Secret Network Overview

One-page overview of Secret Network Secret Network is the first blockchain with customizable privacy. You get to choose what you share, who you share with, and how long you share it for. This protects users and empowers developers to build a better Web3.

The Network's privacy-by-default nature is essential to the security and adoption of the decentralized web. User-side privacy not only enables novel use cases but also puts users back in charge of their sensitive data.

Built with the Cosmos SDK and the Tendermint consensus engine, Secret Network provides a platform for scalable, private, permissionless smart contracts which can connect to the interchain.

Privacy Technology

Secret Network leverages novel key management techniques, encryption schemes, and Trusted Execution Environment (TEE) technology to bring encrypted input, output, and state to the blockchain.

The decentralized network of computers that host Secret Network come to a consensus (delegated Proof-of-Stake—Byzantine Fault Tolerance) without ever obtaining access to the data they process. Users can use “viewing keys” to view their sensitive data or enable third parties to do the same.

Smart Contract Use-Cases

“Secret Contracts”, an implementation of the Rust-based library CosmWasm, enable computation with private metadata. This brings unique use cases to Secret Network which simply aren’t possible on other blockchains.

Secret Contracts have many real-life use cases including user-side encrypted data storage and communication, NFTs with private content and ownership, lending protocols with private collateralization information, and any application requiring true on-chain randomness.

The nature of Secret Network also means that all dApps benefit MEV resistancy. Attacks are not possible due to the encrypted mempool and state of the chain. All users on Secret are protected from front-running and information disparity by default.

The SCRT Coin and Secret Tokens

Secret Network's native coin is called “SCRT”. It is used for gas fees, governance, and staking towards network security.

By wrapping SCRT or any bridged token (from various ecosystems such as Ethereum, Binance Smart Chain, Monero, Cosmos/IBC) into their “Secret Token” (SNIP-20) equivalent, users gain immediate privacy. The balance and every interaction with “Secret Tokens” are private by default.

Secret Tokens can be used to buy/sell NFTs, participate in DeFi, pay in private, escrow for data/content and even get a credit score all while maintaining your financial privacy.

Ecosystem

Secret Network and its applications are built by a community of over 100 dedicated developers and business leads from all over the world. The Network and its builders are supported by the community pool, SCRT Labs, the Secret Foundation, 80 validators, and a multitude of infrastructure and investment partners.

The Secret Network community, known as “Secret Agents,” are the core of the Network, helping to test and enjoy new applications while spreading the importance of web3 privacy online and at in-person events.

Want to better understand the extent of the Secret ecosystem?

Find analytics on SecretAnalytics / Secretnodes or take a look at our Ecosystem roadmap.

History And Roadmap

Secret Network has come a long way, with the core development group starting out in 2017 and the Mainnet launching in early 2020.

The most recent string of updates dubbed “Supernova ” and “Shockwave - Alpha & Delta ” have brought Secret Network IBC interoperability, 200x performance upgrades for encrypted verifications, the launch of query permits for user authentication, multiple performance optimizations for blockchain queries, a more redundant API node infrastructure, and IBC compatible cross-chain smart contract integration. The latter kickstarting Privacy as a Service for the entire Cosmos ecosystem.

With the "Shockwave - Omega" upgrade, Secret Network switched to a more performant smart contract engine increasing throughput significantly. Beyond this, Secret is hard at work to ensure long-term privacy for all users with the introduction

ofSecret 2.0 and expanding Privacy as a Service to Ethereum and other blockchains. The upcoming infrastructure upgrades will bring several features like: Encryption seed rotation, Iterators and upgradeabillity for CosmWasm Contracts, the Gramine SGX backend, support for new generation hardware, and lastly the Wasmer contract engine bringing another significant increase in contract throughput.

In the meantime, research towards MPC, FHE and ZKP's is ongoing. For a first look at Secret 2.0 and the cryptographic primitives coming to Secret check out the most recentforum post and theroadmap section of this documentation.

Transactional Vs. Computational Privacy

Secret Network differs greatly from protocols like Monero and Zcash as it does not aim to provide complete transactional privacy, but focuses on programmable privacy, a different use case entirely.

Unlike other protocols aiming to provide programmable privacy, Secret Network does not utilize “group-oriented anonymous signature schemes” but assures privacy through encryption and specified hardware. Secret Network does not utilize ZK-proofs (ZKPs), Multi-Party Computation (MPC), or Homomorphic Encryption (HME) to achieve privacy due to concerns including poor scalability, technical infeasibility, and information centralization.

However, research is ongoing to include more of the above cryptographic primitives in the Secret Network base layer as ideated in the originalpaper from Guy Zysking at MIT. Read more about the vision of Guy for Secure computation in our Series#BeyondZK .

Conclusion

There has never been a greater need for easily accessible privacy solutions inside and outside the blockchain space. Blockchains that are entirely public are limited in their capacity to generate effective use cases where privacy is a fundamental component of the feasibility of the application.

The intent of Secret Network is to be an open-source protocol that enables a wide range of privacy-preserving tools and applications through programmable privacy—improving the adoption and usability of decentralized technologies.

Last updated1 month ago On this page *Privacy Technology * Smart Contract Use-Cases * The SCRT Coin and Secret Tokens * Ecosystem * History And Roadmap * Transactional Vs. Computational Privacy * Conclusion

Was this helpful? Edit on GitHub Export as PDF