As most of you will have seen by this point, “Secret 2.0” has been teased for a while now and we would like the community’s support in building the best path forward for the Network. Here is the original blog post for reference, but in the past month and with the help of several dozen community members we have evolved the idea quite significantly. Personally, I have never been more excited about the path forward, and seeing so many valued community members work together to bring these ideas into a real, substantial and concrete proposal, is a testament to the strength of our community.

But we’re not nearly finished

. This isn’t meant to serve as a ‘top-down’ proposal for people to rubber-stamp. We’re also not going to put this into a network vote next week. Quite the contrary, we want anyone who cares about Secret, our vision, and our mutual success to comment/provide feedback/bring up new ideas. Nothing presented here is set in stone!

With that context in mind, let’s dig deep into how we envision Secret 2.0 and what it entails.

What is Secret 2.0?

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

: 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.

- 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)

[

secret2-0

2970×1282 179 KB

](https://global.discourse-cdn.com/standard17/uploads/enigma1/original/2X/a/a550749afd0574ab352f0331cedf6b911e660361.jpeg)

1. Constellation of chains

: 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:

- The development of a threshold fully homomorphic encryption (“FHE”) Layer-1 (“L1”)
- The development of consumer chains utilizing Privacy-as-a-Service (“PaaS”)
- The development of privacy-preserving rollups to complement the threshold FHE Layer-1
- 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.**
- Becoming a liquidity hub for privacy-aware projects

: As part of a clear strategy to own and be the focal point of the Web3 privacy narrative, Secret should strive to support liquidity for any other privacy-aware project, whether it is built on Secret or not.

- As a precursor, Secret should reignite its DeFi ecosystem. There are several DeFi projects launching soon (some of which, like Shade, offer a whole suite of solutions!). We should target $50M TVL in strategic pools across these new

products as an immediate and important milestone to achieve

. We would obviously want to grow significantly beyond that and this is only an initial milestone.

- We also hope to create some new structures to grow Secret Network's DeFi suite - to enable users to have a better experience with lower costs. We also want to use this opportunity to provide a platform for developers to build a broader range of applications. We believe the future of Secret Network's DeFi suite will be led by Liquid Staking Derivatives ("LSDs") which will enable people to earn both staking yield and yield from DeFi protocols.**

Secret 2.0 Roadmap

Below is a very high-level description of the major technical advancements we envision for Secret 2.0., and in my opinion the most important piece of Secret 2.0. All of these relate specifically to changes made to the existing privacy-hub chain (i.e., Secret that we know and love…).

Track 1 (Engineering)

:

- Wasm3 Runtime (5x-25x boost)
- Enclave-to-enclave communication
- Rolling network keys
- Bridge migration
- Moving cross-chain (ICA, ICQ, PaaS)
- Replacing TEE-backend (Gramine)
- Light-client verification within the enclave
- Wasmer (100x-200x boost)
- Supporting additional hardware
- Contract migration
- Iterators support
- Revamping key-management

Track 2 (Cryptography)

:

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

Revised Tokenomics

Secret Network is one of the longest-running (and biggest) Cosmos chains. Our original emission parameters were greatly inspired by the original ATOM tokenomics (and frankly, default Cosmos SDK values). These values has served us well, but in our opinion fail in at least two major areas: (1) They aren't long term sustainable (Inflation remains constant over time and is only dependent on % of staked coins).; (2) They cannot currently support the greater vision proposed here.

To solve for these, we proposed a medium-scale revision to current network tokenomics. These changes adhere to these principles in mind, to ensure this is net positive for all stakeholders:

1. Stakers remain ROI-positive and maintain the same %APR initially
2. Inflation slowly decreases over the years, to ensure overall Secret emissions are contained and are significantly lower on a 10-year horizon .
3. Several network-owned funds are created to fund the Secret 2.0 vision. These funds are primarily non-circulating unless used to support any of the expanded vision, for which a reasonable assumption is that this will lead to positive ROI.

Specifically, the current idea is to set inflation to 25.0% and from that to formulaically decrease it each year towards 5.0% (Graphing Calculator). As some reference points, by Year 2, inflation will be 15.0% (the Network's existing inflation rate) and by Year 10, it will have reduced to 7.0%. Such a gradual decrease ensures there aren't any supply shocks that could lead to adverse results.

