Liminal Shorts

How exchanges can earn more through Staking

Table of contents

Staking As A Use-Case

Blockchain networks were initially created to establish a decentralized economy and enable seamless value transfer. However, one of the preliminary chains, **Proof-Of-Work**, was driven by an extremely energy-intensive operational mechanism that **limited its expandability.**

PoW consensus mechanism, being used by Bitcoin and Ethereum, the two chains processing over **90%** of transactions were entirely run on this consensus. Over time it started to show numerous **scalability, feasibility and sustainability** issues leading to a lookout for a finer consensus mechanism that fuels the decentralized ecosystem and enlarges the vision of cryptocurrencies on the whole.

This led to the emergence of **Proof-of-Stake (PoS)** as a powerful and rewarding consensus mechanism.

PoS introduced the concept of staking, which eliminates the need for mining in PoW by allowing validators to confirm transactions on the blockchain by locking a certain number of tokens as a commitment.

Staking As A Use-Case proved invaluable not just for authenticating transactions on blocks but to enable the distribution of rewards earned as well.

Economics of Staking

Staking addresses the limitations of Proof-of-Work (PoW) consensus and offers numerous benefits for blockchain networks. It has evolved into a strategic concept that promotes efficiency, lower fees, faster transactions, and incentivized tokenomics.

POS Network

To achieve an economic equilibrium in blockchain networks, Staking is explicitly explored to achieve imperative execution of trades, for example:

- Ensuring fair transaction validation
- Preventing rewards distribution issues
- Mitigating node monopolization
- Eliminating 51% attacks on staked coins
- Nothing at Stake

How Exchanges Can Earn More Through Staking?

Proof-of-Stake (PoS) focuses on, reducing volatility, increasing ecosystem usage, and decreasing circulating supply. Validators solve two steps in this chain; provide computational power to validate transactions and authenticate logically. Validators stand a chance to be, rewarded upon successful transaction and slashed for a deficient one.

Staking is particularly beneficial for blockchains aiming to establish decentralized validator nodes, maintain token liquidity, reduce sell pressure, and drive network adoption. However, it also presents economic challenges, as PoS mechanism designers grapple with the "**Staking Trilemma**" to achieve an evident and scalable outcome.

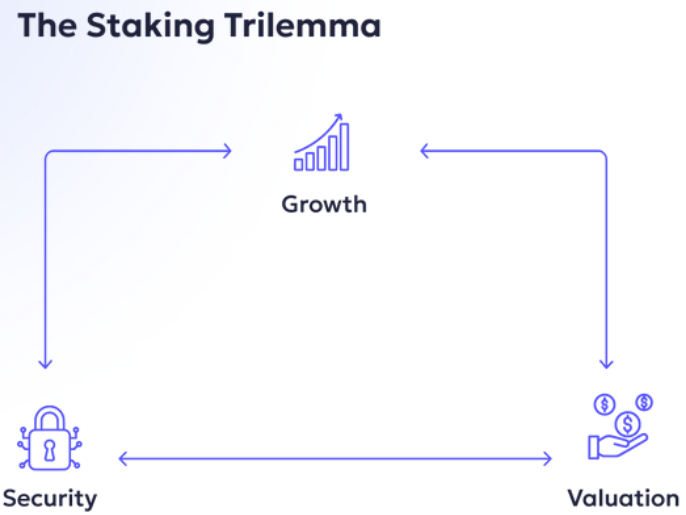
Is Staking Trillema A Concern For Institutions?

The creation of a PoS chain is a complicated process and involves diversified process division to the structure. Staking Trillema addresses three core trade-offs that the consensus designers juggle between to ensure the chains remain either secure, scalable or practical.

Security → Staking Volume
POS mechanism designers aim for a high volume of staking as it is crucial for ensuring the security of a PoS blockchain. By locking up their assets, individuals are motivated to validate transactions and preserve the network's integrity, making it more secure with a larger number of assets staked in the blockchain.

Growth → Transaction Fee
POS mechanism designers aim for low fees to encourage the adoption of their blockchain system, as users consider low transaction fees to be an essential factor when selecting a blockchain to use. Designers must create an efficient and cost-effective system to achieve high growth, and one of the ways to accomplish this is by reducing transaction fees.

