Enshroud Tokenomics

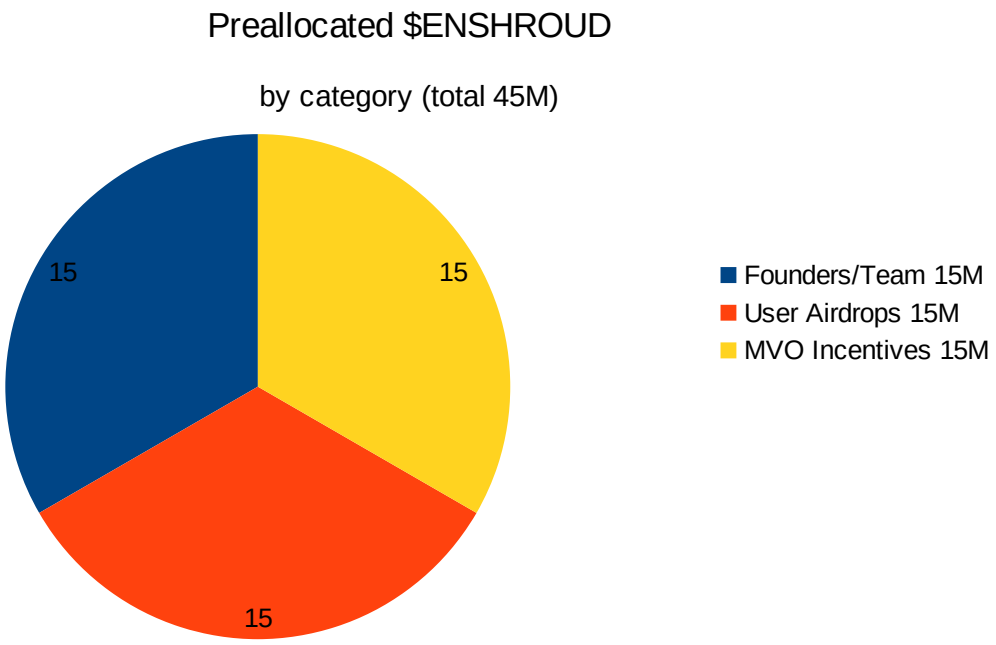
v1.3: 05 June, 2025

I. Tokenomics

There are two basic types of $ENSHROUD tokens: those which are preallocated to different groups, and those sold after Launch to interested buyers. The former type is fixed, the latter open-ended.

A. Preallocated $ENSHROUD Tokens

Enshroud will not be doing an ICO. Instead, there will be two blocks of ERC-20 $ENSHROUD tokens. The first block is of 45 million tokens with finite pre-specified allocations, as follows:



Notes:

- In the spirit of fair launch, no public offering of $ENSHROUD will occur before Launch. All investment will be privately sourced from founders and their associates, with the investment principal repaid 1:1 (i.e. without profits) out of Tier revenue from tokens sold after Launch.

- Founders / Team tokens will have a pro-rated uniform unlocking schedule over 12 months, commencing after a 90 day initial lockup period. That is, 1/365th of a founder or team

member's tokens unlock daily during months 4-15 after Launch. (Succinctly, they have a linear one-year unlock with a 90 day cliff.)

- Locked tokens can be voted for governance, but cannot be withdrawn, sold, or staked for earnings. However they can be staked by an MVO operator. (See Stakings section below.)

- User tokens will be airdropped to active users at some point (TBD) 1 – 2 years after official Launch (i.e., sometime during year two). An account address (on any supported blockchain) will earn 1 point for each for each deposit or withdrawal operation involving meaningful quantities of economically meaningful tokens, at any time during the reference period. (Criteria will be determined and made public prior to each Airdrop.) To prevent abuse, no points will be awarded for spend operations (which also generate no fee income). The number of points will be tallied and divided into the 15 million tokens available. Each address will receive a pro-rated share of Airdrop tokens based on their points, compared with the total across all addresses scoring points.

