: Aave v1, Aave v2 Ethereum, Aave v2 Avalanche/Polygon (slightly different from Ethereum), and all instances of Aave v3.

Even if this variety of deployments across networks and protocol versions gives a lot of value to Aave, it also introduces technical overhead (together with important DAO coordination). So our goal was to have a v2→v3 version of the codebase as close as possible to v3.

To achieve those goals, 3 main types of resources were required:

- Engineering itself of a party knowing really deep both Aave v2 and Aave v3 (BGD).

- Implementation of an ad-hoc test suite, specifically targeting a "hot" upgrade like this: both v2 and v3 have extensive test suites, but the implementation of this upgrade would lead to something in the middle, which should be itself tested.

- Extensive external security procedures. Mainly adaptation of Certora rules (from v2/v3) and both code and upgrade procedures audit by SigmaPrime.

And so, BGD started working on executing and coordinating.

The challenges

As with any development, but especially with one of this magnitude, we did a deep analysis of what would be required for this v2→v3 upgrade. Initially, we identified 2 efforts that could be split into 2 sequential phases:

- Phase I, including a "light" upgrade of the LendingPool

smart contract, together with deployment of the so-called interest rate strategies smart contracts for all assets listed on Aave v2 (re-using part of them between assets).

- Phase II, including a big upgrade of all other components, which should be done atomically in 1 governance proposal. This would include more changes on the LendingPool

, aToken smart contracts, and in summary, almost all components of Aave v2 Ethereum.

Phase I is ready in practice, but during its development, and already looking to Phase II, we noticed some concerning aspects.

- It is not trivial at all to make the v3 events compatible with v2, with some changes causing most likely problems in the off-chain infrastructure of integrators

. These problems of course can be solved by supporting these integrators, but the effort on their side could be important.

- Address and interface compatibility is achievable; strictly nothing would be "broken" for anybody using Aave from a smart contracts perspective

. But the integration of the new v3 features for this v2→v3 version will be certainly different from the integration of v2, and different from the integration of v3. This means that if somebody has let's say Aave v2 Ethereum and Aave v3 Avalanche integrated already, the integration of the v2→v3 upgraded version will be different.

- Security procedures on this are lengthy.

Apart from the BGD testing work itself, we estimate at minimum 1-1.5 months of SigmaPrime, and weeks on the Certora side; given that there is not really a precedent of a "hot" upgrade of this caliber on a DeFi protocol.

- Some assets listed have custom implementations, like AMPL or stETH.

The upgrade path requires treating them ad-hoc, which adds complexity.

- Clearly, this v2→v3 version of the protocol will not be (implementation/maintenance wise) nor v2, neither v3.

What this means is that, whenever a change/improvement is required across all v3 instances, this pool will require in some cases extra integration.

An extensive and more technical analysis of the points summarised before can be found on the following document we produced

https://wheat-guardian-dfc.notion.site/Aave-v3-Ethereum-Technical-analysis-of-Aave-v2-Upgrade-1ba8df0a7b0d4c49bfa9a86d451d88c2

Given that we care about our work being really productive to the Aave community and we really value others' resources like security time, we started wondering how much sense it actually makes to do this upgrade versus doing a new deployment of Aave v3 on Ethereum, following the same approach as on Polygon and Avalanche, with both v2 and v3 living together in parallel.

New Deployment vs Upgrade. Key aspects

Deployment of a new Aave v3 Ethereum

- A new version of Aave v3 on Ethereum can be quickly released

. The codebase is already prepared for network-agnostic deployment, so only technicalities like the oracle denomination should be evaluated.

- No security procedures are needed

. Aave v3 is audited and formally verified, nothing else is required if a new pool is deployed on Ethereum. This means that security resources of the community (SigmaPrime, Certora) can be re-directed to other projects, and there are plenty of them coming not only from BGD.

- The number of development resources (BGD) is significantly reduced, and will be allocated to other projects in the pipeline

: generalized solution for cross-chain governance, Aave governance v3, different improvements on Aave v3, GHO, etc.