Valuation → Inflation
POS mechanism designers strive for low inflation, which is crucial for coin holders as it prevents the dilution of their coins and ensures a return on their investment. Additionally, inflation can reduce the rewards given to stakers. However, it's not possible to achieve all three goals of high security, high growth, and low inflation simultaneously, and designers can only optimize for two objectives at a time.



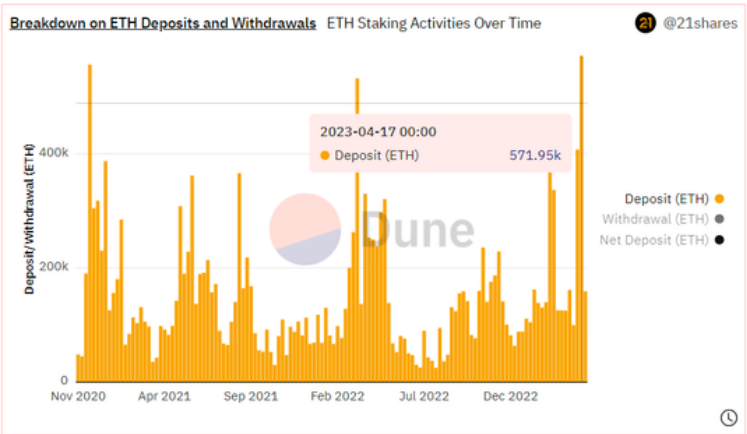
Just like the Blockchain Trillema, Staking Trillema also poses the same hypothesis complication of applying only two out of three goals.

Solving the Staking Trillema directly correlates with the ecosystem adoption of PoS-implemented chains, where they attract Institutional participation to supplement high liquidity and evade the core problems affecting their asset valuation.

What Institutions should look out for while integrating into their subsequent chain, is to engineer a framework that addresses the Staking Trillema premeditatedly and radically.

Institutional Interest In Staking As A Use-Case

The pre-domination of PoW, its exorbitant network and energy consumption and irregular earning pattern had a discouraging effect on institutions especially to build on top of such a technology.



Periodical Rise In $ETH Deposits For Staking By Institutions. Source: Dune Analytics

Using such non-scalable and high-transaction-bearing consensus mechanisms also meant that the reward system in supporting protocol remained only at a single layer and gave no incentive for institutions to share with their users.

This mind shift changed when PoS became the preferred consensus algorithm on which existing protocols started to migrate and develop (A prime example being of Ethereum's shift to PoS and its stable staking yield).

How Exchanges Can Earn More Through Staking?

Realization of the potential of Staking by Institutions got instigated for distinctive reasons like

- To utilize Institutions' native-coin treasury
- A safe outlet while holding the coins for long-term
- And, earn a stable and compounding return as a result

While initially, Staking wasn't an easy deployment and required technical know-how, lately the scenario has changed for Institutions to deploy their liquidity towards Staking, managed and operated by a third party while the Institutions keep complete control of their assets.

Staking as a use-case offsets multifold impediments to using and creating digital assets by Institutions such as:

- Scalability and Cost Efficiency
- Security and Reliability
- Sustainable and Environmentally Friendly
- Consistent and Predictable Returns
- Participation in Governance

Current State of Staking

Staking has grown invariably taking different shapes and formats depending on protocols, pools, returns, locking period and asset market cap. Even though the continuous upcoming of bearish seasons, staking has ensured that PoS assets keep accumulating token-buyers' interest and caching up on the liquidity present.

Market Cap of 35 Top PoS Assets	$190 Billion
Value of Staked Assets	$42 Billion
Annualized Staking Rewards	$3 Billion
Average Yield	11.6%

Source: State of Staking Q1 2023 by Staked_Kraken

By and large, comparatively the yields have gotten down in the past phase and all the crypto has been through increased volatility and asset price downturn, staking has also evolved and now there is a larger asset flow being acknowledged towards self-custody and the non-custodial way that makes staking a safer yield generating strategy for the institutional players.

How Exchanges Can Earn More Through Staking?

According to JP Morgan, with Ethereum onset onto PoS and ETH 2.0 staking yield growing, staking is set to reach $40 billion by 2025 and a major portion of this will be driven by enterprises who have actively initiated putting their crypto treasury to better use now that storing them off-chain. This is a significant journey that staking is destined to cover, sitting at a valuation of $18B in 2021, the present and future of staking will definitely move hand-in-hand with the growth of the entire digital asset industry.