[

secret2-1

1200×750 44.9 KB

](https://global.discourse-cdn.com/standard17/uploads/enigma1/original/2X/5/5b9c573bbd1ae5eadeb314f023f3137f07c08c2a.png)

[

secret2-2

1202×744 43.4 KB

](https://global.discourse-cdn.com/standard17/uploads/enigma1/original/2X/0/071596d61da48f45b85a80ccc43125b1475d6f97.png)

The first two years of the proposed inflation schedule will see higher emissions than today. At the end of Year 2, there will be an extra 26.6m SCRT emitted. By the end of Year 5, the proposed inflationary schedule will have a lower total supply and by the end of Year 10, it will have emitted 293.8m less SCRT

.

[

secret2-3

1204×746 36.8 KB

](https://global.discourse-cdn.com/standard17/uploads/enigma1/original/2X/c/c869e49a091b12b624e10e9dca0f6700d8fc2189.png)

To enable the vision for Secret 2.0, we require the formation of some new structures. These are:

- Growth Fund: Funding acquisitions related to building out the Secret Network ecosystem
- Developer Fund: Funding dApps, infrastructure and tools to grow Secret Network
- Incentive Fund: Funding DeFi dApps to draw short-term incentives to bootstrap their protocol

We have worked to ensure that staker's interests are protected. By front-loading the emission for the Growth Fund, we are able to accrue the required amount in a shorter period of time rather than burdening stakers for a long time.

The continued success of the Terra Grant Fund (which included the funding of Fina Wallet, Kado, Leap, Margined Protocol and others) makes us want to continue this effort with the Developer Fund. It will operate similarly and be open to all developers similar to the Community Pool.

SCRT Labs has been deploying significant funds (to date, roughly 7M SCRT out of 20M) from the ecosystem fund. To clarify, the ecosystem fund is part of SCRT Labs own balance sheet, and we expect to continue to deploy funds from it going forward at our own discretion.

With more sustainable network-owned funds (that are not owned by SCRT Labs or appear on our balance sheet), like the Developer Fund, one angle we are exploring for the ecosystem fund is to take more concentrated bets in projects building on Secret, in return for a meaningful stake that better align everyone's incentives when building on Secret.

Providing incentives to DeFi applications to bootstrap their protocol is something that has been done successfully by many blockchains. It allows dApps to grow their TVL more sustainably which helps its long-term prospects. While this creates some small supply-side pressure on SCRT, it should be noted that a more flourishing DeFi suite will provide greater utility for SCRT which will see its demand increase.

[

secret2-4

1232×760 43.9 KB

](https://global.discourse-cdn.com/standard17/uploads/enigma1/original/2X/5/55c1b032512f6bb98c0618e670852df0d2727eb3.png)

The proposed tokenomics will ensure that stakers maintain positive value accrual from staking SCRT. While in the earlier years, the growth above inflation will be minimal (due to taxes), this will ramp up over time. We have ensured that stakers will not face dilution through this process. Also, note that these figures assume a ‘worst-case’ scenario where all new emissions are circulating, which, unlike today - is clearly not the case and most assets allocated to any of the new funds are non-circulating by definition.

Governing the Funds

While each Fund will have a different duty, it is expected that there will be some overlap in their membership such as representation from SCRT Labs. Note that while the Developer and Incentive Funds look inwards at Secret Network (and present their own potential conflicts of interest), the Growth Fund is looking outwards.

The composition of these Funds has not been determined and we would appreciate the community’s support in recommending entities that should be in each Fund.

[

secret2-5

892×510 52.5 KB

](https://global.discourse-cdn.com/standard17/uploads/enigma1/original/2X/e/e0ce605c3dff92defedd6493bfac842e382dc34b.png)

The above structure enables each Fund to act swiftly while ensuring that the Network can influence decision-making on material expenditure. This means that the Network can veto any expenditures above a de minimis amount (which will be up to the Community to decide).

Requests to You

We would like to leave this open for discussion for a healthy period of time to ensure views across the Network have the appropriate time to help shape Secret 2.0 to be the best direction we can take.

We would like to know what works, what doesn’t work, and your recommendations for changes that you would like - your views on this matter are all appreciated to make Secret 2.0 as great as it can be.

Acknowledgements

I’d like to personally express my gratitude to every one of the dozens of people who actively contributed to this proposal. In particular, I’d like to thank Orageux101 for leading the effort of essentially putting all of the many ideas into a concrete form (writing the main proposal, building out the model/spreadsheet, providing many of the ideas, etc…), Carter and Ranger for taking a big part in shaping the revised tokenomics,

Cheers,

Guy