Secret 2.0

Below info comes from the "Request for Feedback"forum post .

Secret remains today the only privacy-preserving smart contracts L1 in production. We were first to identify the need for privacy beyond transactional and beyond Zero-Knowledge Proofs (which in general are more of a scaling solution rather than a privacy one). With concerns such as MEV and L1 censorship, it appears that others are catching up to the need of having base-layer privacy.

To support further growth (and Secret still has a lot of room for growth) and to ensure we remain the market leaders, it's time to look ahead and revise our short, medium and long term vision that will ensure that Secret grows to become the privacy hub for all Web3.

What does being the privacy hub for all of Web3 actually mean? We identified several areas of focus:

1. Cryptography layer for Secret
2. : SGX was always the pragmatic choice, and TEEs in general (not necessarily SGX), are certainly a big part of any end-game solution. TEEs will continue to evolve into a more robust solution, but for highly sensitive use-cases combining TEEs with MPC (and other cryptographic techniques such as additively HE or ZKPs) is the most secure option (much more than using cryptography alone). Secret 2.0 Cryptographic roadmap will add the building blocks required for this. These primarily include: MPC/Secret-Sharing, Threshold (Homomorphic) Encryption/Decryption, and accompanying Zero-Knowledge proofs in Secret's client libraries.
3.
4. Some examples of the kinds of use cases this would enable or greatly improve include private DAOs, RNGs, threshold wallets (and by extension - threshold key management and stronger Secret NFTs)
5.
6. Constellation of chains
7. : Secret 2.0 will look to collaborate with others to build an ecosystem of blockchains that Secret Network will spearhead and/or support, truly solidifying Secret's position as the hub of Web3 Privacy. Alongside the existing Secret Network blockchain, we expect to see:
8.
9. The development of a threshold fully homomorphic encryption ("FHE") Layer-1 ("L1") -now started as fhenix.io
10. The development of consumer chains utilizing Privacy-as-a-Service ("PaaS")
11. The development of privacy-preserving rollups to complement the threshold FHE Layer-1
12. The addition/inclusion of any chain that shares our mission for privacy. In other words, becoming part of the constellation does not necessitate having an affiliation with Secret. Being a kindred spirit and formalizing all kinds of business relations (see next section on becoming a liquidity hub, as an example) is enough.**
13.

Roadmap items Secret 2.0

More info/detail coming soon!

- Honest-dealer Key Generation
- Validator Threshold Decryption Protocol -On the roadmap
- Distributed Key Generation Protocol
- Additively Homomorphic Encryption Library and API (client and enclave-friendly) -In production
- Client-side proof of encryption ZK API
- Hardened Private Voting (via HE+ZKP) -Under development
- Threshold wallets -In production
- Threshold key-management (e.g., hardened Secret NFTs)
- Threshold Randomness (using Threshold BLS) -In production
-