



CRYPTO LEADERS SINCE 2014

New Frontiers™

YIELD UNCHAINED: EXPLORING STAKING DERIVATIVES

Kent Barton

Head of Research and Development, ShapeShift



This report is for educational purposes only and nothing in it should be construed as investment, legal, or tax advice. Purchasing digital assets, such as those discussed in this report, is risky, and we highly encourage you to understand the underlying technology of digital assets and cryptocurrencies specifically and contact an investment, tax, or legal professional prior to deciding to invest in such assets.

Introduction

It all started in 2012. Faced with the perceived barrier of increasing energy costs related to Bitcoin mining, a few crypto enthusiasts proposed an alternative to its proof-of-work (POW) consensus mechanism. The central insight was that the role of miners could be replaced by holders of a blockchain's token.

Rather than rewarding blocks to nodes that spent energy on solving a difficult math problem, determining who minted new blocks would be proportional to the amount of a blockchain's token that was held, or "staked," by a participating node. The more tokens that were staked, the higher odds that a given node would be selected to add a new block. Thus was born . . . say it in a big booming voice . . . Proof Of Staaaaake (POS).

The first attempts at POS—Peercoin and NXT—were messy and ultimately unsuccessful. In addition to issues with centralized supply, the early builders of POS failed to take into account the deep game theory that this type of consensus mechanism entails. However, things have changed dramatically since those early days.

Gaze at the crypto landscape in 2021, and you'll see a handful of POW stalwarts (Bitcoin, Ethereum, Zcash) chugging alongside many newer platforms employing POS (Cosmos,

Polkadot, Cardano, and NEAR, to name a few). Ethereum has also started its gradual transition to POS, with "Phase 0" launching in December 2020. Now, with wider adoption of POS happening before our eyes, is where things will really get interesting.

Staking, however, has a big downside: there's an associated opportunity cost that comes with locking up your capital in a consensus mechanism. Does it really make sense to earn, say, 5-15% on staking when sexy new DeFi protocols or promising tokens might earn multiples of that? And to make matters worse, most staking protocols have a withdrawal delay for staked tokens. Days, weeks, or even years of capital inaccessibility is not appealing for crypto investors used to instant gratification.

Fortunately for stakers, the permissionless and open-source blockchain ecosystem has come to the rescue with a host of solutions. These are broadly referred to as staking derivatives.

In this report, we'll look at this emerging area of crypto innovation, including types of staking derivatives and specific projects issuing these derivatives. How do they differ, and how might this field evolve in the year ahead? Let's find out!



Table of Contents

01	——	The Derivative Landscape	04
		Types of Staking Derivatives	06
		Native	06
		Exchange	06
		Custodial	07
		Collateralized Tokens	07
		Lending	07
02	——	Staking Derivatives on Ethereum	08
		The Big Centralized Exchanges	09
		Rocketpool	11
		Lido	11
		Stkr	12
		LiquidStake	13
03	——	Staking Derivatives on Other POS Chains	14
		Cosmos	15
		Polkadot	16
04	——	Key Takeaways	17
05	——	Further Learning	20





01 The Derivative Landscape

NEW FRONTIERS





The Derivative Landscape

We live in a yield-hungry world where interest rates are at zero and falling fast.

For investors chasing returns, POS chains such as Ethereum and Cosmos offer an attractive, lower-risk alternative to the high-flying-but-mega-risky DeFi protocols.

Staking derivatives offer a tantalizing, best-of-both-worlds approach where users can enjoy both staking returns and the ability to leverage their capital in DeFi and other applications. These derivatives can also eliminate barriers that would otherwise require a user to stake a certain amount of capital in order to participate or force them to wait weeks or (in the case of ETH 2.0) years to pull their capital out of the staking mechanism.

From the perspective of the staking derivative providers, a few straightforward business models arise out of this setup:

- Pool users' funds and take a cut of the resulting staking rewards
- Charge an additional fee for the service
- Offer the service for free as a value-add

It sounds like a real win-win: for users and providers alike, there's a lot to like about staking derivatives. But what about the risks?

For starters, staking derivatives inherently requires giving up custody of your staking tokens. For most protocols, the only way you can truly ensure self-custody is by validating yourself. For a great many users, that simply isn't practical or possible.

