Multi-point KZG Proof Verification for the EVM

protocolwhisper - Invisible Garden 2025

Why?

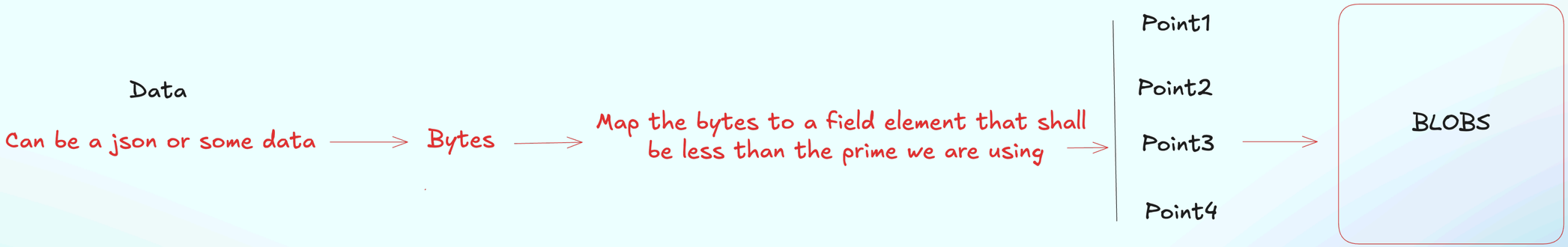
- At the state we are right now if we want to evaluate that some data existed in the blob we will need to call the **KZG point evaluation precompile** that has a fixed price of 50k per call

- As the name states we are only doing one point evaluation but what if we want to evaluate multiple points (multiple data) we will have to pay the fixed price for each call

Scope of this

- Implement the algorithm inside revm (Rust evm) this is used in clients as Reth (Rust on Ethereal)
- Implement the algorithm on chain and do benchmarking to prove the gas we are saving for multiple points
- There was a research of this on the bn254 curve with great results but in this case will be for the bls12381 since it was introduced in Proto-Danksharding

From blobs to data



Explanation : https://github.com/protocolwhisper/arg25-Projects

Blockers

Understanding the notation for the pairing equation in the EVM

$$e(P - Y, -G_2) \cdot e(\text{proof}, x - z) = 1$$

$$e(C, g) = e(C_{\psi_s}, g^{\alpha - s}) \cdot e(g^{\phi(s)}, g)$$

References

- Boneh, D., & Boyen, X. (2010). Short signatures without random oracles. In Advances in Cryptology – ASIACRYPT 2010 (Vol. 6477, pp. 41–55). Springer. https://www.iacr.org/archive/asiacrypt2010/6477178/6477178.pdf
- Boneh, D., Eskandarian, S., Grewal, G. S., & Yeo, K. (2023). Verkle trees: Efficient, verifiable data structures for stateless blockchains. IACR Cryptology ePrint Archive, 2023(033). https://eprint.iacr.org/2023/033.pdf
- Buterin, V. (2020, August 16). Multi-point KZG proof verification in the EVM [Discussion post]. Ethereum Research. https://ethresear.ch/t/multi-point-kzg-proof-verification-in-the-evm/7706
- Buterin, V., & the Ethereum Foundation. (2023). EIP-4844: Shard blob transactions. Ethereum Improvement Proposals. https://eips.ethereum.org/EIPS/eip-4844