- MVO Incentive tokens will be available daily to active MVOs to claim based on their point score. An MVO will score 3 points each time it processes a transaction as the lead MVO (which forms and manages the committee of *N*). Each MVO receives 1 point for processing a transaction where it serves as a concurring member of a committee. Each MVO receives a pro-rated share of the day's allotment based on its share of the point total. The daily allotment will be 1/365th (in leap years, 1/366th) of the annual allotment of tokens for each year. The 15 million tokens in this sub-block will be distributed as follows:

    - 5 million during the first year following Launch (13,699 per day)
    - 4 million during year two (10,959 per day)
    - 3 million during year three (8,219 per day)
    - 2 million during year four (5,479 per day)
    - 1 million during year five (2,340 per day)
    - Incentive payments to MVOs will cease at the end of year 5.

- Airdrop and MVO Incentive tokens will not have a timelock, and are unlocked from issuance.

- Therefore, out of the preallocated $ENSHROUD categories:
    - 1.25M tokens will be emitted in the first three months (to MVOs).
    - 15M additional tokens will be emitted or become unlocked over the next nine months, making a total of 16.25M during year 1.
    - 4.75M tokens will be emitted or unlocked in the first three months of year 2 (not counting user Airdrops).
    - 18M tokens will be emitted over the remainder of year 2 (Airdrops plus MVOs), making a total of 22.75M during year 2.
    - 3M tokens will be emitted (to MVOs) in year 3.
    - 2M tokens will be emitted (to MVOs) in year 4.
    - 1M tokens will be emitted (to MVOs) in year 5.
    - Grand total = 45M minted over 5 years.

It will be noted that the distribution of MVO incentives will depend upon the total number of MVOs. This dynamic should create incentives to add or subtract capacity appropriately based on user demand.

The timelock schedule for insider tokens is intended to ensure that tokens purchased at retail from the Crowdsale contract (see below) will receive an advantage when staking for Yield during the first year, while allowing for insider DAO voting control to become diluted gradually as more tokens are minted.

B. Purchased $ENSHROUD Tokens

This category of tokens is open-ended, meant to be capped only by market demand as follows. A quantity of 1 million tokens will be offered for sale at a fixed price. This will be known as "Tier 1." When that Tier has no more inventory left, the next 1M tokens will be offered in Tier 2 at 2X the price of Tier 1. This will be implemented by means of a Crowdsale smart contract, initialized at Launch, which has the property that a "DAO" seller for Tier 1 will offer up to 1M tokens for ETH at a fixed price, then will offer in Tier 2 another 1M at 2X that price, and so on. $ENSHROUD bought from the Crowdsale represents new mintage. We expect that AMMs will arise organically on DeFi DEXs (such as Uniswap), which feature $ENSHROUD as one side of an asset pair. All regular users may offer to swap any *unlocked* $ENSHROUD they may hold in such an AMM at any price they wish. This effectively allows anyone to step in front of the automated Crowdsale with a lower ask. The intent is that new tokens are minted only to the extent that demand exceeds what can be procured in the secondary market of existing tokens. Note that over the first year, the unlocking schedule will limit insider liquidation.

The Crowdsale prices are expected to start at Tier 1 = approximately US $0.25 in ETH. That is, the first Tier's price ("x") will be initialized to the amount of ETH that represents $0.25 at the time of deployment. The Tier 2 price will be 2x, Tier 3 will be 3x, etc., as illustrated in this table:

Tier Number	Tier price per token (paid in ETH, price doubles on each Tier)	Est. USD revenue from 1M sold (projecting from T1 peg)	Cumulative Revenue (does not reflect ETHUSD changes)
1	1x ETH (= $0.25 at launch)	$250,000	$250,000
2	2x ETH ($0.50)	$500,000	$750,000
3	4x ETH ($1.00)	$1,000,000	$1,750,000
4	8x ETH ($2.00)	$2,000,000	$3,750,000
5	16x ETH ($4.00)	$4,000,000	$7,750,000
6	32x ETH ($8.00)	$8,000,000	$15,750,000
7	64x ETH ($16.00)	$16,000,000	$31,750,000
8	128x ETH ($32.00)	$32,800,000	$63,750,000
9	256x ETH ($64.00)	$64,000,000	$127,750,000
10	512x ETH ($128.00)	$128,000,000	$255,750,000
11	1024x ETH ($256.00)	$256,000,000	$511,750,000
12	2048x ETH ($512.00)	$512,000,000	$1,023,750,000
...	X2	X2	...

