TL;DR

Technical analysis for the Aave community on why the upcoming transition of Ethereum to Proof-of-Stake (The Merge) should not affect Aave's systems.

Ethereum Proof-of-Work → Ethereum Proof-of-Stake

As it is well-known across the Ethereum community, for a pretty long time, the teams involved in Ethereum consensus and execution layers have been working on what is de-facto considered the next stage of the Ethereum network: a transition from a proof-of-work mechanism for consensus, based on computational power; to a proof-of-stake mechanism, based on blocks' validation involving staking of ETH.

In December 2020, the so-called Beacon Chain was launched, representing the new consensus layer to be used on Ethereum Proof-of-Stake, allowing deposits (staking) of ETH for the sake of participating in the new model of blocks' validation. This layer has been running independently from Ethereum mainnet until now, as a way of testing over time so critical system.

The Merge is factually the connection of the running Beacon Chain to Ethereum mainnet, replacing the current Proof-of-Work mechanism to validate blocks. It will be composed of 2 Ethereum upgrades: Bellatrix

, affecting the Beacon Chain; and Paris

, affecting the current execution layer processing Ethereum transactions, and in consequence, the most important from Aave's perspective.

The last testing phase of The Merge, involving an upgrade of the Goerli testnet is programmed for this week, with the Ethereum mainnet upgrade to be happening soon after.

How does the Merge/Paris upgrade affect Aave?

Even if critical from a high-level perspective of the Ethereum network, for our analysis, The Merge/Paris upgrade should affect the Aave system really slightly, with no immediate action needed. This is because the upgrade has been designed to be the less disruptive possible for running applications on Ethereum.

For a full explanation of how The Merge affects the application layer, the Ethereum Foundation has published a detailed analysis HERE.

Regarding the different points where Aave could be affected:

- Block structure.

AAVE IS NOT AFFECTED.

In general, the upgrade keeps all the previous fields on the block header, but the Aave smart contracts don't really depend on the block header's structures at the moment, given that techniques like storage proofs are not used.

- Block time.

ONLY AAVE GOVERNANCE IS SLIGHTLY AFFECTED.

In practice, block slots will become shorter in duration, from a variable time of ~13.5s to a fixed time of 12s (with the exception of missing blocks, which are supposed to happen only 1% of the time). Aave systems, like the liquidity pools, don't do calculations based on blocks, but in seconds, so those don't get affected. However, certain governance parameters, like the voting duration are defined in blocks, so in practice, they will be slightly shorter. This will cause mainly voting time to be slightly lower than 3 days and queuing time slightly lower than 1 day. We don't think this is an immediate concern, but we suggest the community re-evaluate those parameters down the line, to adjust to the 12s block slot time.

- Opcodes' changes.

AAVE IS NOT AFFECTED.

Only blockhash and difficulty will be affected, but the Aave smart contracts don't depend on those.

- Sources of on-chain randomness.

AAVE IS NOT AFFECTED

. There is no mechanism on the Aave smart contracts operating with randomness.

- New concepts of safe head and finalized blocks.

AAVE COULD BE SLIGHTLY AFFECTED, BUT NOT ON SMART CONTRACTS.

2 new statuses are introduced into the “confirmation” lifetime of proposals. This could disrupt certain off-chain infrastructure of Aave (e.g. Aave decentralized UI), but we expect the Web3 libraries to abstract this behavior, keeping complete backward compatibility.

So, from a technical/operational perspective, Aave only gets slightly affected on the duration of on-chain governance mechanisms and potentially on the Aave UI.

But what if there is a fork of the Ethereum chain?

Given the criticality and change of paradigm on the consensus layer of Ethereum, there are some rumors circulating about a potential fork on The Merge, keeping a parallel Ethereum running with Proof-of-Work consensus.

There is not really much substance about this fork, so in practice, The Merge should happen as any other previous upgrade of Ethereum. Aspects that support Aave transitioning transparently with Ethereum to the application layer of Proof-of-Stake (and only there) are:

- From the perspective of an application layer like Aave, The Merge is just another update similar to Gray Glacier, or any other of the previous. It is true that the consensus layer changes, and this is an important paradigm change, but there is not much reason to think that a Proof-of-Work Ethereum fork would get more traction than the Proof-of-Stake, and be considered canonical.
- The Aave protocol doesn’t live in complete isolation on a network like Ethereum, it communicates with other systems, like the assets listed themselves, other liquidity venues like DEXes, oracle systems like Chainlink, wallet providers, etc. We have spoken with Chainlink and got confirmation that their stand will be naturally with Ethereum Proof-of-Stake, the same as other liquidity venues like Parawap. Without any external liquidity and without functional oracles, the Aave system will not really be functional.
- The Beacon chain, even if not even connected to the consensus layer of Ethereum, has been running actively for almost 2 years. There are thousands of validators, and even completely new products and systems building on the future Proof-of-Stake, like Lido and their stETH asset.
- All major Ethereum node clients with a long history (and new ones) are preparing their software for The Merge, so seems unnatural for a movement running an outdated version of that software to get major traction.
- It is expected that centralized stablecoins issuers will fully support The Merge transition. On Aave v2 Ethereum, this includes USDC, USDT, TUSD, BUSD, PAX, GUSD, and USDP.
- There are other assets (especially listed on Aave v2 Ethereum) that don’t have any direct reason for existence on non-Proof-of-Stake Ethereum post-upgrade. This includes DAI, WBTC and, in general, the majority of other assets listed on Aave v2 Ethereum, considering that apart from the asset, whole systems are built on top of them (e.g. governance). Specially stETH, of which there is ~$1.4B deposited on Aave, and created precisely around the transition of Ethereum to Proof-of-Stake and its staking mechanism.
- Aave has supported (and getting supported) the Ethereum ecosystem since its inception with Aave v1. The Aave community and ethos heavily overlap with Ethereum one. It seems natural to follow the approach of supporting the Ethereum community direction.

We think those previous points are strong enough to consider only as Ethereum the post-merge Ethereum with Proof-of-Stake. Given the lack of functioning oracles and liquidity issues on both centralized and decentralized assets, the Aave system will not work properly on any potential Proof-of-Work fork.

Conclusion

The Merge is scheduled for its last phase next week, with the Bellatrix and Paris upgrades happening on the Goerli test network.

Soon after, The Merge will happen on Ethereum mainnet, and from our analysis:

- No smart contract related to the liquidity protocol will get affected.
- Aave governance voting and queueing duration will be slightly lower than 3 and 1 days, it can be updated in one of the upcoming governance proposals, but not critical.
- There could (but should not) be some small adaptations needed for the Aave UI.
- As always, Aave will only work properly on the adopted majority chain, in this case, Ethereum PoS (chainId == 1). So any potential forks should be initially ignored.

- The Aave decentralized UI should only consider as Ethereum mainnet, the post-merge Ethereum Proof-of-Stake. If any user decides to interact directly with Aave smart contracts on any fork, should be under their own responsibility.
- It is possible that there will be more volatility and bridge activity from/to Ethereum. This topic should be further evaluated by other entities working with the community, like Gauntlet. BGD will monitor the situation, for if any technical reaction (e.g. via governance proposal) would be necessary.

We encourage the community to use this thread for if there is any question of technical nature about the topic.