Software Guard Extensions (SGX)

Return to Glossary

Software Guard Extensions (SGX) is a sophisticated technology, but at its core, it is effectively a set of instructions for a Central Processing Unit (CPU) that is used by applications to isolate specific, trusted regions of code and data. It provides a secure enclave for developers to protect sensitive data or code from outside interference or inspection.

Code that runs in a Trusted Execution Environment (TEE) using SGX can produce a signed attestation from within a platform or application that is rooted in the processor and provides authentication that the code has been correctly initialized in a trusted environment. This feature has significant implications for the functionality of Proof of Elapsed Time (PoET) consensus, but also creates an inherent barrier to entry and limitation to its uses.

The memory where the protected code is stored in SGX is even safe from malicious users who control physical access to a platform and have the highest authentication to access its memory. As a security feature, SGX was received with significant expectations due to the potential security afforded by this ability.

In the context of PoET consensus, SGX functions as the mechanism for participants to join the network and verify that they are running the trusted code necessary for the PoET consensus execution.

Source: https://blockonomi.com/proof-of-elapsed-time-consensus/

From:
https://www.omgwiki.org/dido/ - **DIDO Wiki**

Permanent link:
https://www.omgwiki.org/dido/doku.php?id=dido:public:ra:xapend:xapend.a_glossary:s:sgx

Last update: **2021/10/04 11:57**