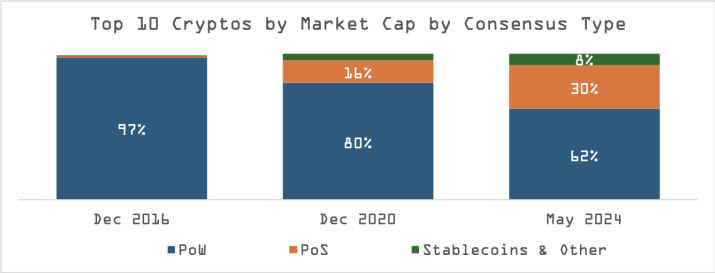
DePIN Staking Pt 1: Medallions

Since founding EV3, we've heard every reason under the sun why DePIN will fail. Skeptics tend to fall into two camps: web2-natives, who think DePIN is *too decentralized*—"there's no way a group of amateurs can compete with the performance of centralized providers"; and web3-natives, who think DePIN is *not decentralized enough*—"blockchains cannot verify real-world (non-digital) events permissionlessly."

Both points are valid, but short-sighted—and both will be overcome with **crypto-economic security**. While staking has played a relatively muted role in DePIN to date, we expect it to become a focal point as DePIN founders & communities adopt learnings from the past half decade of DeFi innovation.[1]



Source: Coinmarketcap

What is crypto-economic security in the context of DePIN? Assume users deposit a DePIN token into a smart contract and subject it to some slashing criteria for a period of time, i.e. staking. Users bear both opportunity costs (of not swapping into another asset) and principal impairment risks (of slashing). We therefore call the value of these deposits a DePIN's *crypto-economic security,* measured in Total Value Locked.[2] TVL is a crude metric because "staking" means different things in different protocols: ideally, we would weight security by length of lock-up and by the stringency and severity of slashing conditions.

There are at least four reasons for DePINs to implement staking mechanisms:

	Pros	Cons	Example
1. To **ensure performance** of supply-side nodes	Top miners earn outsized rewards and re-invest into growing the network.	Centralizing force that pushes control towards top miners.	Filecoin storage providers slashed for missing proofs-of-spacetime.
2. To **determine governance participation**	Backstop for decisions that require human judgment.	Inevitably devolves into politics and bureaucracy.	Akash governance proposals ratified by a majority vote of staked AKT.
3. To **prioritize service** to demand-side nodes	Provides the most direct form of value capture for protocols.	Discourages early adopters from participating.	Pokt prioritizes relay requests to gateways weighted by their staked POKT balance.
4. To **estimate offchain variables**	Creates value by aggregating liquidity around a certain "bet".	Relies on external markets which can be manipulated.	Helium stakers delegate veHNT towards subnets to align mining rewards with future data transfer.

[1] DePIN represents less than 0.5% of the $75B of liquid staking TVL tracked by DeFiLlama (excludes Witness Chain).
[2] This term is roughly, but not exactly analogous to economic security in proof-of-stake networks, which typically refers to the cost for an attacker to control >33% of stake (to halt block finality) and/or >50% of stake (to force block reorgs).

#1: Ensuring performance of supply-side nodes.

If miners in your DePIN use *existing hardware* and *compete entirely onchain*, then miners should stake tokens to secure a greater chance of being allocated the next workload. This is the ideal case for network value accrual since the protocol directly "owns" demand-side traffic, but can be a centralizing force that empower early miners to maintain control. Centralization concerns are mitigated by allowing stakers to delegate their stake in exchange for a share of staking rewards (colloquially known as a "bribe").[3] DePINs in this category, like Livepeer and Bittensor, cap the number of active miners and route workloads between them weighted by staked + delegated balances.[4] Alternatively, networks like Akash route workloads via reverse auction but require winning miners to stake AKT proportional to expected earnings.

