VectorX

VectorX is the implementation of Avail's data attestation bridge that is used to bridge data from Avail to the EVM compatible chains in form of data roots commitments. It is implemented as a set of zero-knowledge proof circuits in SP1. SP1 is the most feature completed zero-knowledge virtual machine that can prove execution of arbitrary Rust and any other LLVM compiled languages.

Verify data availability on Ethereum

In order to verify data availability on Ethereum it is necessary to first submit data to Avail DA as a data submission(DA) transaction. Data submitted this way will be included in Avail DA's blocks, but not interpreted or executed in any way. You can submit data to Avail DA in a variety of ways, but we recommend using our dedicated SDKs.

You can check out examples on how to submit new data to Avail DA in ou<u>API reference</u>. You can check out a complete example on submitting data and verifying the data blob inclusion<u>on our github(opens in a new tab)</u>.

Submit data to Avail DA

To submit new data to Avail DA, you need to sign the extrinsicdataAvailability.submitData(data) with thedata being passed as a param. Once the transaction is included in an Avail DA block and that block is finalized, adata root is generated for the entire block, ready to be bridged to Ethereum.

Bridge data to Ethereum

This way your DA transaction becomes a part of the Avail's blockdata-root and it's inclusion can thus be verified. The data submitted to Avail DA is bridged to Ethereum every 360 Avail blocks and the commitment is included in the VectorX contract. VectorX is an implementation of zero-knowledge proof circuits for Vector, Avail's Data Attestation Bridge in SP1(opens in a new tab).

Deployed VectorX contract for Turing testnet on the Sepolia testnet 0.xe542db219a7e2b29c7aeaeace242c9a2cd528f96 (opens in a new tab) . Deployed VectorX contract for Avail mainnet on the Ethereum network: 0.xe542db219a7e2b29c7aeaeace242c9a2cd528f96 (opens in a new tab) . Deployed VectorX contract for the Holesky network: 0.xe542db219a7e2b29c7aeaeace242c9a2cd528f96 (opens in a new tab) . Deployed VectorX contract for the Holesky network: 0.xe542db219a7e2b29c7aeaeace242c9a2cd528f96 (opens in a new tab) . Deployed VectorX contract for the Holesky network: 0.xe542db219a7e2b29c7aeaeace242c9a2cd528f96 (opens in a new tab) . Deployed VectorX contract for the Holesky network: 0.xe542db219a7e2b29bB13224f3aF289F03bf298d (opens in a new tab) . Deployed VectorX contract for the Holesky network: 0.xe542db219a7e2b276BF74d1C1d30d032F31e19 (opens in a new tab)

Verify data availability on Ethereum

When the data root is bridged to the Ethereum network, it is possible to query for the inclusion proof(Merkle proof) using thebridge-api deployed for Turing testnet.

You can find detailed documentation on ourbridge-API in our API reference. By submitting a Merkle proof to the verification contract it is possible to verify if a piece of data is available on Avail DA.

A merkle proof is a list of hashes that can be used to prove that the given leaf is a member of the Merkle tree. An example of submitting a proof to the bridge verification contract deployed on Sepolia network for Turing (0x967F7DdC4ec508462231849AE81eeaa68Ad01389 (opens in a new tab)) and Ethereum mainnet (0x054fd961708d8e2b9c10a63f6157c74458889f0a (opens in a new tab)) can be done by callingverifyBlobLeaf function. This will call deployed contracts functionverificationContract.verifyBlobLeaf(merkleProofInput) and returntrue orfalse depending on the provided proof.

Cosmos Avail Module Run a Node on Avail