There's also arguably some risk to the overall consensus. One line of thinking is that the game-theoretical landscape [changes](#) when stakers or validators can short their own derivative tokens. More broadly speaking, one could argue that the security budget of a POS system "leaks" value when funds that are locked into its staking mechanism are unlocked as derivatives. (For some deep academic reading into this type of thinking, check out ["Why Stake When You Can Borrow?"](#) by Tarun Chitra and Alex Evans.)

It remains to be seen how this will play out. In practice, it'll likely be a few years before the staking derivative market is large enough to pose any real consensus risk to the larger POS chains. For the time being, builders and early adopters are taking the "we'll worry about these theoretical risks later" approach and forging ahead at full speed.





Types of Staking Derivatives

Broadly speaking, staking derivatives can be bucketed into one of the following categories; each has its own unique characteristics, benefits, and risks:

1. *Native*

These staking derivatives are baked into a blockchain's core protocol.

In-protocol derivatives make the process easy and frictionless and remove any smart contract risk from the equation (assuming you trust the blockchain's developers to have coded the derivatives properly). Custodial risk is nearly eliminated as well.

While there aren't many examples of chains doing this just yet, Acala (a Polkadot-based chain) is employing this technique. One might expect a certain number of self-sovereign Cosmos Zones to follow suit at some point.

2. *Exchange*

This implementation is already becoming commonplace, and it's perhaps the easiest to understand. Johnny McCryptoface deposits his staking token with an exchange. In return, the exchange gives him an equal amount of staking derivative tokens that represent that staked asset.

Exchanges are in a great position to abstract away the complexities of staking and their derivatives. By pooling staked assets, they can operate large (and profitable) nodes. Meanwhile, staking rewards that accrue to the user can be deposited directly to their account, off-chain.

There's one big nasty systemic risk that grows out of exchange-based staking derivatives: it encourages centralization of validator nodes. A POS chain's security weakens if a relatively small handful of players garner a large share of the stake. Exchanges are already in a good position to snap up a disproportionate share of tokens. Staking derivatives could exacerbate this dynamic.

There's not much that individual users can do to counter this problem, other than simply vote with their crypto wallets and choose a non-exchange alternative.



3. Custodial

In this case, a centralized entity holds the users' staked tokens and issues derivatives.

While technically exchanges fall under this definition as well, I've parsed them out due to the fact that custodial providers don't have to be exchanges.

While exchanges can leverage their reputations and pre-existing user bases,

newfangled custodial solutions will have to fight harder for their share. As such, they may be incentivized to offer more attractive terms—specifically, taking a smaller cut of the staking rewards or charging a smaller fee than their exchange-based competitors.

4. Collateralized Tokens

From the standpoint of injecting liquidity, collateralized tokens are the most interesting approach, and arguably more decentralized. Here's how they work on Ethereum:

1. A user sends their ETH into a staking contract.
2. The owner of said contract stakes that ETH on their behalf.
3. A 1:1 representation of that ETH is issued as an ERC-20 token.

Since everything is on-chain and permissionless, liquidity can easily flow from staked ETH into other applications such as yield farming or automated market maker ("AMM") pools. We'll cover a few examples of tokenized derivatives shortly.

5. Lending

This approach takes a page from the tried-and-true, collateralized-crypto playbook that's been successfully employed by MakerDAO and many other DeFi platforms. A separate entity (which could even be a decentralized smart contract) issues

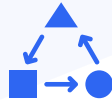
stablecoins backed by the ETH that's been staked by users. While this offers a nice way to unlock liquidity following the well-defined mechanics of crypto lending, there are no tokenized representations of that stake.





02 Staking Derivatives on Ethereum





Staking Derivatives on Ethereum

The advent of Ethereum 2.0 is perhaps the most important catalyst driving intermediate-term adoption of staking derivatives. Ethereum's take on POS went into production in early December and thus far has been running smoothly. Eventually this chain will be "merged" with the existing ETH 1.0 chain.

Although it's still business as usual on the good ol' POW Ethereum, make no mistake: the new POS chain is an economic force to be reckoned with. Currently protecting [\\$3 billion in value](#), it's delivering an annual return of roughly 10%.