If miners in your DePIN use *existing hardware* but *compete both onchain & offchain* (e.g. based on location, brand or customer service), then you can't use stake-weighted routing. Instead, DePINs like Filecoin use staking to ensure service quality—effectively as onchain SLAs.[5] Slashing events typically benefit all tokenholders via a token burn, but we think this is a mistake: slashing penalties should be shared with clients in the form of "onchain refunds" that can help bootstrap early demand.[6] Refunds can happen in-protocol (like GIANT's eSIM refunds) or out-of-protocol, via re-staking protocols (like Parasail). Users are more willing to try out new, unproven internet providers on GIANT because they can claim onchain refunds (permissionlessly!) if the service is faulty. We expect similar protocols to emerge in sectors like electric vehicle charging, with onchain refunds for users who drive to a faulty charger, logistics networks, with onchain refunds for shippers whose packages are sent to the wrong address, and driving navigation apps, with onchain refunds for drivers who are late due to unforeseen traffic.

If miners in your DePIN require *newly-purchased hardware*, then you don't want to make them buy-&-stake tokens after dropping hundreds of dollars on hardware. Instead, networks like Helium IoT and Dimo implement staking at the manufacturer level as a requirement for minting "licenses" to onboard devices and/or as "collateral" for every device onboarded.[7] These costs are passed on to miners anyway in the form of hardware markups, but the reduced friction lowers the barrier to participation and helps drive viral growth. That said, managing hardware manufacturers at scale has proven challenging: Helium IoT is the only DePIN with multiple third-party manufacturers (18) and even they rely on a 7-person committee to revoke licenses (without governance oversight). The DePIN community's focus on manufacturer diversity has waned over time: more recently, projects like Hivemapper, Dimo, and WeatherXM have sold millions of dollars of hardware before approving a single third-party vendor. This is analogous to the Ethereum L2 ecosystem, where chains in the stage 0 phase of decentralization have nevertheless attracted $20B+ of TVL by leveraging single/permissioned sequencers to mitigate MEV.[8]

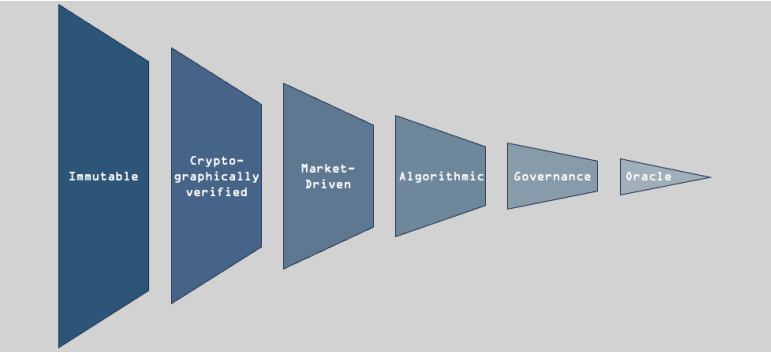
A final consideration is whether miners should stake *highly-liquid cryptoassets* like ETH or USDC instead of native tokens. The downside is reduced demand to buy and hold the native token, which increases token velocity and negatively impacts value. The upside is bootstrapping economic security much faster than would otherwise be possible: Glow's USDC staking has attracted $400k+ TVL in six months from 20+ solar farms.[9] Since DePINs in this category can't rely on native token staking to drive value accrual, they must find alternative ways to monetize the network. Glow, for example, periodically auctions off the carbon credits generated by its miners and uses the proceeds to buy-and-burn GLW tokens.

---

[3] This architecture is known as delegated proof-of-stake and was pioneered by BitShares in 2015.
[4] Active set consists of 100 orchestrators for Livepeer and 64 validators per subnet for Bittensor.
[5] Filecoin storage providers that fail proof-of-spacetime stop earning block rewards after 1 day and are slashed after 42 days.
[6] Such penalties represent >85% of Filecoin's onchain revenue over the past 180 days.
[7] Helium: 1 HNT per device with one-year lock-up. Dimo: 100k DIMO per license plus 25 DIMO per device with six-month lock-up.
[8] In DePIN, MEV = Manufacturer Extractable Value. We estimate $10m+ of MEV profits generated during Helium's IoT buildout.
[9] Eigenlayer grew from 10k to 5m ETH staked in less than a year.

