Privacy Technology

Privacy-Preserving Smart Contract Introduction

Smart contract blockchains are typically public by default. This means that the ledger, the transactions, and the data contained in the smart contract are accessible to anyone. However, this is not the case with Secret Network as it's the first blockchain that offers programmable privacy through privacy-preserving smart contracts ("Secret Contracts"). "Secret Contracts" have both public and private metadata. Private data on Secret Network is encrypted at input, state, and output and therefore never accessible to any nodes, developers, users, or everyone else.

Programmable Privacy

Programmable privacy is the ability to compute with private data while allowing for not only transfers (transactional privacy) but arbitrarily private complex computations. This allows developers to include sensitive data in their smart contracts without moving off-chain to centralized (and less secure) systems; allowing for truly private and scalable decentralized applications —the true vision of the decentralized web.

To achieve such programmable privacy, Secret Network uses a combination of techniques which will be explained in the further sections of this documentation.

Topics Covered Steps Of A Private Transactions

Private Computation & Consensus Flow

Encryption - Key Management

Trusted Execution Environments (TEE) - Intel SGX

Access Control

Plans Beyond SGX

Theoretical Attacks Want to learn about Privacy for smart contracts and the Secret network techstack? Check out the following video series for an introduction:

Last updated1 month ago On this page Was this helpful?Edit on GitHub Export as PDF