These double-digit returns, however, come with a major caveat: ETH 2.0 is a one-way

bridge. ETH that's locked in the POS chain will not be liquid until the aforementioned merger happens.

Surely there must be a better way!

Enter ETH 2.0 staking derivatives. Even in these early days of POS staking, a multitude of options have emerged, employing most of the implementation designs we outlined above. How do these differ? What are their benefits, trade-offs, and risks? Let's take a closer look at some of the derivatives that are already live, or will be going live in the near future.



The Big Centralized Exchanges

Not surprisingly, some of the very first entities to embrace Ethereum staking derivatives are centralized exchanges (CEXes). For all their custodial counterparty risk, CEXes also have the ability to reduce friction for users and pool funds in a way that benefits both parties.

The advantage of pooling funds for these exchanges is clear: since they're running their own validator, their profits stand to increase in tandem with the amount staked. Meanwhile, representations of staked ETH can be dished out for each ETH locked in their validator. This

can happen either on-chain (via an ERC-20) or via a ledger entry on the exchange. The latter provides an easy way to accrue staking rewards to users.

In addition to the obvious custodial risk that inevitably accompanies centralized exchanges, users are limited by not being able to withdraw their derivatives and rewards to the Ethereum mainnet. Yes, one could simply exchange their derivative for ETH or an ERC-20, but this does entail added friction and fees.





Coinbase

Coinbase [rolled out](#) its staking plans in December: “While staked ETH2 tokens remain locked on the beacon chain, Coinbase will also enable trading between ETH2, ETH, and all other supported currencies providing liquidity for our customers.” It’s unclear whether Coinbase’s ETH2 will be tradable elsewhere, and if/how rewards will accrue to stakers. More details should be arriving early this year.



Binance

Binance also posted [details](#) about their approach to staking. Binance’s ETH 2.0 derivative (BETH) is minted on a 1:1 basis. Rewards accrue to users’ Binance accounts (not on-chain), and users can view both their staked holdings and rewards in their Binance spot wallets.



Kraken

Kraken has a similar approach with its staking derivative (ETH2.S). This does not appear to be an ERC-20, and is instead confined to the exchange. Notably, trading of the derivative [has been geo-fenced](#): “The market will NOT be available for users located in or residents or citizens of the US and Canada (these clients can stake ETH, but not trade their staked ETH for unstaked ETH).” Kraken’s legal team must see some degree of risk in their implementation.



Huobi

Recently returning to the U.S. market after being absent for about a year, Huobi has its own [Beacon Chain variant](#) called BETH. The implementation is similar to Binance; both the token and rewards exist as representations in users’ accounts.



Bitfinex

Another on-exchange token, ETH2, [will be provided](#) to Bitfinex users. Like Kraken, Bitfinex has excluded residents of the U.S. and Canada. Rewards will accrue to users’ accounts as a distinct “ETH2 Rewards” ledger entry.



Rocketpool

This is the O.G. Ethereum staking pool. It's been around for years, gaining adherents on Reddit's [r/ethereum](#) and [r/ethfinance](#) in anticipation of the day when POS would finally come to ETH. Now that staking is live, derivatives are a core part of its functionality. Users receive Rocketpool's tokenized derivative (rETH), and also reap staking rewards via the same token.

Rocketpool is an intriguing beast. It aims to be far less centralized than exchanges or custodial services. Smart contracts hold and move funds, while a distributed [network of node operators](#) handles the actual staking:

"Your deposit will be allocated to a node operator who will perform Proof of Stake duties. Node operators are required to stake as much ETH as they are assigned—this means they have skin in the game; they are highly incentivised to perform their duties diligently due to this economic bond."

Lido

Leveraging smart contracts for custody and other functions, Lido aims to be more decentralized in its approach. The DApp also provides stakers with ERC-20 derivatives they can [use anywhere](#) in the Ethereum ecosystem:

"Upon depositing ether into Lido's smart contracts, a user receives stETH (staked ETH) ERC-20 tokens that represent the user's staked ETH balance of beacon chain along with staking rewards accrued or penalties inflicted on validators in the beacon chain... stETH can be transferred or traded, unlike beacon chain ether."