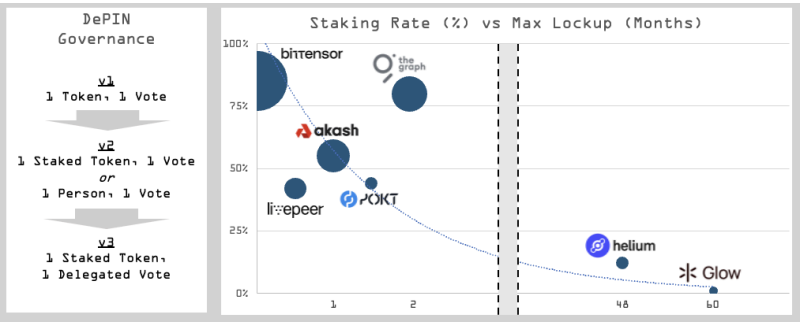
#2: Determining governance power.

We believe in governance-minimized protocols: parameters should be immutable wherever possible; when immutability is unviable, they should be cryptographically-verified; when verification is unviable, they should be market-driven; when fair markets are unviable, they should be algorithmically-driven; and only after exhausting all other options should decisions revert to governance or governance-elected officials.



The hierarchy of decentralization.

Where governance is unavoidable, the first question is suffrage—who gets to vote? The simplest model (1 token = 1 vote) introduces vulnerabilities from tightly coupled economic and governance power.[10] Adding a staking requirement (1 staked token = 1 vote) helps align governance decisions with long-term tokenholders, but long lock-ups tend to drastically reduce staking participation rates and therefore crypto-economic security. Attempts at sybil-resistant voting (1 person = 1 vote) suffer from low voter engagement and misallocation of voting power across the various types of network participants.



DePIN staking rate vs max lockup; bubble size represents staked TVL.

Mature DePIN ecosystems are evolving their governance in two directions: representative and/or multicameral democracies. The former is when stakers delegate votes to representatives, who then ratify proposals directly.[11] The latter is when governance power is partitioned across different types of network participants.[12] For new DePINs with no "governance debt", we suggest designing protocols with: 1) minimal governance surface area (no more than 5-10 types of proposals), 2) thoughtful governance defaults (well-defined veto rights), 3) delegated voting (for high vote participation), and 4) guaranteed representation for all types of network participants (for long-term balance of powers).[13]

---

[10] In October 2020, BProtocol borrowed $7m worth of MKR from Dydx via flash loan to influence a Maker governance vote.
[11] TAO implements "strong" representative democracy: proposals are ratified by a 12-delegate senate with no staker input. GRT has a "weaker" implementation: tokenholders vote in non-binding snapshots but proposals are ultimately ratified by a 10-person council.
[12] Pokt's new governance structure assigns 10% of voting power to citizens (1 person 1 vote), 45% to builders (weighted by contributions), and 45% to stakers (weighted quadratically). Filecoin's FIP-36 was ratified by majority vote of at least 3 of 5 groups: storage providers (weighted by capacity), storage providers (weighted by utilization), storage clients (weighted by utilization), tokenholders (weighted by FIL holdings), and core devs (1 person 1 vote).
[13] See Glow's six proposal types and transparent veto procedures for an example of #1 and #2.

#3: Prioritizing demand-side traffic.

DePIN is constrained by demand, not supply. So why would protocols implement demand-side staking?

Demand-side staking creates market-driven signals for user preferences. These signals can be used to drive (short-term) resource allocation and (long-term) protocol development decisions, ultimately creating more dynamic and useful networks. For example, Pokt users stake to secure throughput on 75+ different chains, where stake-weights are then used to allocate rewards to supply-side RPC nodes.

To avoid adding friction for end-users, most DePINs implement staking at the *gateway* level. Gateways are centralized entities that interact directly with the underlying protocol, abstract away low-level complexity from end-users, and resell network access under a traditional business model (e.g. subscriptions or volume-based). For example, Grove is a gateway that resells RPC requests from Pokt wrapped in a developer-friendly API for $7.5 per million calls. Helium Mobile is a gateway that resells mobile data from Helium wrapped in a $20/mo unlimited cell phone plan.

