

Encryption Schema

In this section we will describe the encryption schema used in Fhenix. While the network itself is Schema agnostic - i.e. it can support any encryption schema - the current default schema is TFHE.

TFHE - FHE over the Torus

Fully Homomorphic Encryption over the Torus (TFHE) represents an advanced method of Fully Homomorphic Encryption (FHE) that offers notable improvements over traditional FHE technologies.

Blockchains, at their core, primarily deal with integer operations—whether it's for handling the quantities of cryptocurrency transactions, managing smart contract states, or updating block indices. All these essential operations are based on integers. Therefore, the fact that TFHE can efficiently process computations on integers in their encrypted form is tremendously valuable.

Additionally, most blockchains operate on a consensus mechanism that involves numerous complex integer-based computations. TFHE's ability to handle these operations quickly and efficiently can significantly increase the blockchain's overall performance, reducing computational bottlenecks. This efficiency becomes crucial as blockchains scale and the volume of transactions and complexity of smart contracts increase. As a result, TFHE is not just a viable, but an ideal, encryption solution for maintaining privacy and optimizing performance in blockchain technologies. [Edit this page](#)

[Previous](#) [Differences](#) [Next](#) [FHE Contracts](#)