Proposal: Allow Access to L1 Block Hash on Arbitrum

Hello everyone,

I'd like to discuss here a proposal from theArbitrum Forum initiated by @zemse

regarding the integration of L1 block hash access on Arbitrum.

This proposal has significant implications for the security and functionality of cross-chain applications.

Context:

The proposal suggests integrating the L1 block hash directly into Arbitrum's block header and enabling access through a precompile or opcode. This would align Arbitrum with other Layer 2 solutions like the Optimism Stack, which already implements such feature. The Optimism Stack's implementation of L1 block hash access serves as a practical reference. Their approach can be reviewed in detail here.

Motivation and Security Implications:

As suggested by original poster access to the L1 block hash can reduce reliance on third-party oracles, which are susceptible to manipulation. By directly integrating the L1 block hash, we enhance the security of cross-chain interactions and enable more robust verification processes for cross-chain transactions.

Technical Specs:

- Ensure recent L1 block hashes are included in Arbitrum's block header, allowing for efficient retrieval and verification.
- Modify the ArbSys contract to include a getL1BlockHash()

function.

Community Feedback:

The proposal has garnered positive feedback and constructive suggestions. I encourage the research community to deep-dive into the technical aspects and potential impacts of this proposal.

For more detailed information and to join the discussion, please visit the original Arbitrum Forum thread linked in the introduction.

Additional information:

I work as a researcher for the vlayer Labs (vlayer.xyz), and such feature would be a great thing, especially for projects in multi-chain zero-knowledge communication.

Looking forward to the community's input!

Best regards,

Maciej