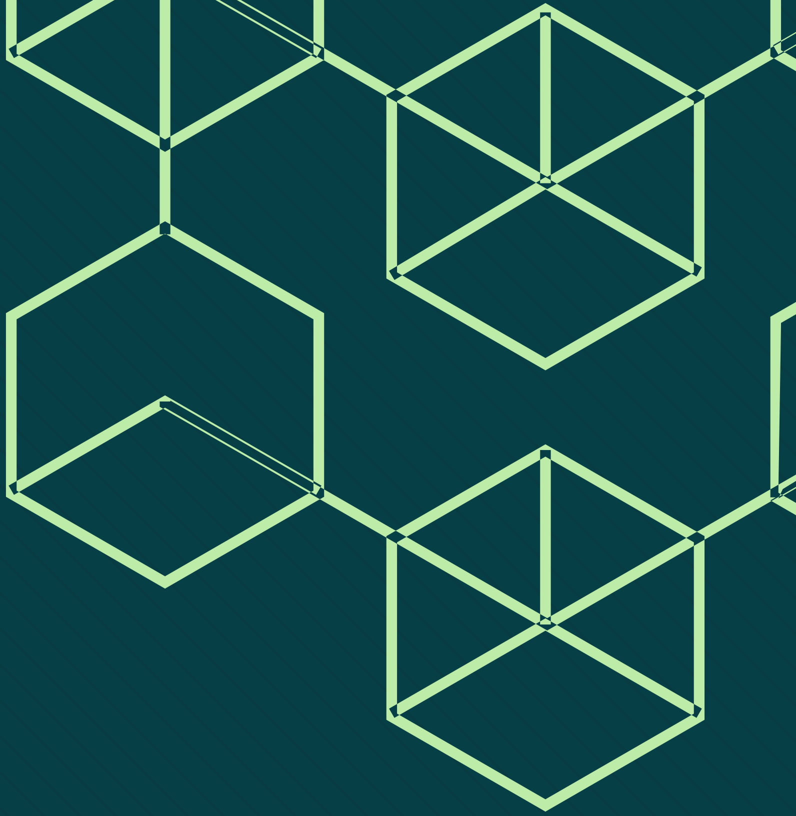
CHORUS



Liquid Staking Research Report

Implications of Proof-of-Stake Assets in Decentralized Finance

Prepared by Chorus One
with contributions from the **Liquid Staking Working Group**
and supported through funding by the **Interchain Foundation**

https://chorus.one

June 2020

Earn Rewards on Cryptoassets

The following research report was put together by **Chorus One**.

We operate highly reliable infrastructure that allows you to participate in major cryptonetworks while staying in control of your assets.

Support our work and increase your holdings by staking with us:

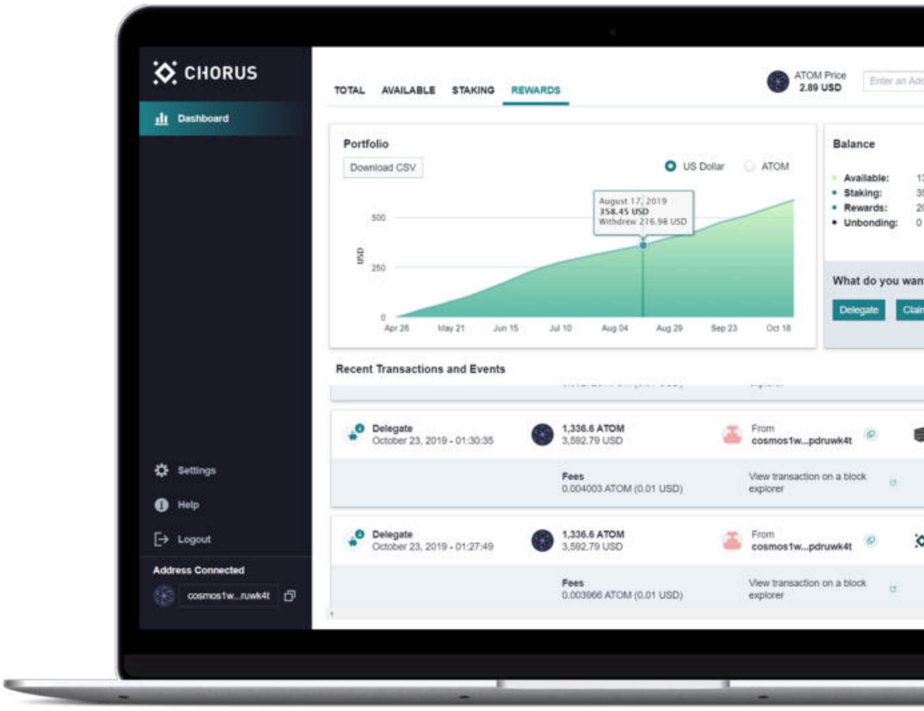
Cosmos Polkadot Terra Celo Solana Kava Centrifuge Band & More Soon

Multi-Network Staking with Anthem

connect
any address on Cosmos, Celo, Oasis, or Terra.

earn
by staking tokens from your Ledger device.

track
your earnings and export reward and transaction data as a CSV file.



Recent Transactions and Events

Delegate October 23, 2019 - 01:30:35 1,336.6 ATOM 3,592.79 USD From cosmos1w...pdruwk4t
Fees 0.004003 ATOM (0.01 USD) View transaction on a block explorer

Delegate October 23, 2019 - 01:27:49 1,336.6 ATOM 3,592.79 USD From cosmos1w...pdruwk4t
Fees 0.003966 ATOM (0.01 USD) View transaction on a block explorer

TRY OUT ANTHEM

Abstract

Proof-of-Stake is becoming the prevalent way of securing decentralized networks. Proof-of-Stake has many advantages over the battle-tested Proof-of-Work, including faster block times and finality, lower operational costs, higher throughput, and a lower ecological impact. As a result, the vast majority of new blockchains rely on Proof-of-Stake for their security.

In Proof-of-Stake networks, virtual assets are used as collateral to determine participants (“validators”) in the consensus process (“staking”). Since these assets serve to incentivize and enforce the correct behavior of validators, protocols may need to be able to confiscate or destroy them in case of misbehavior. So, Proof-of-Stake protocols escrow staked assets, which prevents them from being transferred or used in decentralized finance applications. Also, a delay ("unbonding period") is often enforced by protocols when one wants to stop participating to recover staked assets.

Such restrictions impose economic costs on the holders of staked assets. As a consequence, solutions to circumvent the limitations on staked assets are being developed. Centralized exchanges can easily circumvent these limitations by pooling assets and allowing off-chain agreements to encumber these assets without relying on on-chain enforcement. A burgeoning field has arisen under the moniker of liquid staking, which is seeking to tokenize staked assets to remove restrictions on staked assets and to increase possibilities of how they can be used.

In this report, we introduce and decipher the implications of common restrictions used by current Proof-of-Stake protocols. We establish desired characteristics for liquid staking, analyze the solutions that centralized custodial entities can provide, and contrast those with non-custodial approaches. We highlight a variety of benefits and risks - from improvements in liquidity and price discovery to the impact on network security, protocol governance, and validator centralization.

We conclude that liquid staking is rapidly developing and inevitable. Proof-of-Stake protocols should see liquid staking not as a threat but as a positive force that could accelerate innovation, open up new business models, and most importantly, provide a decentralized alternative to the ever-growing power of centralized exchanges.

Table of Contents

Background

History of Proof-of-Work

Satoshi Nakamoto's Bitcoin whitepaper emerged from the global financial crisis of 2008.[1] In early 2009, the Bitcoin network launched with a headline in the genesis block: “Chancellor on brink of second bailout for banks”. The motivations of the project were clear. With the frailty of our financial systems exposed, the quest to create an alternative, voluntary, transparent currency and peer-to-peer payment network began.

This had been a long-pursued dream among crypto-anarchists and cypherpunks. Previous attempts like DigiCash[2] and E-Gold[3] suffered from a critical flaw. As these systems required a central operator, they were not resilient. By targeting this central point of failure, powerful adversaries like a government could shut them down. Satoshi’s critical breakthrough was the invention of Nakamoto consensus. In Nakamoto consensus each miner produces cryptographic hashes and only if the hash includes a certain amount of leading 0s, the network’s nodes accept the corresponding block as valid. This process is also known as mining or Proof-of-Work.

Participating in the Proof-of-Work process is as simple as downloading software, syncing the blockchain, and using the machine’s computational power to look for hashes. The chance of producing a block depends on the rate at which one can produce these hashes. Since that is primarily a function of the computational power of the machine and energy deployed in the process, mining is a capital intensive competitive game in which parties aim to reach the lowest cost through economies of scale. The advantage of mining is that as long as a majority of the hashing power is controlled by honest miners, the network can be trusted. If an attacker wanted to disrupt the network, they would need to invest a tremendous amount of resources to gain control of a majority of the hashing power. This ensures the security of the network.

Proof-of-Work powers the most popular cryptocurrencies to date including Bitcoin and Ethereum. But despite this track record, there are significant downsides of Proof-of-Work. These limitations have driven work on alternative Sybil resistance mechanisms for many years, most notably Proof-of-Stake.

[1] "Bitcoin: A Peer-to-Peer Electronic Cash System - Bitcoin.org." https://bitcoin.org/bitcoin.pdf. Accessed 19 May. 2020.

[2] "DigiCash - Wikipedia." https://en.wikipedia.org/wiki/DigiCash. Accessed 19 May. 2020.

[3] "E-gold - Wikipedia." https://en.wikipedia.org/wiki/E-gold. Accessed 19 May. 2020.

Introduction to Proof-of-Stake

Proof-of-Stake (PoS) is an umbrella term for Sybil resistance mechanisms that use native cryptoassets as collateral to determine participation in the consensus process of a blockchain network.

The term collateral stems from the medieval Latin collateralis, from col- "together with" and lateralis (from latus, later) - "side", indicating that collateral is something that is pledged in addition to the main obligation of a contract. In the context of Proof-of-Stake, the main obligation is for participating nodes to faithfully follow the protocol's rules, which is ensured by putting up native cryptocurrency tokens as a security deposit - the collateral.

Nodes associated with private keys that run the protocol's software are called validators. They order and validate transactions, communicate with each other, and update their ledger to stay in sync with other participants in the network. As described above, validators in Proof-of-Stake networks are backed by collateral in the form of cryptocurrency tokens ("stake"). Token holders that stake ("stakers") contribute to the network security by selecting trustworthy validators and increasing the cost of a potential attack. They receive tokens as compensation for this in proportion to their stake backing ("staking rewards"). The size of these rewards is also impacted by further factors such as network issuance rates, transaction fees spent within the network, staking participation rates, and validator-specific factors such as uptime and commission rates.

Well-known networks that currently use some type of Proof-of-Stake mechanism include Tezos, Cosmos, Algorand, EOS, Stellar, Hedera Hashgraph, Solana, Celo, Keep, Terra, Ontology, TRON, Neo, and ICON. Many other well-funded projects that are expected to launch with or introduce some form of PoS include Ethereum 2.0, Polkadot, Cardano, Chainlink, Dfinity, NEAR, NuCypher, Oasis, Coda, SKALE, and AVA. At the time of writing, the market capitalization of live PoS networks is already exceeding ten billion dollars.[4]

All Proof-of-Stake protocols require collateral to be placed in escrow controlled by the network in order to register validators in the consensus process. In most protocols the staked collateral can be seized should the associated validator provably deviate from the protocols' rules ("slashing"). This mechanism is used to disincentivize attacks on the network, such as signing two different blocks of transactions at the same height ("double-signing"). Some protocols such as Avalanche and Ouroboros do not use slashing and instead rely solely on honesty assumptions.

[4] "Global Charts | Staking Rewards." https://www.stakingrewards.com/global-charts. Accessed 27 May. 2020.

Finally, a core principle in many Proof-of-Stake implementations is the concept of delegation. This term refers to the ability for token holders to allocate the voting power associated with their staked collateral to an entity that will run the validator infrastructure on their behalf. In many cases, delegation is built into the core protocol (e.g. Cosmos and Tezos), while others (e.g. Ethereum 2.0 and NEAR) rely on smart contracts to introduce this feature.

Why Proof-of-Stake?

There are a variety of advantages that Proof-of-Stake has over Proof-of-Work for securing decentralized networks:

1. **Faster and Absolute Finality**
   In PoS networks it generally takes significantly less time for a transaction to irreversibly be included in the ledger. This massively improves the user experience of participating in the decentralized economy. It also makes cross-chain interoperability easier.

2. **Higher Performance**
   PoS protocols can scale to higher transaction throughput which makes them suitable for applications that are computationally intensive or require many interactions.

3. **Environmental Sustainability**
   PoS does not require operating specialized large-scale data centers to perform Proof-of-Work computations. This dramatically lowers the energy consumption and CO^2 emissions of decentralized networks.

4. **Larger Design Space for Economic Incentives**
   The ability to program economic incentives into PoS protocols enables game theoretic designs that can be more resilient to attacks and efficient with respect to what is paid for the security and the computation provided.

5. **Lower Cost of Security**
   In Proof-of-Work, block rewards and transaction fees are all used to build and operate mining infrastructure or result in profits for the mining industry. As such, they are fully dilutive for token holders.

Rewards in Proof-of-Stake networks mostly go to token holders that stake and only a fraction goes to validators. Thus, the effective cost of securing Proof-of-Stake networks is mostly below 1% annually.[5]

Protocol Restrictions on Staked Assets

One of the most difficult aspects of designing a decentralized network is that once launched, it is controlled by many different stakeholders that act in their own interests. Those interests and the interplay between them are hard to predict upfront. But teams designing protocols need to do exactly that when they define the initial architecture, rules and parameters of a network.

Bitcoin itself offers a demonstration of this challenge. There is no question that Satoshi did an exceptional job at setting the initial Bitcoin project up in a way that would lead to a sustainable ecosystem. But based on historical records, it seems that Satoshi did not anticipate the advent of mining pools or ASICs.[6] Those two innovations have become defining factors in the make-up of the Bitcoin mining industry today. Bitcoin mining works, but it looks radically different from the "one CPU one vote" vision that Satoshi outlined in the whitepaper.

This point illustrates that Proof-of-Stake ecosystems might also turn out radically different from the way the protocol designers originally envisioned. In this paper, we argue that this is already happening. Besides the general difficulties in anticipating the evolution of complex systems, a reason for this is also that Proof-of-Stake protocols were mostly designed by people strong in cryptography, distributed systems and consensus theory. Rigorous economic and game theoretic thinking about the interplay of the incentives of token holders, validators and other key players has not been at the forefront of Proof-of-Stake design.

We will revisit this topic, but for now, let's examine the two primary restrictions that Proof-of-Stake protocols impose on staking assets:

[5] As an example, at the time of writing, Cosmos has an effective inflation rate of 6.4% that is distributed to stakers. On average, validators charge a 8% commission rate resulting in an effective cost of security of about 0.512% (6.4%*8%). Data: https://www.stakingrewards.com/asset/cosmos

[6] "The Book of Satoshi." https://www.bookofsatoshi.com/. Accessed 19 May. 2020.

Escrow

In Proof-of-Stake networks, staking assets are used as collateral to register validators in the consensus process. This means that while assets are staked, they are held in an escrow on the network. Consequently, staked assets are inaccessible to the token holder while they are being used to secure the network. This is true for all PoS protocols so far.

In PoS networks with slashing, the deposited collateral is also used to ensure the proper behavior of validators. In those networks, staking assets behave similarly to the security deposit a tenant might put into a restricted account before moving into a rented apartment. Just like the landlord will be able to draw from that account to compensate for infractions, the network has access to the collateral to enforce penalties.

Unbonding Period

Another restriction in most PoS protocols with slashing is that even when a token holder decides to exit a staking position, they are only able to do so with a delay. This is most commonly referred to as the unbonding period. Some protocols also enforce minimum staking durations with stake maturing and becoming withdrawable only after the selected period has passed.

One reason to enforce a delayed withdrawal is so that if a validator violated the protocols' rules, but the infraction is only discovered later, on-chain evidence can still be presented and cause a slashing event during the unbonding period.[7]

Another reason is that this delay reduces how often a light client has to connect to the network to stay informed about rotations in the active validator set. The unbonding period ensures that there will be a detectable fault if an incorrect history is provided to a light client node that is syncing the headers of the chain at least once within the span of an unbonding period.[8]

Finally, there are a variety of other considerations for why protocols need unbonding periods and similar delays to activate or deactivate stake. These include limiting validator turnover, the enforcement of correlated slashing to encourage resilient validator node setups, and ensuring cryptographic primitives like randomness schemes are unbiasable.[9]

[7] "Proof of Stake FAQs · ethereum/wiki · GitHub." https://github.com/ethereum/wiki/wiki/Proof-of-Stake-FAQs. Accessed 25 May. 2020.

[8] "Cosmos Network Whitepaper" https://cosmos.network/resources/whitepaper. Accessed 25 May. 2020.

[9] "Serenity Design Rationale - HackMD." https://notes.ethereum.org/s/rkhCgQteN. Accessed 19 May. 2020.

The Unbonding Premium: Estimating the Cost of Protocol Restrictions

Restrictions enforced by Proof-of-Stake protocols come with costs to those staking. These take on three dimensions: the opportunity cost associated with staking assets being locked in escrow, the cost due to the enforced exposure to the underlying staking assets price during the unbonding period, and the cost associated with the lack of liquidity during this time. In the following section, we aim to analyze how market participants may price these costs.

As it is helpful to consider the staking lifecycle for this exercise, we will use the Cosmos staking design to illustrate. We will also use a variety of assumptions, including a constant price of $2/ATOM for the purpose of the following discussion.

Cosmos

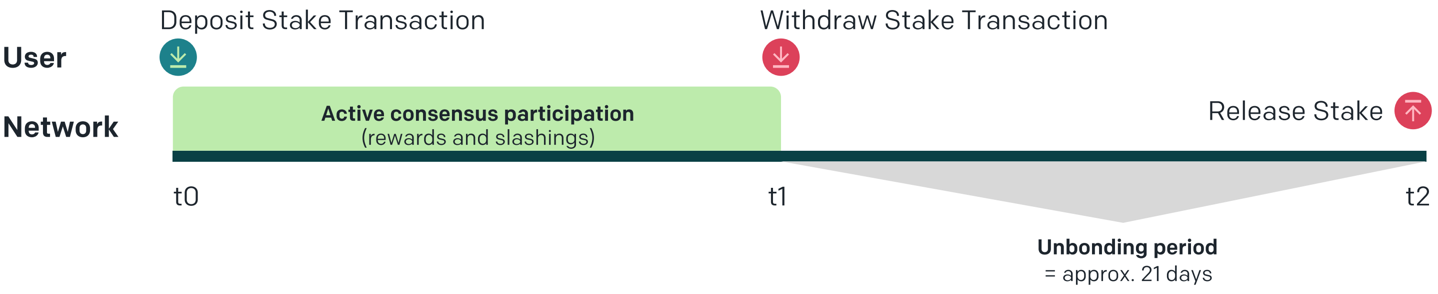


Figure 1 : Staking Lifecycle on Cosmos. *t0: begin staking, t1: initiate withdrawal, t2: reclaim collateral.*

Opportunity Costs

A token holder exiting a staking position will forgo the staking rewards that would accrue during the unbonding period. While unbonding, stake is locked and unproductive, thus the staker is forced to miss out on staking rewards. This opportunity cost to staking should be taken into account in yield calculations.

Let's say ATOM holder Alice wants to unbond her 1,000 ATOM position and the expected annual reward rate is 8%. Given her ATOM position is not receiving any rewards for 21 days, she will miss out on around 4.61 ATOM ($9.22), or 0.46% of her balance.[10]

[10] 1,000 * (21/365) * 8% = 4.61 ATOM. 4.61 ATOM / 1,000 ATOM = 0.46%.

To deduct the opportunity cost of the unbonding period it may make sense to frame it in terms of alternative investment opportunities for the respective asset that are not subject to staking protocol restrictions. This could e.g. include Compound-like money market protocols. Since such a market does not yet exist on a large enough scale for any PoS token, we will need to make assumptions around associated borrowing and lending rates. There are reasons to assume that these might converge to the staking reward rate of the asset.[11]

We will, for the illustrative purpose of this section, assume that there exists a money market that offers borrowing and lending for the respective staking asset at the assumed reward rate of 8%.

The Cost of Illiquidity and Neutralizing Volatility

The price of the inability to liquidate stake when trying to exit a position can be reasoned about as follows. When Alice issues her withdrawal transaction, she will know when and how many tokens she will receive, meaning she could sell those future tokens to someone. Provided a futures market exists for the underlying staking asset, Alice could use it to get instant liquidity meaning she will not be exposed to the risk of ATOM volatility any longer. It should be noted that she will still be subject to slashing risks of her validators during the unbonding period.

Since such markets do not yet exist for staking assets, at least not on a large scale, we may reason about costs associated with the illiquidity of unbonding stake differently.

Essentially, what Alice could try to do is to lock in the price of ATOM at the time of the withdrawal. This would not enable her to get liquidity on her position, but it will neutralize the price volatility of ATOM as measured with respect to a global reserve currency. To do this in practice, Alice would short the equivalent amount of ATOM that she is withdrawing for the duration of the unbonding period. This will make her indifferent to price movements since the gains or losses on the short position will inversely mirror those of her unbonding tokens. By combining the long position enforced by the unbonding period with an equal sized short position, Alice is able to create a neutral position.

[11] "Competitive equilibria between staking and on-chain lending." 4 Feb. 2020, https://arxiv.org/abs/2001.00919. Accessed 25 May. 2020.

As discussed above, there is limited data on borrowing rates for ATOM, so we will assume the interest rate to equal our example reward rate for ATOM for this illustration. To calculate the price to neutralize volatility during the unbonding period, we will also need to take into consideration the capital cost of upholding the short position, which we will do using borrowing rate data for USD stablecoins from decentralized finance lending protocols on Ethereum. We will also assume Alice will need to overcollateralize her short position by 150% in USD, pay 8% interest on her borrowed ATOM, and 4% interest on her borrowed USD collateral.[12]

Using these assumptions, the capital cost to neutralize the enforced volatility exposure in our example would amount to $16.12, or 0.81% of her initial 1,000 ATOM ($2,000) balance. [13]

Doing this Alice has locked in the price of her unbonding tokens, but she will still only get the liquidity after the unbonding period has finished. If Alice wants to receive cash at the point when she issues the withdrawal transaction, she could take on a loan for the duration of the unbonding period with the repayment amount equal to what she knows she will receive when the unbonding has finished ($2,000). The interest paid on this loan, which in our case amounts to $4.59 (or 0.23% of her initial balance)[14] could be regarded as the cost of the illiquidity associated with the unbonding period.

Conclusion

This example tried to illustrate how to think about the unbonding premium, which reflects the costs associated with unbonding periods taking into account opportunity costs, capital costs of neutralizing the volatility of the underlying asset, and the cost of the inability to instantly liquidate a staking position. Using some realistic assumptions, we found that offsetting volatility and accounting for opportunity costs and illiquidity together results in a unbonding premium amounting to 1.5% of the final staking balance in our Cosmos example ($29.93 ($16.12+$9.22+$4.59) of the $2,000 position).

[12] "DeFi Rate." https://defirate.com/. Accessed 19 May. 2020.

[13]

Borrowing Cost ATOM:	$2,000 * (21/365) * 8% = $9.22
Required USD Collateral:	$2,000 * 150% = $3,000
Capital Cost USD Collateral:	$3,000 * (21/365) * 4% = $6.9
Total:	$9.22 + $6.9 = $16.12. $16.12 / $2,000 = 0.81%

[14]

Liquidity Loan (USD):	x * (1+(21/365)*4%) = $2,000
(no overcollateralization)	x = 1,995.41
	interest = $2,000 - $1,995.41 = $4.59. $4.59 / $2,000 = 0.23%

The Futility of On-Chain Restrictions

Given the costs imposed by restrictions on staked assets, the question naturally arises if there are ways in which they can be removed. Could assets be staked without requiring stakers to give up liquidity? How can staked capital be used as efficiently as possible?