- It gives the possibility for the community to reassess the risk configuration of the assets currently listed on v2

. With an upgrade v2→v3, everything will remain the same as currently, that is not possible. It is important to highlight that this also allows for the listing of for example fewer Aave-custom implementations for some assets, like wstETH, instead of the current stETH version listed on v2.

- Integration of Aave v3 Ethereum becomes plug-and-play for all projects who are already connected to other Aave v3 instances

. Major projects around the ecosystem are fully compatible with Aave v3 (e.g. Dune), so this approach will make their integration straightforward.

- GHO's first facilitator can be a "fresh" instance of Aave v3

, which makes things simpler for testing and simulation purposes pre-deployment.

- For the future, a single Aave v3 codebase

. This means less maintenance overhead, and the possibility to do batch updates on all networks, with the same code. This means reducing future technical debt in the future, which translates to fewer operational expenses by the DAO.

- Aave v2 will not be dismissed, or deprecated anyhow.

Aave v2 is a really solid protocol, working well and extensively battle-tested. Therefore, there is no need to anyhow declare it as dismissed, only not doing incremental additions, like new asset listings (that will go to Aave v3 Ethereum, with even better risk assurances).

- A pure Aave v3 deployment will be cheaper gas-wise.

Aave v3 introduces important gas optimizations, which become quite important in an environment like the Ethereum network. An upgrade of the contracts would still keep those optimizations, but there would be some sacrifices on them, mainly because of compatibility with the previous storage layout (e.g. "live" user positions on Aave v2).

Upgrade of v2 smart contracts

- "Automatic" migration of positions. Users of Aave v2 would automatically become users of v3, as the addresses of the v2 smart contracts will be exactly the same as v3.

This means no transaction or migration procedure is required from the Aave v2 Ethereum users.

- Some integrations will just work out of the box from the existing v2.

Especially those integrations on the smart contracts layer will just work without doing major changes to their on-chain infrastructure.

- Some off-chain integration will also work without changes.

Most probably not so many in this case, but those that only touch certain parts of the system could work potentially without change.

- No liquidity segregation

. If doing an upgrade, all the Aave available liquidity at the moment will remain exactly the same. While with a new deployment, technically the Aave v2 liquidity will be separated from the liquidity of the new Aave v3. It is important to highlight that everything will still be Aave liquidity, and the access to it by integrators/users will work almost exactly the same way.

How would it look the procedure to deploy Aave v3 Ethereum?

1. The community discusses on the forum the path to go.

2. A Snapshot is voted on for Aave to make a decision. Assuming positive result on deployment a new Aave v3 Ethereum for example's sake. The Aave community authorizes BGD to deploy.

3. Discussion on the community for all initial configurations of the Aave v3 Ethereum. Including the initial set of listings and all other protocol parameters.

4. In parallel with 3), some improvements are to be applied to all v3 instances, including an audit pre-deployment.

5. Smart contracts deployed: everything not active, paused.

6. Governance proposal for the community to activate the pool.

BGD conclusion and next steps

The duty of BGD with the Aave community is, apart from delivery on development, to give a critical/expert point of view of topics related to the tech of the Aave ecosystem.

Our opinion is that the advantages of doing a new deployment of an Aave v3 Ethereum holistically and importantly outweigh those of upgrading the current Aave v2 smart contracts.

That being said, our ethos is to be always transparent with the community, and submit these types of important topics to the discussion here on the forum; for the community to actually do a decision, using our analysis as a base.

We ask everybody to participate in the discussion of this important topic, supporting one direction or the other. After some days, we will also create a Snapshot vote for the community to decide on how to proceed.

Links

- https://github.com/bgd-labs/v2-mainnet-interest-rates-upgrade
- https://github.com/aave/aave-v3-core
- https://github.com/aave/aave-v3-periphery
- https://governance.aave.com/t/aave-bored-ghosts-developing-bgd/7527
- https://github.com/aave/protocol-v2