Because the price of ETH-USD fluctuates daily, the USD quantities shown will not be accurate. They are shown merely to illustrate the concept of doubling prices and Treasury revenues in each Tier.

Therefore, if for example a total of 11M $ENSHROUD were purchased from the Crowdsale contract, the market would be in Tier 12, with new mintage available at 2048x in ETH. The price doubling

feature will provide ample opportunities for existing token holders to supply liquidity at a wide range of lower prices. The "market price" of $ENSHROUD (as measured in other pools on other DEX/AGG platforms or CEXs) will differ from the current Crowdsale Tier price, normally being lower. A new Tier will get opened *only* when demand demonstrably exceeds available existing supply, as evidenced by a lack of tokens available at lower prices. The expectation is that at some point existing supply will balance demand, and progression to new active Tiers will become infrequent. Note that even assuming ETH-USD remained constant, over $1B in capital would be required to mint 12M new tokens. If Ether goes into another bull market in future, and as USD inevitably loses value due to inflation in years to come, significantly more capital may actually be required.

Note that there is no inherent mechanism for burning $ENSHROUD. This is a necessary consequence of the open-ended supply feature, as deliberately burning tokens could speciously raise the Tier level.

Permitted uses for Crowdsale revenues (100% paid to DAO multisig Treasury) include:

- Reimbursement of all sunk costs for development incurred prior to Launch (without profit).
- 5% allocated for future development and operations costs.
- Additional code audits and/or insurance against smart contract or other software fault risks.
- Maintenance of reserves for solvency, e.g. in ETH or BTC.
- Deployment to additional blockchains, and possibly bridging of the $ENSHROUD token.
- Legal defense and indemnity for team, devs, founders, MVO operators, admins, DAO officers, etc., should any of these come under attack by regulatory, tax, or other authorities as a consequence of providing a pro-privacy service to end users. (Naturally, no indemnity would be provided in cases of malfeasance affecting users.)
- To support marketing, joint business ventures and opportunities with other synergistic projects. This may take the form of grants or rewards to projects for integrating with Enshroud.
- Seeding AMMs involving $ENSHROUD, as a market maker.
- As may be determined by the EnshroudDAO according to its bylaws.

II. Token Staking

The staking of $ENSHROUD serves two basic purposes: generating an APY for token holders, and securing the network. All stakings are at-will, and have no fixed durations (unstake at any time).

A. Staking for Yield (APY)

The list of token assets that can be Enshrouded is set by the users (ERC-20, ERC-777, or ERC-4626 compatible). For each asset type, the system earns small (e.g. by default 0.3%) percentage fees whenever that asset is deposited or withdrawn. (Non-default special rates can be set per-asset by the DAO.) Nothing is earned on spends of eNFTs backed by assets already deposited. System earnings are therefore dependent on both TVL and velocity of deposits/withdrawals. Earnings from other supported blockchains are withdrawn, bridged and imported into the DAOPool contract on Ethereum Mainnet, so that users need to stake on only one chain. $ENSHROUD (the ERC-20 token) may or may not be deployed or bridged to other supported blockchains.

Across all supported assets, 5% of the earnings are allocated to the project Treasury, to be utilized as described above for Crowdsale revenue. (This fraction can also be changed by the DAO, via a supermajority vote.) The other 95% are claimable across all users who have staked their $ENSHROUD on the platform, pro-rated based on the number of tokens they have staked compared to

the total. Consequently, each staker will earn some of every supported asset each interval (unless there were no deposits or withdrawals of that particular asset made during that epoch).