It turns out that there are many different ways of circumventing the restrictions Proof-of-Stake protocols impose upon staked assets. In addition to bringing liquidity to holders of staked assets, most of these approaches also enable stakers to use their assets as collateral in other contexts. Expanding the collateral base for financial protocols in this way introduces a new kind of composability. It opens up a large design space for applications that allow stakers to improve their capital efficiency and to manage their risk exposure.

In the remainder of this paper, we will examine different proposed approaches to circumvent Proof-of-Stake protocol restrictions and discuss their implications and tradeoffs.

We will begin with the topic of exchange staking. Exchange staking is particularly important to understand, since it is largely unaffected by on-chain rules around staking.

Cryptocurrency Exchanges and Custodians

To understand how exchanges can circumvent protocol restrictions, it helps to consider how a cryptocurrency exchange works on a high level.

An exchange is an entity that stores customer funds and enables them to use services on the exchange platform. By abstracting away the blockchain component and using an internal database to keep track of customer interactions, a cryptocurrency exchange is able to offer trading with near instant settlement and other services that are not limited by protocol rules which using a blockchain for transaction settlement entails.

In practice, an exchange is pooling assets deposited by their customers in a few accounts controlled by the exchange team. Funds held in these accounts are able to participate in decentralized networks in the same way that they are for an account owned by a single user; from the protocol perspective an exchange account looks exactly like any other.

How Pooling Staked Assets Circumvents Limitations

To use an example, an exchange with $50 million worth of a particular staking networks' tokens in customer deposits can use those tokens to stake, earn associated rewards, and share those with customers. At the same time, exchange users are able to continue to utilize their tokens on the platform, e.g. exchanging tokens with each other, or using tokens as collateral for margin trades. This is possible because updates to customer balances are tracked in an off-chain database and do not require on-chain interactions. The ability to reuse collateral is seen as a significant driver in turning cryptocurrency exchanges into full fledged platforms that offer many different financial products. See the Multicoin report on Binance as an example.[15]

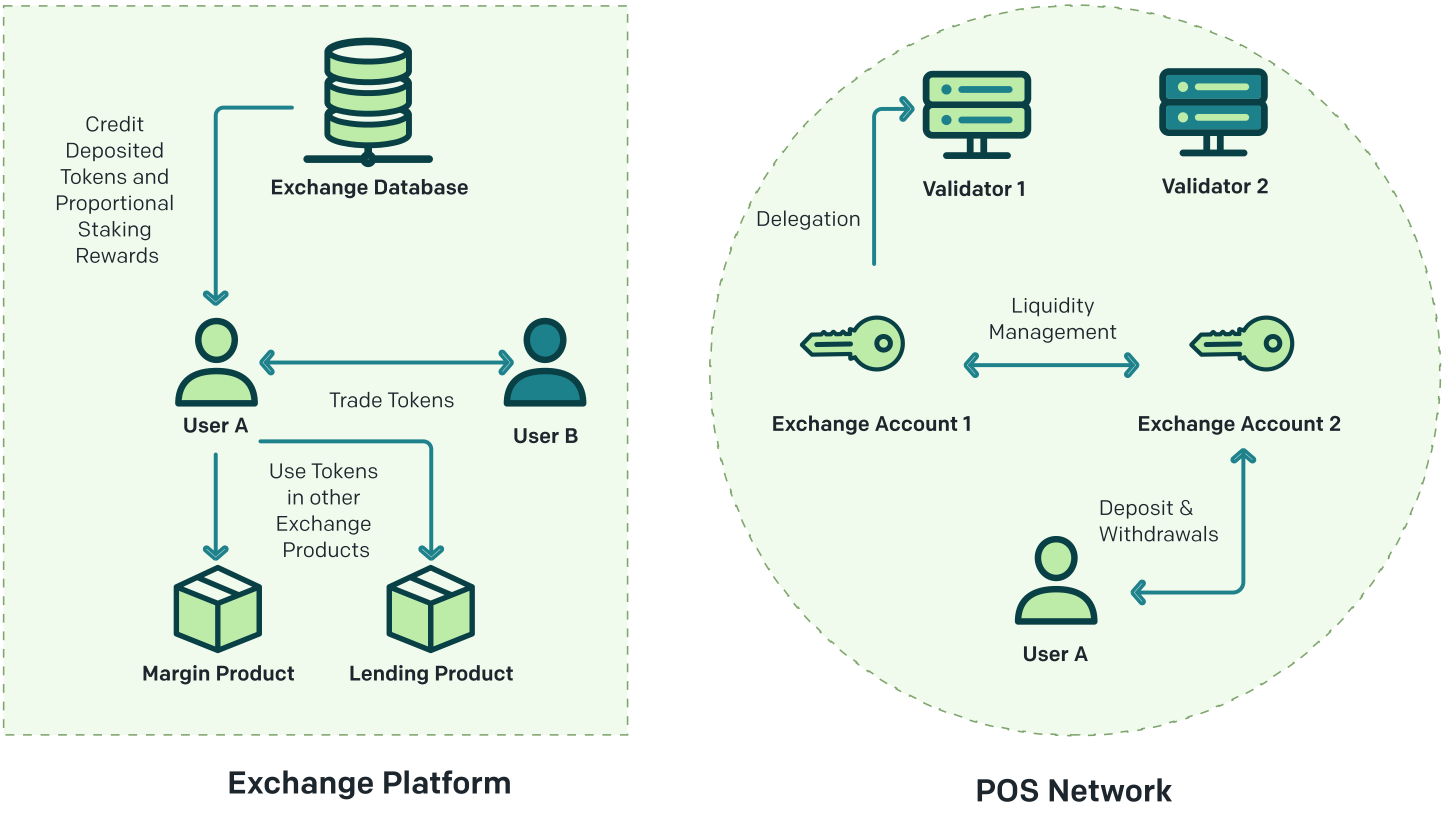


Figure 2: Exchange Staking Illustration.

[15] "Multicoin Capial - Binance is Blitzscaling" https://assets.ctfassets.net/qtbqvna1l0yq/6pDLEyWGLWffhvCDDD3R0c/030aac52f2a70a0ca2a1404497d426b4/Binance_is_Blitzscaling.pdf. Accessed 19 May. 2020.

With most staking protocols, the exchange team still needs to worry about slashings and customers withdrawing tokens among other things, but by managing the associated processes well, they are able to optimize capital efficiency and offer a vastly superior product compared to self-custodying holders of staking tokens in most current protocol designs.

As an example, an exchange could stake only 80% of the deposited tokens and ensure liquidity by reacting to withdrawal demand accordingly. Even in the case of an unexpected large influx of withdrawals, exchange users would still simply need to wait for the unbonding period to pass, which is what they would need to do anyway when self-custodying.

Current Exchange Staking Examples

To illustrate that this is not just theory, we will shortly explore how cryptocurrency exchanges and other custodial entities are offering staking to their customers. At the time of writing, the three exchanges Binance, Coinbase, and Kraken in combination control nearly 20% of the active stake on the currently largest Proof-of-Stake network Tezos.[16] The trajectory on other networks looks largely similar, with exchanges often controlling double-digit percentages of a network’s stake.

Binance

Binance is operating their own validators on various networks including Algorand, Cosmos, Tezos, and many others. By depositing supported tokens on Binance, users earn staking rewards which the exchange calculates by taking frequent snapshots of user balance and distributing all of the earned rewards accordingly.[17] In addition, the Binance validator on Cosmos e.g. charges only a 2.5% commission and accepts delegations from self-custodying token holders.[18]

Binance also allows users to trade tokens and to utilize the balances they hold on the platform in other financial products, e.g. margin trading or lending.[19] It is unclear how Binance would deal with slashing events from publicly available material, potentially the exchange’s insurance fund would cover those.[20]

[16] "Tezos Blockchain Explorer - TzStats." https://tzstats.com/cycle/234.

[17] "Binance Staking | Staking Coins | Staking." https://www.binance.com/nl/staking.

[18] "Binance - Mintscan." https://www.mintscan.io/validators/cosmosvaloper156gqf9837u7d4c4678yt3rl4ls9c5vuursrrzf.

[19] "Binance Now Lets Users Borrow Against Crypto ... - CoinDesk." https://www.coindesk.com/binance-now-lets-users-borrow-against-crypto-holdings-to-fund-futures-trades.

[20] "Secure Asset Fund for Users (SAFU) - Binance" https://www.binance.vision/glossary/secure-asset-fund-for-users.

All accessed May 19, 2020.

Bitfinex

Bitfinex has recently entered the staking game and offers staking for Cosmos, EOS, Tezos and V.Systems with Algorand and Tron to be added soon. Bitfinex specifically allows trading of staked tokens on their platform. The exchange will only stake a portion of tokens to manage withdrawal liquidity, similar to what we described above. In the official FAQ[21] Bitfinex states:

"In the unlikely event that withdrawals by other users exceed the "un-staked" portion of the tokens we hold, it is possible that withdrawals will be delayed until the staked tokens are released. The duration of the potential delay would depend on the applicable protocol."

Coinbase

Coinbase is offering optional staking to clients of its custodial service Coinbase Custody and for Coinbase retail users (but not for Coinbase Pro). So far, this service is available on Tezos, Cosmos, and Algorand. On Tezos, Coinbase is posting the funds that are subject to slashing themselves and charges a 25% commission rate.[22] On Cosmos, Coinbase is also covering slashing penalties for customers.[23] There are plans to expand this offer to other networks, e.g. Polkadot.[24] At the time of writing it is unclear whether Coinbase users will be able to trade protocol tokens with an unbonding period amongst each other.

Kraken[25]

Kraken offers staking for Tezos, with plans to add Cosmos and Dash. Kraken does not allow trading while staking, but since there is no unbonding period for delegated tokens on Tezos, users can move tokens instantly from their staking to their trading wallet. It is unclear from public documentation how Kraken handles slashing. Interestingly, staked tokens on Kraken do impact margin trading equity. Staked XTZ can be used as collateral, but a 50% haircut is applied, potentially to account for slashing risks.[26]

[21] "Bitfinex Coin Staking." https://staking.bitfinex.com/.

[22] "Earn Tezos Proof of Stake Rewards - Coinbase." https://www.coinbase.com/staking.

[23] "Coinbase Custody launches staking for Cosmos" 20 May. 2020, https://blog.coinbase.com/coinbase-custody-launches-staking-for-cosmos-56898adf579e.

[24] "Coinbase Custody to Support Polkadot Staking." 14 Apr. 2020, https://www.coindesk.com/coinbase-custody-to-support-polkadot-staking-with-up-to-20-returns.

[25] "Overview of Staking on Kraken – Kraken." https://support.kraken.com/hc/en-us/articles/360037682011-Overview-of-Staking-on-Kraken.

[26] "Collateral currency – Kraken." https://support.kraken.com/hc/en-us/articles/204585998-Collateral-currency.

All accessed May 22, 2020.

Benefits and Risks of Exchange Staking

In the previous section, we described how exchanges are pooling assets and how this allows their users to circumvent on-chain restrictions that protocols impose on staked assets. These additional degrees of freedom allow exchanges to create staking products that are far superior to what non-custodial staking providers can offer.

In particular, an exchange can allow trading of staked assets and effectively remove the impact of the unbonding period for their users through efficient liquidity management. An exchange can also allow usage of staked assets as collateral for other applications as long as they happen within the confines of the exchanges. This could include things like margin trading, lending, and supplying collateral for derivative trading. And these are just some of the possibilities. An exchange can also offer insurance for slashing events with relative ease.

Moreover, as exchanges have another lucrative business model through charging trading fees, it is easy for them to charge 0% commission on validation to attract staking assets to their platforms and strengthen network effects. Finally, exchanges can provide an excellent user experience, since people don't have to worry about managing private keys and can rely on the more familiar web 2.0 username / password paradigm. Exchange staking also has the advantage that no changes to the base protocols are required, since it is entirely handled off-chain.

On the other hand, there are downsides to exchange staking as well. Users are required to store their staking assets on accounts controlled by the centralized exchange, which means a large scale exchange hack could have devastating consequences. But even more important are the long-term effects on the health of Proof-of-Stake networks.

When staking through a custodial entity, one delegates control over all rights associated to the asset. Even if the entity is regulated and instituted schemes that enable greater decentralization, e.g. by enabling customers to choose validators they are staking with, the entity ultimately is in control and theoretically able to change rules or to abuse its power. This is especially dangerous in protocols with on-chain governance, a topic we will return to in a later section.

In addition, a downside is that assets on such a custodial platform will largely be limited to using that platform's services. As an example, it is not possible to store a staked asset on Binance and then use it as collateral in BlockFi or Maker to take out a loan. This dynamic might lead to increasing concentration among exchanges and reinforce the network effects of large exchanges.

To level the playing field for non-custodial staking and to incentivize self-custody of cryptoassets to foster true decentralization, a variety of other approaches designed to minimize the impact of protocol restrictions are emerging. This research paper bundles these approaches under the moniker *liquid staking*.

Liquid Staking

Definition

We use the term *liquid staking* to describe protocols that issue on-chain representations of staked assets in a decentralized network. Through tokenization, liquid staking protocols allow users to get liquidity on staked assets and enable the usage of staked assets as collateral in (decentralized) financial applications. Other terms that have been used to describe such protocols are *staking derivatives* and *programmable staking*.

Derivative staked tokens are a claim to the underlying, illiquid staking positions that remain exposed to above mentioned protocol limitations. These tokenized and thus liquid representations of a claim can be used in various financial products. This means stakers could earn additional yields or easily manage their risk exposure in various ways, e.g. with respect to slashing risks associated with validators. We will expand on this type of composability and highlight the potential benefits and risks of tokenized staking positions in decentralized finance after introducing our taxonomy of liquid staking approaches.

Taxonomy

In the process of this research, we identified four categories of liquid staking: native, non-native, synthetic, and custodial.

Native liquid staking solutions are those in which the issuance of derivative tokens is implemented as part of the main protocol at the core level of the respective network. We separate this category out from other non-custodial approaches because in this special case liquid staking is intrinsically linked with the protocol. Thus, there may not be an incentive for other entities to create liquid representation of staked assets as the protocol itself already offers a solution to limitations associated with staked assets.

Non-native refers to non-custodial liquid staking solutions in which a separate, trustless protocol is issuing the tokenized staking position. This category offers a wide design space and includes approaches to liquid staking that are based on smart contracts custodying staked assets (DAOs[27]), controlling accounts from different blockchains via interoperability protocols (e.g. interchain accounts[28]), or through other cryptographic techniques including secure multi-party computation (secure MPC[29]).

[27] "Decentralized autonomous organization - Wikipedia." https://en.wikipedia.org/wiki/Decentralized_autonomous_organization. Accessed 19 May. 2020.

[28] "chainapsis/ethereum-interchain-account - GitHub." https://github.com/everett-protocol/ethereum-interchain-account. Accessed 19 May. 2020.

[29] "Secure multi-party computation - Wikipedia." https://en.wikipedia.org/wiki/Secure_multi-party_computation. Accessed 19 May. 2020.

Synthetic liquid staking refers to purely financially engineered staking positions. This category differs from the others as it does not involve the core staking protocol and its associated restrictions as described above, but instead refers solely to a contractual agreement between two (or more) parties. This could e.g. mean two parties agree to exchange cash flows mirroring staking rewards of a particular Proof-of-Stake protocol and some other (potentially fixed) cash flow in an interest rate swap.

Custodial liquid staking refers to approaches in which a centralized entity in control of the private keys participating in staking issues tokenized representations of staked assets to enable users to receive benefits of staking while abstracting away protocol restrictions.

To summarize, we introduce the following taxonomy to help categorize approaches to liquid staking:

Table 1: Liquid Staking Taxonomy Examples.

	Liquid Staking				
	Native	**Non-Native**	**Synthetic**	**Custodial**	**Exchange Staking**
Details	Liquid staking as part of the core protocol design. Tokenized representations of staked assets are issued by the core protocol itself.	A secondary, trustless on-chain protocol is in charge of the staked assets and issues tokenized claims. This protocol can exist as a smart contract or on another blockchain that is in some way able to communicate with the core staking protocol.	Tokenized financial agreements between entities that mirror the cash flows associated with staked assets. Restrictions of the core staking protocol do not apply.	Custodial entities in control of private keys issue tokenized representations of staked assets.	Custodial entities allow users to trade and use assets in other products on their platform without explicitly tokenizing stake.
Examples	Delegation Vouchers	Everett, Stafi, StakeDAO, Acala, Rocket Pool (from Eth2 rollout phase 2), any smart contract-based protocol	Synthetic Staking Reward Swap	StakerDAO, Rocket Pool (during Eth2 rollout phase 0 and 1).	Binance, Bitfinex, Kraken

In addition to these categories there are solutions that achieve some of the benefits of liquid staking solutions, but do not fall into our taxonomy because they do not tokenize staked assets. B-Harvest's delegation exchange is an example of this.[30]

It should also be noted that concrete implementations often consist of a mix of custodial, non-custodial, and sometimes also synthetic elements. As an example, StakerDAO's governance process is entirely on-chain, but operations involving staking are managed in a custodial, centralized, and regulated manner.[31]

We will return to discuss implementations introduced in this taxonomy after taking into consideration the wider implications of liquid staking.

[30] "Cosmos Network Forum - Enabling transfer of delegation ownership" 17 Jun. 2019, https://forum.cosmos.network/t/discussion-enabling-transfer-of-delegation-ownership/2324. Accessed 19 May. 2020.

[31] "StakerDAO: The Future of Decentralized Financial Governance." https://www.stakerdao.com/. Accessed 19 May. 2020.

Risks and Benefits of Liquid Staking

So far we have learned about Proof-of-Stake and its advantages, as well as common protocol restrictions and associated costs. We went into how exchanges are able to circumvent restrictions without changing the base protocol and what this may mean for Proof-of-Stake networks. We defined liquid staking and introduced our taxonomy and different approaches that currently exist. The following chapter will take a holistic look at the risks and benefits of liquid staking regardless of the particular implementation. The final part of this research paper will discuss current proposed and implemented designs.

A Building Block for Decentralized Finance

Tokenized staking positions may be used as building blocks for other financial applications. This composability is an essential feature of decentralized finance and has proven to foster innovation in the Ethereum ecosystem. As an example, MakerDAO's stablecoin DAI can be borrowed and lent using the Compound protocol.[32] This ability in turn led to other applications automating interactions between the two protocols to optimize yields and to lower risks for token holders engaging with these protocols.[33]

Tokenizing staking positions will give token holders a higher degree of freedom in managing their assets and will accelerate decentralized finance innovation. The following section expands on potential use cases and goes into benefits of liquid staking approaches before covering concerns and risks.

Staked Assets as Collateral

One of the primary arguments in favor of liquid staking is the ability to use staked assets as collateral in other financial applications. For example, instead of having to choose between lending a staking asset in a Compound-like on-chain lending protocol and staking it, tokenized staking positions could be integrated in such protocols enabling stakers to manage their risk exposure and to earn additional returns on their staked assets.

[32] "Dai is now available on Compound - Compound - Medium." 30 Nov. 2018, https://medium.com/compound-finance/compound-adds-dai-437d66190588. Accessed 19 May. 2020.

[33] "Maker - Compound bridge - InstaDApp." https://instadapp.io/bridge/. Accessed 19 May. 2020.

Improving Liquidity of Staked Assets

As described above, a core limitation of Proof-of-Stake protocols are restrictions that result in an inability to liquidate staked assets, e.g. the common unbonding period. Liquid staking solution will allow stakers to trade a representation of their staked assets and thus improve liquidity of staked assets.

Enabling Advanced Financial Products

As alluded to before, tokenized stake opens up permissionless innovation for staking assets and enables other financial products to be built on top, allowing stakers to more easily manage their exposure, e.g. with respect to:

- Slashing risk of a particular validator (slashing insurance).
- Diversifying across multiple networks and validators (e.g. tokenized ETF-like index products).
- Other structured products (e.g. combining tokenized staking positions with put options on the underlying token to create fixed income products).

In addition, derivative staked tokens provide additional on-chain information that can be used to inform protocol parameterization.

Improving User Experience

Tokenized staking positions could make it easier to participate in staking and simplify the creation of advanced financial products. There is an argument to be made that simply owning a token will improve the user experience of staking by reducing complexity on multiple levels:

- No need for users to send delegation, reward withdrawal, re-staking and similar transactions to the network.
- Less need for normal users to understand protocol details around restrictions such as unbonding periods.

- Simplified integration for wallets and other interfaces since they will mostly only need to track token holdings and respective prices. This also simplifies accounting for users and may potentially come with tax benefits to users due to capital gains-based taxation instead of being income-based.
- Simplify staking integration for custodians and exchanges alike since they would only need to custody and list associated tokens.
- For some native solutions: simplified accounting in the staking protocol itself since iterations can be made on a per validator basis instead of considering every delegation separately.

Improving Price Discovery for Staking Assets

Tokenized staking positions are priced by the market and will thus help the price discovery of both underlying staking assets, as well as validator-specific risk, although the latter varies depending on the proposed implementation.

To illustrate the intuition behind this, let us first consider price discovery in a world without staking derivatives or centralized exchanges staking on behalf of their customers. Most Proof-of-Stake protocols design incentives in a way that a large portion of tokens are utilized in the staking process to ensure the protocol is costly to attack. In longer standing live networks like Cosmos and Tezos between 70-80% of tokens are at stake at all times. In a world where these tokens are locked, only the remaining portion of unstaked tokens can actively participate in price discovery. In an extreme scenario, this could mean that the lack of trading liquidity increases the volatility of the underlying asset. The existence of liquid markets for staking derivatives, both on centralized exchanges and in the decentralized finance ecosystem, alleviate this risk.

In addition, validator-specific derivative tokens could in the long-term allow the market to price risks associated with respective validator nodes. Tradable derivatives of stake will reflect the risk of a (set of) validator(s) getting slashed or earning subpar returns in their price. If the market expects a particular (set of) validator(s) to be at a high risk of getting slashed or going offline and missing out on returns, this will be reflected via a discount of the market price in that derivative token. It should be noted that there are other reasons why a particular derivative token could be trading at a discount, e.g. based on differences in liquidity.

Network Security and Systemic Risk

We will now turn to potential negative consequences, especially focusing on the impact liquid staking may have on network security and governance.

Systemic Risk

Drawing parallels to historic failures of the financial system, liquid staking may increase systemic risk in the decentralized finance ecosystem by adding another layer of complexity. Given the many different protocols and ways to interact with cryptoassets in decentralized finance, there is a chance that the collapse of one particular part of the stack will lead to a greater domino effect potentially damaging the entire ecosystem as it becomes more interwoven.

However, there are some major differences between the cryptoassets space that makes a catastrophic unwind as we saw in the financial crisis less likely. These are:

1. **Transparency**
   Almost all information on a blockchain is publicly accessible.[34] This means that the information needed to identify mispricings and systemic risks will be available to anyone. A major issue in the traditional financial system is the lack of transparency. For instance, information about the individual mortgages making up mortgage-backed securities were hard to obtain, making it much harder to understand their risks.

2. **Lack of moral hazard**
   There is no deposit insurance or possibility of a central bank stepping in to provide unlimited liquidity to financial institutions in distress.[35] The increased risk that market participants in the cryptoasset industry have and the lack of possible bailouts should lead to more prudent risk management.

3. **Overcollateralization**
   Most financial contracts in the cryptoasset industry today are overcollateralized. For example, lending platforms generally require in excess of 150% collateralization. The high collateralization and thus low leverage common in cryptocurrencies should decrease systemic risk.

[34] Innovations in cryptography such as zero-knowledge proofs might negate these benefits. However, a liquid staking solution that would making use of such technologies would probably still need to expose key metrics to be adopted.

[35] One might view instances like the "The DAO" hard fork as such a bailout. At this point, it is hard to forecast how PoS network governance will develop and deal with similar situations in the future.

With all that being said, cascades of failures are possible. In addition to financial risks, cryptoassets also rely on, or are held in, relatively untested protocols that can be subject to scams, bugs, and hacks. Systemic risk is a real threat and the decentralized financial ecosystem will need to figure out how to manage risks and how to mitigate potentially catastrophic scenarios.