This sounds cool, but how do rewards accrue to derivative holders? Lido can't employ the exchange approach, where rewards can be reported as a database entry in users' accounts. Nor can they send incremental

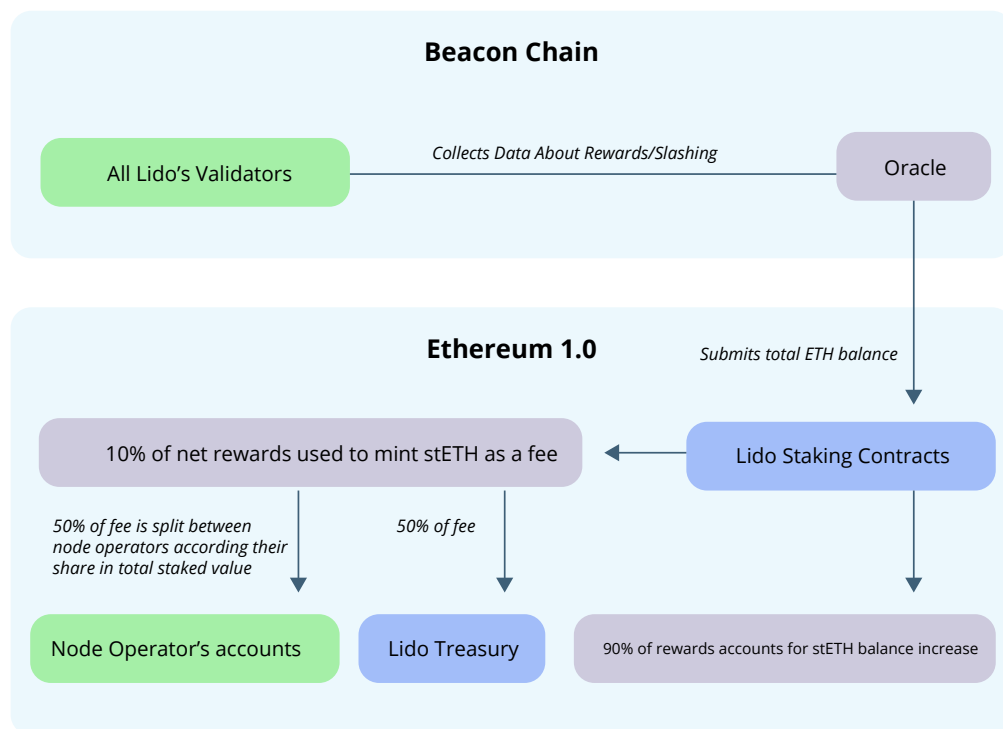
All sorts of interesting questions arise out of this approach. Just how decentralized is this network of nodes? How secure are the smart contracts holding and moving the funds? Are there admin keys for the smart contracts? Can rETH maintain its 1:1 ETH peg if something goes wrong with the system?

These questions are a good jumping-off point for further vetting of the protocol. At a high level, however, Rocketpool appears to be a tempting derivative choice for a user who doesn't want to cede unilateral control to a centralized counterparty. Also, keep in mind that the security of staked ETH itself is backed by the protocol's Beacon Chain and the validators supporting it. In any type of derivative implementation other than self-staking, users are ultimately betting on the safety and uptime of their validator(s).

reward tokens as rewards build; token-transfer fees would make this untenable. (Layer-2 scaling might change this some day).

The solution lies in an [oracle contract](#) that reports on the collective performance of Lido's validators. Data on rewards and slashing events are reported by an oracle, and token balances are updated based on the oracle's reports. Holders of stETH are thereby exposed to the performance of the overall validator pool: "Lido makes the stETH token balance track a balance of corresponding balance of beacon chain ether. A user's balance of stETH tokens corresponds 1 to 1 to an amount of ether a user could receive if withdrawals were enabled and instant" (<https://lido.fi/static/Lido:Ethereum-Liquid-Staking.pdf>).





Source: Lido blog, "How Lido Works," November 2020, <https://blog.lido.fi/how-lido-works/>.

This approach introduces an additional layer of risk in terms of oracle reporting. It's also worth noting that even though Lido has developed a way to manage the overall stETH supply, the price of the asset will still fluctuate freely on the secondary market—and as such, it could lose its "peg" with the adjusted supply. This might give rise to interesting arbitrage possibilities between stETH and other ETH 2.0 derivatives.