Stakers may withdraw from their balance whatever quantity of an asset they have earned, once each epoch (an epoch = ~1 week). To save on gas, it is permitted to "bulk withdraw" from a list of multiple assets in the same transaction (up to 20 distinct tokens at once). Naturally, withdrawals in the form of eNFTs will be supported, via "withdrawing" as a deposit for the staker to the EnshroudProtocol contract. Nevertheless, for participants with smaller amounts of $ENSHROUD staked, earnings may not always justify the gas cost.

Drilling down into the details, when claiming earnings the staker specifies which asset(s) they with to claim (ETH is always claimed automatically), and the amount of such asset(s) claimable by them is calculated using the ratio of *msg.sender*'s stake compared to the total stake at the time of claiming, against the DAOPool.balanceOf() each asset. This allows each staker to specify precisely which assets they want to claim, and which they'd rather hold off claiming until the balance is higher. The claimable ratio of a given asset is then modified as a function of the time since *msg.sender*'s last claim, with the amount being set to zero for any asset already claimed within the epoch. This implements a "cool down" period, and is intended to prevent active and larger claimers from functionally depleting the available balances beyond their actual stake ratio.

Unstaking can be requested at any time, but one epoch must elapse before the tokens can be withdrawn.

B. Staking by MVO Operators (only) to Secure Network

Every MVO owner/operator is required to stake in the MVOStaking contract a certain minimum quantity of $ENSHROUD (fixed by the DAO, initial value will be 150,000). They may also stake extra, in order to improve their chances of being selected to process user transactions, for which they are paid in $ENSHROUD during the first 5 years following Launch. This staked $ENSHROUD does not need to be unlocked. (Q.v. discussion of MVO selection algorithm in the white paper.)

Only *unlocked* $ENSHROUD staked by MVO operators in the DAOPool contract earns the APY as described in the previous section. (That is, an MVO operator can stake locked or unlocked tokens in MVOStaking, but only their unlocked tokens earn in DAOPool, just like other users.) After the 5-year subsidy period, a new policy to reward MVOs for transaction processing should be implemented. For example, a fixed percentage of fee revenue could be allocated to MVO stakers. (The DAO will need to determine this policy in advance.) The idea of the 5-year subsidy is that MVO operators can either sell their $ENSHROUD in AMMs to provide liquidity (especially after the first two years when all other allocated emissions are completed), or "hodl" them to augment their future earnings (similar to a form of "sweat equity").

Again diving into the details, the amount of $ENSHROUD reward accrued by an MVO in a given interval is based on the ratio of *msg.sender*'s pointsBalance compared to totalPoints (the sum of all MVOs' current pointsBalances) at the time of points redemption and claim, minus any MVO pool dues applicable to that *msg.sender* (which are sent to the poolAddress instead). The base amount per epoch takes into account the declining yearly total reward amounts. The tokens available per-epoch are fixed by the contract (rewards available for applicable year / blocks per day); but the calculation of an individual MVO's claimable reward is essentially (their points / total points) * remaining rewards

available for that epoch. The MVO's pointsBalance is reset after claiming. Points earned by an MVO on other supported blockchains are exported, and imported into MVOStaking on Ethereum Mainnet.

Other MVO Rules. The DAO may elect to restrict the number of MVOs allowed at any given time. It may also remove or disable MVOs for cause (such as dishonesty demonstrated by Auditor records), or assess fines or offsets for actual damages against their staked $ENSHROUD. MVO operators (alone among stakers and users) must be identified rather than anonymous. While known to the DAO, operators are not made public and are strongly requested to keep their identities strictly private. (The reason for this is to prevent their being targeted by parties desiring to suborn an MVO operator.)