Gateway staking has three main drawbacks:[14]

1. Gateways must earn a positive (long-term) economic return to attract funding and talent. This requires charging a markup over core protocol services and/or monetizing adjacent value-added services.

2. The first gateways on a network are typically owned and operated by the same core developer team who built the network. This creates conflicts of interest and jeopardizes claims of decentralization.

3. Gateways that become sufficiently-large are incentivized to fork the network. By doing so, gateways can optimize the protocol for their specific customer base while also “re-rating” to protocol-like valuations.

There are two axes on which to evaluate gateway risk: *diversity* and *dynamism*. Diversity means that having more gateways and a lower gini coefficient reduces the leverage any single gateway has. Dynamism means that a more competitive environment between gateways, such that new entrants are on equal footing, reduces the risk of any one gateway building compounding moats. Pocket is further ahead than Helium on both axes, given it has four active gateways (vs one Helium service provider) and its gateways continuously re-delegate to different chains (vs once up-front to create a Helium subDAO).

Instead of end-users and/or gateways signal demand-side preferences, some DePINs choose to open up the market entirely by allowing anyone to burn a small amount of tokens towards a [region] for a share of revenues.[15] While there are benefits to opening up the market completely, there are also second-order consequences to linking governance and economic rights. For example, The Graph currently has 4.4m GRT ($1.5m) of “curator signal”, implying that less than $150k of GRT burn is needed to accrue $15m of curator signal power and reduce everyone else’s indexing priority by 90%.[16]

Networks that incorporate end-user preferences will drive stronger flywheels than those that don’t. That said, protocol designers looking to incorporate these preferences face a trilemma between adding friction for end-users, dependencies on third-party gateways, and/or market and liquidity risks.

---

[14] These concerns are not theoretical. (1) Study Planetwatch, who built a global community of 50k+ devices only to institute a centralized licensing fee and drive token price -99%. (2) Study Pollen, which was briefly seen as a viable Helium competitor only to rug-pull their token. (3) Study Irys, who considered forking AR after bundling 90%+ of Arweave transactions.
[15] Curators signal which subgraphs are most promising and earn a 9.9% share of all query fees generated by each subgraph.
[16] Curators pay a 1% tax to delegate GRT to a subgraph to increase its curator signal, which gets burned.

#4: Estimating offchain variables.

DePINs, by virtue of interacting with real-world (non-digital) economies, need to estimate offchain variables to allocate capital and/or manage risk effectively. These variables are often too dynamic and/or politically-controversial to set algorithmically or through governance votes. For example, Helium needs to estimate the relative future data transfer revenues from IoT vs Mobile in order to split HNT block rewards across the two subDAO treasuries. Similarly, a DeGen[17] protocol might need to estimate the relative value of building renewable energy capacity across power grids in different regions.

Helium has the only live implementation of this design that we're aware of. The community passed HIP-51 in June 2022, implementing a vote-escrow mechanism whereby tokenholders stake HNT in exchange for non-transferable veHNT which can then be delegated to wireless standard-specific subDAOs for yield.[18]

Helium stakers' principal is held in HNT, while their yield is earned in subDAO tokens. The value of HNT is underpinned by data transfer across all subDAOs, while the value of each subDAO token depends on the amount of devices onboarded, data credits burned, and veHNT delegated to each specific subDAO. SubDAOs offer different nominal yields to stakers at any given time, reflective of stakers' aggregate views on each one (where lower risk + higher potential = lower yield). Sophisticated stakers will form their own projections and rebalance yields as they delegate to under-valued (or "under-delegated") subDAOs.

HIP-51's critics tend to cite its complexity,[19] arguing that a multi-token structure inherently fragments HNT liquidity and dilutes tokenholders.[20] While there is some truth to these statements, they account for all the downsides and none of the upsides: on a longer time horizon, the subDAO architecture transforms Helium into a *decentralized market for betting on wireless technologies* backed by HNT liquidity.