On the "how does Lido make money?" side of the equation, 10% of staking rewards are

minted as a stETH fee, which in turn is split between node operators and the Lido DAO. The latter has a native governance token called LDO.

The project is already showing signs of early adoption, including recent integration into Zerion. To date, more than [180,000 ETH](#) have been staked using Lido. Like many of its staking derivative counterparts, Lido is not currently open to U.S. users.

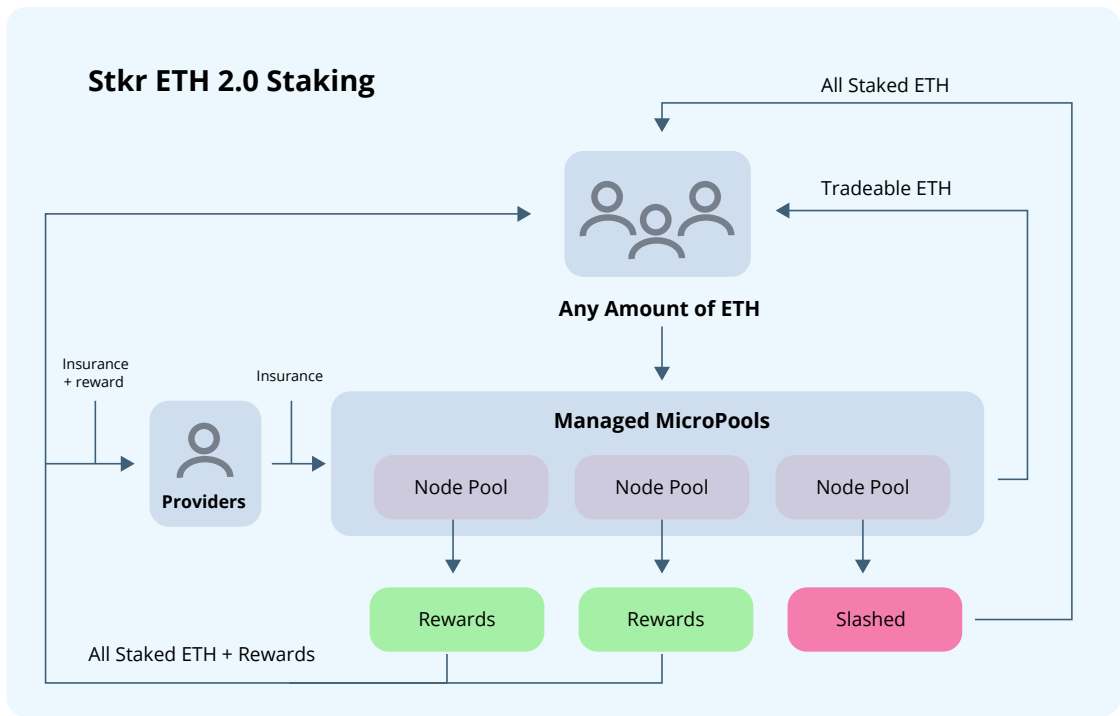
Stkr

Stkr is a project created by the Web3 infrastructure team at Ankr. To date, the platform has locked more than 30,000 ETH staked by nearly 1,300 users.

Architecturally speaking, Stkr is unique in the way it incentivizes individual contributors (or what it calls "providers") to support the platform's pooled validator services. These providers pony up funds into an insurance

fund to safeguard against slashing penalties and receive a 15% fee for their services. Stakers receive a synthetic asset called aETH, which is initially minted on a 1:1 basis with the staked ETH. The project [also mentions](#) a process by which rewards accrue to the token, although it's unclear how exactly these rewards pass through to the ERC-20.





Source: Stkr by Ankr, Staking Simplified Whitepaper version 1.0.0, https://assets.ankr.com/files/stkr_litepaper.pdf.

LiquidStake

LiquidStake—an arm of Darma Capital—falls squarely into the collateralized lending category. However, the resulting derivatives aren't ERC-20 representations of staked ETH. Instead, staked ETH is used as collateral on USDC loans. Darma makes money by adding a fee to the staking yield and by charging interest on these loans.