Operators must provide their own hardware and/or hosting according to minimum specifications, and agree to install and run only the official MVO node software as published by the dev team. The DAO will issue (and revoke) VPN credentials, and provision and maintain the VPN. MVOs must agree to install SSH pubkeys belonging to the dev team and/or admins on all of their MVO devices, so that these can be accessed for maintenance and code certification and inspection purposes. MVOs will have no user support responsibilities, but may participate in forums, Discord / Telegram groups, etc. The arrangement here is not unlike certain projects which feature licensed mining nodes. MVOs may be sponsored or fronted tokens by Founders, Team members, devs, or other insiders. (There will be approximately 20 MVOs online at Launch.) The intention however is that over time, the majority of transactions will be processed by MVOs controlled by arms length third parties, just as voting control over the DAO itself will ultimately be diffused away from the founding team and devs.

The MVOStaking smart contract natively supports establishing and joining MVO mining pools. A pool operator offers to assist members with running their MVO node, potentially performing all tasks under contract, in exchange for a fixed rate of dues subtracted from the MVO's revenues. This will make it easier for MVO owners inexperienced at crypto-mining to participate, and provide a business opportunity for pool operators. Any number of independent mining pools may be established, and an MVO may join or leave any of them, or go solo. (Some minor restrictions aimed at avoiding dues payment do apply.) An initial pool known as the '49ers Pool will be spun up by Founders at Launch.

No special staking shall be necessary in order to participate in voting or other DAO governance. Governance functions will always be open anonymously to any and all holders of $ENSHROUD.

III. Tokenomics Goals

The following are the design goals of the token system described above:

1. Distribute tokens to pro-privacy groups.
2. Sell tokens to any interested purchaser via Crowdsale.
3. Reward Founders, Team, and node operators.
4. Provide incentives to users and prospective node operators.
5. Secure DAO voting control in the hands of pro-privacy owners.
6. Prevent centralization of control, even among Founders and Team.
7. Deter hostile takeover of the DAO by monetary means.
8. Avoid the speculative boom-bust trajectory so common to crypto projects.

Let's examine each of these intentions in a bit more detail and explore how they interrelate.

At Launch, there will be 15M tokens issued to Founders, Team, and certain independent MVO node operators (known as Privacy ‘49ers). All MVOs operating at Launch will be staked and controlled by this group. This addresses goals #1, #3, and #5. Presumably these people are all believers in financial privacy, and as a group are responsible for bringing Enshroud to market. Initial voting control will inure to this group. Furthermore no single party within this group will control more than 25% of starting tokens, in line with goal #6. At the same time, all of these starting tokens have a timelock schedule of 15 months following Launch. (More below on the reasons for selecting this timetable.)

Beginning at Launch, tokens will be available via Tier Crowdsale to all comers (goal #2), whether they’re privacy advocates by principle or merely by convenience. Because it would require well over $1B worth of token purchases for any party to acquire enough tokens to outvote the insiders group (not counting tokens resold to anyone else), it’s highly unlikely that anyone would make this attempt (goal #7). But if they did, that would put over $1B into the DAO Treasury.

A second 15M bloc of tokens will be minted (without timelock) to MVO operators over 5 years. This aligns with goals #1 and #3. Additionally, an incentive is offered to outside parties to acquire sufficient tokens (150k) to operate their own MVO node(s). This serves goals #2, #4, and #6. Note that there’s a virtuous feedback effect in that the purchase of Tier tokens generally bids up the price, making operation of an MVO *more* profitable, rather than less (as usually results from adding more validators to a network). This in turn provides more incentive for large token purchases to spin up new MVOs. When a point of equilibrium is reached beyond which additional MVOs do not make economic sense, it is planned that a system of delegated staking will be introduced, in which new participants can stake on existing MVOs to earn a proportional share of their earnings.

During year 2 after Launch, the final bloc of 15M preallocated tokens will be distributed in a series of one or more Airdrops to users. User account addresses will score a point for each fee-earning transaction (deposits and withdrawals) they perform during the reference period prior to each Airdrop. (Criteria will be determined and published ahead of time to frustrate behavior such as spamming deposits of worthless tokens.) Points are totaled and the user receives a pro-rated share of the Airdrop based on the ratio of their points to the total points. To provide an incentive to keep using Enshroud, address point totals will run cumulatively, so that a qualifying user will receive a share of each Airdrop, but may get a bigger share if they continue using Enshroud during each period. The user Airdrops serve goals #4, #6, and hopefully #5.

