TL;DR

To support Aave's multichain mission and expand cross-chain experiences, we propose the deployment of Aave V3 to zkSync 2.0 on behalf of the community.

The zkSync team will submit a snapshot to launch Aave V3 on ZkSync V2 testnet, and thereafter another snapshot for mainnet (when the criteria for DEX liquidity and other items are met).

- zkSync ecosystem has over 200 projects committed to launching on mainnet, including top DeFi protocols, infrastructure, on/off ramps, etc.
- Deploying on zkSync will onboard new users & increase user activity on Aave by decreasing costs compared to Ethereum without security degradation
- zkSync shares Ethereum's ethos as a free open-source project with a commitment to personal sovereignty, decentralization and community ownership

We welcome feedback from the community on the proposal, including suggestions on how it can be improved.

UPDATE

Snapshot live: VOTE HERE

Start date

Oct 30, 2022, 3:00 PM CET

End date

Nov 2, 2022, 3:00 PM CET

About zkSync

zkSync 2.0 is a ZK Rollup that supports generalized EVM compatibility for the Ethereum blockchain. The primary benefit of zkSync 2.0 is that developers who have created EVM dApps can port to zkSync 2.0 effortlessly and realize significantly lower gas fees and more transactions per second without compromising on security.

zkSync 2.0 is a significant leap forward in Layer 2 technologies with long awaited improvements and benefits for Ethereum developers:

- EVM Compatible - supporting generalized EVM smart contracts on a ZK rollup making it easy to deploy existing dApps
- ToolChain Compatible - able to port smart contracts with existing tools
- Ethos Compatible - aligned with the ethos of decentralization and open-source
- Certainty - using zero knowledge proofs offering certainty of security not probability
- Future Proof - ecosystem partners that adopt zkSync 2.0 now will enjoy all future improvements without the need to change their code

There is broad consensus that ZK rollups are the endgame for scaling Ethereum. zkSync's EVM compatibility, ease of use, and composability will accelerate developer and retail adoption. Top researchers including Vitalik Buterin recognize ZK rollups as the long term scaling solution.

Security & Bridges

ZK rollups are the most secure scalability solution available today as they rely purely on math to fully inherit the security of Ethereum. There is a general L1<>L2 communication bridge which will support arbitrary message passing and secured by validity proof and Ethereum consensus.

Bridge validators can't pass an incorrect message or change the content, the worst case would be to censor everyone. Importantly, we'll be building out additional safety functionality and monitoring off & on-chain activity.

Security is top of mind for zkSync. We are currently working with tier-1 auditors for zkSync 2.0 and specifically in the review process for the bridge code. Audits will be conducted before each major upgrade. Besides audits, we offer a substantial bug bounty program.

Proposal

There's significant value in Aave being available on an EVM compatible ZK rollup. Deploying early on zkSync helps solidify Aave's place as the number one liquidity market and thought leader.

Furthermore, it will help grow a large list of projects that can be built on Aave V3. Established projects like Argent, Curve, 1inch and Yearn have committed to launch along with over 200 more projects and big infrastructure players like Chainlink, The Graph, Gnosis are supporting the ecosystem.

Additionally, growing the public smart contract libraries interfacing and using Aave v3 codebase will solidify Aave's influence in the Ethereum ecosystem which is moving on to ZK rollups. There are already a number of projects committed to mainnet deployment that require Aave to integrate.

While the zkSync ecosystem is already experiencing very fast growth, the team is planning programs to attract and fund innovative projects and research partners to accelerate the network's adoption and in turn, top protocols usage (in particular Aave's).

Timeline

zkSync has been on testnet since February 2022 and plans to launch mainnet late October. A timely assessment of the deployment of Aave v3 code to zkSync is important: our team has already tested the smart contract library (mostly key ones) it was compiling and looked like it was working fine.

Proposal Stages:

1. The zkSync team will first submit a snapshot for testnet deployment, following the community guidelines.
2. Then when the time comes, another snapshot for mainnet (when the criteria for DEX liquidity and other items are met).

References

- Matter Labs Github: Matter Labs · GitHub
- zkSync 2.0 Testnet Docs: zkSync Documentation | zkSync — Accelerating the mass adoption of crypto for personal sovereignty
- Blog Posts: https://blog.matter-labs.io/
- zkSync Mainnet Alpha Registration: form

Technicalities

- Solidity/Vyper support; recommended to use ^0.8.0 and Vyper ^0.3.3
- RPC is public: We fully support the Ethereum JSON API, with some additions for L2-level features.
- The Graph is currently indexing zkSync v1 and v2
- Covalent available immediately after mainnet
- Working on all other plugins (ape, founders, remix, truffle, tenderly)
- Chainlink finalising, deploying shortly after mainnet

Audits in progress with multiple tier 1 auditors andBug Bounty Program | zkSync Documentation

Conclusion

zkEVM rollups are the most eagerly anticipated innovation to the Ethereum community after the merge, and zkSync is positioned as a pioneer & at the forefront of making this a reality. Our commitment to security and the safety of our users is absolutely paramount, and we have taken no shortcuts in ensuring the utmost quality controls for this.

zkSync believes our current and future infrastructure solution will prove itself to be the most robust and reliable solution for a market like Aave, and as such is ready to onboard Aave to its ecosystem and looks forward to the opportunity to build a long-term, sustainable, and mutually-beneficial relationship.