#	Asset	Price	24h	Reward	Adj. Reward	Staking Marketcap	Market Cap	Staking Ratio	Add
1	Ethereum ETH	$1,834.42	-0.38%	6.16%	6.91%	$36,079,221,512	$224,485,067,667	15.97%	
2	Solana SOL	$18.63	-0.75%	6.7%	-0.42%	$7,443,459,364	$7,418,234,811	71.59%	
3	Cardano ADA	$0.32	-3.33%	3.18%	0.47%	$7,036,884,701	$11,009,465,494	60.81%	
4	BNB Chain BNB	$259.59	0.01%	2.53%	9.12%	$6,102,517,293	$40,458,450,330	14.84%	
5	Avalanche AVAX	$13.8	-1%	7.54%	1.25%	$3,713,706,136	$4,759,363,129	61.77%	
6	Tron TRX	$0.08	0.19%	3.89%	1.8%	$2,955,472,597	$5,163,023,192	42.27%	
7	Polkadot DOT	$4.99	-0.2%	14.87%	7.59%	$2,830,596,961	$6,193,754,325	42.65%	
8	Polygon MATIC	$0.78	0.25%	4.71%	2.58%	$2,761,512,171	$7,202,404,053	38.02%	
9	Cosmos Hub ATOM	$9.28	-2.73%	20.96%	2.79%	$2,310,824,297	$3,229,580,083	70.26%	

Source: Staking Rewards

It is imperative to the type of advantages staking offers as it presents a much clear picture of where the yield is coming from, when the staked tokens will be unlocked, how exactly the system will benefit from staked assets volume and actuates capitalization of long-term asset holding.

Why Institutions Are Invested In Staking?

From the moment Staking introduced a direct way for investors to lead protocol governance and augment the foundation, it opened up an oracle for two types of institutions:

- Firstly those who were already vested in those protocols
- Secondly, those looking to integrate into digital asset ecosystems

Right at the edge of 2021, PoS-based Staking started piquing and so did the Institutional interest. As compared to mining, staking facilitated a simpler execution and setup assembly for Institutions to earn and secure.

The category of institutions that are entering into staking is a rich list encapsulating players in both the realms of CeFi and DeFi looking for an outlet to park their assets and earn handsomely:

- **Crypto Native Protocols**

  For all those who are building on chains supporting PoS staking, it becomes inevitable for them to initiate staking on the sidelines to provide better network stability, protocol growth and participation in governance-level decision making which can turn them into a profitable commodity.

- **Exchanges and Marketplaces**

  Considered the gateway for crypto investing, exchanges and marketplaces hold an enormous amount of assets in their wallets and what better way for them to add on this liquidity by staking and offering a portion of yields to their users as well by opening up staking pools.

How Exchanges Can Earn More Through Staking?

- **Crypto Treasuries**

  Treasuries form a crucial part of digital asset securities and holds-up a large chunk of liquidity for blue-chip tokens also the PoS chains supported tokens that can be easily put into staking to continue their asset management journey and also add a layer of incentivizing as well for their clients.

- **Custodians**

  Custodians also fall under the similar category of crypto treasuries, more focused towards securing the assets, and also fit perfectly under the list of institutional parties who ought to enter into staking to continue their promise of securing assets secured by locking them up onto the native protocols itself.

All the above institutional categories entering into staking have two-three reasons to choose it and carry a single commonality to not go fully onboard; asset security.

Bottlenecks In Staking For Institutions

Staking can be a lucrative way for institutions to earn passive income from their cryptocurrency holdings, but it requires careful consideration of various risks and challenges. Factually, it inhibits the idea of simply taking the treasury and locking it in expectation of promised returns from the protocol when they start releasing rewards.

But there are deeper layers of staking functioning which isn't as straightforward for institutions as it may seem.

Out of all factors that combine to picture a troublesome staking experience for institutions some are very straightforward to tackle and eliminate and some can be tricky to instrument given the non-linearity of how digital assets perform. Here's a comprehensive list of the most predominant bottlenecks in staking faced by institutions:

1. Technical Expertise

Protocol-level staking is definitely a complex process that requires technical expertise and knowledge of the blockchain network, how validator nodes function on top of it, their setup framework and dedicated resources to build the entire system up and running. Institutions without complete in-house technical expertise may struggle to set up and maintain staking operations.