The most notable limitation with this approach is that there's no obvious way to flow ETH 2.0 staking rewards to its users—although loan amounts could perhaps increase in tandem with accrued rewards.

The project, which targets both retail and institutional money, seems to be counting on partnerships with validator heavyweights like Consensys and Bison Trails to grow its user base. Darma co-founder Andrew Keys, formerly Head of Global Business Development at Consensys, has a strong reputation in the crypto space and could be instrumental in getting more institutions on board.





03 Staking Derivatives on Other POS





Staking Derivatives on Other POS Chains

Of course, Ethereum isn't the only game in town. Nearly all of the "competing" smart contract platforms also employ POS consensus mechanisms, and the promise of more liquid and capital-efficient staking capital is generating innovation across these chains.

Each POS chain has its own idiosyncrasies—for instance, different staking withdrawal periods—and unique architecture for how staking is implemented.

While hypothetically any POS chain could be fertile ground for a related staking derivatives market, the relatively smaller ecosystems of platforms like Solana, Cardano, NEAR, and Tezos means it may take longer for native projects to emerge as meaningful players. In contrast, both Cosmos and Polkadot have more vibrant ecosystems of DApps and users and have already seen notable progress.

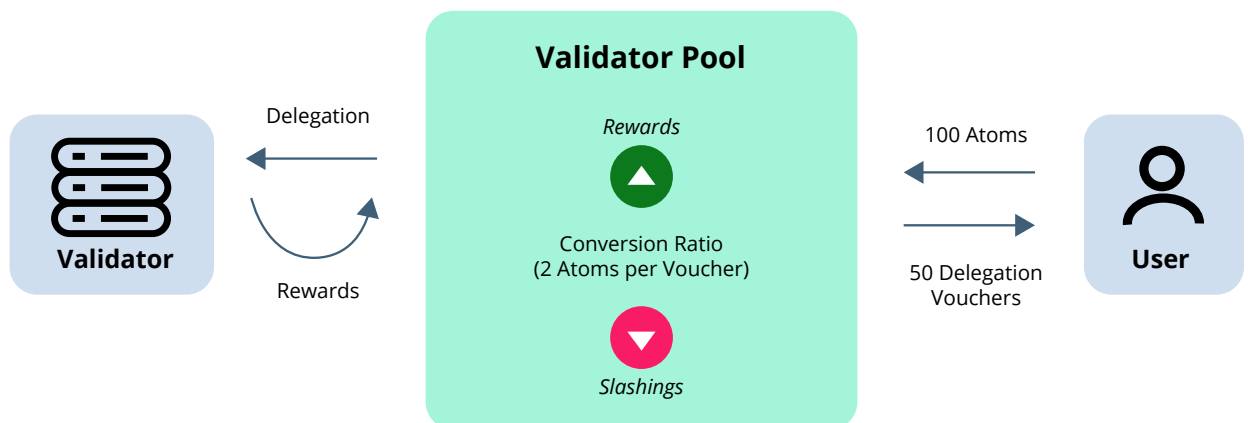
Cosmos

Cosmos staking takes place in the context of an entirely different paradigm than ETH 2.0, where anyone with 32 ETH can validate. Cosmos stakers utilize a delegated proof of

stake (DPOS) system, whereby their ATOMs are bonded to validators. Thus, staking derivatives must coexist with this delegated-validator architecture.

Chorus One describes one such approach:

Instead of directly delegating to a validator, delegators transfer their Atoms to their desired validator's pool. The pool automatically delegates to the respective validator and accrues rewards on behalf of the collective of delegators. Delegators receive delegation vouchers representing their share of the pool in return. These vouchers are fungible tokens that can be redeemed with the pool to receive their share of the pool's updated holdings (a fraction of the delegated Atoms + accrued rewards - slashings).



Source: Chorus One blog, "Delegation Vouchers—A Design Concept for Liquid Staking Positions," June 20, 2019,

<https://blog.chorus.one/delegation-vouchers/>.



Staking derivatives are especially attractive for users who might be seeking immediate liquidity after unbonding their ATOMs, rather than waiting for the protocol-mandated three-week withdrawal period.