Stake Centralization

Another vector that requires examination is under which circumstances liquid staking could lead to increased network centralization. We have discussed extensively how the absence of liquid staking will be a major driver for exchange staking. Thus, by making self-custody a more viable and profitable option, one effect will be towards more decentralization. However, it's worth asking whether there are other factors at play that could lead to increased centralization as well. This is important since Proof-of-Stake networks rely on no single entity being able to control the network's consensus process. In most implementations ⅓ of the voting power can stall the network and >⅔ can double-spend tokens.[36]

One of the key benefits of liquid staking is to provide a tokenized version of the staked asset. If this can be traded and used as collateral in decentralized finance applications, it delivers substantial value to the staker. However, if there are no liquid markets or integration into other applications, a tokenized version of the staked asset is basically useless. Thus, there will be network effects, where more usage around a particular liquid staking protocol increases liquidity and utility as collateral, which further drives adoption of that solution relative to competitors. As a result, we can expect that we will only have one or a small number of liquid staking issuance protocols.

Whether this has a centralizing influence on a network will depend to a great extent on the particular design of the liquid staking protocol. For example, we could have a large number of tokens end up being controlled by another blockchain that issues a liquid staking token. This could decrease resilience overall if the validator set of that other chain is smaller, if it has a separate staking token that is less valuable, or if its distribution is more concentrated.

[36] "Consensus without Mining - Tendermint." https://tendermint.com/docs/tendermint.pdf. Accessed 19 May. 2020.

Impact on Validator Incentives

A big concern around liquid staking is the impact that a change in the staking logic could have on validator incentives. The introduction of derivative tokens and associated financial products built on top of them could introduce new behaviors that may challenge the game theoretic assumptions underlying a Proof-of-Stake system.

A core functionality of liquid staking is to create market mechanisms for transferring staking-associated risks between market participants. Most interesting staking-related structured financial products that could be thought of are designed to help participants in the staking economy to adjust their risks. One could e.g. imagine swap instruments becoming popular for staking providers seeking to stabilize their cash flows by selling their future revenue streams for a fixed interest rate to investors that seek to go long on a particular staking network's reward rate.

While most of these products help create a healthy market, there could be some that introduce perverse incentives for validators acting maliciously to profit from their own behaviors or information advantage. We will now expand on two such scenarios that liquid staking may help to enable.

The first scenario requires a liquid lending market for validator-specific tokenized staking positions. A validating entity that is able to borrow large amounts of its tokenized staking positions could be incentivized to act against the interest of token holders staking with it. Essentially, a validator could short its own derivative token and profit from decreases in its price following its (malicious) behavior. Going offline and missing out on rewards or double-signing and getting slashed will decrease the value of derivative tokens. A validator entity that borrowed large amounts could thus profit from this decrease since it will be able to pay back the borrowed tokens at a lower price. The likelihood of such an attack might be negligible for multiple reasons:

1. A large amount of derivative tokens need to be supplied to the lending market and it is unclear if the extra yield from doing so will suffice to incentivize holders to do so, especially because a large borrowing demand would likely raise suspicions.
2. In practice validators are usually known entities that have to expect legal repercussions and loss of reputation should such behavior be uncovered.

It should be noted that there is an element of leverage inherent in this attack. This entity could accumulate stake by touting increased yields (due to the high borrowing demand). To get to a point where this could actually be detrimental to network security, this entity would need to have large amounts of capital available to sustain borrowing demand while setting up this attack. Additionally, the associated stake increase should again raise suspicions in the community.

There is another, potentially more realistic, scenario in which a hacker or another entity manages to gain control of a validator's singing keys and carries out this kind of shorting attack. Interestingly, the threat of such an attack is actually a positive force from the network's perspective, as it should incentivize validators to institute resilient security measures. One can think of this as a decentralized bug bounty program.

A second thought experiment plays out similarly: a validating entity acts maliciously, but bought slashing insurance beforehand and is thus able to net a profit (basically a type of insurance fraud). The reputation and legal arguments presented above would also hold in this scenario. Additionally, there would need to be enough risk underwriters willing to insure that particular validator. If it is an unknown entity this is unlikely to happen. Finally, there is no additional risk on network security in this case, as only the insurance pool would suffer losses.

To guard against these types of scenarios taking place, some Proof-of-Stake implementations introduce self-stake ratios to force validators to have skin-in-the-game. This usually means the address controlling a node needs to stake some portion or a fixed number of tokens itself (e.g. Tezos). In practice, we have witnessed validators on Tezos entering into revenue share agreements with other entities providing a part of this "self-stake" (bond pooling[37]). If the key for self-staking can be a smart contract, validators could also issue tokenized claims on this bond. Overall this practice seems to lead to another variation of liquid staking analogous to tranching in traditional finance. In this example, there are two tranches and only one of them is at risk of slashing, which is the self-stake bond, whereas the second tranche (delegations) are not exposed to this risk and thus earn lower rewards. One could build various other tranching structures for Proof-of-Stake protocols with varying risk sharing parameters.

[37] "What is a bond pool? - Tezos Stack Exchange." 5 Feb. 2019, https://tezos.stackexchange.com/questions/196/what-is-a-bond-pool. Accessed 19 May. 2020

Protocol Governance

Governance of a blockchain refers to the processes by which its rules can be modified. There are various reasons why changing the rules of the blockchain could be necessary. One could increase parameters like the block size to expand the throughput of the system. Or add additional protocol rules to introduce new features. Governance can also come into play when it comes to undoing the effects of hacks or software bugs. The Ethereum hard fork to reverse the theft of the tokens stolen in the "The DAO" hack is the best known example of this.[38]

All blockchains have governance processes, though often they are not explicitly defined, nor managed on-chain. In the example of Bitcoin, some governance power resides with the developers who control the Bitcoin Core repo on Github[39] and some with the miners who choose what software to run. The lack of a clear process by which decisions are reached or conflicts resolved was the main reason why the argument whether the Bitcoin block size should be increased resulted in years of stalemate and ultimately the split of the network into Bitcoin and Bitcoin Cash.[40] It should be noted that many in the Bitcoin community see the complicated governance process as an advantage since the extremely high barrier to changes creates security and predictability.

Ever since the Bitcoin block size debate and Ethereum's The DAO hard fork, governance of decentralized networks has been widely recognized as an important problem. Many newer blockchain networks differentiate by instituting explicit governance processes that are run on-chain. Early examples of these include Decred and Dash that are both Bitcoin forks with added governance features.

Governance and Proof-of-Stake

One of the governance challenges in Proof-of-Work networks is that different constituencies have influence. Miners often invest large amounts of capital into building up large-scale data centers and have considerable say by controlling the consensus process. But their interests can diverge from those of token holders.

This is different in Proof-of-Stake networks. Because staking assets provide the ultimate security guarantees, they are used to select the validator set.

[38] "The DAO (organization) - Wikipedia." https://en.wikipedia.org/wiki/The_DAO_(organization). Accessed 19 May. 2020.

[39] "Bitcoin Core integration/staging tree - GitHub." https://github.com/bitcoin/bitcoin. Accessed 27 May. 2020.

[40] "Block size limit controversy - Bitcoin Wiki." 24 Apr. 2019, https://en.bitcoin.it/wiki/Block_size_limit_controversy. Accessed 19 May. 2020.

As a result, validators are less of an independent constituency and instead accountable to act in the interest of token holders. An obvious option that arises from this is to hand complete control over the governance process to token holders.

Indeed, most Proof-of-Stake networks have chosen to pursue that path. While the particular designs of their governance systems can vary quite widely, they do share the characteristic that the ultimate decision making power lies with the token holders.

Today, there are various Proof-of-Stake networks in operation that have on-chain governance. A well known example is Tezos, which emphasized governance as a key differentiator already in its whitepaper published in 2014.[41] Other Proof-of-Stake networks with on-chain governance that are in operation today include EOS, Celo, Cosmos, Dash, Decred, and Terra. Of the many upcoming protocols set to launch in the coming year many have on-chain governance processes, e.g. Polkadot. However, the support for on-chain governance is not unanimous. Most notably, Ethereum has embraced a more loosely defined off-chain approach to reaching decisions and plans to maintain that even after the switch to Proof-of-Stake.

It is too early at this point to make a general judgement on the success of on-chain governance in Proof-of-Stake systems. For both Cosmos and Tezos, on-chain governance has been successful. In the example of Cosmos, it has been used to activate token transfers, coordinate software upgrades, vote on new features, gauge community sentiment, and even to disburse funds from the on-chain treasury.[42] Similarly, the Tezos governance protocol has been utilized to enact multiple automated chain upgrades, each of which bundled multiple improvements to the core protocol. [43]

Despite these successes, incidents in other networks have pointed to the risks surrounding on-chain governance. As an example, in EOS, token holders can vote for block producers (validators) and the top 21 block producers participate in the consensus process and share inflationary rewards. Since private keys controlling EOS tokens can also vote in governance, exchanges have effective control over the governance rights of the tokens custodied with them. Huobi, one of the largest cryptocurrency exchanges, was found to accept bribes from block producers in order to elect them.[44]

[41] "Tezos - a self-amending crypto-ledger. White Paper - Tezos.com." https://tezos.com/static/white_paper-2dc8c02267a8fb86bd67a108199441bf.pdf. Accessed 22 May. 2020.

[42] "Cosmos Governance Proposals - Mintscan." https://www.mintscan.io/proposals. Accessed 22 May. 2020.

[43] "Tezos Governance Proposals - TzStats." https://tzstats.com/election/. Accessed 22 May. 2020.

[44] "Vote Buying Scandal Stokes Fears of EOS ... - CoinDesk." https://www.coindesk.com/vitalik-called-it-vote-buying-scandal-stokes-fears-of-eos-failure. Accessed 19 May. 2020.

Essentially, Huobi sold the voting rights of their customer's EOS without disclosure or consent for its own gains. A similar situation occurred recently in an ongoing conflict between parts of the Steemit community and Tron founder Justin Sun, who leveraged his influence with exchanges to change who is in charge of the protocol.[45]

Buying Votes

The previous examples do raise the important topic of vote buying. One of the best known investigations of this topic was published by Phil Daian of Cornell University.[46] He demonstrated that vote buying is possible in any on-chain voting system and that blockchains can allow doing this in a more efficient, trustless and even anonymous way.

Daian showed that this is largely independent of the particular design of a governance system or the cryptography used. The challenge is that the blockchain needs to verify cryptographic proofs to tally votes. But those same proofs can also be used to provide evidence of having voted in a certain way enabling token holders to enter into financial agreements to sell votes.

Thus, the key questions that arise are what the impact of on-chain vote buying is and how liquid staking impacts this.

Democracies or Plutocracies

Daian's essay particularly aimed at attempts to replicate democratic voting systems on-chain. In a democracy, you want to have each person's vote count equally. Some will value that vote more than others, but you do not allow payments for purchasing votes.

The important thing to realize is that the governance protocols of Proof-of-Stake systems have little to do with democracies. They are much more akin to the governance mechanism of a stock corporation, where owning more shares confers correspondingly more voting rights. It is less clear in such a system, where control of more assets already results in more influence, whether the buying of votes has negative implications. Notably, it is legal to buy shareholder votes in the US.[47] Given the extensive history of the stock corporation, it seems highly unlikely that this would not have been outlawed in case it was detrimental to shareholder value.

[45] "Why Crypto Should Care About Justin Sun's ... - CoinDesk." 2 Mar. 2020, https://www.coindesk.com/why-crypto-should-care-about-justin-suns-steem-drama. Accessed 19 May. 2020.
[46] "On-Chain Vote Buying and the Rise of Dark DAOs." 2 Jul. 2018, https://hackingdistributed.com/2018/07/02/on-chain-vote-buying/. Accessed 19 May. 2020.
[47] "Shareholder Votes for Sale - Harvard Business Review." https://hbr.org/2005/06/shareholder-votes-for-sale. Accessed 22 May. 2020.

It's worth pointing out that what caused the uproar around Huobi's actions was that they sold the voting rights of tokens that they did not own and without the consent of the actual token holders. In a way, Proof-of-Stake systems like Cosmos and Tezos provide already an indirect way by which validators can purchase voting rights. For instance, in Tezos only validators (bakers) can vote. Thus, by delegating to a validator, the user does transfer voting rights over their tokens. In protocols where validators set commission rates, validators may deploy a strategy to gather voting rights through offering validation services for free (as demonstrated by the Sikka validator on the Cosmos Hub).[48]

Liquid Staking and Governance

The key thing that happens with liquid staking is that the design space opens up. Tokens can be moved across chains. The rights associated with tokens can be separated and owned by different entities. They could be collectively managed by a DAO. All of this can be terrifying when it comes to considering the governance of these networks, since it's simply unpredictable where it will go. Thus, it is useful to keep in mind that the holders of staking assets have a strong interest in ensuring that the governance rights associated with those assets are used in ways beneficial to the overall system.

The most positive influence from liquid staking on governance could come from incentivizing people to custody their own assets. This will diminish the share of tokens that are held with custodial entities, and as discussed earlier, instances when exchanges have used the governance rights of their users have led to the most controversial governance outcomes so far.

[48] "Cosmos is vulnerable: Governance and the Validator - Medium." 25 Oct. 2019, https://medium.com/figment-networks/cosmos-is-vulnerable-governance-and-the-validator-15d698e53b90. Accessed 19 May. 2020.

Approaches to Liquid Staking

For the final part of this report, we will introduce liquid staking solutions, explain their designs, and go into some detail about their potential strengths and weaknesses.

Desired Characteristics

To assist our evaluation, we need to figure out what an ideal liquid staking solution should deliver to a network and its stakeholders. We established the following criteria in discussion with the Liquid Staking Working Group:

Liquidity

The title of this research foreshadows the core outcome that solutions we discuss in the course of this report aim to achieve. Liquidity is a word that is notoriously (ab)used in the decentralized finance ecosystem. The classic definition of liquidity goes as follows: liquidity is the degree to which an asset can be easily converted into cash in the market. A liquid asset can be converted at short notice without incurring significant discounts because there is a reasonable degree of buying and selling volume.

A core premise for liquid staking solutions is to achieve exactly that. Solutions that fragment liquidity across different assets may be less attractive to users than others since there is a higher chance of having to tolerate discounts or not being able to convert staking positions at all.

Fungibility

If several goods are fungible, it means that they are indistinguishable from each other and it shouldn't matter which good exactly one receives. Cryptocurrencies including Bitcoin and staking assets are generally fungible. However, this property is not easy to maintain for liquid staking solutions. Without modifications, a staking position with one validator is different from one with another validator, since validating nodes have different performance, fees, and risk profiles.

An ideal liquid staking solution will be generalizable to different users and validators and fungible among them to limit the fragmentation of liquidity.

Value Divisibility

Another dimension related to fungibility in the context of staking assets is the ability to partially trade a staking position. This is best described in the context of NFTs. In contrast to standard ERC20-like tokens, NFTs can only be traded in their entirety or not at all. A liquid staking solution that allows stakers to partially sell their positions will generally provide higher utility to users than one that does not.

Decentralization-Friendly

One of the desiderata from the network's perspective is to have a solution that doesn't drive centralization with a few entities. In Proof-of-Stake blockchain networks, a single entity or a set of colluding entities with enough cumulative power in the network could effectively control and arbitrarily change the rules of the protocol. There are differences in how specific liquid staking implementations may encourage centralization of stake.

Non-Subtractive to Network Security

Liquid staking solutions shouldn't impact incentives in a way that endanger the operation of the network. The concerns we covered above around liquid staking introducing systemic risk to Proof-of-Stake and enabling new behaviors for stakers are important to consider. Aside from increased risk through financial engineering, the main potential to impact network security arises from high degrees of stake centralization that may be encouraged via liquid staking.

Non-Subtractive to Governance

In networks with on-chain governance implementations, some liquid staking approaches may abstract governance power from users. Thus it is important to consider how liquid staking solutions can be built to take on-chain governance features into account.

Composability

An optimal liquid staking solution will be flexible and allow for permissionless innovation to happen on top of it. This is a core point that we expanded on in a previous section. A solution that enables composability is likely to bring more utility to the decentralized finance ecosystem. A minimal, safe, and modular design allows for more complex products to be built on top. An example of such a product could be ETF-like validator index products or other structured products, e.g. bundling a tokenized staking position with slashing insurance.

Transparency
The 2008/09 financial crisis has shown that being able to identify the sources of systemic risk in an economy is vital. Any sustainable liquid staking protocol must allow analysts to get full visibility of all relevant protocol functions and parameters, as well as the collateral that is underpinning their solution. In practical terms that means we should prefer solutions with on-chain records of collateral over approaches where these records are hard to identify and reconcile. Cryptographic tools like zero-knowledge proofs should be applied, so that liquid staking token holders can verify collateral is available without necessarily disclosing who owns it. Where DAOs are involved their governance processes should be clearly defined and inspectable. Finally, simple liquid staking designs in which risks can be easier to identify should be preferred over highly complex designs.

Evaluation of Approaches

The following section will introduce different approaches to liquid staking and discuss the key strengths and weaknesses of each one.

Standard Delegation

To begin we will describe a standard delegation scheme to familiarize the reader with the illustration style used. In a Proof-of-Stake network like Cosmos, holders of the native staking token can choose validator nodes to participate in the consensus process and earn staking rewards in return.

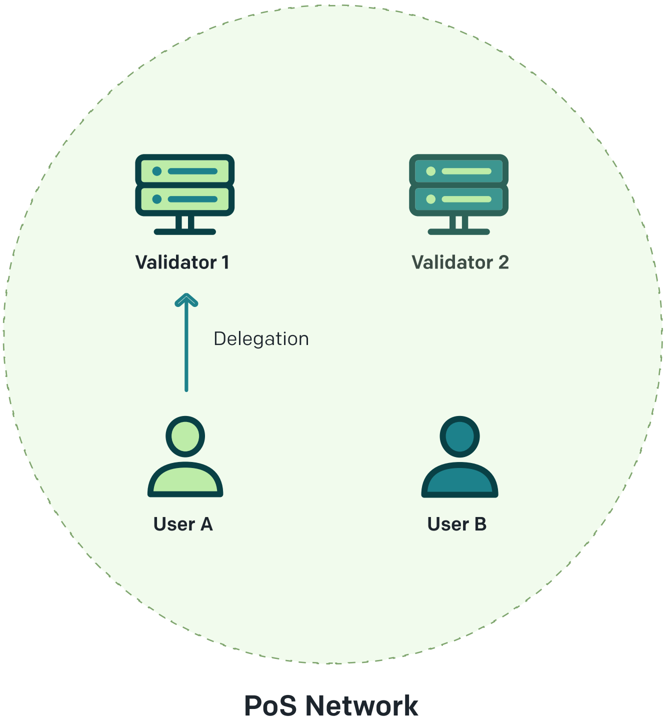


Figure 2: Standard Delegation Illustration

In this scheme, delegated balances cannot be traded directly with other token holders. In some cases, validator nodes can be switched without needing to stop staking, but this usually either takes some time to take effect or leaves the token holder exposed to the slashing risks of both validator nodes for the duration of an unbonding period.

Delegation Exchange

The delegation exchange design, which was first conceptualized by B-Harvest, is an extension to the standard protocol that allows users to trade delegated balances with others. Instead of tokenizing stake, a delegation exchange protocol would allow users to (potentially partially) transfer ownership of their staking account to other accounts.

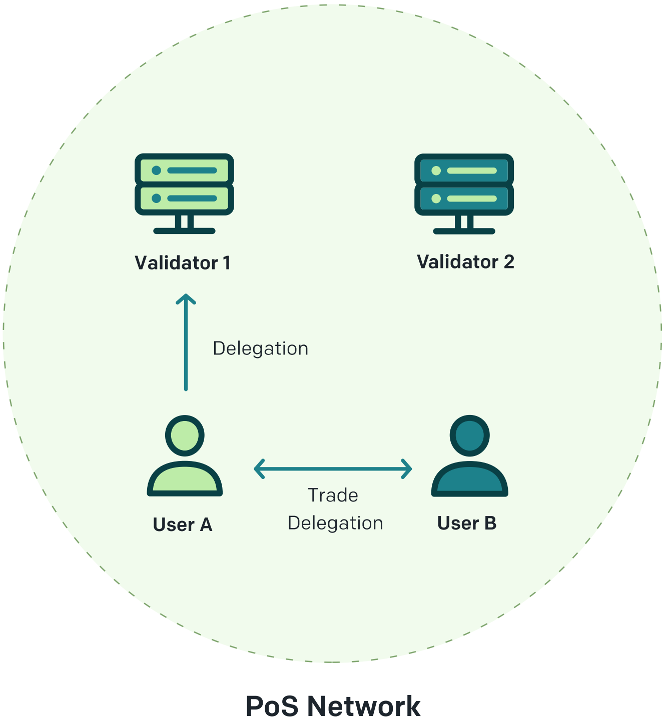


Figure 3: Delegation Exchange Illustration

Strictly speaking, this approach is not a liquid staking solution since it doesn't tokenize stake. However it does solve the problem of a user seeking to get liquidity on their staked assets bypassing the common unbonding period, so we have included it here.

The first iteration of the solution would allow the staked position to be sold via the transfer of the rights to control an account. The position would have to be sold in one piece, and so is not divisible (although a protocol change to split delegations without unbonding periods could potentially fix this in the future) meaning a (trustless) OTC market would be best suited for this design.

B-Harvest's solution requires a group account feature (subkeys) combined with atomic transactions and transaction timeouts. Group accounts allow control over an asset to be reassigned to another account. It also allows for multiple accounts to have a say in the control of an asset. The group account defines a "Delegation Policy", where the rules around what actions can be taken and when are defined, e.g. by a simple majority of members, or some threshold percentage, or maybe a more complicated weighted algorithm.

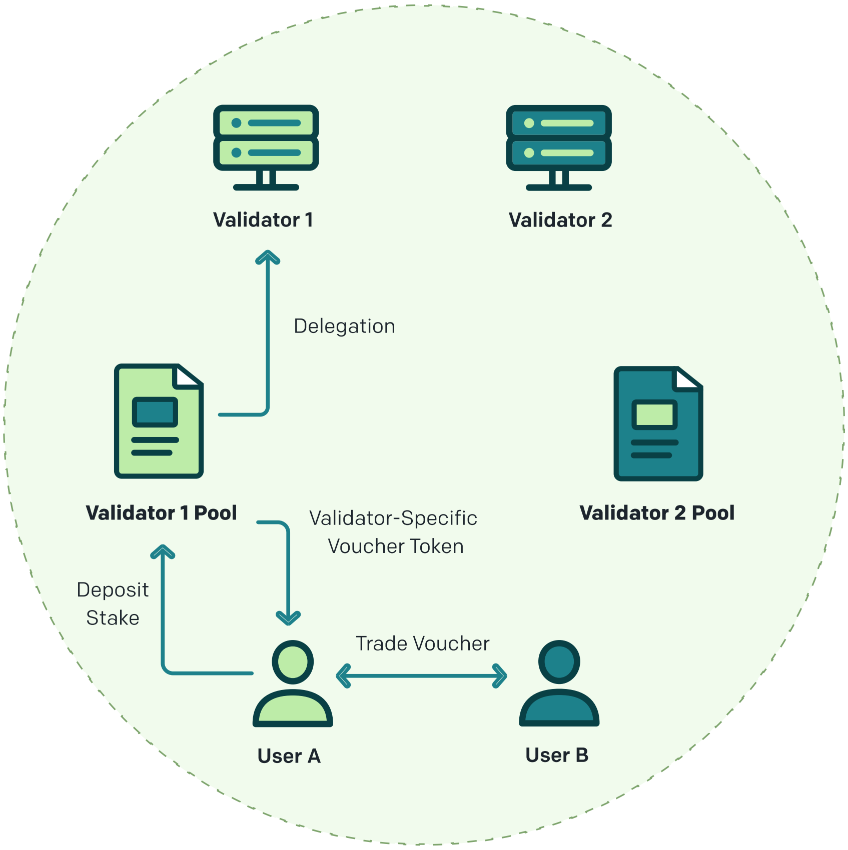
By using simple primitives to build the Delegation DEX, B-Harvest can deploy their solution as soon as Cosmos Hub supports group accounts (scheduled for Cosmos Hub 4).

Key Strengths	Possible Weaknesses
A simple and safe way to deliver liquidity to stakers.	Difficult to build up liquidity in an OTC market.
Completely trustless model that doesn't add any security risks for users.	Not designed to solve the problem of collateral reuse.
Working solution could be ready in very short timescales.	Staking positions are not easily divisible.