2. Network Congestion

This is more of a network-oriented problem and continues to be a serious problem for multiple facets of digital asset adoption including staking. As more participants enter the staking market, network congestion can lead to stuck transactions, reward aggregation and delay in distribution as well, which wouldn't be an ideal situation, especially for institutions who have relayed that staking further to their end-users.

3. Wallet Security Risks

The most vulnerable risk for the entire digital asset class is wallet security where the staked tokens are held. When going for staking, what type of wallet institutions choose to put their tokens on while they are being churned for rewards determines their ultimate security. Generally, hot wallets are more susceptible to hacks and thefts but on the other hand, self-custody cold wallets also pose the risk of losing private keys and the inability to recover the wallet that holds accumulated staked tokens and rewards which can disastrous for any institution.

4. Regulatory Compliance

Staking while may not be a relatively new area of the cryptocurrency market, it is incomparably a newer type of use-case that is now coming under the light of regulations and compliance bodies around different jurisdictions and there are reservations on how investors can and can not comply with staking. Still in its evolving phase, the regulations and compliance around staking, for any institution it imposes a practical risk of confiscation of assets or worst complete stoppage of operations in a particular jurisdiction.

5. Liquidity Risks

Staking is a multi-fold process that ends with ultimately withdrawing the staked portion and the earned interest as well. But there had been liquidity issues where the network is just not able to process the withdrawals and the whole amount gets stuck on the network until adequate liquidity is restored. For institutions, this is a major red flag and they need to ensure that the platform they choose to stake with maintains sufficient liquidity to fulfil all of the deemed returns.

6. Reputation Risk

Participating in staking can expose institutions to reputation risk, particularly if they participate in networks with questionable governance or environmental impact. With so many bad actors in the space of Web3, it is essential that institutions pick the right partner to stake with and carry forward their legacy, respectfully and with indemnity.

Wallet Security As A Key Concern For Institutional Staking

Out of all the factors mentioned above, asset security and wallet management, which holds the assets to be staked, consummate the essential complication in Institutions actively participating in Staking as a primary service for themselves or as a secondary service to provide it further along to their platform users.

Integration of Staking as a means of investment strategy for Institutions is a critical challenge since ensuring primordial wallet security adds an extra extension on top of the validator settings to fortify Institutions' assets, transactions and withdrawal activity before and after Staking.

Some paramount Wallet Security predicaments include the following elements of security, private key management, compliance systems and transaction monitoring at a very fundamental level.

- **Protecting Institutional Assets**

  Institutional investors typically manage significant amounts of digital assets, making them prime targets for malicious actors. Primordial wallet security refers to safeguarding the primary wallets used for staking activities, which hold the staked tokens and generate rewards. Failure to implement robust security measures can expose institutions to the risk of theft, unauthorized access, or loss of assets.

How Exchanges Can Earn More Through Staking?

- **Securing Private Keys**

  The foundation of wallet security lies in protecting private keys, which grant access to the staked tokens. Institutional investors must adopt best practices to safeguard these keys, such as utilizing Cold wallets or secure multi-signature schemes. Employing industry-standard encryption methods, secure key storage, key retrival mechanism and strong access controls are essential to prevent unauthorized individuals from accessing the keys.

- **Governance and Compliance**

  Institutional stakers must adhere to stringent governance and compliance standards. Establishing robust policies and procedures, including segregation of duties, access controls, and thorough identity verification, ensures that only authorized individuals can access and manage staking wallets and whitelisted addresses be used to sweep or refill liquidity. Compliance with regulatory requirements, such as anti-money laundering (AML) and know-your-customer (KYC) regulations, further enhances security and mitigates risks associated with illicit activities.

- **Ongoing Monitoring and Incident Response**

  Constant monitoring of wallet activities is crucial for detecting any suspicious or unauthorized transactions. Institutions should implement real-time monitoring tools and automated alerts to promptly identify potential security breaches. Additionally, establishing an incident response plan, including predefined procedures and roles, enables quick and effective responses to security incidents, minimizing potential damages.

