

What will we need in order to develop on the Enigma testnet?

Our first release will be compatible with Solidity, and the business logic for contracts is contained in smart contracts deployed on Ethereum.

What is private computation?

Private computation describes a host of techniques for computing over encrypted data. At a high level, the goal of these technologies is to make it possible to learn from and react to data that is never shared in an unencrypted way. It is important to note in the blockchain context, this is also known as “computational privacy”. This is in contrast to “transactional privacy” (i.e., Monero, ZCash), which can utilize some of the same technologies but with the goal of obfuscating transactions. See our [Private Computation](#) subsection for more detailed discussion.

What is the motivation for implementing trusted execution environments (TEEs) as Secret Contracts 1.0 prior to implementing secure multi-party computation (sMPC)?

The primary reason is that TEEs are much simpler and faster to deploy. They also provide strong cryptographic guarantees around data privacy, correctness and randomness. Enabling secret contracts 2.0 (sMPC) is on our roadmap. Check out the forum section “private computation” to discuss this topic in more detail.

What will it take to run an Enigma node?

In our initial testnet release, nodes will need to run Intel SGX, a trusted execution environment (TEE) solution. We will have more information about the requirements (hardware, software, and attestation process) in coming weeks.

Will I need to run a full node in order to develop secret contracts?

No. Running a secret contract does not require specialized hardware. If you want to actually perform the computations for the Secret Contract (i.e. run an Enigma node), then you would require the specialized hardware. The computations happen on the Enigma network, and the dApp receives the results of the computation.