Delegation Vouchers

Delegation vouchers describe staking protocols that introduce validator-specific pools that issue tokenized representations to a user depositing tokens. These pools are essentially delegating and accumulating staking rewards, as well as slashing penalties on behalf of their users.

Tokenized vouchers represent a claim on assets within the pool and can be redeemed or traded with other users. This design can both replace the core staking protocol or be built on a second layer with the use of smart contracts. Delegation Vouchers were initially developed by Chorus One and Sikka.[49]



PoS Network

Figure 4: Delegation Vouchers Illustration.

[49] "Delegation Vouchers - A Design Concept for ... - Chorus One." 20 Jun. 2019, https://blog.chorus.one/delegation-vouchers/. Accessed 19 May. 2020.

Delegation Vouchers are a comparatively simple liquid staking protocol. Users could freely trade the vouchers or use them as collateral in applications. The protocol also removes the need to withdraw and re-stake rewards, which improves user experience.

Delegation vouchers are linked to a particular validator, which gives them exposure to their slashing risk and commission rate. However, each voucher is backed by some known amount of tokens enabling users to easily deduct an exchange rate from staking tokens to vouchers.

There is no direct business model associated with Delegation Vouchers to capture value from the system. This makes Delegation Vouchers a more neutral solution that doesn't involve another token designed to capture value. The downside of this is that no single party might have a strong economic incentive to drive Delegation Vouchers to adoption.

In a native solution like Delegation Vouchers, the rules that determine how liquid staking operates are subject to the governance by the staking token holders (as opposed to the holders of some other token or the whims of an exchange owner). This means that the system should evolve more in line with the overall interest of the network.

Another advantage is that Delegation Vouchers remove the concept of token holders "earning" rewards, which could be subject to income tax. Vouchers operate more like a share of a pool, so the only taxable event might be on exit of your position, as opposed to every time a reward is accumulated.

The original doesn't allow support for fees paid in tokens that are not the staking token of the native chain. Chorus One built a version of Delegation Vouchers that includes on-chain auctions to sell off fees earned in other tokens.[50] Sunny Aggarwal has an alternative design that creates fungible Delegation Vouchers without the need for fee auctions, but this design introduces other complexities around transferring account control and requires restrictions due to issues with unbonding periods.[51] The Matic Network team is currently developing their staking design based on the Delegation Vouchers work.[52]

[50] "Decentralized Payment Processing for the ... - Chorus One." 5 Aug. 2019, https://blog.chorus.one/babelfish-payment-protocol/. Accessed 19 May. 2020.

[51] "A design for fungible staking-derivatives - Research-Staking ...." 9 Jul. 2019, https://forum.cosmos.network/t/a-design-for-fungible-staking-derivatives/2441. Accessed 19 May. 2020.

[52] "Derivatives(Liquidity) | Matic Network | Documentation." https://docs.matic.network/docs/validate/validator/derivatives. Accessed 19 May. 2020.

Key Strengths	Possible Weaknesses
Easy to reason about the value of vouchers and easy to use.	Since different delegation vouchers exist for each validator, liquidity gets split across many assets. That might require additional pooling of vouchers on top.
Governance control remains with staking token holders.	No direct associated business model complicates adoption.
Can be built into the core staking protocol avoiding fragmentation of liquidity into second layer solutions.	Fee rewards in multiple token denominations introduce edge cases that complicate the otherwise straightforward design.

Stake DAO[53]

The Stake DAO is a smart contract-governed DAO focused on decentralized finance services, such as issuing derivative tokens (LTokens) to users depositing staking tokens. Users of this liquid staking protocol can specify a predetermined maturity when depositing staking tokens and in return receive tradable LTokens that are fungible for a given network and maturity. The DAO smart contract then stakes tokens with validators that are determined through governance. Stake DAO lives on Ethereum and will start with supporting ERC20 staking protocols such as Livepeer and NuCypher.

The LToken is modeled on Dan Ronbinson's Yield Protocol[54], where the underlying assets (plus rewards, minus any slashing penalties) can be unlocked at a specific date in the future, and so the price approaches the locked value as it gets closer to the redemption date. A Livepeer (LPT) token might be locked for 12 months, along with the rewards from LPT inflation and network fees. LTokens are a claim on a specific pool of assets. When the maturity of a particular pool is reached, LTokens backing that pool are worth exactly what is in the pool, but before that, they might trade at a discount to the value in the pool, where the discount is due to the lack of liquidity.

[53] "research/Stake Capital DAO Light Paper.pdf at master - GitHub." https://github.com/stake-capital/research/blob/master/Stake%20Capital%20DAO%20Light%20Paper.pdf. Accessed 19 May. 2020.

[54] "The Yield Protocol - Paradigm." 31 Dec. 2019, https://research.paradigm.xyz/Yield.pdf. Accessed 19 May. 2020.

This delta between the value of what is in the pool and market value of the LToken, can be used to infer an "interest rate" that is payable on the LToken between now and the maturity date.

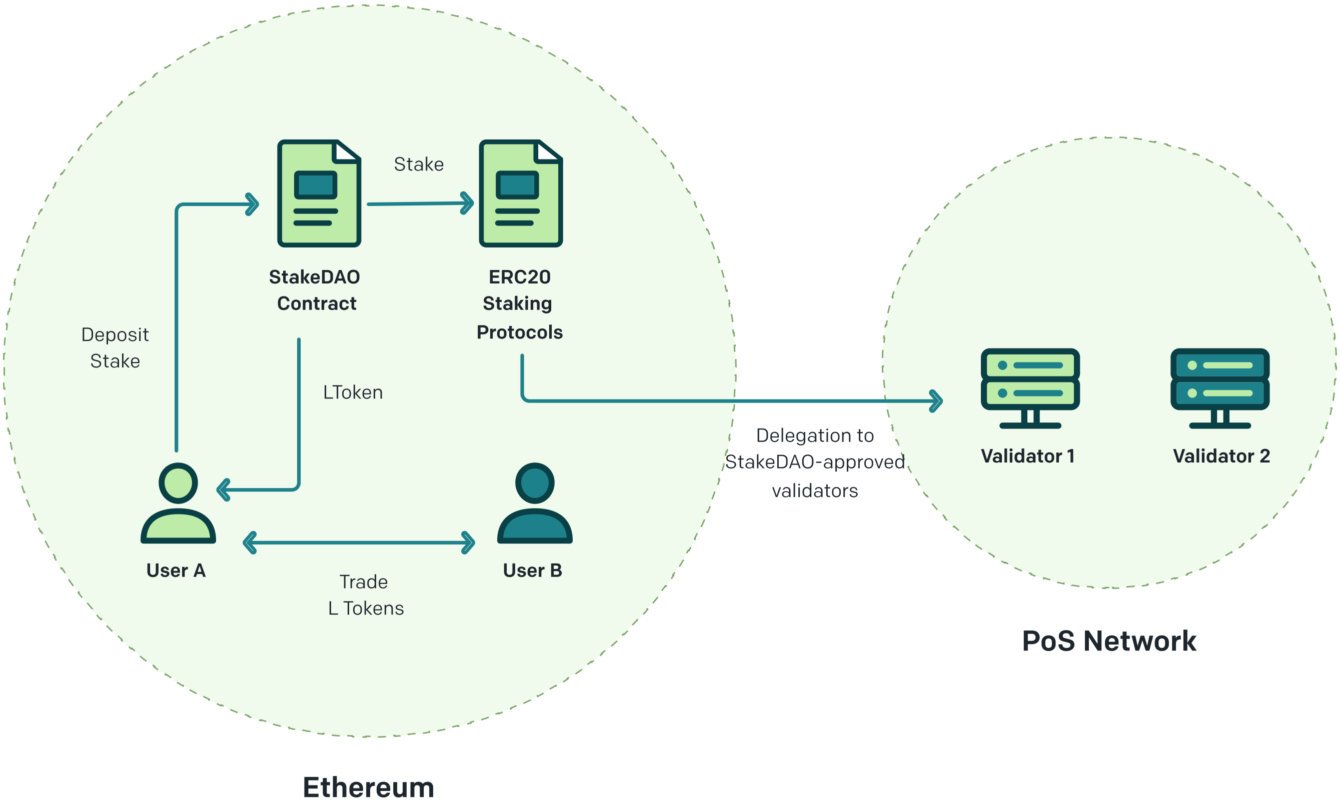


Figure 5: Stake DAO Illustration.

The Stake DAO allows investors to earn Stake DAO SCT tokens in return for providing capital. The core idea is a cashback pool to give rebates to early backers of StakeDAO. Initially, token holders will be able to earn SCT for staking with Stake Capital validators or providing capital to a Uniswap liquidity pool. In the future Stake DAO plans to support other validators to the service and expand into arbitrage services.

Commissions from the invested capital are pooled in a DAO, where some portion goes towards building out and running the DAO code, with the remainder going back to SCT stakers as dividends. The SCT tokens have a fixed supply and are minted over time, with early investors earning more tokens and thus a larger share of DAO rewards when they stake their SCT.

Key Strengths	Possible Weaknesses
Easy to reason about the valuation of liquid staking tokens, due to similarity with bond pricing.	Currently only for ERC20 staking protocols. Not clear when and how bridges will be operational to allow for cross-chain features.
Built on Ethereum, so LTokens have access to DeFi protocols and there are fewer security risks than projects built on less proven chains (of course, the risk of smart contract exploits remain).	Only partially fungible in that each LToken is tied to a specific pool of assets with a specific maturity date.
Smart contract model allows for fast iteration and makes it easy to add new features	Governance voting and validator choice resides with SCT token holders.

Acala

Acala is a decentralized finance project building on Substrate that aims to become a Polkadot parachain. Acala is building two protocols: a stablecoin protocol (Honzon[55]) using Maker-style collateralized debt positions and a staking liquidity protocol (Homa[56]) that allows DOT token holders to receive liquid representations of their staked assets (L-DOTs). Issued L-DOTs will also be accepted as collateral in the stablecoin protocol.

L-DOTs issued by the Homa protocol are fungible since all DOT supplied to the protocol are pooled and staked with validators chosen by Acala Network Token (ACA) holders collectively. In addition, DOT owned by the protocol are rebalanced frequently to keep a portion of unstaked DOT tokens to allow instant redemptions for L-DOT holders who pay a redemption fee that decreases proportionally to how long they are willing to wait for receiving the underlying DOT tokens. The protocol is designed to be generic for any staking asset with Polkadot being the first implementation.

[55] "2. Honzon Stablecoin · AcalaNetwork/Acala Wiki - GitHub." https://github.com/AcalaNetwork/Acala/wiki/2.-Honzon-Stablecoin. Accessed 19 May. 2020.
[56] "7. Homa Liquid DOT · AcalaNetwork/Acala Wiki · GitHub." https://github.com/AcalaNetwork/Acala/wiki/7.-Homa-Liquid-DOT. Accessed 19 May. 2020.

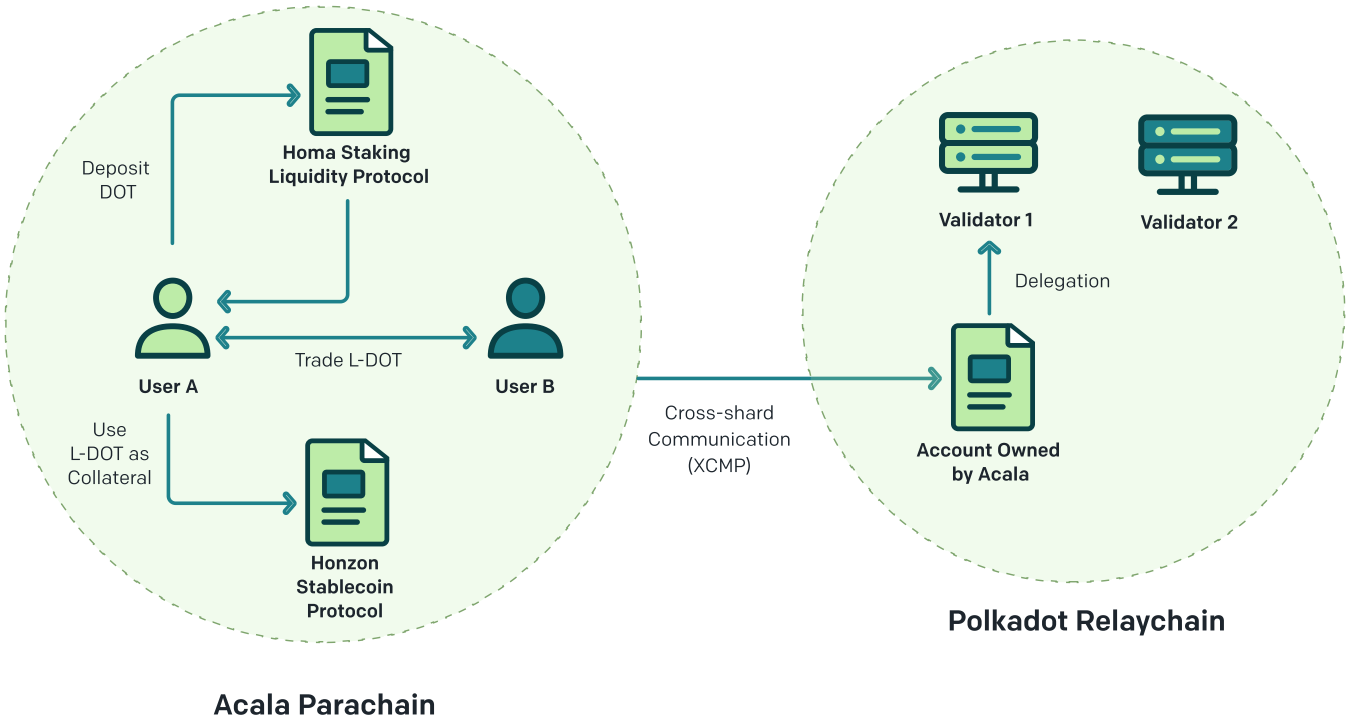


Figure 6: Acala Protocol Illustration.

Key Strengths	Possible Weaknesses
Clear synergies with Acala's Honzon stablecoin protocol.	First iteration only works on Polkadot.
Flexible liquidity management and redemption mechanism.	Governance voting and validator choice resides with Acala token holders.
Only one type of tokenized stake, which provides fungibility and increases liquidity.	Potential for conflicts of interest since both the stablecoin and staking liquidity protocol are governed by Acala token holders.

Everett[57]

Everett was a project that aimed to issue synthetic staked tokens pegged to the original staking token. It consists of its own blockchain that can control so-called interchain accounts on other blockchains through the usage of inter-blockchain communication (IBC).

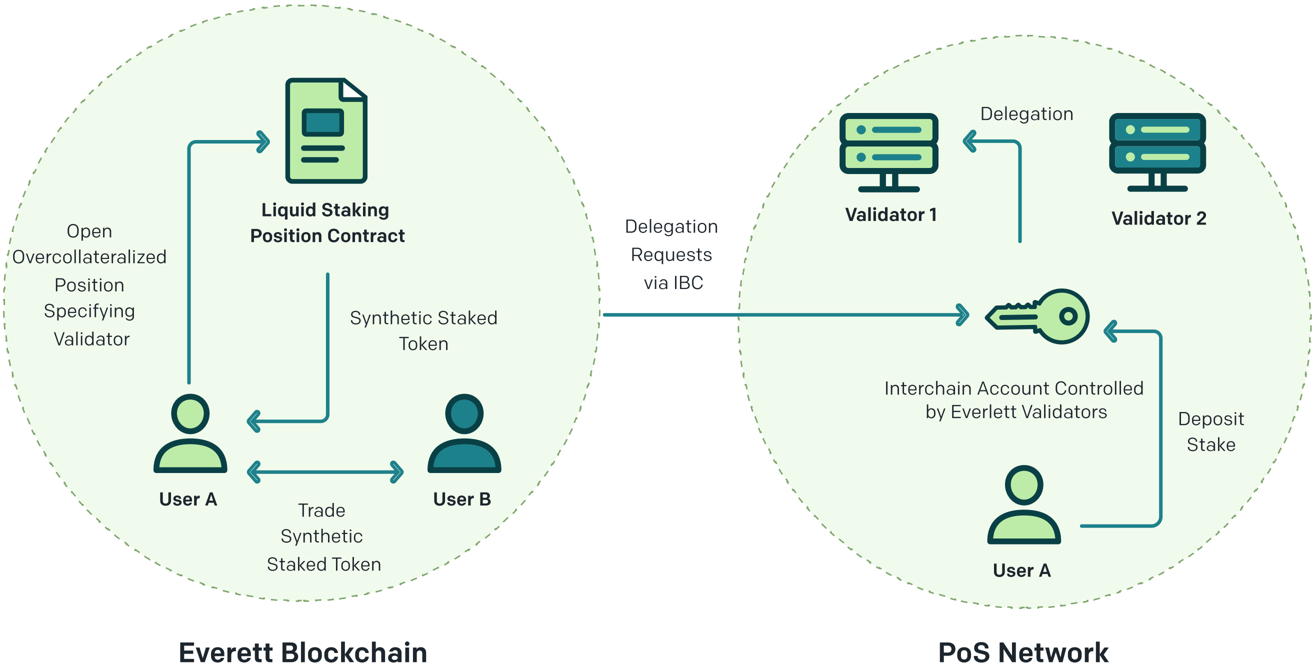

Liquid Staking Position Contract
Open Overcollateralized Position Specifying Validator
Synthetic Staked Token
User A
User B
Trade Synthetic Staked Token
Everett Blockchain
Delegation Requests via IBC
Delegation
Validator 1
Validator 2
Interchain Account Controlled by Everlett Validators
Deposit Stake
User A
PoS Network

Figure 7: Everett Protocol Illustration.

Users are able to deposit staking tokens into the externally owned account to open overcollateralized liquid staking positions (LSP) and mint tradable synthetic staked tokens for the respective network on the Everett blockchain. LSPs work similarly to Maker vaults and use overcollateralization to account for slashing penalties.
Everett's approach is powerful as it provides a unified experience across all Proof-of-Stake chains. Issued generated synthetic staked tokens are fungible on a per-network basis, increasing their liquidity. This cross-chain approach could create powerful network effects if DeFi services start to use their bonded tokens as collateral.

The Everett team, who have in the meantime started other ventures, asserted there will be a peg that will hold between synthetic staked tokens (e.g. "bAtoms") and the original staking tokens (e.g. ATOMs). The basis for this remains unclear. The two instruments have very different properties.

[57] "EVERETT - The DeFi Hub for Staking." https://www.everett.zone/. Accessed 19 May. 2020.

It seems likely that synthetic staked tokens would fluctuate with DeFi demand, whereas the LSPs are much easier to value and likely to be price stable concerning the underlying staked token.

The other issue we see with Everett is around the security risk. The Everett chain would be in control of a large number of PoS staking tokens, so the market capitalization of the Everett tokens would need to be high too, to ensure that an attacker cannot easily take control of the network. To attain a high valuation they would need to have high fees and a high volume of transactions. Potentially, some model of shared security (where they borrow security from other PoS chains) would reduce this risk.

There is also a big unknown around governance. If the Everett model was successful, and a high percentage of staked PoS tokens are used to issue LSPs, then a high percentage of voting power would end up with these LSP holders. It is not clear who would hold these LSPs - possibly only specialized financial institutions will be able to accurately price the slashing risk. So over time, this could change the distribution of voting rights, potentially creating a centralizing effect.

Key Strengths	Possible Weaknesses
Potential to build a unified liquid staking experience across all PoS networks with powerful network effects.	Prone to security issues if the Everett token value is low.
The liquid tokens are fungible.	PoS governance is in the hands of LSP issuers.
High liquidity would make liquid tokens ideal for use as DeFi collateral.	Concerns remain on whether a price peg from synthetic to staked tokens can hold.

Stafi[58]

The Stafi Protocol is another design in which accounts on staking networks are controlled externally. Stafi uses a form of multi-party computation (threshold signatures[59]) instead of relying on blockchain interoperability protocols.

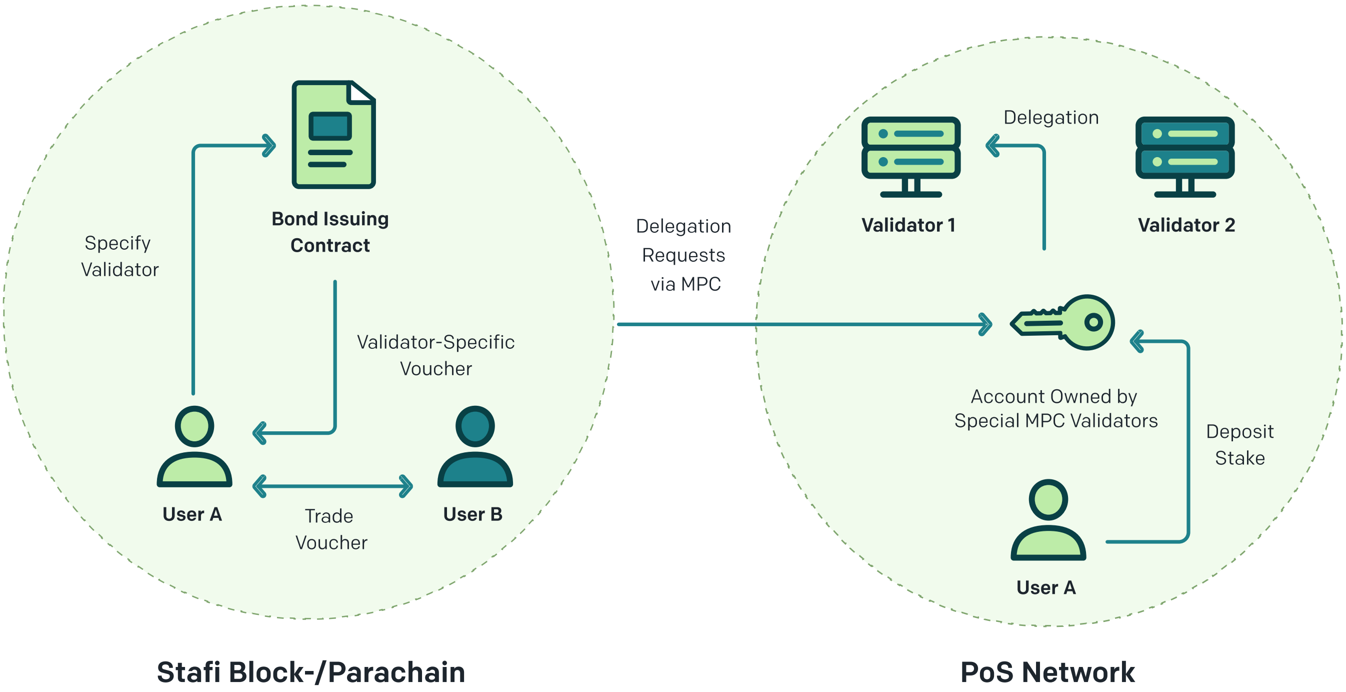


Figure 8: Stafi Protocol Illustration.

A subset of Stafi nodes that are determined through the Stafi token are assigned to create and control account keys on Proof-of-Stake networks via distributed key generation. These nodes then use a threshold signing algorithm that requires a majority of nodes to sign to carry out transactions from the respective account on the Proof-of-Stake network. This allows users to mint tradable liquid staking positions with their deposited staking tokens, because ownership of a specific account with an active staking position can be transferred relatively easily within the protocol.

A subset of Stafi nodes that are determined through the Stafi token are assigned to create and control account keys on Proof-of-Stake networks via distributed key generation. These nodes then use a threshold signing algorithm that requires a majority of nodes to sign to carry out transactions from the respective account on the Proof-of-Stake network.

[58] "Stafi." http://www.stafi.io/. Accessed 19 May. 2020.

[59] "Threshold Signature Schemes - MPC for Cryptocurrency" 15 Aug. 2019, https://www.unboundtech.com/threshold-signatures/. Accessed 3 Jun. 2020.

This allows users to mint tradable liquid staking positions with their deposited staking tokens, because ownership of a specific account with an active staking position can be transferred relatively easily within the protocol.