Liminal Presents A Sophisticated Staking-As-A-Service Solution

In our journey of building streamlined solutions catered directly to solve the pain points for Web3 native institutions, Staking is the most demanded solution amongst the group and also the most underestimated and underutilized.

There is clear evidence of PoS network-based Layer 1 and Layer 2 on-chain adoption and the assets that support the chains. With this growth, the ecosystem around these chains is also expanding aggregating Centralized and Decentralized protocols looking to build natively on these chains and holding a lot of liquidity in their native assets.

While some just look to keep a safe custody of these assets and some are actively swapping them either with their internal wallets earmarked for very specific transaction types- deposits or withdrawals, connected with the real-world trading platform and user-individual accounts.

We are taking this one step further for institutions and integration staking right into our custody and security infrastructure that gives institutions much less to think about and more to act upon what they want to do with their secured asset liquidity.

How Exchanges Can Earn More Through Staking?

Staking-As-A-Service at Liminal expands way beyond offering the basics, decent returns. We have deployed an intricate back-end system of inputting the staking very instinctively into our existing wallet solutions so that it renders unequivocal decision-making for our partner to start off staking in a completely decentralized environment and have self-custody of assets at all times.

By utilizing our existing infrastructure, incorporating staking further strengthens the ecosystem we have created, enabling users to delegate and utilize the assets held in their wallets to help improve the network. Staking allows users to become primary validators, leading decentralized asset custody operations, even while their assets are being staked.

There are some very distinctive features that we offer as a part of our Staking-As-A-Service:

Partnering With Figment

Through our partnership with Figment, a company renowned for developing solutions that enable institutions to incorporate staking into their portfolio, we have established one of the most precise and superior staking reward systems. As part of our commitment to providing top-quality services, we are delighted to introduce a premium staking platform that delivers excellent returns for leading institutions in the market.

How Exchanges Can Earn More Through Staking?

Initiating Staking With $ATOM & $MATIC

- We are introducing a new phase of secure institutionalised staking by offering staking services for two of the most significant TVL-led blockchain tokens, $ATOM and $MATIC.

- We are currently providing highly competitive fixed returns for staking these tokens, with returns of up to 20.53% for $ATOM and 8% for $MATIC.

- In addition, we are planning to incorporate other high-market cap coins such as $ADA, $BNB, and $DOT to further enhance their FDV after the initial launch period.

Cold Wallet Staking Linkage

- As institutions prioritise the security of their assets, we are innovating the staking module to address their needs. Given that many institutions store the majority of their assets in cold wallets, we have integrated staking into our cold wallets to enable users to earn passive income without compromising the security of their assets.

- Our industrial-level framework adheres to secure practices and compliances to better support institutions with digital asset custody.

- We are thrilled to expand the scope of our self-custody infrastructure with the addition of staking, creating a new facet of secure and immutable earnings while ensuring full control of assets. This integration creates a perfect amalgamation of features, allowing for secure, composable earnings.

Emphasis On Cold Wallet Staking

- At Liminal we emphasize utmost asset security over anything - transaction processing, staking rewards and issuing funds in and out of wallets to put into different actions. Inherently, Staking is deployed through Hot wallets but it adjourns a variety of security threats that inhibits Institutional participation in Staking.

- When it comes secure custody and directing those same assets towards Staking, a common practice is to advance it through a Hot Wallet where Institutions store only a portion of their asset treasuries. When and if they wish to put in more liquidity onto Staking and earn additionally, they have to process funds from their cold wallets to hot wallets and then initiate staking again for that new pool created.

- To go a notch higher than the security infrastructure Hot Wallet provides for the assets safeguarded for Staking, Cold Wallet is the ultimate wallet structure that completes the two essential parameters for an Institution to participate in Staking without hindering the security firewall entirely.

Offline Storage

Cold wallets elementary store private keys offline, downright reducing the risk of exposure to the most trivial of threats used in Hot wallets. By keeping the keys off-chain, institutions can mitigate the risk of unauthorized access, save all transaction fees while transferring assets to Hot wallets and maintain exhaustive access to wallets that transacts with Staking contracts, collect all Staking rewards and compound the sum considerably.

Multi-Factor Authentication

Hardware wallets typically offer strong multi-factor authentication mechanisms, such as PIN codes or biometric authentication, to authorize transactions. There are and always will be instances of losing wallet access, keys and devices that can be infiltrated by a simple password-breaking computation.