The fees earned by Enshroud-DAO, other than a 5% override which flows to the Treasury, are awarded to users who stake in the Yield pool. These yields are paid in the deposited assets, not $ENSHROUD. The Yield pool serves goal #4, and also #2 and #6 to the extent that Tier token sales are stimulated.

The final goal (#8, avoiding boom/bust) deserves some separate explanation. All too often over the past several years we’ve seen projects with a price trajectory that “moons,” usually fairly early, and then crashes severely. This really isn’t good for anybody, and is arguably caused by needlessly restricted supply in the face of sudden popularity, plus an influx of speculators. The restricted supply is usually due to one or both of two factors: a very long (2-5 year) vesting schedule for insiders, and long staking lock-in periods for users in order to obtain the highest APYs. With so many large holders unable to sell into the sudden demand, the price rises much higher than it has any business doing. And once there are no more greater fools, the price collapses by like 80% within only a few months. The result is a token which is widely regarded as a dog that’s had its run, and which few want to buy because it mooned already. Meantime since the emission rate cannot be adjusted downward the token’s

supply thereafter outweighs demand, virtually guaranteeing further price declines over time. This common scenario is universally sub-optimal:

- Insiders cannot liquidate tokens during the boom period, forcing them to sell after the bust has occurred. This prevents them from being rewarded properly for their achievements.

- Users who stake with longer duration because they believe in the project end up earning a negative ROI regardless of their yield, because the token depreciates by far more than the yield.

- It's well known that most speculators buy at or near the top, chasing momentum. So we can't even say that the speculator class made out – the majority of them probably made small gains or even losses, depending on when they sold.

- The project's reputation suffers. Even if successful and with ongoing utility as a "major" in its sector, it may never overcome the stigma of being a "dog" that's in everybody's rear view.

Enshroud's tokenomics aims to address this in several ways. First, the insider timelock schedule is shorter (linear 1 year unlock with 90 day cliff after Launch). This prevents early dumping ICO-style but allows at least a partial exit in the near term, provided a reasonable level of success is achieved. In the meantime insiders are able to stake their still-locked tokens on one or more MVOs which they operate. (However, only their unlocked tokens can earn Yield.) This allows them to earn unlocked tokens which they can retain, stake for Yield, or sell on the secondary market (once AMMs are established organically by the market). We should also note that goal #6 (decentralization of control) is actually well-served by insiders exiting. Since a popular privacy project naturally has a higher regulatory attack profile than most, this is not a bad thing so long as goal #5 (majority control by privacy advocates) does not suffer as a consequence.

The most important source of early supply however is bound to be the Crowdsale mechanism rather than the secondary market. It is difficult to know *a priori* how many tokens may be needed, so the supply is left open-ended. However at some point the secondary market will necessarily be able to supply demand, since the Tier price keeps doubling every million tokens. In this way the total issuance of $ENSHROUD is not explicitly capped, but will be capped by the market.

Because the supply is kept elastic, any abrupt "moon" trajectory should not become extreme. There are also *two* earnings use cases for the token, apart from governance: MVO staking and Yield staking. Neither of these cases compel any specific staking duration, other than locked tokens being unsalable. The number of active MVOs and the total volume of tokens staked for Yield should therefore find an equilibrium point based on market token prices. The utility of $ENSHROUD should provide a floor under the price.

With more flexible supply any amount of demand can be accommodated. Hopefully this results in a more stable and consistent price over time, a price which truly reflects the success Enshroud achieves in serving the needs of its customers, rather than mere speculative excesses.

Tokenomics is critical to the long term health of a crypto project. At Enshroud we aim to learn from history and past experience to do better.