In Stafi, if N nodes generate a key, M of N are required to sign a transaction. As long as M of N nodes are online and not acting maliciously then all works fine. But if N-M+1 nodes are offline or act maliciously the transactions will fail. The values for M and N will be parameters chosen when the network launches. The set of nodes controlling an account will be rotated regularly to ensure that nodes don't have enough time to collude to steal funds. How often this rotation takes place is yet to be determined (note: the example in the whitepaper refers to 16 of 21 nodes, with keys rotated every 24 hours, but this may not be the parameters chosen at launch).

Stafi's token will need to generate enough value to secure all of the bonded assets. There are issues around validator collusion to steal private keys, which means the Stafi chain will require a high number of nodes to minimize the probability of collusion. Stafi has an incentive protocol with slashing mechanisms to guarantee security and correct behavior of Stafi nodes, which plans to include multiple assets as collateral in the long run. These security requirements imply that Stafi will need to extract a lot of value in fees to pay for this security.

Key Strengths	Possible Weaknesses
Potential to build a unified liquid staking experience across all PoS networks with powerful network effects.	Prone to security issues if Stafi token value is low.
Doesn't require interchain accounts so is portable to any PoS chain that can support threshold signatures with distributed key generation.	Risk of node collusion to steal private keys, so needs a high number of nodes.
Governance rights stay attached to tokens, allowing for a more flexible governance model.	Potentially limited liquidity because tokens will only be fungible for a specific validator.

StakerDAO

StakerDAO is a DAO governed by STKR token holders on the Tezos blockchain. The goal of the DAO is to issue regulated investment products for the blockchain space. The first product is a liquid staking design with custodial elements and a token called Blend. StakerDAO annually elects a council that votes on proposals proposed by their operations team and STKR token holders that are then implemented by the StakerDAO operations team. Aside from the governance process that happens on-chain, all operations are carried out manually by humans meaning this solution is trusted. However, all processes will be fully transparent and on-chain with real-time data, including, but not limited to, wallet balances, rewards generated, and buybacks.

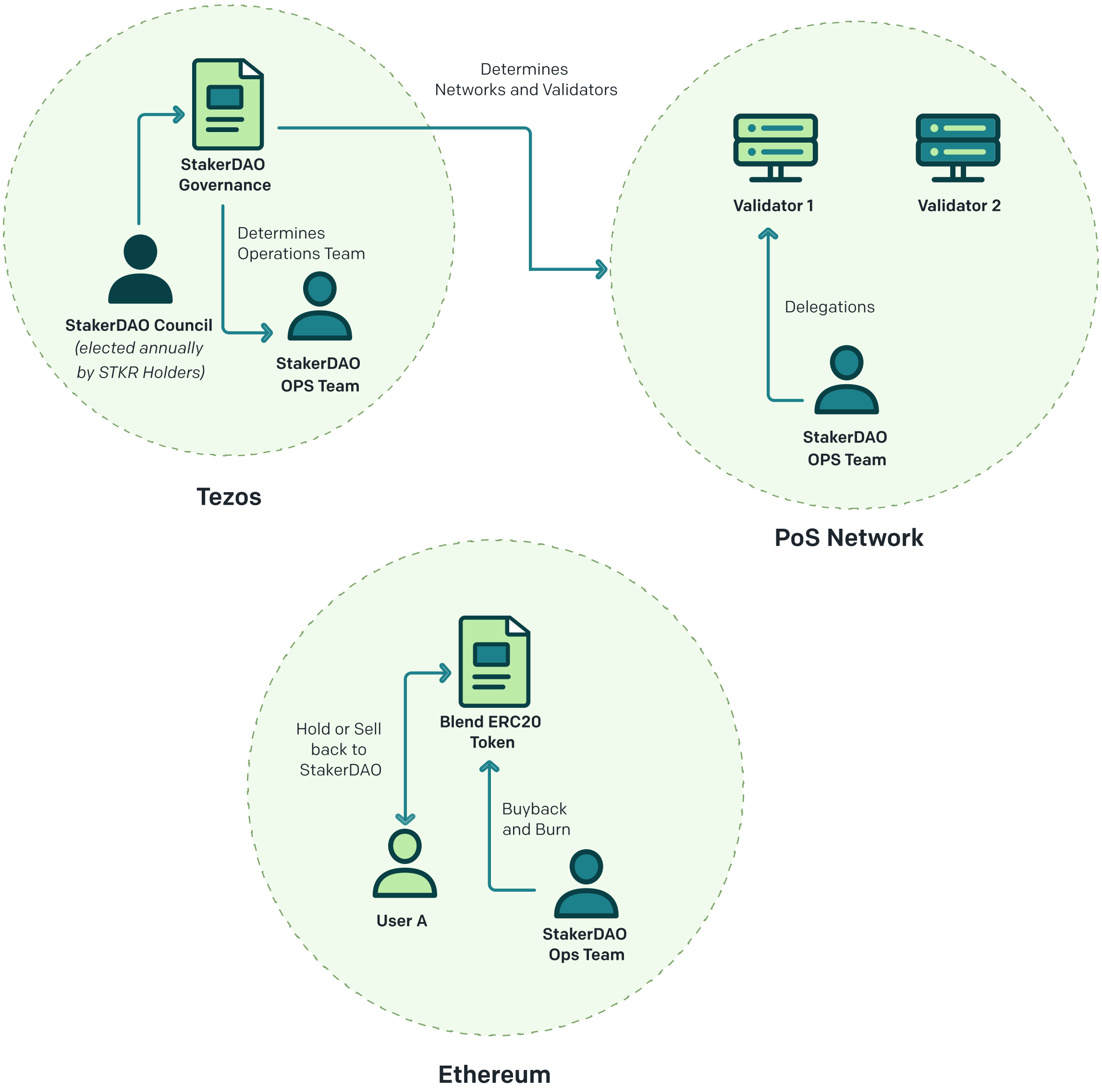


Figure 9: StakerDAO Illustration.

[60] "StakerDAO: The Future of Decentralized Financial Governance." https://www.stakerdao.com/. Accessed 19 May. 2020.

StakerDAO's first product Blend is an ERC20 token that seeks to incorporate staking rewards across different networks and validators without requiring holders to engage with the respective staking protocols. Holders of Blend need to register with StakerDAO and are able to sell their tokens back to the DAO in recurring auctions, which uses accumulated rewards to buyback and burn Blend tokens.

The initial version is governed by a council of five individuals made up of representatives of funds (Polychain, Lemniscap, DTC Capital), StakerDAO CEO Jonas Lamis, and Luke Youngblood from Coinbase Custody.

Blend will focus on large PoS networks, which will include Tezos, Cosmos, and Algorand. The product will expand to include other large PoS networks.

Key Strengths	Possible Weaknesses
Makes it very simple for crypto users to get exposure to a basket of PoS returns.	The service is custodial, requiring token holders to meet regulatory requirements and trust the StakerDAO Ops team with their assets.
Low regulatory risk as this solution is designed with current regulations in mind.	Currently highly centralized, although they are making efforts to build a community and to evolve governance.
BLEND tokens as an ERC20 can benefit from integration in the existing DeFi ecosystem.	A small set of owners of STKR governance token have a significant say over the system, and especially over BLEND holders.

Rocket Pool[61]

Rocket Pool is an Ethereum-based project that has been developing a staking pool/delegation system in preparation for Ethereum's move to Proof-of-Stake since 2016. During this time, the design and specification of Ethereum's staking protocol has changed frequently and Rocket Pool has constantly adapted their protocol to those changes. Recently the project overhauled its own design substantially and switched to a liquid staking model that seeks to tokenize Ether stake delegated to the project's staking pool.

Rocket Pool's protocol aims to connect node operators and token holders to allow for a smart contract-based delegation system for the sharded Ethereum 2.0 PoS network. In Rocket Pool, at least half of the stake in the system needs to be contributed by node operators forcing them to have skin-in-the-game. The protocol is using a three token model at launch:

rETH: Tokenized Ether staked with Rocket Pool nodes. This fungible liquid staking token is a claim on staking deposits and rewards after commissions minus penalties in excess of what is covered by node operators.

nETH: Node operators receive this token when they withdraw from the network before smart contracts are enabled on Ethereum's PoS network. It is a claim on their own deposited stake and rewards, as well as commissions earned for running a Rocket Pool node.

RPL: The project's native token that is used to incentivize high uptime and to discourage incurring penalties for node operators. Staking RPL enables node operators to receive a higher share of protocol commissions, but also puts their RPL at risk in the case of slashings. If a node operator incurs a penalty, his staked RPL will be burned proportionally. RPL will in the future also be used to govern parameters of the protocol.

[61] "Rocket Pool 101 — FAQ - Rocket Pool - Medium." 12 Dec. 2017, https://medium.com/rocket-pool/rocket-pool-101-faq-ee683af10da9. Accessed 1 Jun. 2020.
"Rocket Pool 2.5 — Tokenised Staking - Rocket Pool - Medium." 29 May. 2020, https://medium.com/rocket-pool/rocket-pool-2-5-tokenised-staking-48601d52d924. Accessed 1 Jun. 2020.
"White Paper - Rocket Pool." 18 Oct. 2018, https://www.rocketpool.net/files/RocketPoolWhitePaper.pdf. Accessed 1 Jun. 2020.

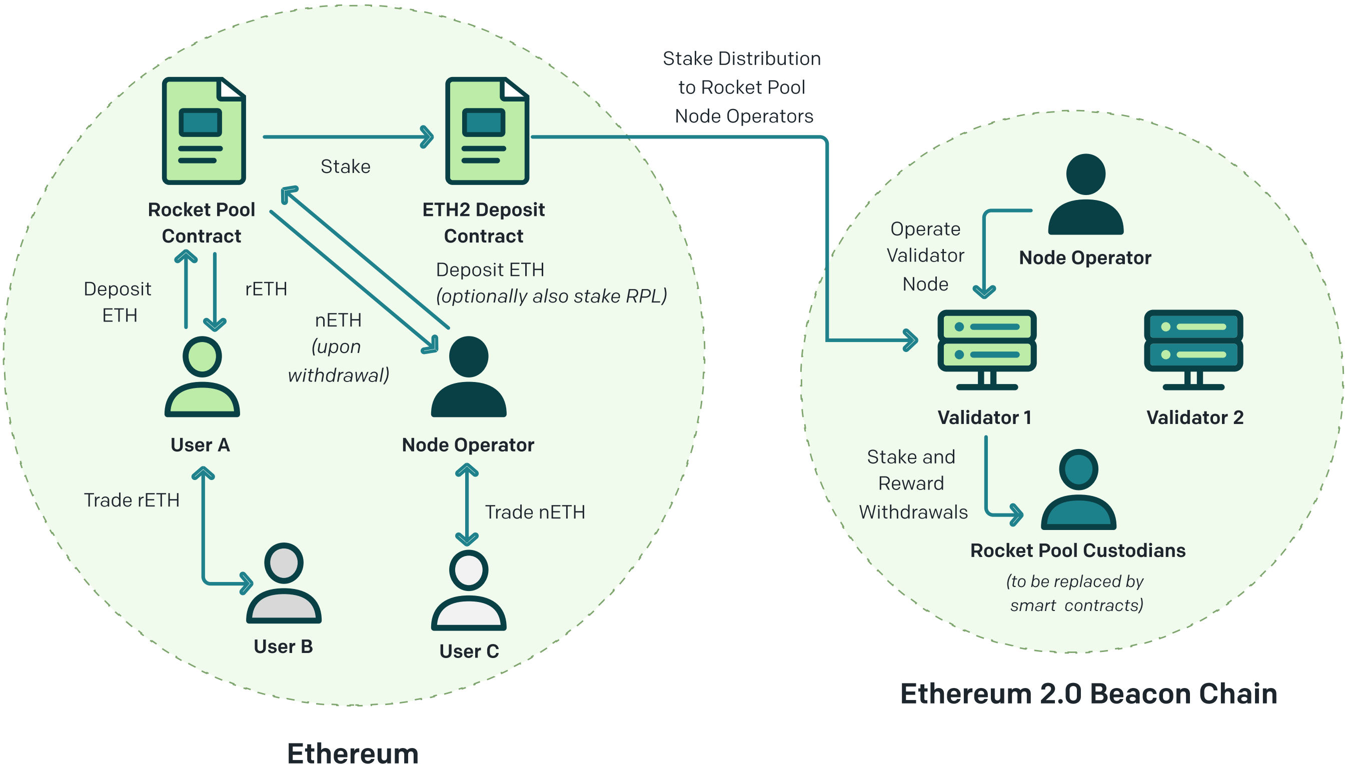


Figure 10: Rocket Pool Illustration.

The Rocket Pool protocol charges a commission on ETH staking rewards that dynamically adapts based on capacity of node operators, meaning it will charge a higher commission should there be a lack of node operators. Deposited stake and commissions are distributed among node operators proportional to their own ETH contributions and RPL stake. Slashings are first absorbed by node operator stake (ETH), and are socialized by the entirety of rETH holders in case they exceed what has been collateralized by the penalized node operator. In this sense, Rocket Pool is essentially a tranched protocol not too dissimilar to the Tezos bond mechanics described further above, with the difference that in Ethereum 2.0 a complete loss of stake is theoretically possible meaning that all tranches carry some risk.

Since smart contracts on the sharded Ethereum PoS network are only enabled in phase 2 of the rollout, stake contributed to Rocket Pool and rewards earned before that cannot be withdrawn. These limitations in the first two phases of the PoS rollout also mean that withdrawal addresses on the beacon chain cannot be controlled by smart contracts. Because of this, Rocket Pool will be a trusted solution at launch. Rocket Pool and their investors will custody the keys associated with these withdrawal addresses. This means they will be in control of all deposits and associated rewards that will accrue on Ethereum's beacon chain when the PoS migration begins. Currently, there are few details available on how exactly transforming rETH and nETH to ETH will work and how the dynamic unbonding periods of Ethereum 2.0 will be taken into account.

Key Strengths	Possible Weaknesses
The team has long experience and developed various iterations specifically for Ethereum's PoS protocol.	Keys that will control funds on Ethereum's beacon chain will be custodially controlled at launch, so this is a trusted/custodial solution until smart contracts are enabled (ETH2 phase 2).
Built on Ethereum, so rETH has access to DeFi protocols and there are fewer security risks than projects built on less proven chains (of course, the risk of smart contract exploits remain).	High requirements for stake contributed by node operators may prove to be a limitation of this solution.
Very simple user experience for non-node operating ETH stakers.	Highly specialized and completely focused on Ethereum staking, not a cross-protocol solution.

Legal Considerations

Disclaimer: *This document does not constitute legal, financial or other advice and is not intended to be relied upon or used by any person for any purpose, other than informational and educational purposes. No attorney-client relationship or privilege is intended to be created or implied. No representation or warranty is being made as to the quality or fitness for any purpose of this document.*

Like most uses of blockchain technology, liquid staking involves novel questions of law and entails legal uncertainties. In this section, we provide a brief overview of the most important legal considerations related to liquid staking. We use the term "StakeToken" to refer to a token that represents any kind of liquid staking arrangement, although the exact nature of the StakeToken will vary based on the type of liquid staking at issue. We refer to "validators" as those who have a direct power to validate or produce blocks as part of the native consensus-forming activity of the network, to "stakers" as those who natively or non-natively delegate validation-power to validators by locking up tokens and to "staked tokens" or "staking tokens" as the native tokens that must be natively locked up on the network to exercise validation power. Included in the **Appendix** of this report is an extended analysis of liquid staking legal issues which explains the reasoning behind our conclusions in greater depth.

Legal Engineering

The use of legal agreements—contracts written in natural language—may be necessary or advisable for certain forms of liquid staking. We refer to this as a form of "legal engineering." The importance and aims of legal engineering will vary based on the type of liquid staking at issue:

Delegation Exchange. Delegation exchange would likely require moderate legal engineering, with the details depending on the exchange method used. One simple (albeit non-cybersecure) method would be for a user to sell their private key (and all associated usage rights) which controls the staked tokens to another user through a bill of sale or similar agreement. A delegation exchange system like B-Harvest allows stake to be controlled by a group of accounts and traded among such accounts. Such groups might be analogized to partnerships or investment clubs, and may call for different legal engineering depending on the purposes intended by a particular group with respect to a particular pool—e.g., if stakes are to be exchanged among the group members, then contractual covenants will be needed to enforce payment obligations and determine the exact moment when title to the staked tokens changes hands.

Native Liquid Staking. Generally native liquid staking/delegation vouchers will require little to no legal engineering. Participants in native PoS network mechanics may be seen as implicitly agreeing to a kind of code deference arrangement whereby they accept the results of the operation of the PoS network, including any applicable native liquid staking mechanics. In many PoS networks, validators and stakers have no direct social or contractual relationship with one another, but only interact indirectly through the protocol; as a result,, they have little or no ability to cause harm to one another and the risk of disputes between them is low. In such contexts, legal engineering is not required, although validators may still wish to publish some general disclaimers of liabilities. Even when a validator and its stakers do have a relationship, such as in Tezos (where validators must directly distribute staking rewards to stakers), the relationship may be a relatively conventional commercial relationship defined by a fairly simple written terms of service.

Non-Native Liquid Staking. Non-native smart contract liquid staking systems may call for different forms of legal engineering, depending on the specifics of the solution and how much flexibility or governance it contemplates. The core dynamics of Stake DAO's StakeTokens (LTokens) are rather simple and predictable and afford little discretion to anyone—the LTokens function like notes or certificates of deposit that can be turned into the smart contract to receive stake and staking rewards—thus, a kind of 'code deference' approach might be possible, and legal engineering might not be needed. On the other hand, the interest-rate features of Stake DAO and the rules for the DAO itself may require legal engineering. Systems like Everett and Acala that attempt to make the StakeToken ("bAtoms" for Everett, "L-DOTs" for Acala) do double duty as a stablecoin pegged 1:1 with the underlying staking token ("Atoms" for Everett, "DOTs" for Acala) will present a more complex risk profile that could implicate legal engineering concerns more strongly. Because such systems will presumably be governed by token holders proactively (to hold the peg), the obligations of the governors and the rights of the StakeToken holders should be carefully defined in a terms of service or similar legal agreement. Systems like StakerDAO, whose StakeTokens will likely be securities governed by representatives of token holders, will obviously require extensive legal engineering to define the rules of representation and collective action, provide indemnification and insurance to the representatives, and so on.

In all cases, the complexity and novelty of non-native liquid staking systems means the requisite legal engineering will not be as simple as copy-pasting boilerplate terms of service for a simple consumer-facing website. Legal engineering may also be required to deal with some of the extra regulatory risks involved in non-native liquid staking (*see below*).

Custodial Liquid Staking. Custodial liquid staking is inherently tied to contract law. In order for a custodian (like a traditional cryptocurrency exchange, but also like Rocket Pool in its initial version) to hold tokens on behalf of a staker, there must be a legal agreement which defines the parties' respective rights and obligations as part of that relationship. The law provides for different types of custody—trusts, bailments, escrows, etc.—and custodians should take pains to define which type applies to the staking tokens entrusted to the exchange for staking. Similarly, since the StakeTokens are not defined by a decentralized protocol, legal engineering is required to define them.

Are the StakeTokens transferable legal instruments, i.e., "a form of electronic title document…represent[ing] a record of title to" the staked tokens and associated awards?[62] Or are they a mere certificate of deposit from the custodian? Or something else? Who bears the risk of loss of tokens due to slashing events—the StakeToken holder or the custodian? Does the answer differ depending on the validator's level of fault (negligence vs. gross negligence vs. recklessness) or on the type of slashing event (double-signing vs. downtime)? For custodial liquid staking, legal engineering will be required to answer all of these questions and more.

Synthetic Liquid Staking. Synthetic liquid staking will feature a 'swap contract' defining the terms and conditions of payouts based on market events affecting the value/price of the staked tokens or slashing of the staked tokens. This will initially require significant legal engineering, but over time certain standard forms of such swap may become prevalent and reduce the expense of legal engineering.

[62] "Digital and Digitized Assets: Federal and State Jurisdictional Issues," American Bar Association Derivatives and Futures Law Committee Innovative Digital Products and Processes Subcommittee Jurisdiction Working Group. http://www.klgates.com/files/Publication/cb8c685a-9523-4ad9-821e-73304b09b55f/Presentation/PublicationAttachment/0c93ed2b-f704-4c51-ab36-5f3e2a444980/ABA_Digital_Assets_White_Paper.pdf. Accessed June 11, 2020.

Regulations

The application of regulations to PoS networks is still generally poorly defined and tested. Even regulatory agencies such as the Securities & Exchange Commission (“*SEC*”), Commodities Futures Trading Commission (“*CFTC*”) and Financial Crimes Enforcement Network ("*FinCEN*") which have been relatively proactive in tackling blockchain regulatory issues generally, have nevertheless failed to provide significant guidance specific to PoS; instead, their guidance typically discusses Bitcoin or Ethereum 1.0, which are Proof-of-Work networks, despite the fact that there are many potentially legally important distinctions between the two types of networks. Accordingly, there remains a much greater “gray area” for how regulations apply to PoS networks than to Proof-of-Work networks.

Liquid staking for PoS involves the creation of derivative instruments on top of PoS, and thus adds even more legal complexity and uncertainty to PoS. Nevertheless, if certain forms of liquid staking are more likely to carry heavier regulatory burdens than others, it is important to understand and wrestle with that risk as early as possible in the game, since it may inform where people should best apply their efforts to develop liquid staking and avoid misallocation of capital into types of liquid staking that are non-starters from a regulatory point of view.

Delegation Exchange. Delegation exchange would likely not be subject to significant regulations. In the B-Harvest system, depending on the details of how a particular group account uses a particular pool, some commercial and contracting regulations could be implicated, but they are likely to apply in a very similar way to how they apply to other situations where people get together and co-manage assets. Of course, if the group is very large and trading in staking positions among the group members is extensive, regulations regarding securities exchanges, commodities exchanges, commodities pools and/or investment funds could be implicated; however, considering that these groupings are inherently short-lived because they apply to a specific set of staked tokens, and the underlying staking interest is itself likely to be lightly regulated, it is unlikely such group accounts would ever reach sufficient scale to implicate these regulations.

Native Liquid Staking. Native liquid staking will generally be the least likely to implicate regulations. No one in particular controls or has the power to change the blockchain network or protocol supporting native liquid staking functionality, and thus there is no natural target for regulation.

When relying on decentralized blockchain systems, users may face risks from poor software design, but generally do not face the kinds of risks that require heavy regulations—risks from custodians, fiduciaries and similar types of intermediaries who are most apt to abuse information asymmetries or pose other risks based on conflicts of interest. Moreover, the development and deployment of software in and of itself is heavily protected in countries like the U.S. by freedom of speech principles, meaning that governments may lack the power to regulate such systems heavily without violating civil rights. However, there is some residual risk of regulations applying even to native liquid staking; for example, we cannot completely rule out that in some PoS networks the native token could be a security and thus the StakeToken could be a securities derivative.

Non-Native Liquid Staking. Actively governed smart contract systems for liquid staking may face higher regulatory burdens:

1. The stakers may be seen as having "loaned" the staking tokens to or deposited the staking with 'the system' or the unincorporated association of governance token holders, in which case the StakeTokens could represent a kind of promissory note or certificate of deposit. This characterization will be more likely for systems like Stake DAO, which tie each StakeToken to a specific stake and pay interest to the staker during the lock-up period. Alternatively, the smart contract system may be seen as having "loaned" the StakeTokens to the stakers. This characterization may be more likely for systems like Everett and Acala which follow a MakerDAO-like collateral/foreclosure design pattern. Either perspective may implicate lending/credit regulations, banking regulations or (if the StakeTokens are analogized to bonds) securities regulations, but in general we regard the case for the applicability of such regulations being weaker or the adverse effects of complying with such regulations if they do apply as being less severe than for some of the other regulations mentioned below.

2. The stakers may be seen as having disposed of/sold the staking tokens (or a portion of the staking tokens, or the associated staking rewards) with an option to re-acquire them at a later date in exchange for the StakeTokens, which may under certain circumstances be considered a CFTC-regulated option or a CFTC-regulated "swap" (note: many commodities options may also be swaps, so the two categories are not mutually exclusive). From this point of view, the smart contract system embodies an option, with the StakeToken being the "exercise price" required to receive the extra collateral and the staking rewards. Swaps are required to trade only on CFTC-registered "designated contract markets".