Cold Wallets' multi-factor authentication is first from the hardware side, second in the software login and third in the These additional layers to authenticate logins and signatures of accredited admins in Cold Wallet consolidate signer-prone hacks for Institutions.

Transaction Confirmation

Cold wallets require manual confirmation of transactions directly on the device itself. This physical verification step ensures that only authorized individuals with physical possession of the hardware wallet can approve and initiate staking transactions.

Now, it is principally for downsizing the possibility of unsure transactions executed and the staked amount gets entrenched according to the staked assets protocols un-bounding period.

But, it also transpires into the signer tracking each transaction whether they are getting fulfilled on-chain from off-chain as well, which notably happens either when the network is congested or a fraud address is shared for transaction confirmation.

Backup and Recovery

Cold wallets have an incredible functionality of key regeneration, a feature that lacks tremendously across Institutional setups in hot wallets. With such an instrumental recovery mechanism the idea of staking become further viable for Institutions.

They can securely leave their assets staked linked from the cold wallet and store backup seeds or recovery phrases offline in multiple secure locations in order to build a system of earning passively and securely.

This redundancy ensures that under any circumstance when assigned assets for Staking, Institutions will always be able to access the wallet and the assets stored in it.

Liminal's Cold Wallet Staking Solution

Liminal offers a cutting-edge Cold Wallet solution precisely designed to address the prototypical needs of Institutions seeking to participate in Protocol-level Staking.

With a focus on security, efficiency, and user experience, Liminal's Staking nested in Cold Wallet security framework, provides an absolutely unique proposition to investors seeking to earn passively while their digital assets are parked as safely as possible.

To change the conjecture of how Institutional Staking can be made more lucrative, we have categorized and fractionalized measures of security and efficiency to deliver a quintessential Staking experience:

- Multi-Layer Security
- Multi-Party Security

Our showcase of functionalities we have built around the wallet infrastructure has aided in bringing the same level of sophistication in Staking-As-A-Service as well, where we as custody providers have manufactured a persuasive solution towards earning passively, a use-case that attracts Institutions invariably but also confines their utmost integration to really take advantage of Staking.

The highlights of our Cold Wallet Staking, vary from signer allocation, policy setup, wallet integration, and private key management to transaction confirmation algorithms and unified dashboard view for Staking.

1. Multi-Sig and MPC Security

Participating in staking can expose institutions to reputation risk, particularly if they participate in networks with questionable governance or environmental impact. With so many bad actors in the space of Web3, it is essential that institutions pick the right partner to stake with and carry forward their legacy, respectfully and with indemnity.

2. Private Key Management and Recovery

Liminal's Cold Wallet houses an exceptional Private Key Management and Recovery module tailored specifically for institutional use. Institutions can fully shard their private keys, encrypting the key fragments and distributing them to designated signers.

Moreover, Liminal's Cold Wallet incorporates a recovery function that can generate a new private key, even if one of the signers' portions of the private key gets compromised. This feature makes it virtually impossible for unauthorized parties to collate the key fragments and gain access to the staked wallet, ensuring the highest level of security for institutional stakers.

3. Transaction Confirmation Guarantee

Liminal's Cold Wallet Staking introduces a Transaction Confirmation Guarantee mechanism. Leveraging advanced algorithms, Liminal's solution provides a secure and reliable transaction confirmation process for every staking transaction and reward redemption. Institutions can trust that their transactions are validated and executed accurately, minimizing the risk of errors or fraudulent activities.

4. Hardware Device Compatibility

Liminal supports integration with the two leading hardware wallet devices, Trezor and Ledger. By leveraging these mainstream hardware wallets, institutions can seamlessly connect and integrate with Liminal's Cold Wallet infrastructure.

This plug-and-play capability enables fast wallet integration, allowing institutions to quickly set up their wallets and start staking within the secure confines of the Liminal ecosystem. Additionally, Liminal's Cold Wallet infrastructure encompasses other wallet types, including Hot and Warm wallets, providing a comprehensive solution for managing the complete wallet infrastructure.