Despite the extensive research that's gone into Cosmos staking derivatives, as of now there

are no implementations in production. This should change with the advent of the inter-blockchain communication ("IBC"), which will allow staking derivatives to be transferred between chains. Additionally, Cosmos-based DEXs and AMMs will allow easy access to and arbitrage between derivative tokens.

Polkadot

Readers of our prior report—[New Frontiers: A Deep-Dive Analysis of the Cosmos, Polkadot, and NEAR Protocols](#)—may recall that Polkadot staking entails an unbonding period of 28 days. Sounds like a great fit for derivatives!

In fact, a few options are already springing up in this ecosystem. These include:

Bifrost – A parachain designed specifically for staking liquidity. It utilizes its own token and a native DEX to swap between staked liquidity and derivatives.

Acala – This parachain aims to provide both stablecoin and liquid staking functions. Its "[Homa Protocol](#)" is designed to create staking derivatives using the following implementation:

The Homa protocol will provide liquidity to DOT holders who decide to stake. DOT holders who stake via the Homa protocol will receive the DOT derivative—L-DOT, which are liquid and fungible yield bearing tokens. L-DOTs can be used as collateral in Honzon, which will allow users to take out a loan while still earning rewards from the underlying staked DOT.

StaFi – Short for "staking finance," this project issues a synthetic, tokenized derivative using a mostly-on-chain implementation. Interestingly, the project is chain-agnostic and is positioning itself to provide derivatives for both DOT and ETH.

A deeper analysis of these Polkadot projects can be found [here](#).





04 Key Takeaways





Key Takeaways

Staking derivatives are a boon to the entire crypto ecosystem. Consider the simple fact that staked tokens effectively morph into Schrödinger's cat and exist in two realms simultaneously; as locked liquidity in the POS chain's consensus mechanism, and as liquid

tokens on the mainnet. High-level systemic risks notwithstanding, this arrangement looks like a win-win for users, providers of derivatives, and holders of the POS network's native token.



Expect this field to evolve quickly and keep an eye on how network effects develop. Some protocols might be in a good position to lower fees as they obtain more pooled stake. Others, such as those with an underlying utility or governance token, might see increased usage due to tokenomics—much like we've seen with liquidity mining. As such, we're likely to see a

fat-head, long-tail distribution emerge over the next year. Due to their pre-installed user bases and ease of use, centralized derivatives are in a particularly good position to be among these early winners.

Exciting stuff. But what does this all mean for crypto users?



We're still early

Only a few months have passed since ETH staking launched. Meanwhile, staking derivatives on other chains haven't gained meaningful traction (or haven't been implemented at all). It may make sense to wait a few months before deciding whether to use any of the derivative platforms discussed above. For starters, it seems likely that any obvious exploits (there are probably multiple attack vectors for the smart contract derivatives) would be taken advantage of in these first months. A "shake-down" period

would de-risk these platforms to some extent, along with potentially revealing problems with DApp-specific scaling as more ETH is staked.

It's also likely that the supporting infrastructure will quickly evolve. The most probable development is the rise of staking derivative pools on Curve, which already excels in providing arbitrage opportunities between stablecoins—another asset sub-class with similar prices.

Expect uncertainty on the regulatory and tax front

As we've seen, a number of implementations have blocked U.S. users. Perhaps their attorneys are concerned that the CFTC could view staking derivatives as . . . well . . . derivatives. On the other hand, some projects appear to be less concerned about these risks.

Your author is not an attorney, nor does he play one on Twitter, but it seems likely that a number of staking derivative interpretations might emerge over the next few years; regulators are inevitably slow to understand new crypto technologies, and it'll probably take some time for positions to solidify around this area too.

With respect to taxes, there seem to be a number of grey areas. Would these be considered normal income? Capital gains? Something else? The answers will likely depend on the type of implementation. For instance, a collateralized loan might be taxed differently than receiving fungible staking tokens. Again, this is a field that's likely to evolve in the intermediate-term as tax experts and regulators begin to form opinions. The nature of taxation could ultimately inform your own staking derivative strategy.





05 Further Learning



Further Learning

[Why Stake When You Can Borrow - Tarun Chitra and Alex Evans](#)

[Putting Staking to Work: DeFi and POS Derivatives](#)

[Delegation Vouchers on Cosmos](#)

[A Design for Fungible Staking Derivatives - Sunny Agarwal](#)

