Attestation

There are 4 kinds of verifiable attestations happened in Automata VRF in Automata 2.0. The dependencies among these attestations can be found inattestation protocol .

Attestation: TEE software program

Type:Optimistic Attestation

The TEE program arrives at a reproducible MRENCLAVE value when rebuilding the code in a base builder docker hosted in AWS Nitro Enclave. Find more details inSoftware attestation .

Because the whole compilation is reproducible and the attestation is provided by the builder docker which already attested by the AWS Nitro Enclave, we leverage the root of trust from the AWS Nitro Enclave and choose optimistic attestation, which doesn't provide a challenge method during this attestation.

Attestation: TEE hardware

Type:Consensus-based Attestation

Current Automata VRF is hosted in Azure, which usesIntel DCAP to finish the TEE attestation, which ensure the hardware execution environment and the running code is matched as expected.

Since the Intel DCAP Quote verification is quite complicated and it will cost a lot of gas, we choose to use consensus-based attestation and introduce a certain of the trusted parties' attestors to validate the correctness of the quote uploaded by the off-chain TEE VRF Oracle.

Attestation: DRAND Input parameters

Type:Verifiable Attestation

Leveraging the BLS12-381 curve verifiablecircuit provided by0xPARC's circom-pairing , other than the BLS verification in the off-chain TEE VRF worker, this parameter is also able to be verified on chain.

Attestation: TEE submitted randomness

Type:Verifiable Attestation

Based on theTrusted Off Chain Oracle Workflow , since the signers in the workers are known in advance, the submitted randomness can be attested and verified on chain by recovering the signer.