However, non-native liquid staking systems do have some noteworthy differences from options, particularly if they also involve the payment of a variable stability fee (which is less like an option exercise price and somewhat more similar to payments of interest on a debt) and swaps (particularly because title to the staking tokens and potential rewards moves with the StakeTokens, rather than merely risk). Even if non-native liquid staking systems do facially meet the definition of "swaps," it is at least possible that one of the exceptions may apply in at least a subset of cases, such as the exception for "commercial merchandizing transactions" involving deferred delivery'. These details would require extensive analysis that is beyond the scope of this report.

3 The stakers in overcollateralized stablecoin systems like Everett and Acala may be seen as seeking to acquire the future staking awards (and extra collateral) on a "leveraged, financed or margined" basis. From this perspective, non-native liquid staking may be considered a type of CFTC-regulated retail commodities transaction that is required to occur only on CFTC-registered "designated contract markets" unless all participants are "eligible contract participants" (i.e., generally having $5M-$10M in assets).

The terms "leverage", "finance" and "margin" have not been strictly defined for purposes of the applicable regulations, and the CFTC has interpreted them broadly in the past so that "indebtedness in the traditional sense (i.e., the use of borrowed money) is not required."[63] Indicia of leverage are said to include "allowing a customer to control a large amount of a commodity with a comparatively small amount of [another commodity]" and "allow[ing] customers to significantly boost their profits with a relatively small investment while also magnifying their losses".

Although the StakeTokens are "overcollateralized" in a certain sense (since users will presumably deposit more of the staking tokens than they receive in StakeTokens), when the potential staking rewards and slashing events are taken into account, the can be seen as "leveraged": after all, it could become "insolvent" in certain situations (massive slashing events, or a "black swan" event like the auction efficiency failures observed in MakerDAO's "Black Thursday," etc.).

[63] "Swaps and Retail Commodity Transactions (Leverage, Margin or Financing: Will We Know It When We See It or Only After It Has Been Identified As Such?)", Andrew P. Cross, https://www.derivativesandreporeport.com/2018/10/swaps-and-retail-commodity-transactions-leverage-margin-or-financing-will-we-know-it-when-we-see-it-or-only-after-it-has-been-identified-as-such/. Accessed June 15, 2020.

Expressed another way, the locked-up collateral is both the "margin" for obtaining the potential staking rewards and the "margin" for the associated stablecoins that are supposed to have a 1:1 peg—when all of that value is taken into account, the system may be seen as having the same of kind of capital-multiplying effects as more conventional margin trading, notwithstanding the apparent "overcollateralization". The governance token holders may also be seen as providing "financing" to the stakers, since they are (or are at least often presented as) "lenders of last resort" charged with holding the peg by diluting themselves in insolvency events.[64]

Because the arguments for regulations applying are fairly persuasive, and the consequences of such regulations would be devastating, engagement with the CFTC should be a priority for teams involved in these systems. Their goal will need to be convincing regulators either that: (a) the decentralized, automated/autonomous or transparent nature of the system eliminates the risks that make regulation appropriate when they occur on a centralized basis; or (b) the regulations should be modified to allow such systems to be registered with the CFTC as regulated designated contract markets.

4. Depending on the extent of their governance powers, the association of governance token holders involved in certain of such systems may be seen as performing a money services business role by accepting staking tokens from stakers and depositing them with / for the benefit of validators, or may be seen as subject to other custodial regulations. If so, there may be a requirement that the system be registered with FinCEN or other regulators, perform KYC checks on depositors, etc.—which obviously would be very challenging for a smart contract system.

5. The governance tokens in systems like Everett and Acala, or the StakeTokens themselves in systems like StakerDAO, may be seen as securities, particularly if a particular entity or group of persons holds a large percentage of the governance tokens and has principal responsibility for promoting or developing or maintaining the system; in such a case, the governance tokens may be limited in the venues on which they can trade and those who hold them may have securities disclosures obligations.

[64] "The DAI Stablecoin System: Whitepaper" (https://makerdao.com/whitepaper/DaiDec17WP.pdf.): "MKR....serves as a backstop in the case of insolvent CDPs". Accessed June 15, 2020.

See also this Reddit comment believed to be from Rune Christensen (https://www.reddit.com/r/MakerDAO/comments/8biua7/some_criticisms_of_makerdaos_multicollateral/dx8i2t2/?utm_medium=web2x&utm_source=share) : "It is unfortunately not possible to change the fundamental feature that MKR holders are on the hook for all the dai in the system - this is because it[']s a crucial requirement that all dai has to be fungible, so ultimately they have to have the same backing of last resort."

This would be a particularly challenging result for governance tokens when they are minted as a source of last-resort funding when the system is insolvent—such issuances would be new securities sales which must be either registered with the SEC or exempt from registration (the latter being unlikely in a decentralized transaction).

6 The StakeTokens may be seen as bearer instruments subject to certain tax penalties, especially when they are analogous to bonds or other kinds of debt instruments.

Custodial Liquid Staking. Custodial liquid staking will in general present a risk of the custodian being subject to money services business regulations—similar to any cryptocurrency exchange business. However, such regulations may be less likely to apply if the exchange itself is also a direct validator and thus is not transmitting funds on behalf of the stakers to a third party. Custodial liquid staking could also implicate the same commodities regulations as were mentioned immediately above for non-native liquid staking; if so, then the exchange would likely need to become a registered CFTC-regulated exchange. Custodial liquid staking will also present other similar regulatory concerns as mentioned above for non-native liquid staking—but the case for them applying will be even stronger, because the exchange is more clearly an ordinary centralized business of the kind usually targeted by such regulations. On the other hand, a traditional centralized custodial like an exchange can also respond to such regulatory issues more nimbly. For example, an exchange could deliver staking tokens back to U.S.-based stakers every 28 days and thus avoid being subject to the CFTC's regulations of retail commodities transactions involving leverage, margin or financing. Likewise, an exchange can easily impose KYC requirements and thus lock out U.S. investors from liquid staking entirely.

Synthetic Liquid Staking. Synthetic liquid staking is simply a commodities swap and thus would be subject to all of the swap regulations under the Commodities Exchange Act as amended by the Dodd-Frank Act, including generally being limited to trading only on designated contract markets registered with the CFTC. Again, there may be an opportunity to persuade regulators that the normal policy concerns with swaps should not apply, and therefore that the regulations should not apply, to the extent that the swap logic can be embedded in autonomous smart contracts which eliminate the kinds of counterparty risks that made swaps an existential market threat in the 2007-2008 financial crisis.

Conclusion

We are on the cusp of massive transition in how most blockchain networks are secured. While the best-known networks Bitcoin and Ethereum still run on Proof-of-Work, with Tezos and Cosmos - two major Proof-of-Stake networks launched in 2018 and 2019. Now, countless others have launched or are coming to market in the next 18 months.

Blockchains are still in their early phase of building out fundamental infrastructure and finding use cases capable of reaching mainstream adoption. But what has become clear is that staking will play a crucial role in securing most blockchain networks - and thus likely also in providing the foundation for the financial system of the future.

But the design space around Proof-of-Stake is vast and so far little systematic analysis around the best economic designs have been done. There has not been enough thinking about the long-term impact of restrictions commonly imposed on staking assets. In particular, the inability to use staked assets collateral in other applications and the often lengthy unbonding periods have serious economic costs.

In our view, the most existential risk for Proof-of-Stake networks is exchange staking. Partly driven by their ability to circumvent on-chain restrictions and partially by the simpler user experience and brand, exchanges have rapidly gained market share and accumulated staking assets on their platforms. The negative repercussions are large if this continues. They range from defunding community validators to decreasing network resilience to potential corruption of the governance process. If a few single parties can shut off a blockchain network or censor transactions, Proof-of-Stake networks can only provide a mediocre degree of censorship resistance.

With liquid staking, in a short time a burgeoning field has emerged that could address the issue of exchange staking and unleash a wave of rapid staking innovation. Just like with the decentralized finance ecosystem on Ethereum, liquid staking offers composability, permissionless innovation, and an endless playground for experimentation. In this paper, we looked at liquid staking on a high level and analyzed the key factors that will determine if liquid staking ends up benefiting a blockchain network over the long run.

There are many considerations ranging from the degree of liquidity provided, dependency on other networks, handling of governance rights, to regulatory aspects. At this point, it’s not entirely clear what the best solutions are, but over the coming years as the first liquid staking designs are implemented we will get much more data.

Overall, liquid staking is a crucial next phase for Proof-of-Stake. If done right, it could improve network resilience, decentralization, and open up many new business models. This is something that Proof-of-Stake protocols should embrace as a tremendous opportunity.

Future Work

This research aims to lay the foundation for future discussions and projects involved in the liquid staking space. There is a large potential for future work. We see analyzing and figuring out how to deal with systemic risk and other dangers associated with the financialization of staked assets, such as increasing centralization, as the core issues that the wider crypto community will need to address.

Specifically, more work on modeling and observing risks in blockchain protocols needs to be done. Agent-based simulations like that of Tarun Chitra[63], e.g. using tools like cadCAD[64] could help improve implementations. A major focus should lie on tools that help to observe and manage risks associated with staking assets in decentralized finance.

Finally, native liquid staking token issuance could open up a large design space for shared security and increase the possibility of value capture for staking tokens. In essence, models in which smaller blockchains rent security from a larger blockchain's validator set can be designed using tokenized staking derivatives. Such designs may lead to a more efficient market for blockchain security and enable developers to build decentralized applications without needing to worry about building out their own validator set.

In general, the design space and interest in liquid staking is continuously expanding. Many other interesting ideas related to tokenized stake have surfaced in the process of writing this report. Among them are thoughts on using automated market makers to manage staking liquidity, e.g. from Curve Finance65 or Terra's proposed passive income product Anchor[66] that aims to make use of staking derivatives.The Liquid Staking Working Group[67] welcomes new members and will continue to hold discussions focused on these topics.

[63] "Competitive equilibria between staking and on-chain lending." 4 Feb. 2020, http://arxiv.org/abs/2001.00919. Accessed 19 May. 2020.

[64] "cadCAD – A Python package for designing, testing and …." https://cadcad.org/. Accessed 19 May. 2020.

[65] "Building liquid staking with Curve - Curve Finance." 24 Feb. 2020, https://blog.curve.fi/building-liquid-staking-with-curve/. Accessed 25 May. 2020.

[66] "An update on Anchor(Terra money market) - dApps - Terra …." 9 Apr. 2020, https://agora.terra.money/t/an-update-on-anchor-terra-money-market/221. Accessed 25 May. 2020.

[67] Find us on Telegram at https://t.me/liquidstaking.

Appendix

Appreciation

This report was authored by Felix Lutsch (Chorus One) with sections and feedback contributed by Brian Crain (Chorus One), Gabriel Shapiro (BSV Law), and Brendan Dillon (Chorus One).

A special thank you goes out to Marouane Hajji (Unslashed), Sam Hart (Interchain Foundation), and Billy Rennekamp (Interchain Foundation), who provided invaluable feedback and extensively reviewed this report.

We'd also like to thank all Liquid Staking Working Group (LSWG) members for attending LSWG calls[68], participating in discussions on Telegram, and leaving comments on drafts of this report, which meaningfully contributed to the research we presented here. Finally, thank you to the teams and individuals that presented on the LSWG calls and helped us understand their work in preparation for this report.

Glossary

List of terminologies and definitions relevant to understand this document:

Sybil Attack:
In a permissionless network, where the identities of participants are unknown, an attacker can subvert the network's reputation system by creating a large number of pseudonymous identities and use them to gain a disproportionately large influence over the network.

Sybil Resistance:
Refers to mechanisms used in public, permissionless networks that are able to deter Sybil attacks by increasing their cost.

Proof-of-Work:
The term for Sybil resistance mechanisms that require energy-intensive hashing to determine as participants of the consensus process. Abbreviated as PoW.

[68] "Liquid Staking Working Group Community Calls - YouTube Playlist" https://www.youtube.com/watch?v=gCMa1k5pbJk&list=PLKK1s-ywEfTtkqF9TGDrv9HUOJQamGxvr. Accessed June 11, 2020.

Hash Rate:
The measuring unit of the processing power on a Proof-of-Work blockchain. Hash rates give an indication of how many hashes the entire network (or a single node) is performing per second.

Miner:
The nodes in a Proof-of-Work network performing the hashing and proposing transactions to be added to the blockchain. The more hashes are performed - the higher the hash rate and the higher the likelihood of getting to propose a block and earning associated rewards.

ASIC (Application-Specific Integrated Circuit)
An integrated circuit (IC) chip customized for a particular use, rather than intended for general-purpose use. In the context of Proof-of-Work, ASICs are hardware specifically designed for performing Proof-of-Work hashing.

Mining Pool:
An organized collective of miners in a Proof-of-Work network who bundle their hashing rate to increase the likelihood of becoming the proposer of a block and earning the rewards.

Nakamoto Consensus:
The consensus protocol used by Proof-of-Work blockchains like Bitcoin abiding by the longest chain rule, which states that the blockchain with the most work behind it, as measured by the collective hash rate, is the one that nodes in the network will follow.

Collateral:
Collateral is something that is pledged in addition to the main obligation of a contract that can potentially be seized should the main obligation not be met. In the context of Proof-of-Stake, the main obligation is for participating nodes to faithfully follow the protocol’s rules, which is ensured by putting up native cryptocurrency tokens as collateral into escrow.

Proof-of-Stake:
An umbrella term for Sybil resistance mechanisms that use cryptoassets as collateral to determine participants of the consensus process. Abbreviated as PoS.

Staking:
Staking refers to locking up cryptoassets to participate in the selection mechanism for network roles (e.g. consensus nodes (“Validators”) in Proof-of-Stake). Participation in staking is incentivized by redistributing collected transaction fees and/or newly issued tokens to those staking (“Staking Rewards”). Staked assets are kept as collateral that in some protocols can be retracted should malicious behavior be detected (“Slashing”).

Validator:
Consensus nodes in a Proof-of-Stake network. The physical machines participating in the consensus process by running the protocol software and proposing blocks and verifying transactions are called validators. Validators are identified by private keys and backed by collateral in the form of the protocol’s native cryptoasset, e.g. XTZ in Tezos. We distinguish between validator operators or entities, i.e. the individual or company operating the nodes and the nodes themselves.

Validator Set:
The collection of validator nodes that together maintain a Proof-of-Stake network at a given point in time.

Staking Rewards:
Earnings participants in a Proof-of-Stake network (“Stakers”) receive in return for putting up their tokens as collateral. Rewards consist of transaction fees and/or newly issued tokens which are distributed to incentivize participation in the network.

Slashing:
Destruction or retraction of cryptoassets pledged as collateral in the staking process. Proof-of-Stake protocols employ differing slashing conditions and parameters depending on what kind of behavior they seek to discourage. Examples include slashing for downtime (usually low amounts) or slashing for double-signing (i.e. signing two blocks at the same height, which could be seen as an attack on the network).

Delegation:
Determining which validator node one’s collateral will back in the staking process. We distinguish between delegated stake, i.e. collateral is provided by a separate entity and self-stake, i.e. collateral is provided by the entity operating the validator(s) itself.

Delegator:
A delegator is the entity providing the backing collateral for validator(s) that they do not themselves operate.

Self-Stake:
Staked collateral that is provided by the entity operating the validator node itself.

Staker:
Staker is the umbrella term for both delegators and self-staking validators. Participation in the Proof-of-Stake process by pledging collateral is what defines a staker, regardless of which validator(s) the stake is backing.

Staking Position:
Refers to tokens associated with a blockchain account that are staking on the network.

Finality:
The notion of a transaction being irreversibly confirmed within a network. In the blockchain context we distinguish between probabilistic and absolute finality. With probabilistic finality (e.g. in Nakamoto consensus) the likelihood of a transaction being reversed decreases when more blocks are added on top of the chain, as it will require increasingly more hashes to change it. Other consensus protocols (e.g. Tendermint or similar protocols often used in Proof-of-Stakenetworks) are able to achieve absolute finality guarantees by requiring a (super)majority of all participating nodes to confirm a certain block before it is regarded as accepted.

Unbonding Period:
A commonly used enforced withdrawal delay period that needs to pass before previously staked assets become available to their owner again. This delay is enforced for various reasons; one of them being the ability to enforce penalties against stake that did not follow the protocols' rules at an earlier point in time.

Full Node:
A node that directly interfaces with other nodes on the network and validates all data (blocks of transactions) going back to the first block of the blockchain.

Light Client:
A node that interfaces with the network through a full node. Light clients do not verify all blocks of transactions on the blockchain themselves, but instead only verify a subset of information (block headers) provided by the full node through which they are connecting with the network.

Liquid Staking:
Protocols that issue on-chain representations of staked assets in a decentralized network. Through tokenization, liquid staking protocols allow users to get liquidity on staked assets and enable the usage of staked assets as collateral in (decentralized) financial applications. Other terms that are often used to describe liquid staking protocols are staking derivatives and programmable staking.

Unbonding Premium:
The economic cost associated with the unbonding period taking into account opportunity costs, capital costs of hedging risks associated with the volatility of the underlying asset, and the inability to instantly liquidate assets when trying to exit a staking position.

Native Liquid Staking:
Tokenized stake is issued as part of the core staking protocol.

Non-Native Liquid Staking:
A secondary protocol, e.g. in the form of smart contracts, or on a different blockchain or platform is issuing representations of tokenized stake.

Non-Custodial:
Describes protocols in which users remain in control of the private keys associated with their cryptoassets.

Custodial:
Describes protocols in which users hand over control of the private keys associated with their cryptoassets to a third-party entity, e.g. a cryptocurrency exchange.

Synthetic Liquid Staking:
Refers to purely financially engineered positions that do not interact directly with the associated Proof-of-Stake protocol.

Bond Pooling:
Refers to the act of entering into off-chain agreements to supply the self-stake required for operating a validator node on the Tezos network.

Liquidity:
Liquidity is the degree to which an asset can be easily converted into cash in the market. A liquid asset can be converted at short notice without incurring significant discounts because there is a reasonable degree of buying and selling volume

Fungibility:
Fungibility refers to a property of goods and commodities whose individual parts are indistinguishable from each other.

Value Divisibility:
Refers to the ability to partially trade a staking position as opposed to only being able to sell a position in its entirety.

Shared Security:
A term used for protocols that allow sovereign blockchains to rent security from the validator set of another blockchain. Sometimes also referred to as rented security or validator set projection.

DAO (Decentralized Autonomous Organization):
An organization represented by rules encoded as a program that is transparent and fully controlled by its shareholders.

MPC (Multi-Party Computation):
A subfield of cryptography with the goal of creating methods for parties to jointly compute a function over their inputs while keeping those inputs private.

Threshold Signatures:
A distributed multi-party computation protocol that includes distributed key generation, signing, and verification algorithms..

ERC20:
Ethereum’s token standard for fungible tokens which is used by most token projects deployed on Ethereum.

NFT (Non-Fungible Token):
Tokens that have unique characteristics and can only be traded in their entirety.

APPENDIX – EXTENDED LEGAL CONSIDERATIONS

Disclaimer*: This document does not constitute legal, financial or other advice and is not intended to be relied upon or used by any person for any purpose, other than informational and educational purposes. No attorney-client relationship or privilege is intended to be created or implied. No representation or warranty is being made as to the quality or fitness for any purpose of this document.*

1. Legal Engineering

"Legal engineering" refers to the use of mechanisms of the law, such as contracts, to encourage intended results. From the standpoint of ordinary parties, legal engineering typically means creating legal agreements/contracts that can be enforced in a court of law. However, writing or amending the laws or adjudicating legal disputes can also be seen as exercises in legal engineering. In this section, we will primarily focus on legal engineering through contracts, though there is likely some opportunity to enhance liquid staking through statutory changes such as clarifying the treatment of StakeTokens under the Uniform Commercial Code.

The importance of legal engineering to liquid staking will vary depending on the specific type of liquid staking at issue. Our legal engineering needs will be heaviest for custodial, trust-requiring liquid staking solutions and lightest for trust-minimized, non-custodial liquid staking solutions.

A. Delegation Exchange

Delegation exchange occurs when one user simply transfers their delegated staking position to another user, without representing the staking position as a separate token. Non-native delegation exchange would likely require moderate legal engineering, with the details depending on the exchange method used. One simple (albeit non-cybersecure) method would be for a user to sell their private key (and all associated usage rights) which controls the staked tokens to another user through a bill of sale or similar agreement. A delegation exchange system like B-Harvest allows stake to be controlled by a group of accounts and traded among such accounts. Such groups might be analogized to partnerships or investment clubs, and may call for different legal engineering depending on the purposes intended by a particular group with respect to a particular pool—e.g., if stakes are to be exchanged among the group members, then contractual covenants will be needed to enforce payment obligations and determine the exact moment when title to the staked tokens changes hands. At the more extreme end of complexity, B-Harvest staking groups could be DAOs themselves and require similar legal engineering as DAOs—if not formation of a business entity like an LLC or corporation, then at least attention to the partnership laws of the relevant jurisdiction(s) and the preparation of a partnership agreement that spells out the partners' rights and obligations.

B. Native Liquid Staking / Delegation Vouchers

A key benefit of peer-to-peer public blockchain networks is the elimination of the need for certain written legal agreements. Properly designed blockchain systems replace contractual rights and obligations with powers and incentives, and the results can be as good as, or even superior to the results achieved by parties entering into verbally defined commercial agreements enforceable in courts of law.

Proof-of-Stake validators for a blockchain system like Cosmos do not have express legal agreements with the ATOM holders who delegate stake to them ("stakers"). Any ATOM holder can stake with any of the 100 Cosmos validators; the validator has no power to choose who its stakers are or to require them to sign a legal agreement. Importantly, there is no custodial risk. The staker permissionlessly receives all staking rewards to which it is entitled, directly through the protocol. The staker can switch validators or un-stake his ATOMs at any time (subject to the unbonding period); meanwhile, the validator has no ability to steal, sell or encumber the holder's stake or staking rewards. If the validator commits a slashable offense and thus the stakers' ATOMs get slashed, the staker will simply move on to a new validator after suffering a predictable loss: The staker accepted this risk from the beginning, and the staker's maximum liability for a single slashable incident was capped in advance by the protocol rather than a legal agreement. Even when a validator and its stakers do have a relationship, such as in Tezos (where validators must directly distribute staking rewards to stakers), the relationship may be a relatively conventional commercial relationship defined by a fairly simple written terms of service.

Accordingly, stakers and validators may be rationally indifferent to legal engineering to the extent that their entire "relationship" may be governed by the protocol. This is not to say there are no contractual arrangements—there could be a kind of implicit "code deference" agreement providing that the staker and validator are both legally bound to the outcomes dictated by the protocol, and, once again, for Tezos, a limited aspect of the interaction is more direct. But, in effect, the protocol has done most of what "legal engineering" would ordinarily do. Of course, absence of legal engineering does not entail a total absence of law or legal remedies. But, in the unlikely event of a network-wide dishonest majority or an intentionally harmful action taken by a validator, the stakers will likely have remedies in tort law or under applicable regulations that are more powerful than contract remedies.

Native liquid staking would be inherently trust-minimized and thus extend the same dynamics as illiquid staking systems. A native StakeToken would represent specific ATOMs and staking awards delegated to a specific validator. Any holder of the native "StakeToken" would have the power to redeem the associated staked ATOMs and staking awards at the end of the applicable un-bonding period. If the relevant validator suffers a slashing event, the ATOMs and staking awards subject to the StakeToken would be slashed. If a different validator suffers a slashing event, that will have no effect.

Importantly, in this model, the StakeToken holder would not need to worry about the StakeToken legally *representing* or constituting *legal title to* or a *transferable instrument* with respect to the staked ATOMs and staking rewards. The StakeToken is autonomously redeemable for the stake and staking rewards. There are no counterparty risks or powers, all participants have very little discretion, and thus legal engineering as such is not required.

