Sealing

Trusted Execution Environments are essentially stateless. To preserve information that's stored in an enclave, it must be explicitly sent outside the enclave to untrusted memory. SGX provides a capability calleddata sealing which encrypts enclave data in the enclave using an encryption key derived from the CPU. This encrypted data block can only be decrypted, or unsealed, on the same system. This SGX-specific method for storing data is not used to store computation input/output data in the Secret Network. It is used to store the enclave's signing key.

We seal the signing key because this key is created during the remote attestation process. We do not want the enclave to be required to performremote attestation between each computation. If the enclave fails for some reason, and the key is lost, the worker would be obligated to go through the remote attestation process again. The only way to store persistent data from the enclave is through sealing.