As Helium adds more subDAOs and as subDAOs mature, increasingly sophisticated financial actors and derivatives will emerge on top of the network. Risk-averse stakers can simultaneously short subDAOs token to lock-in future yield while earning a funding rate. Traders can create index products that long a basket of established wireless standards (4G + WiFi) and short a basket of emerging standards (5G + LoRa). SubDAOs can also implement their own staking mechanisms, enabling veHNT yield to be re-staked within subDAOs to further enhance yield.

Under HIP-51, staking yields serve as a market-driven signal for the relative cost of capital for competing wireless technologies. It turns what would have otherwise been a "cost center" to the network - figuring out how to allocate rewards across competing wireless standards effectively - into a profit center that drives more liquidity and demand for HNT and strengthens Helium's three-sided network effects.

While HIP-51 creates a modular funding market for wireless technologies, it suffers from a fragmentation of liquidity and value around multiple tokens. Instead, we propose a *medallion-based* architecture - inspired by hybrid NFT projects like MutantMon and ArtGobblers, Berachain's proof-of-liquidity, and Serum's MegaSerum - that achieves the same benefits under a single token.

Shoutout to Anirudh Pai (partner at Dragonfly), Jason Badeaux (founder of Daylight) and Neil Chatterjee (founder of Andrena/DAWN) for their endless discussions and invaluable help developing these ideas.

---

[17] DeGen = decentralized generative energy networks.
[18] Yield is funded by a 6% share of all subDAO token emissions which is fixed and set by governance. Stake is weighted by lock-up period, with a maximum of four years for a 100x voting power multiplier.
[19] A year after the Solana migration, 8% of circulating HNT is delegated to the Mobile subDAO and another 4% is delegated to IoT.
[20] At time of writing, HNT has 50% DEX liquidity, 77% CMC-reported volume, and 79% of market cap across HNT+MOBILE+IOT.

#4 Cont'd: Estimating offchain variables <u>with medallions</u>.

HIP-51 creates a modular funding market for competing wireless technologies, but suffers from a fragmentation of liquidity and value around multiple tokens. Instead, we propose a *medallion-based* architecture that achieves the same benefits under a single token.

1. Stakers lock tokens to mint **medallions**. The number of tokens that need to be locked increases along a bonding curve such that every subsequent medallion is more expensive than the last.

2. Medallions are **delegated** to a [region] for a share of the **revenues and/or capacity** generated in that [region], weighted proportionally by how long each medallion has been delegated for.

3. Medallions can be transferred, traded, un-staked, or re-delegated to a new [region] at any time.

Like HIP-51, medallions incentivize tokenholders to stake tokens and continuously re-delegate to the most under-valued [regions]. However, Helium relies on the fact that subDAO token inflation is highest in year 1 to compel stakers to evaluate new subDAOs quickly; medallions achieve the same effect by incentivizing stakers to maximize time-weighted delegation power towards the highest-earning [regions].

The subtle difference drives a profound impact: veHNT holders get paid in subDAO tokens that are *immediately liquid*, while medallion-holders get paid *only once a [region] generates onchain revenue and/or capacity*. veHNT holders are not inherently long-term aligned with subDAOs. Helium enforces long-term alignment with the main DAO by requiring stakers to lock HNT for up to four years, during which (unlike medallions!) veHNT cannot be transferred, traded, unstaked, or used as collateral in DeFi.

We use brackets around the word [regions] everywhere because medallions are fully generalizable: nothing necessitates stratification by regions or technology standard. Stakers in a wireless network could delegate to location-frequency pairs (NYC-3.5GHz or LON-6GHz), stakers in a ridesharing network could delegate to markets based on who the local incumbent is (Uber-dominated or Lyft- dominated), or stakers in a labor marketplace could delegate to professional domains (engineering or marketing).

