Attestor

In the digital realm, particularly within the context of security and identity verification, the term "Attestor" holds significant importance. By standard definition, an Attestor is an entity that vouches for the veracity of an attestation. In simpler terms, it's the role that confirms the correctness of an attestation.

However, in our design, the definition of an Attestor varies based on the nature of the attestation process:

1. SingleStepOptimisticAttestation
2. : In scenarios where the attestation is directly verified on-chain, the Attestor is the on-chain contract itself. The process is straightforward: the attestation is submitted, and the on-chain contract immediately verifies its authenticity.
3. MultiStepOptimisticAttestation
4. : This is a more intricate process. Initially, the attestation is optimistically accepted without immediate verification. However, there's a subsequent challenge phase. In this design, the Attestor is a combination of the on-chain contract and any potential challengers. The on-chain contract accepts the attestation, but it's the challengers who can dispute its validity if they find inconsistencies.
5. ConsensusBasedAttestation
6. : Here, the verification process is entirely off-chain. The Attestor, in this case, is the off-chain party responsible for validating the attestation. Multiple parties might collaborate to reach a consensus on the attestation's validity, ensuring a decentralized and robust verification process.
7.

In essence, the role of the Attestor is pivotal across different attestation designs. Whether it's an on-chain contract, a combination of a contract and challengers, or an off-chain consensus group, the Attestor ensures the integrity and authenticity of the attestation process.

Previous Attestation Next Smart Contract Last updated6 months ago On this page Was this helpful?