5. Unified Dashboard View

To enhance the staking experience for institutions, Liminal's Cold Wallet aggregates all essential information, including assets staked, utilized wallets, balances, and reward calculations. This unified dashboard view provides a comprehensive overview of the staking activities, making it easy for designated signers and administrators to monitor and manage the staking process. With distributed access based on Multi-Sig or MPC policies, relevant stakeholders can collaborate efficiently while maintaining security and control.

Liminal's Cold Wallet Staking Solution

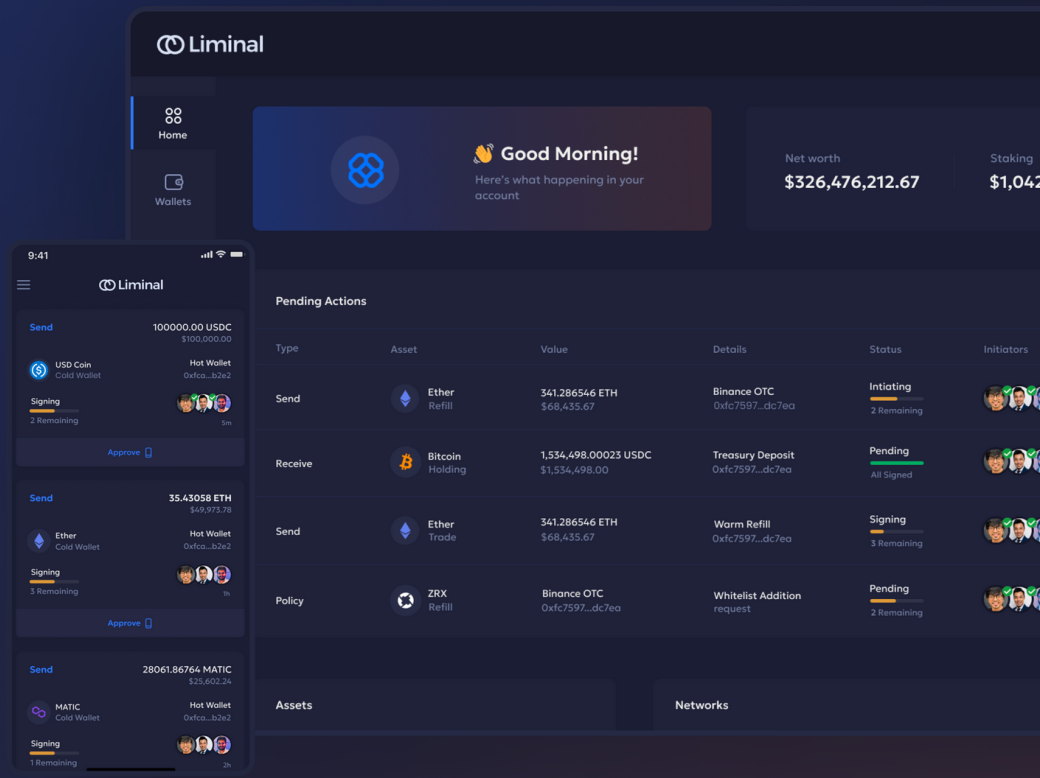
Working with a diverse section of Web3 projects and protocols, servicing them with industry-grade custody, wallet and security solutions, we have identified one of the biggest ecosystem gaps for Institutions to scale and blockchains to become impregnable and scalable, Staking.

The uprise of PoS-driven networks and the development of dApps around those blockchains will mean the market consumption of PoS-based coins will increase seemingly and along with it will increase the reward systems adding more opportunities to earn passively.

The bridge between Institutions wanting to Stake, lacking the infrastructure to activate protocol-level staking and needing best-in-class security architecture, is currently far apart to make a leap and we have now made bold strides to close this gap and bring Institutions closer to utilizing their liquidity in a sensible fashion, driving maximum output while ensuring the assets remain in the safest of custodies, entirely in the authorization of institution.

Liminal

Follow Us For More Updates On The Groundbreaking Innovation We Put Into Our Wallet Infrastructure and Custody Platform



$550 Mn+
Assets under protection

$600 Mn+
Wallet refills processed

$6000 Mn+
Transactions processed

1000 +
Manual hours saved

CCSS
Qualified Service Provider
Cert ID: CCSS00001 Issued by C4

AICPA SOC 2
Formerly SAS 70 Reports

PRESCIENT SECURITY

www.liminalcustody.com