C. Non-Native Liquid Staking

Non-native liquid staking occurs via smart contract systems which pool stakable tokens into smart contracts, stake them "on behalf of" users into the native protocol, and issue the users StakeTokens which are essentially non-native vouchers representing a claim against the pool for a pro rata share of the staking tokens and staking rewards (*minus* applicable commissions, slashing deductions, etc.). Like native liquid staking, non-native liquid staking is mediated by blockchain mechanisms that are at least partially autonomous and may in certain respects be trust-minimized. However, non-native liquid staking through smart contracts adds complexity to the equation: In non-native liquid staking, the StakeToken holder is at least once removed from the native protocol and is two or three times removed from the validator: The StakeToken is a claim to a claim—a claim against a smart contract for a *pro rata* portion of that smart contract's claim on a *pro rata* portion of staking rewards. Because of this complexity, non-native liquid staking is more likely to require legal engineering, but the extent of such legal engineering may differ depending on the type of non-native liquid staking at issue.

Non-native liquid staking systems like Stake DAO tie the StakeTokens (LTokens) to a specific stake and thus issue non-fungible StakeTokens that are likely to trade at an appropriate risk-based and time-based discount (reflecting the risks of slashing and the time value of money) to the staking positions. Such systems are likely to require little or no legal engineering, at least as far as the StakeTokens themselves go—like with native staking, there will essentially be a kind of implicit code deference agreement where parties can simply rely on the predictable operation of the smart contracts to get the benefit of their bargain. However, if, like Stake DAO, there is also interest paid on the staking positions, and further if determining the rate of interest requires governance, some legal engineering could be required to define the participants' rights and obligations regarding such governance. However, even if governance is required, these arrangements may have many similarities to traditional adjustable-rate loans or public bond indentures, and thus they may not be particularly novel or challenging to implement.

For non-native token systems that deliver fungible, stable StakeTokens and require active governance, we anticipate that significant legal engineering would be advisable to spell out in detail how StakeToken holders have certain rights and the governance token holders have certain obligations in regard to how the system is managed. For example, such a legal agreement could define the standard of care that the governors must use in trying to maintain stability, the circumstances under which they can change the system parameters or initiate an 'emergency shutdown,' and how they handle conflicts of interest. For the protection of the governance token holders, the relevant legal agreement should likely disclaim fiduciary duties and specify a lower standard of care such as commercial reasonableness. As further discussed below, because of the potential for risk obfuscation, such systems may also face a higher regulatory burden than native liquid staking systems, which may be an additional reason for careful legal engineering.

Systems like StakerDAO, whose StakeTokens will likely be securities governed by representatives of token holders, will obviously require extensive legal engineering to define the rules of representation and collective action, provide indemnification and insurance to the representatives, and so on. However, such legal engineering may have many similarities to the agreements required for traditional investment funds or exchange-traded funds or asset-backed securitization arrangements; this may alleviate some of the burdens of legal engineering by allowing StakerDAO to draw from existing standards and practices in mainstream finance.

D. Synthetic and Custodial Liquid Staking

Synthetic liquid staking and custodial liquid staking are inherently creatures of contract law and thus require significant legal engineering.

Synthetic liquid staking is literally and simply a "swap contract" and thus a legal agreement is necessary to define each party's rights and obligations to pay or receive certain amounts to or from one another. In the event one party does not make the required payment, the other party needs a clear contract so that a lawsuit can be initiated and a judge and governmental apparatus can force the breaching counterparty to honor the swap contract's terms. Needless to say, this will require a carefully drafted contract written in words rather than code, including a provision for choice of law and the choice of venue to handle legal disputes. However, similar to swaps in mainstream capital markets, we would expect that such swaps would rapidly become standardized and from that point would not involve significant ongoing legal overhead.

Custodial liquid staking is also a creature of contract law. When a user stakes ATOMs through a cryptocurrency exchange like Binance, Coinbase or Kraken, that user is agreeing to the exchange's Terms and Conditions of Service, which will specify the commission rates charged by the exchange and the power of the exchange to alter those commission rates and other aspects of the arrangement. If the exchange issues a StakeToken to represent the custodied staking token, then the Terms and Conditions will also need to define the legal properties of this StakeToken: Is it a certificate of deposit?

A voucher? An IOU? If it is transferable, is it a "bearer certificate" that always confers the right to receive the staked token on the latest holder, or can the exchange deny redemptions to certain types of people? Is the exchange's custody of the staking tokens defined as a bailment, an escrow, a trust, a rental, or something else? Can the exchange's creditors put liens on the staking token or is the exchange required to judgement-proof the staking tokens against the exchange's liabilities? Can the exchange vote with the staking tokens however it wants?

The custodian will likely be required to KYC all users. Thus, it will need consent, copies of identifying information and a privacy policy. Since the custodian will be relaying staking rewards to the user, the custodian will likely also need a Form W-9 or Form W-8BEN to confirm that the user is not subject to backup tax withholding. The custodian will want to choose which jurisdiction's law applies and the forum for dispute (e.g., mandatory arbitration with a class-action waiver). All of this requires significant legal engineering.

Typically, the terms and conditions of a cryptocurrency exchange will limit the exchange's liability to the maximum extent permitted by law—for example, limiting the exchange's duty of care to a gross negligence standard. The custodian will likely reserve the right to refuse service to anyone for any reason and will not be obligated to open its books up for audits by ordinary customers.

Thus, in many ways, these "contracts of adhesion" make custodial liquid staking the riskiest form of liquid staking, since the legal agreements are the user's sole form of trust-reduction but do not provide the user with many rights, while the exchanges have absolute dominion over the staked cryptocurrency. On the other hand, in dealing with such centralized entities users may receive the benefit of insurance on their staked tokens that may be preferable to the uninsured risks posed by potentially buggy decentralized smart contracts. Users may also benefit from the fact that cryptocurrency exchanges are supervised by regulators who will monitor the policies and practices of the exchange for the protection of users.

2. Regulations

A. Intro to Regulations – Uncertainties Regarding PoS

The application of regulations to Proof-of-Stake networks ("***PoS***") is still generally poorly defined and un-tested. Even regulatory agencies such as the Securities & Exchange Commission ("***SEC***"), Commodities Futures Trading Commission ("***CFTC***") and Financial Crimes Enforcement Network ("***FinCEN***") which have been relatively proactive in tackling blockchain regulatory issues generally have failed to provide significant guidance specific to PoS. On the contrary, most guidance provided by regulators to date implicitly or explicitly uses proof-of-work systems ("***PoW***") like Bitcoin as their blockchain exemplar. Yet PoS differs in many potentially legally relevant ways from PoW. Accordingly, there remains a much greater "gray area" for how regulations apply to PoS than for PoW.

Liquid staking for PoS involves the creation of complex derivative instruments on top of PoS, and thus adds more complexity and uncertainty to a PoS ecosystem that is already in a regulatory gray area. Much as a hypothetical StakeToken may be a kind of "claim on a claim on a claim" to a set of staked tokens and staking rewards; so, too, projecting how legal regulations will apply to liquid staking is a kind of "legal speculation on a legal speculation on a legal speculation." Nevertheless, if certain forms of liquid staking are more likely to carry heavier regulatory burdens than others, it is important to understand and wrestle with that risk as soon as possible, since it may inform where people should best apply their efforts to develop liquid staking and avoid misallocation of capital into types of liquid staking that are non-starters from a regulatory point of view.

B. Framework for Analyzing Liquid Staking Regulations

Which regulations apply to liquid staking depends primarily on two factors: (1) the legal classification of the underlying staking token; and (2) the type of liquid staking:

- Regulatory burdens are likely to be heaviest when: (a) the underlying staking token is a regulated asset such as a security; or (b) the liquid staking is custodial or otherwise involves information or power asymmetries or conflicts of interest which could enable one party to harm others.
- Regulatory burdens are likely to be lightest when: (a) the underlying staking token is classified as a commodity which is not a security or other contractual instrument; and (b) the liquid staking is a trust-minimized blockchain native transaction and is tightly coupled with ownership of the underlying staking token.

Regulations also cannot be considered in isolation from each other or other areas of the law. For example, a StakeToken could be a commodity, but may not actively be subject to commodities regulations because it is also a security and the securities regulations take precedence. More importantly, regulations must be assessed against a broader backdrop of civil rights and constitutional law. For example, jurisdictions like the U.S. which equate software code to speech and have strong free speech protections may allow software developers to push back on overly expansive regulations by asserting their free speech rights. [1]

C. Banking, Depository and Lending Regulations.

Certain liquid staking transactions resemble deposits or loans and may be subject to banking depository or lending regulations. For example, we could view a staker as lending staking tokens to a custodian (custodial liquid staking) or smart contract system (non-native liquid staking) essentially in exchange for the right to receive interest payments in the form of staking rewards. This is rather similar to a banking customer depositing funds in an interest-bearing account, and may implicate similar regulatory concerns to banking regulations. The StakeToken would be viewed as a certificate of deposit, or perhaps transferable debt instrument like a promissory note. Alternatively, in a non-native liquid staking system, the "system" or the association of governance token holders may be seen as lending StakeTokens and holding the native staking tokens as collateral. This could implicate truth-in-lending regulations, usury laws limiting interest rates and other laws designed to prevent predatory loans. However, there are also dissimilarities to these traditional relationships. While cryptocurrency exchanges in certain cases are regulated similarly to banks (for example, Coinbase's custody arm is a depository trust company supervised by the New York Department of Financial Services), the application of banking regulations to smart contract systems or "DeFi" remains speculative. To date, there has been little apparent interest from regulators in attempting to regulate smart contract systems as banks or lenders.

D. Commodities Regulations.

Commodities laws are the regulatory regime most likely to be implicated for liquid staking. In the United States, Title VII of the Dodd-Frank Wall Street Reform and Consumer Protection Act of 2010 (the "***Dodd-Frank Act***"), as codified in the Commodity Exchange Act, 7 U.S.C. §1 et seq. (the "***CEA***"), provides that certain transactions in commodities are subject to extensive regulations. These laws are very complex. As a matter of necessity, in summarizing these laws we will be paraphrasing and simplifying them to a certain extent.

[1] *See* "Electronic Cash, Decentralized Exchange, and the Constitution" by Peter Van Valkenburgh, March 2019 Coin Center Report.

Commodities transactions fall into essentially five main types: [2]

- spot sales (a sale/purchase of a commodity consummated in essentially one atomic transaction without delay—i.e., settled "on the spot");
- forwards (a bespoke over-the-counter agreement between two parties to sell/purchase a specific quantity of a commodity at a set price at a future date, with the commodity to be actually delivered to the buyer upon consummation of the sale/purchase)
- futures (a standardized combination of agreements between an exchange on the one hand and a buyer and a seller of the commodity on the other hand, providing for the sale/purchase of a specific quantity of a commodity to/from the exchange at a future date on a margined and dynamically priced basis, not always involving actual delivery of the commodity);
- retail commodities transactions (sales of commodities to retail purchasers); and
- swaps (including any option for the purchase/sale of or based on the value of any commodity, any contingent commodity purchase agreement based on a consequential event or the exchange of payments based on the value of commodities or interests therein and having the effect of transferring risk without transferring ownership).

Many commodities transactions are not subject to heavy regulation. Examples of such lightly regulated commodities transactions include: (a) spot sales in general, (b) retail commodities transactions which do not occur on a leveraged, margined or financed basis and do not constitute swaps; (c) commodities that are physically delivered (generally within 28 days of purchase or otherwise for *bona fide* commercial or consumer purposes satisfying certain conditions); and (d) transactions occurring solely between "eligible contract participants" ("***ECPs***") (generally individuals or entities with $5M-$10M in assets, depending on whether their trading is hedging-based or speculative). These more lightly regulated commodities transactions can generally be executed on any venue (for example, cryptocurrency exchanges) and will be subject to CFTC action only in the event of fraud or fraudulent market manipulation. By contrast, many other commodities transactions are required to take place on a CFTC-approved and -regulated commodities exchange and by regulated commodities intermediaries that are subject to various clearing and trade execution requirements, recordkeeping and real-time reporting rules and other CFTC-supervised rules and regulations.

Needless to say, the Cosmos, Tezos, Ethereum blockchain networks and other PoS networks are not regulated commodities exchanges and many people who transact on them are not registered commodities dealers or ECPs. Furthermore, because these networks are decentralized and pseudonymous, it is unlikely (under the current rules) that they could ever qualify for CFTC-regulated status. Thus, if liquid staking implicates the more expansive commodities regulations and does not fall under one of the exceptions where the CFTC's authority is more limited, the results could be problematic.

To date, the CFTC has primarily given guidance on how custodial exchanges handling virtual currencies will be regulated, not on how the regulations apply to decentralized virtual currency systems in complicated transactions executed in their native trust-minimized environments. Our main hints about how the regulations apply in a more decentralized context come from asides in broader CFTC guidance and in unofficial remarks by CFTC staff in their personal capacities. Consider the following remarks, for example:

- In determining when a virtual currency purchaser receives "actual delivery" of the token, the CFTC has stated that it will assess whether the "offeror" and other participants in the transaction "do not retain *any* interest in, legal right, or control over any of the

[2] https://www.cftc.gov/PressRoom/SpeechesTestimony/tarbertstatement032420a

commodity…at the expiration of 28 days from the date of the transaction." In that context, the CFTC has noted that the CFTC "could, depending on the facts and circumstances, view 'offerors' as any persons presenting, soliciting, or otherwise facilitating 'retail commodity transactions, ***including by way of a participation interest in a foundation, consensus, or other collective that controls operational decisions on the protocol, or any other persons with an ability to assert control over the protocol***…" At a minimum, this could be read as a thinly veiled call-out of smart contract systems like MakerDAO, Everett and Acala, which are actively managed by governance token holders. However, even broader readings are possible—for example, the reference to "consensus" could rope-in validators, block producers or miners, and the reference to "assert[ing] control over the protocol" could be read to apply to developers who contribute code to or have "merge access" to the core network client.[3]

- In a personal speech at a conference, Commissioner Brian Quintenz of the CFTC espoused a relatively aggressive view of developer liability for smart contracts that do not comply with CFTC regulations:

> "*In the context of decentralized blockchains, like Ethereum, on top of which multiple applications can run autonomously via smart contracts, [the CFTC's regulatory regime] requires identifying who is responsible for ensuring that activity on the blockchain complies with the law…If the contract is a product within the CFTC's jurisdiction, then regardless of whether it is executed via a written ISDA confirmation or software code, it is subject to CFTC regulation. ... Let's say the hypothetical product at issue is within our jurisdiction, but is not being executed in a manner compliant with CFTC rules. Who should be held responsible for this activity?…[I]t seems unreasonable to hold [core developers] accountable for every subsequent application that uses their underlying technology… Similarly, miners and general users of the blockchain are not in a position to know and assess the legality of each particular application …That leaves us with the developers of the smart contract code that underlies these event contracts…I think the appropriate question is whether these code developers could reasonably foresee, at the time they created the code, that it would likely be used by U.S. persons in a manner violative of CFTC regulations. [If] the code was specifically designed to enable the precise type of activity regulated by the CFTC, and no effort was made to preclude its availability to U.S. persons… a strong case could be made that the code developers aided and abetted violations of CFTC regulations. As such, the CFTC could prosecute those individuals for wrongdoing.*"[4]

The above quotes, while being far from the final word on the subject, would tend to indicate that commodities regulations may be equally applicable to decentralized systems as to centralized ones. At first glance, this may appear surprising—after all, as we will discuss below, FinCEN has indicated that decentralized non-custodial solutions may be regulated differently than custodial ones[5], and the SEC appears willing to regard many of the policy concerns underlying the securities laws to be inapplicable to tokens in sufficiently decentralized systems[6]. Why wouldn't the CFTC also recognize that a "sufficiently decentralized" system should not be subject to antiquated commodities exchange regulations? A possible justification may be that, whereas money transmitter laws pertain

[3] [actual delivery guidance]

[4] "Remarks of Commissioner Brian Quintenz at the 38th Annual GITEX Technology Week Conference," October 16, 2018.

[5] Application of FinCEN's Regulations to Certain Business Models Involving Convertible Virtual Currencies

[6] " Digital Asset Transactions: When *Howey* Met Gary (Plastic)," William Hinman, Director, Division of Corporate Finance

expressly to financial intermediaries and the securities laws pertain expressly to securities *issuers* with information asymmetry advantages over holders of their securities, the commodities laws are different—they are primarily meant to regulate certain types of market *risks*. For example, the risks of credit default swaps which led to the global financial meltdown in 2008 which ultimately inspired many Bitcoiners. The resulting policy approach has been described as "a bedrock principle of 'mandatory intermediation'"[7] embodied in U.S. commodities regulations; thus it is not hard to see how such regulations may vex blockchain systems, which are expressly designed to provide *disintermediation* (often at the cost of incurring many inefficiencies like low transaction throughput). Given the systemic risks and potential for black swan events that can occur even in decentralized finance—"Black Thursday" being an arguable example[8]—it is not inherently surprising that the commodities laws may appropriately seek to address such risks and potential domino effects in decentralized systems just as they do for centralized ones. However, to the extent that decentralized systems can eliminate such risks *without* using intermediaries, they would be better, not worse, than solutions involving regulated intermediaries, and then it should be possible to persuade the CFTC or legislators to modify the regulations to recognize the legitimacy of such systems.

While recognizing the many uncertainties involved, the authors of this report would speculate that the applicability of commodities regulations to liquid staking should be analyzed as follows:

- Delegation Exchange.
    - Non-tokenized exchanges of staking positions should, in our view, be regulated as simple spot transactions in commodities. Two parties trade a staking position "on the spot"—whether through exchange of a private key, some native delegation-trade function in the protocol or a system like B-Harvest's—and the trade will likely settle almost immediately.

- Native Liquid Staking/Delegation Vouchers.
    - Transactions in native StakeTokens would likely be deemed either spot transactions or simple forwards the primary purpose of which is to transfer ownership of the underlying stake and staking rewards. On this theory, transactions in native StakeTokens would not be limited to taking place on CFTC-approved exchanges or subject to the other heavy CFTC regulations reserved for futures, swaps and similar derivatives. Because such StakeTokens are validator-specific and can be seamlessly redeemed for the underlying stake and staking awards, the purpose of such StakeTokens is not to hedge or transfer the risks of slashing separately from an entitlement to the stake and staking awards; rather, it is simply to have additional liquidity. Moreover, this style of liquid staking can enhance market transparency and pricing because the validator-specific nature of the StakeTokens allows markets to dynamically price risk, reward good validators and punish bad validators. Thus, such StakeTokens should be seen as *reducing* systemic risk and thus justifying lighter regulations rather than tougher ones.
    - However, we cannot rule out that the CFTC would impute a more contractual logic even to native StakeTokens—for example, the CFTC could argue that since the staking rewards are uncertain, the risk of slashing is always present, and physical

[7] Andrew P. Cross, "Swaps and Retail Commodity Transactions (Leverage, Margin or Financing: Will We Know It When We See It or Only After It Has Been Identified As Such?)"
[8] "Black Thursday for MakerDAO: $8.32 million was liquidated for 0 DAI" by whiterabbit.

delivery may take longer than 28 days due to the un-bonding period or other factors, that native liquid staking poses the same risks as leveraged, margined or financed retail commodities transactions as discussed for non-native liquid staking below. Or the CFTC could be concerned about the potential moral hazard of a validator deliberately causing a slashing event and profiting through an insurance arrangement, as referred to in the main body of this report, and argue for application of commodities regulations for deeper policy-based reasons. That being said, we view this approach as unlikely to be reasonable for native liquid staking, and we note that the CFTC has committed to take a functionalistic approach in analyzing such issues.

- Non-Native Liquid Staking.
  - StakeTokens issued by smart contract systems are the most complex and legally uncertain type of liquid staking to analyze from the standpoint of commodities laws. This make sense, since derivatives are a major target of commodities regulations and the StakeTokens synthesized by such systems are essentially blockchain-based derivatives.
  - Non-native liquid staking systems like Everett and Acala that attempt to make the StakeToken ("bAtoms" for Everett, "L-DOTs" for Acala) do double duty as a stablecoin pegged 1:1 with the underlying staking token ("Atoms" for Everett, "DOTs" for Acala) will have a particularly high risk of falling under burdensome CFTC regulations. In many ways, these StakeToken systems resemble either: (a) retail commodities transactions occurring on a margined, leveraged or financed basis or (b) swaps:
    - The stakers in such systems may be seen as seeking to acquire the future staking awards (and to re-acquire extra collateral intended to secure the value of the StakeTokens) on a "leveraged, financed or margined" basis. From this perspective, non-native liquid staking may be considered a type of CFTC-regulated retail commodities transaction that is required to occur only on CFTC-registered "designated contract markets" unless all participants are ECPs. The terms "leverage", "finance" and "margin" have not been strictly defined for purposes of the applicable regulations, and the CFTC has interpreted them broadly in the past so that "indebtedness in the traditional sense (i.e., the use of borrowed money) is not required."[9] Indicia of leverage are said to include "allowing a customer to control a large amount of a commodity with a comparatively small amount of [another commodity]" and "allow[ing] customers to significantly boost their profits with a relatively small investment while also magnifying their losses". Although the StakeTokens are "overcollateralized" in a certain sense (since users will presumably deposit more of the staking tokens than they receive in StakeTokens), when the potential staking rewards and slashing events are taken into account, the system is likely leveraged inasmuch as it could become "insolvent" in certain situations (massive slashing events, or a "black swan" event like the auction efficiency failures observed in MakerDAO's "Black Thursday," etc.). Expressed another way, the locked-

[9] *See* Andrew P. Cross, Swaps and Retail Commodity Transactions (Leverage, Margin or Financing: Will We Know It When We See It or Only After It Has Been Identified As Such?).

up collateral is both the "margin" for obtaining the potential staking rewards and the "margin" for the associated stablecoins that are supposed to have a 1:1 peg—when ***all*** of that value is taken into account, the system may be seen as having the same of kind of capital-multiplying effects (and to pose the same kinds of risks) as more conventional margin trading, notwithstanding the apparent "overcollateralization". The governance token holders may also be seen as providing "financing" to the stakers, since they are (or are at least often presented as) "lenders of last resort" charged with holding the peg by diluting themselves in insolvency events.[10]

- Alternatively, the stakers in such systems may be seen as having disposed of/sold the staking tokens (or a portion of the staking tokens, or the associated staking rewards) with an option to re-acquire them at a later date in exchange for the StakeTokens, which may under certain circumstances be considered a CFTC-regulated option or a CFTC-regulated "swap" (note: many commodities options may be swaps). From this point of view, the smart contract system embodies an option, with the StakeToken (or the amount of staking tokens represented by the StakeToken) being the "exercise price" required to receive the extra collateral and the staking rewards. Like leveraged, margined or financed retail commodities transactions, transactions in swaps are restricted to CFTC-registered "designated contract markets". From a policy perspective, these systems also present risks similar to swaps, in that they may enable the transfer of some of the risks of staking onto the smart contract system (or perhaps the governance token holders, as lenders of last resort) without transferring ownership of the underlying collateral; the "risk discount" on staking is being artificially obscured through clever blockchain engineering, which could be seen as posing market risks that implicate regulatory concerns. On the other hand, non-native liquid staking systems do have some noteworthy differences from options, particularly if they also involve the payment of a variable stability fee (which is less like an option exercise price and somewhat more similar to payments of interest on a debt) and swaps (particularly because title to the staking tokens and potential rewards moves with the StakeTokens, rather than merely risk). Even if non-native liquid staking systems do facially meet the definition of "swaps," it is at least *possible* that one of the exceptions may apply in at least a subset of cases, such as the exception for "commercial merchandizing transactions" involving deferred delivery'. These details would require extensive analysis that is beyond the scope of this report.

The above may paint a pessimistic picture of the future for systems like Everett and Acala. There is no denying the conflict between a policy of "mandatory intermediation," on the one hand, and the disintermediating design principles of blockchain technology. However, we have seen other situations—like the imbrication of ICOs and securities laws—where regulators have come up with surprisingly creative ways of honoring regulations while also allowing blockchain systems to flourish. For example, the SEC has softly endorsed a philosophy in

[10] *See* e.g. The DAI Stablecoin System: Whitepaper: "MKR….serves as a backstop in the case of insolvent CDPs". *See also* Reddit comment believed to be from Rune Christensen*:* "It is unfortunately not possible to change the fundamental feature that MKR holders are on the hook for all the dai in the system - this is because it[']s a crucial requirement that all dai has to be fungible, so ultimately they have to have the same backing of last resort."

which the securities laws may cease to apply to an ICO token once the system is "sufficiently decentralized," and FinCEN has articulated that unhosted wallets as such are not required to register as money services businesses. Assuming that CFTC regulations do facially apply to these systems as discussed above, then the goal for proponents of these systems will need to be convincing regulators either that: (a) the decentralized, automated/autonomous or transparent nature of the system eliminates the risks that make regulation appropriate when they occur on a centralized basis; or (b) the regulations should be modified to allow such systems to be registered with the CFTC as regulated designated contract markets.