Inevitably, HNT liquid staking protocols will emerge. They will be forced to choose between maintaining 100% HNT exposure (requires selling subDAO tokens) or re-staking subDAO tokens to boost yields (requires diversifying the treasury). The latter strategy will win out given crypto users' focus on nominal yields and the fact that subDAO tokens are redeemable for HNT anyway. Eventually, the leading liquid staking protocol will be rebranded to a "Helium ecosystem index token" backed by a diversified pool of staked HNT+subDAO tokens. When this happens, demand for the index token will cannibalize demand for HNT, fragmenting liquidity even further and sparking community backlash against liquid staking.

Unlike in multi-token systems, liquid staking is non-cannibalistic in medallion systems. Consider a liquid staking token that mints HNT staking derivatives (sHNT) and subDAO yield tokens with a claim to future data revenues (yIOT).[21] While the tickers are similar, yIOT is nothing like IOT today: owning yIOT is a narrow bet that the market is mispricing Helium IoT's future data transfer revenues; on the other hand, there are many good reasons to own IOT: betting on growing hardware sales (onboarding fees), more delegated stake (treasury growth), stronger governance rights… or, of course, future data revenues. Because yield tokens are narrow instruments with purely economic rights (and no governance rights), LSTs will siphon much less liquidity under the medallion system vs with subDAOs.

[21] Market equilibrium occurs when (1 sHNT) + (1 yIOT) = (1 HNT) + (the present value of delegating 1 new HNT to the IoT subDAO).

A final point is scalability. The HIP-51 model works up to a handful of subDAOs - 3-5 at most - after which fragmented liquidity & governance becomes unsustainable. Every new subDAO token incurs legal fees, exchange listing fees, market maker loans, and paying other middlemen in the token-industrial complex. On the contrary, medallions can scale to hundreds or even thousands of [regions] under a single token.

Geodnet's SuperHex staking is the closest we've seen to a live implementation of a medallion system.[22] Geodnet stakers earn a fixed yield based on a binary outcome - whether a miner is deployed in the hex within 180 days - rather than a variable yield based on revenues generated in the hex.[23] The boosted hexes are selected by the Geodnet Foundation rather than set by the market, so there is no notion of using yields as a source of information for the network (the primary benefit of the medallion architecture). Nevertheless, SuperHexes help grow the supply-side in a more-targeted, semi-decentralized manner.[24]

Summary

We believe the medallion-based staking is a strictly better architecture for DePINs looking to incorporate market-driven information into their protocols. The only exception is in cases where subDAOs require independent governance to function properly, and therefore governance fragmentation is unavoidable.

	Medallion-Based	Multi-Token
Bootstrapping Mechanism	Stakers incentivized to delegate early for cheapest medallion & max stake-weight.	Stakers incentivized to delegate early during each subDAO's max inflationary period.
DeFi Compatibility	Medallions can be transferred, traded, or unstaked at anytime.	veHNT cannot be transferred, traded, or unstaked.
Time Horizon	Medallions earn yield only *after* revenue-generation.	veHNT immediately starts earning yield & can dump subDAO tokens.
Scalability	Can scale to dozens or hundreds of unique [regions].	Max 2-5 subDAOs before liquidity fragmentation takes over.
Governance	All goverance controlled by a single set of tokenholders.	Each subDAO runs independent governance processes.

At least two DePINs will launch with medallion-based staking in 2024: Daylight, a decentralized residential energy co-operative, and DAWN, a decentralized backhaul network for last-mile internet connectivity.

On the back of their success, we hope the medallion architecture (or future iterations of it) becomes the standard method by which DePINs embed market-based information into protocols, creating a new path for token value accrual beyond status quo burn-and-mint mechanisms.

If you're a DePIN founder, investor or trader with feedback on medallion-based staking, please reach out to us at founders@ev3.xyz and/or join us at the crypto medallions dinner hosted by Andrena / DAWN June 26th in NYC.

---

[22] Stakers lock tokens in 'SuperHexes' for 12-months with a fixed 20% return if a miner deploys in the hex within 180 days.
[23] Hexes eligible for SuperHex staking are selected by the Geodnet Foundation with no oversight from governance.
[24] Geodnet's successful pilot saw a 100% staking rate across 91 hexes and they are now doubling-down with 500 more.