Non-native liquid staking systems like Stake DAO are somewhat less likely to implicate commodities regulations. In some ways, such a system can be viewed as the inverse of non-native liquid staking systems like Everett and Acala: Users in Everett and Acala could be seen acquiring stablecoins and/or staking rewards "on margin" from the system or the governance token holders, in exchange for which such users will likely pay the governance token holders "interest" in the form of stability fees. In contrast, with Stake DAO, it is the smart contract system or the collective of DAO token holders that is borrowing staking tokens *from* and paying interest *to users*.[11] In theory, then, Stake DAO style systems could also be viewed as involving leveraged, margined or financed retail commodities transactions—just with the roles of lender and borrower switched. However, in our view, this is not really "leverage," but simply "debt". Unlike with Everett/Acala-style systems, these transactions do *not* have capital-multiplying effects—indeed, here the StakeTokens should always be discounted based on risk and the time value of money, whereas Everett/Acala-style systems are designed to reduce and/or hide such discounts. Likewise (and, again, in contrast to Everett/Acala-style systems), assuming the Stake DAO smart contracts function reliably, insolvency should simply not be possible. Accordingly, the authors of this report suspect that Stake DAO-style systems would be regulated more like either simple commodities loans or forward contracts for purchasing a specific asset at a specific price in the future , and thus should not be subject to the heightened regulations requiring "mandatory intermediation" on a CFTC-regulated exchange.

- Systems like StakerDAO are obviously at high risk of being subject to elevated regulations of some kind, but commodities regulations may not be at the top of the list. We assume that in most cases the synthetic StakeTokens issued by such systems are likely to be securities and that SEC jurisdiction would apply largely to the exclusion of CFTC jurisdiction, though the agencies have joint jurisdiction over certain kinds of swaps. In this case, securities law may be preferable to commodities laws anyway, since there is no "mandatory intermediation" principle embodied in the securities laws like there is for the commodities laws. Indeed, the security itself (the StakeToken) can be registered with the SEC and then trade relatively freely, whereas there is no option to register a particular type of commodity with the CFTC to obtain freer trading—rather, it is the platform and/or traders who must be registered with the CFTC in order to be allowed to transact in certain kinds of commodities, and that may be impossible for blockchain systems. Thus, "opting

[11] The reason why it is economically attractive for the DAO token holders to borrow staking tokens from users (and pay them interest for the privilege) is that the DAO can then stake such staking tokens with a specific validator, Stake Capital, whose commissions flow to the DAO. Again, it goes the other way in MakerDAO-like systems: there, it is economically attractive for the users to borrow from the DAO token holders in order to leverage the underlying collateral.

into" the securities laws may be the best bet for systems like StakerDAO, and we assume that they will do so.

- Custodial Liquid Staking.
  - Custodial liquid staking will be analyzed differently depending on the exact mechanics involved.
  - An easy way for an exchange to ensure that custodial liquid staking is not subject to onerous regulations would be to deliver all stake and staking rewards to each user's wallet (or to an independent financial institution acting as the user's agent) every 28 days, with no automatic re-delegation. However, this may not be feasible or may undermine the purpose of liquid staking—to allow for liquidity despite un-bonding periods. It would also impose a significant administrative burden and extra transaction costs.
  - Therefore, it is likely that exchanges would need to analyze whether liquid staking on behalf of users could be considered to be occurring "on a leveraged or margined basis, or financed by [the exchange or associated persons]".
  - If there is no leverage, margin or financing, then liquid staking with an exchange should simply be a spot transaction and treated the same as spot transactions in BTC, ETH and other native tokens.
  - If leverage, margin or financing are involved, then the exchange would need to be registered with the CFTC and comply with the rules for complex commodities derivatives. There is a non-zero risk of this result occurring. After all, an important reason for users staking with an exchange instead of directly would be to reduce the users' own risks from staking, on the theory that the exchange will spread any slashing losses across the pool or, better yet, insure against slashing. This may mean that the staking transaction and StakeToken are "financed" by the exchange and may trigger a requirement for the exchange to be a CFTC-supervised exchange and not allow the StakeTokens to trade in any other venue.

- Synthetic Liquid Staking.
  - Synthetic liquid staking is simply a commodities swap and would be subject to all of the swap regulations, including generally being limited to CFTC-registered exchanges.

E. Securities Regulations.

Liquid staking will be subject to securities law regulations if either: (1) the native PoS tokens are securities; or (2) the underlying staking transaction between the validator and the staker represents a securities transaction and the thus StakeToken are securities derivatives.

To date, to the knowledge of the authors, the SEC and other securities regulators have issued no substantial guidance specific to how the securities laws apply to PoS networks. On the contrary, most regulatory guidance has been about "tokens" in general or "blockchain" in general, and typically seems to include implicit assumptions most appropriate to PoW systems like Bitcoin and Ethereum in its current form. Even when PoS systems have been the subject of a direct challenge, as in the recent U.S.

federal court litigation between the SEC and Telegram, the issues seem to be litigated and adjudicated without regard for the specific properties unique to PoS.

To an informed and careful student of both blockchain systems and the securities laws, however, PoS systems should in general be viewed as having at least a slightly elevated risk of being subject to the securities laws as compared to PoW systems. Whereas PoW systems create a separation of concerns by making block production and the profit interests associated with receiving new tokens from the protocol theoretically quite separate from token holding, PoS systems eliminate the separate class of "miners" and thus potentially give all token holders who can directly or indirectly stake an interest in benefitting from the issuance of additional tokens by the protocol. This means the value of all tokens is now associated with a payment flow, or income, and makes tokens look at least slightly more like traditional securities. Many PoS blockchains also provide for "on-chain governance" via token voting, which is similar to equity securities. "Delegation" of powers associated with a token to "validators" or "bakers" also resembles the kind of "proxy delegation" frequently used for voting securities.

However, on deeper examination, the types of payment flows associated with staking in PoS systems at the network level are rather dissimilar to the "investment contract" securities the SEC has been focused on for tokens. Whereas holding a share of Apple stock is a bet that Apple management will make skillful efforts to increase Apple profits and thus make the shares more valuable, there is typically no equivalent centralized entrepreneurial management of PoS networks. In general, this should mean that merely holding a PoS token does not implicate the securities laws on the basis of the *Howey* test for investment contracts.

When stakers delegate to a particular validator, the analysis may be different. Depending on the design of the PoS system, it is possible that some validators may deliver much better returns to their stakers than others. If better returns primarily result from the validator being better at avoiding slashing events or simply providing a larger "bond" at the validator's own expense, then this may not implicate the securities laws because these types of advantages are not the sort of "entrepreneurial efforts" which typically matter under the securities laws. However, if one validator can perform significantly better at delivering returns to stakers than another due to entrepreneurial finesse—marketing, commercial partnerships, proprietary equipment and software optimizations, etc.—then a reasonable argument can be made that staking with a particular validator is a bet on the validator's entrepreneurial efforts, and that the securities laws should apply to the staking transaction, even if they do not otherwise apply to the staking token.

When such entrepreneurial dynamics are present, they would be exacerbated by the issuance of per-validator StakeTokens. The StakeTokens could be deemed to be securities and the validators could be deemed the issuers of those securities. On a PoS system like Tezos, each validator only has a finite capacity to receive delegations (based on the amount of "bond" the validator has staked). Thus, many of the top validators are at or very close to their full capacity to receive delegations. In such situations, the risk of securities laws applying would be even more strongly exacerbated—now, not only would it be the case that the price of a StakeToken might be strongly affected by the entrepreneurial prowess of the validator, but also, since the opportunities to directly get exposure to that prowess by staking with the validator are limited, the StakeTokens could be subject to supply/demand mechanics tending to result in hype bubbles and runaway profits for holders and traders.

While the above risks are theoretically present for liquid staking, at the present time an examination of the relative yields from different validators does not support them. For example, the top 100 Tezos bakers listed on www.mytezosbaker.com all deliver yields around 3-6%, with most delivering yields of 5.5% - 6%. These types of yields do not strongly suggest that validators are able to materially outperform one another in delivering differential staking yields; thus, their entrepreneurial efforts are likely not the kind of efforts contemplated by the securities laws. However, the introduction of per-validator StakeTokens could undoubtedly offer validators new opportunities to differentiate themselves, and thus it will be important for community participants to think carefully about securities laws risks in deciding on an implementation for liquid staking.

Alternatively, the SEC could choose not to focus on "entrepreneurial efforts" and could instead try to argue that PoS tokens or StakeTokens are a simpler type of enumerated security. For example, the SEC could apply the "family resemblance test" for debt securities and argue that staking transactions—which lock-up capital similar to how loaning capital does and also pay something similar to "interest"—are bonds or other debt securities. In that case, the nature of the validators' "entrepreneurial efforts" could be irrelevant. Similarly, the SEC could argue that PoS tokens or StakeTokens are "shares" because staking rewards could be analogized to dividends and, like shares, many PoS tokens carry governance rights.

In the event that PoS tokens or staking transactions were deemed to be securities, then StakeTokens would likely also be securities. The securities laws can be burdensome, not only for capital-raising in the first instance (here, the initial issuance of StakeTokens) but also for ongoing compliance. If StakeTokens are deemed "equity securities", then, under Rule 12g-1 promulgated under the Exchange Act, the validator would have the same reporting obligations as Apple Inc. as soon as the validator has $10M+ in assets and the StakeTokens are owned of record by more than 499 unaccredited investors or more than 1,999 investors. Needless to say, this would be extremely burdensome for a validator. However, it is also possible that StakeTokens would be seen as similar to bonds and thus debt securities, and that the Exchange-Act-reporting regime thus would not apply.

Even if PoS systems are otherwise exempt from securities laws, certain forms of liquid staking could still implicate the securities laws. For example, the governance token in non-native liquid staking could be deemed a security and this could also become an obstacle to using the StakeTokens generated in non-native liquid staking.

Finally, there remain major question marks around the SEC's informal guidance and practice of treating tokens within "sufficiently decentralized" systems, such as Ethereum in its current PoW form, as non-securities.[12] In a system like Everett, how many different holders must hold the governance token for the system to be "sufficiently decentralized"? Is there a specific Gini coefficient at which the system becomes sufficiently decentralized? Or is it not a matter of how many people hold the token, but rather of how many actively and consistently participate in governance on an informed basis? Are other types of decentralization—such as software contributions being made by many unaffiliated competent volunteer smart contract developers—required as well? What if the token is held by many people, but they a majority of them happen to also be investors in something else like Microsoft Inc.? should that count as decentralized or centralized?[13]

F. Banking/Money Transmission Regulations.

Both the native tokens of a PoS network and any associated StakeTokens are likely to be considered "value that substitutes for currency" and thus "convertible virtual currencies" ("***CVCs***") in the U.S. and to have similar status in other countries. Thus, blockchain ecosystem participants who provide certain kinds of services with respect to such tokens could be deemed "money services business" in the U.S. (or could have a similar status under other countries' laws). Money services businesses are regulated as financial intermediaries at the U.S. federal level by FinCEN and in many individual U.S. states by individual state regulators. MSBs are subject to stringent audit and reporting requirements, including know-your-customer requirements and suspicious activity reporting rules.. However,

[12] Digital Asset Transactions: When *Howey* Met Gary (Plastic)," William Hinman, Director, Division of Corporate Finance

[13] For a detailed examination of the criteria by which "sufficient decentralization" may be assessed for securities law purposes, *see* "Defining Decentralization for Law," Gabriel Shapiro, April 15, 2020.

regulators such as FinCEN have published guidance to the effect that the providers of non-custodial solutions such as unhosted wallets will not always be money services businesses.

This suggests a number of issues and questions:

- Are validators on a normal PoS network (without liquid staking) acting as money services businesses?
- Are validators with a validator-specific StakeToken acting as money services businesses?
- Are liquid staking smart contract systems or their governors acting as money services businesses?
- Are participants in a liquid staking swap or exchanges that engage in liquid staking on a custodial basis acting as money services businesses?

We consider each of these questions in turn.

1. "***Are validators on a normal PoS network (without liquid staking) acting as money services businesses?***"

The answer to this question may not be the same for all PoS networks or all validators.

On Cosmos, stakers face zero custodial risk from validators and validators never accept any CVC from or transmit any CVC to any staker. In theory, it could be argued that validators still have some power over the tokens staked with them—the power to vote it or to cause it to be slashed—but: (a) only the voting power is discretionary; (b) slashing is highly unlikely to benefit the validator (but is actually likely to harm the validator) and thus would only occur by mistake; and (c) these are not the types of powers or risks one would typically associate with custody. Moreover, it is simply impossible for a Cosmos validator to conduct any KYC on or monitor the transactions of a staker—thus, treating the validator as a money services business that must conduct KYC, file suspicious activity reports and follow similar obligations would mean that it is illegal to be a Cosmos validator because validators cannot comply with the law; an absurd result!. In the opinion of the authors of this report, the best view is that Cosmos validators simply run validation software and hardware and that other ATOM holders may utilize that software and hardware for a fee paid by the network itself to the validator. On this view, Cosmos validators would not be money services businesses.

However, staking on other PoS systems may be different and arguably create a greater risk that validators are money services businesses. On Tezos, although stake is delegated on a non-custodial basis, the rewards from staking are initially allocated to the validator—referred to as a "baker" in the Tezos community. The baker will typically pool all rewards and distribute them on a *pro rata* basis to all stakers, *less* commissions and costs. This means that the distribution and allocation of awards is *not* trust-minimized and *not* mediated by the protocol; thus, stakers face custodial risk from their bakers. And, in fact, various Tezos bakers have abused their custodial powers by failing to distribute staking rewards, giving rise to third party services such as Baking Bad and My Tezos Baker that attempt to audit the trustworthiness of bakers and blacklist untrustworthy bakers. Tezos bakers also have sought to add non-native features to staking such as automatic re-delegation of awards to the baker, which requires them to have their own policies and procedures and arguably a separate, direct contractual relationship with each staker. All of these factors arguably place Tezos bakers at greater risk of being money services businesses than Cosmos validators, notwithstanding that Tezos bakers and Cosmos validators are superficially very similar. Nevertheless, even Tezos bakers may not be money services businesses because they receive staking rewards from the network and transmit them back to the stakers, rather than receiving money from the stakers and transmitting money to other persons on behalf of the stakers; the bakers' receipt and transmission of staking rewards may therefore fall under the "merchant exception" to the money services business test.

2. "***Are validators with a validator-specific StakeToken acting as money services businesses?***"

For any validators who are already money services businesses, this question is somewhat irrelevant. But for validators who might not otherwise be money services businesses, the question is important to assessing the risks of liquid staking, and can be usefully re-framed as follows: "*Does liquid staking, in and of itself, turn a validator into a money services business?*"

Overall, we would expect the analysis of this question to closely parallel the more general analysis of whether validators on a given network are money services businesses. In native liquid staking, the protocol will automatically generate and enforce rules regarding a validator-specific StakeToken, and this should not materially increase the risk that a validator is a money services business. If validators are already money services businesses on a given network, then adding a native StakeToken should not materially worsen their position in itself.

However, if the StakeTokens are staking vouchers issued and redeemed by validators extrinsically from the protocol, the validators would be like custodial exchanges which conduct liquid staking, and would then be at greater risk of being money services businesses no matter the ordinary situation on their networks, especially if these vouchers are issued and/or trade anonymously or pseudonymously like bearer instruments. Indeed, FinCEN in its 2019 guidance on CVRs seemed to take some pains to cover this type of situation under money transmission regulations by observing that "the issuance and subsequent acceptance and transmission of a digital token that evidenced ownership of a certain amount of a commodity, security, or futures contract" can make the issuer a money services business if such digital tokens are "repurposed to serve as a currency substitute." The only escape hatch offered by FinCEN from this result would be for the validator to embrace registration under an alternative regulatory regime, such as by becoming a bank or a person registered with and functionally regulated or examined by the SEC or CFTC.

3. ***"Are liquid staking smart contract systems or their governors acting as money services businesses?"***

Actively governed liquid staking smart contract systems are at greater risk of being deemed custodial or hosted and thus potentially subject to money services business regulations than are native liquid staking systems, but less risk than true custodial liquid staking solutions. The governors of the system actively manage the system for profit, and have a degree of control over its. It is true that such governors do not have all of the powers of a typical custodian, but the powers that they do have, together with their profit motive and active involvement, may be a sufficient basis for arguing that they should have the same obligations as a more traditional money services business. Moreover, such smart contract systems both accept and transmit value on behalf of users: they accept staking tokens from users and then transmit those tokens (or certain interests in such tokens) by staking them. This creates a heighted risk of such systems or the association of their governance token holders being deemed money services businesses.

To the extent that such smart contract systems may be analogized to "DApps" as that term is understood by FinCEN, then the following language from FinCEN's CVC guidance may be applicable: "*[W]hen DApps perform money transmission, the definition of money transmitter will apply to the DApp, the owners/operators of the DApp, or both.*" This suggests that FinCEN could regard the smart contracts themselves as money transmitters and may seek to hold the creators of the smart contracts responsible for their failure to design the smart contracts to comply with money transmitter laws. When the smart contracts are operated as a business by governance token holders, FinCEN would likely have strong arguments on this point; however, if the smart contracts are pure autonomous software, the creators may have powerful defenses based on freedom of speech principles.[14]

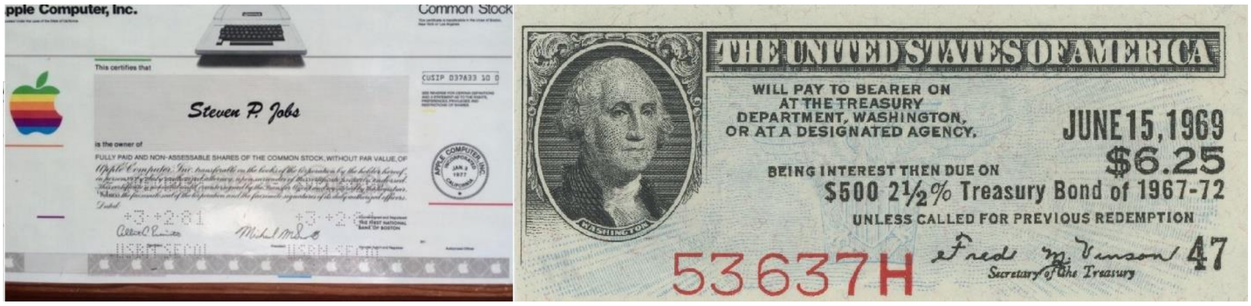
4. *"Are participants in a liquid staking swap or exchanges that engages in liquid staking on a custodial basis acting as money services businesses?"*

Typically, exchanges offering liquid staking solutions would be at significant risk of being money services businesses due to the custodial nature of their offerings, especially if they accept *fiat*. This should not be surprising, as exchanges are very similar to banks, and some are actually supervised by baking authorities such as the New York Department of Financial Services, FinCEN and state money services regulators.

Two parties simply entering into a liquid staking swap are likely to be "users" and thus not subject to money services business regulations. However, a business that traded such swaps or brokered such swaps could be subject to money services business regulations.

G. Taxes - Regulation of Bearer Instruments.

A StakeToken could be viewed as a "certificate" or "bond" or "instrument" which represents the associated stake and staking rewards and confers upon the holder of the StakeToken the legal right to redeem the stake and staking rewards. Viewed in this light, a StakeToken will be a *bearer* certificate, *bearer* bond or *bearer* instrument if it is issued and redeemable on an anonymous or pseudonymous basis. Bearer bonds and bearer stock were once common in many jurisdictions across the world and were valued for the privacy they afforded to investors. Unlike typical instruments—which are issued in the name of the first holder and then may be endorsed over to the name of a second holder, etc.—bearer instruments are issued and transferred simply to "the bearer". Absent extraordinary circumstances such as a known theft, bearer instruments are presumed to be lawfully held and their rights lawfully exercisable by whoever in fact holds them.



pple Computer, Inc.

Common Stock

This certifies that

Steven P. Jobs

is the owner of

FULLY PAID AND NON-ASSESSABLE SHARES OF THE COMMON STOCK, WITHOUT PAR VALUE, OF

Apple Computer, Inc.

CUSIP 037833 10 0

THE FIRST NATIONAL BANK OF BOSTON

THE UNITED STATES OF AMERICA

WILL PAY TO BEARER ON
AT THE TREASURY
DEPARTMENT, WASHINGTON,
OR AT A DESIGNATED AGENCY.

JUNE 15, 1969

$6.25

BEING INTEREST THEN DUE ON

$500 2½% Treasury Bond of 1967-72

UNLESS CALLED FOR PREVIOUS REDEMPTION

53637H

Fred M. Vinson
Secretary of the Treasury

47

Figure 11: *A non-bearer stock certificate from Apple Inc. and a bearer bond coupon from the U.S. Treasury.*

In contemporary finance, bearer instruments have become heavily disfavored—in large part because of regulations that outright prohibit them or impose heavy compliance burdens when they are used. In the United States, The Tax Equity and Fiscal Responsibility Act of 1982 ("***TEFRA***") imposed adverse tax treatment on most bearer bonds and other un-registered "obligations"—prohibiting the issuer to deduct interest, imposing an excise tax on the issuer, requiring the holder to treat all gains as ordinary income rather than capital gains, prohibiting the holder from deducting losses and eliminating withholding tax exemptions for foreign bearer bond holders. The elimination of withholding tax

[14] *See* "Electronic Cash, Decentralized Exchange, and the Constitution" by Peter Van Valkenburgh, March 2019 Coin Center Report.

exemptions is particularly important, because it meant that the issuer of a bearer bond must obtain a Form W-9 or Form W8-BEN from the bond holder—thus effectively eliminating all anonymity. Similarly, for bearer stock certificates, the corporate laws of all U.S. states have prohibited bearer stock certificates since 2007, when the last holds outs—Wyoming and Nevada—amended their corporate laws to prohibit them.

Outside, the U.S., bearer instruments are similarly disfavored. For a time, a few jurisdictions such as Panama which sought to be tax havens for the wealthy still permitted bearer instruments. Nominally, many such jurisdiction still do permit bearer instruments. However, almost all of them, including Panama, have now passed laws requiring bearer instruments to be "immobilized"—meaning that they effectively are registered instruments rather than bearer instruments. In effect, all major jurisdictions have been pressured into eliminating bearer instruments in order to be removed from or avoid being added to the FATF blacklist or FATF greylist, which carry sanctions from the FATF member nations.

In general, the risk of StakeTokens being viewed as bearer instruments will be greatest where legal engineering is most required and lowest for trust-minimized solutions:

- In native liquid staking, it is possible to reasonably take the position that the StakeTokens are not legal instruments at all, and do not represent a debt or other contractual obligation, but simply have a functional role within the protocol. In such a case, the penalties associated with bearer instruments would arguably not apply even though the StakeTokens trade anonymously.
- A similar argument could apply to non-native liquid staking through smart contract systems. However, considering that the StakeTokens minted by such systems would be 'issued in bearer form' since they are not issued to the name of a particular person and do not require being endorsed to the name of a new holder for transfer, it would not be entirely unreasonable to argue that this type of StakeToken is a type of bearer instrument similar to a bearer bond. On this theory, the StakeTokens would represent an "obligation" of the association of persons holding and utilizing the system's governance token, and since the instrument representing that obligation would be un-registered, the tax penalties would apply. At present it is entirely unclear which analysis is correct.
- For synthetic and custodial staking, which are inherently contractual, one would expect that they are at high risk of being deemed bearer instruments and having the associated penalties if issued and trading anonymously—accordingly, to avoid this issue, one would generally expect synthetic and custodial staking to be done on a named/registered basis, mediated by business intermediaries such as centralized exchanges or broker-dealers who KYC their customers and have tax reporting obligations.